UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS

FACULTAD DE INGENIERÍA

CARRERA DE INGENIERÍA DE REDES Y COMUNICACIONES

Diseño de un Sistema de Gestión de la Seguridad de la Información (SGSI),
basada en la norma ISO/IEC 27001:2013, para el proceso de servicio Post-
Venta de un integrador de soluciones en Telecomunicaciones.

TESIS

Para optar por el título de: INGENIERO DE REDES Y COMUNICACIONES

AUTOR

TORRES LEÓN, MARTIN RENZO (0000-0003-3201-6552)

ASESOR DE TESIS

SEMINARIO GARCÍA, HERNÁN (0000-0001-6971-355X)

Lima, Abril del 2018

Dedicatoria

Dedico esta tesis a Dios que siempre ilumina mi camino, a mis padres y familiares que me dieron todo su amor y me enseñaron a ser perseverante, me alientan en todo momento y me cambian el día con una sonrisa. Son el motor de mi vida.

RESUMEN

El presente trabajo de tesis describió los conceptos involucrados al diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) y su despliegue asociado al proceso de Servicio Post-Venta de un Integrador de Telecomunicaciones. Asimismo, este diseño contempló la adopción de los procedimientos y lineamientos indicados en la norma internacional ISO/IEC 27001 en su versión 2013 y los controles de seguridad asociados en el Anexo A de la misma.

Por otro lado, el presente trabajo buscó demostrar que los beneficios de este diseño al proceso de servicio Post-Venta en estudio fueron: La clasificación de los principales activos de información, la determinación de los principales riesgos a lo que los activos de información están expuestos, la propuesta de un Plan de Tratamiento de Riesgos (PTR) sobre los activos de información, y la definición de roles y responsabilidades dentro de la adopción de una estructura organizacional de un Sistema de Gestión de Seguridad de la Información (SGSI), los cuales se ajustaron a los requerimientos de seguridad y negocios definidos por la organización.

Por último, cabe destacar que todo lo comentado se logró mediante establecimiento de una metodología de la gestión de la seguridad de la información propia y adaptada de las buenas prácticas en el mercado, así como su puesta en marcha dentro del alcance definido en el presente trabajo.

Palabras clave : Sistema de Gestión de Seguridad de la Información, Servicio Post-Venta, Telecomunicaciones, ISO/IEC 27001, activos de información, Plan de Tratamiento de Riesgo.

ABSTRACT

This thesis work described the concepts involved in the design of an Information Security Management System (ISMS) and its deployment associated with the Post-Sale Service process of a Telecommunications Integrator. Likewise, this design contemplated the adoption of the procedures and guidelines indicated in the international standard ISO / IEC 27001 in its 2013 version and the associated safety controls in Annex A of the same.

On the other hand, the present work sought to demonstrate that the benefits of this design to the process of post-sale service under study were: The classification of the main information assets, the determination of the main risks to which the information assets are exposed , the proposal of a Risk Treatment Plan (PTR) on information assets, and the definition of roles and responsibilities within the adoption of an organizational structure of an Information Security Management System (ISMS), which they were adjusted to the security and business requirements defined by the organization.

Finally, it should be noted that all that was mentioned was achieved through the establishment of a methodology for managing information security itself and adapted to good practices in the market, as well as its implementation within the scope defined in this work.

Keywords: Information Security Management System, Post-Sale Service, Telecommunications, ISO/IEC 27001, information assets, Risk Treatment Plan.

Índice

RESUMEN.....	2
ABSTRACT	3
INTRODUCCIÓN	15
CAPÍTULO 1: ESTRUCTURACIÓN DEL PLAN DE TESIS	16
1.1. Tema y Titulo.....	16
1.1.1. Tema	16
1.1.2. Título del Proyecto.....	16
1.2. Introducción - Motivación del Tema	16
1.3. Organización Objetivo	17
1.3.1. Visión.....	18
1.3.2. Misión	18
1.3.3. Objetivos Estratégicos	18
1.3.4. Estructura de la Empresa	19
1.4. Campo de Acción en la Organización Objetivo	21
1.4.1. Procesos	21
1.4.1.1. Gestión de Venta o Renovación de Contratos de Mantenimiento	21
1.4.1.2. Generación de Ticket para Soporte Remoto	21
1.4.1.3. Generación de Ticket para Soporte en Sitio	21
1.4.1.4. Atención de Soporte en Sitio en Cliente	22
1.4.1.5. Registro de Incidencias de Soportes Atendidos.....	22
1.5. Situación Problemática y Problemas en el Campo de Acción.....	22
1.5.1. Situación Problemática	22
1.5.2. Problemas a Resolver.....	23
1.6. Objetivos del Proyectos General y Específicos	24
1.6.1. Objetivos General	24
1.6.2. Objetivos Específicos.....	24
1.7. Indicadores o Mecanismos del Logro de los Objetivos	25
1.8. Justificación del Proyecto	25
1.9. Descripción del Contenido.....	26

1.10.	Plan de Actividades y Cronograma.....	28
CAPÍTULO 2: ESTADO DEL ARTE Y MARCO TEORICO		29
2.1.	Estado del Arte.....	29
2.1.1.	Introducción	29
2.1.2.	Seguridad de la Información	29
2.1.3.	¿Seguridad de la Información o Ciberseguridad?	30
2.1.3.1.	Ciberseguridad	30
2.1.3.2.	Diferencias entre Ciberseguridad y Seguridad de la Información	31
2.1.4.	Gobierno de Seguridad de la Información	32
2.1.5.	Gobierno Corporativo	32
2.1.5.1.	Gobierno de Seguridad de la Información	34
2.1.5.2.	Gobierno de Tecnología de la Información (TI).....	35
2.1.5.3.	Marcos de Referencia	36
2.1.5.3.1.	COBIT.....	36
2.1.5.3.2.	ISO/IEC 38500.....	39
2.1.6.	Ley de Protección de Datos Personales	41
2.1.6.1.	Directiva de Seguridad aplicada a la LDPDP	43
2.1.7.	Metodologías de Gestión del Riesgo	45
2.1.8.	ISO/IEC 27005.....	46
2.1.8.1.	Proceso de Gestión de Riesgos de la ISO/IEC 27005.....	46
2.1.9.	ISO 31000	48
2.1.10.	Magerit.....	49
2.1.10.1.	Características	49
2.1.10.2.	Método de Análisis de Riesgos.....	49
2.1.10.3.	Otras Metodologías	50
2.1.11.	Metodologías de Seguridad de la Información	50
2.1.12.	ISO/IEC 27001:2013	50
2.1.13.	O-ISM3	51
2.1.14.	Comparativa ISO/IEC 27001:2013 y O-ISM3	52
2.1.14.1.	ISO/IEC 27001:2013	53
2.1.14.2.	O-ISM3	54
2.2.	MARCO TEÓRICO.....	55
2.2.1.	Introducción	55
2.2.2.	Definición de la Seguridad de la Información	55

2.2.3.	Definición de Activo de Información	56
2.2.3.1.	Clasificación	56
2.2.4.	Definición de Riesgo.....	57
2.3.	Descripción de la relación causa-efecto en Riesgo-Activo de Información	59
2.4.	Gestión de Riesgos.....	60
2.4.1.	Introducción	60
2.4.2.	Análisis de Riesgo.....	60
2.4.3.	Proceso de Evaluación de Riesgos.....	60
2.4.3.1.	Identificación y Valoración de Activos	61
2.4.3.2.	Identificación de Requerimientos de Seguridad	61
2.4.3.3.	Evaluación de la posibilidad que las Amenazas y Vulnerabilidades ocurran	62
2.4.3.4.	Cálculos de los Riesgos de Seguridad	62
2.4.3.5.	Selección de Opciones de Tratamiento de Riesgo Apropriadas	63
2.4.3.5.1.	Aceptación del Riesgo	63
2.4.3.5.2.	Transferencia del Riesgo.....	64
2.4.3.5.3.	Reducción del Riesgo	64
2.4.3.5.4.	Evitar el Riesgo.....	64
2.4.3.6.	Selección de Controles para Reducir los Riesgos a un Nivel Aceptable	65
2.5.	Sistema de Gestión de Seguridad de la Información	66
2.5.1.	Introducción	66
2.5.2.	Definición del SGSI como herramienta de gestión de procesos.....	67
2.5.3.	Importancia y características.....	68
2.6.	Norma ISO/IEC 27001:2013	73
2.6.1.	Familia de la norma ISO/IEC 27000	73
2.6.2.	Evolución de la norma ISO/IEC 27001:2013	77
2.6.3.	Definición de la norma ISO/IEC 27001:2013	78
2.6.4.	Importancia y Características.....	78
CAPÍTULO 3: DEFINICIÓN DEL PROBLEMA Y TOMA DE REQUERIMIENTOS		
		81
3.1.	Introducción	81
3.2.	Análisis del Problema	83
3.3.	Impacto del Problema en la Organización	84
3.4.	Causas Origen del Problema.....	85

3.5. Solución al Problema	86
3.6. Resultados esperados	86
3.7. Análisis actual de Seguridad de la Información en la Organización (Análisis de Brechas - GAP Analysis)	87
3.7.1. Definición del Marco de Seguridad y Privacidad en la Organización	88
3.7.2. Implementación del Plan de Seguridad y Privacidad de la Información	93
3.7.3. Monitoreo y Mejoramiento continuo	96
3.7.4. Análisis de Seguridad actual en la Organización	100
3.7.5. Resultados del Análisis de Seguridad actual en la Organización	101
3.8. Registro de Interesados	103
3.9. Toma de Requerimientos	103
3.10. Estructura de Desglose de Trabajo	105
3.10.1. Información del Proyecto	105
3.10.2. Aprobaciones	106
3.10.3. Vista Jerárquica	106
3.10.4. Mapas de Procesos - EDT	108
CAPÍTULO 4: PLANTEAMIENTO DE PROPUESTA DE SOLUCIÓN	109
4.1. Introducción	109
4.2. Elaboración de especificaciones	109
4.3. Compromiso de la Dirección	110
4.4. Documentación del SGSI	112
4.4.1. Alcance del Sistema de Gestión de Seguridad de la Información	113
4.4.2. Estructura Organizacional del Sistema de Gestión de Seguridad de la Información	114
4.4.2.1. Comité de Gestión de Seguridad de la Información (CGSI)	115
4.4.2.2. Grupo Interdisciplinario de Seguridad de la Información (GISI)	116
4.4.2.3. Oficial de Seguridad de la Información (OSI)	116
4.4.2.4. Dueño del Riesgo	117
4.4.2.5. Propietarios de Activos de la Información	117
4.4.2.6. Custodio de los Activos de Información	118
4.4.2.7. Usuario de activos de Información	118
4.4.3. Metodología de Evaluación de Riesgos	119
4.4.3.1. Identificación de Activos de Información	119
4.4.3.2. Valoración de Activos de Información	121

4.4.3.3. Análisis e Identificación de Vulnerabilidades y Amenazas.....	126
4.4.3.4. Análisis y Evaluación de Riesgos	126
4.4.3.5. Matriz de Riesgos	130
4.4.3.6. Apetito del Riesgo.....	131
4.4.3.7. Opciones de Tratamiento de Riesgos.....	131
4.4.3.8. Riesgo Residual	131
4.4.4. Identificación de Activos de Información.....	132
4.4.5. Valoración de Activos de Información	136
4.4.6. Análisis e Identificación de Vulnerabilidades y Amenazas.....	140
4.4.6.1. Vulnerabilidades	140
4.4.6.2. Amenazas	144
4.4.7. Análisis y Evaluación de Riesgos	148
4.4.8 Plan de Tratamiento de Riesgos.....	156
4.4.9. Declaración de Aplicabilidad.....	161
4.4.10. Manual del Sistema de Gestión de Seguridad de la Información	169
4.4.10.1. Objetivo.....	169
4.4.10.2. Alcance del Manual de Seguridad de la Información	170
CAPÍTULO 5: EVALUACIÓN Y VALIDACIÓN DE LA PROPUESTA	171
5.1. Introducción	171
5.2. Flujo de trabajo para la evaluación y validación de la propuesta	171
5.3. Análisis de los Objetivos específicos trazados y métricas asociadas	172
5.3.1. Objetivo Específico I	173
5.3.1.1. Plan de Pruebas	173
5.3.1.2. Ejecución.....	176
5.3.1.3. Resultados y Validación	179
5.3.1.4. Plan de Mejoras:	181
5.3.2. Objetivo Específico II	182
5.3.2.1 Plan de Pruebas	182
5.3.2.2. Ejecución.....	186
5.3.2.3. Resultados y Validación	190
5.3.2.4. Plan de Mejoras:	196
5.3.3. Objetivo Específico III.....	197
5.3.3.1. Plan de Pruebas	198
5.3.3.2. Ejecución.....	201

5.3.3.3. Resultados y Validación	205
5.3.3.3.1. Controles del Anexo A de la norma ISO/IEC 27001:2013.....	205
5.3.3.3.2. Controles Técnicos Auxiliares propuestos a la norma ISO/IEC 27001:2013	207
5.3.3.4. Plan de Mejoras.....	209
5.3.4. Objetivo Específico IV	209
5.3.4.1. Organigrama	213
5.3.4.2. Plan de Mejoras.....	217
5.3.4.3. Encuesta sobre el desempeño de la Estructura Organizacional del Sistema de Gestión de Seguridad de la Información (EOSGSI)	217
CAPÍTULO 6: CONCLUSIONES Y RECOMENDACIONES	218
6.1. Introducción	218
6.2. Conclusiones	218
6.3. Recomendaciones	219
7. RECOMENDACIONES PARA TRABAJOS FUTUROS	220
8. BIBLIOGRAFÍA.....	221
9. GLOSARIO	223
10. SIGLARIO.....	224
11. ANEXOS.....	226

Índice de Figuras

Figura 1: Organigrama de la Organización	19
Figura 2: Gantt de actividades del desarrollo de capítulos de la Tesis.....	28
Figura 3: Relación de Gobiernos de Protección de la Información.....	34
Figura 4: Áreas de Enfoque del Gobierno de TI	35
Figura 5: Procesos para la Gestión de la Tecnología de la Información según COBIT 5.....	38
Figura 6: Modelo de Gobierno Corporativo de TI según ISO 38500.....	40
Figura 7: Estructura Orgánica de la Autoridad Nacional de Protección de Datos Personales (APDP).....	42
Figura 8: Relación Causa-Efecto Riesgo-Activo de la Información	45
Figura 9: Proceso de gestión de riesgos de seguridad de la información ISO/IEC27005	47
Figura 10: Estructura ISO 31000.....	48
Figura 11: Modelo de Gestión de Mejora Continua PDCA	51
Figura 12: Principios Fundamentales de la Seguridad de la Información.....	55
Figura 13: Relación Causa-Efecto Riesgo-Activo de la Información	59
Figura 14: Proceso de Evaluación de Riesgos.....	61
Figura 15: Ciclo de mejora continua del Ciclo de Deming o PDCA.....	70
Figura 16: Ciclo de Deming aplicado a un SGSI	71
Figura 17: Historia de las normas de la familia ISO/IEC 27000.....	74
Figura 18: Historia de las normas de Seguridad de la Información	77
Figura 19: Dominios, objetivos de control y controles establecidos por la norma ISO/IEC 27002:2013	79
Figura 20: Línea del Tiempo de Violaciones de Datos	81
Figura 21: Principales Sectores que sufrieron Violaciones por Número de Identidades Expuestas e Incidentes	82
Figura 22: Mapa de Procesos – EDT	108
Figura 23: Organigrama de la Organización	115
Figura 24: Interacción entre componentes de la Estructura Organizacional de Seguridad de la Información.....	118
Figura 25: Ítem de Identificación de Activos de Información.....	120
Figura 26: Integración del Análisis y Evaluación del Riesgo	127

Figura 27: Componentes de la Matriz de Riesgos	130
Figura 28: Matriz de Riesgos.....	149
Figura 29: Nivel de Aceptación del Riesgo.....	158
Figura 30: Flujo de trabajo para Evaluación y Validación de la Propuesta	171
Figura 31: Porcentaje de Activos según su criticidad o impacto.....	181
Figura 32: Porcentaje de Activos de Información Vs Interpretación del Riesgo Resultante	195
Figura 33: Porcentaje de Activos de Información Vs Nivel de Aceptación del Riesgo.....	196
Figura 34: Relación de Aplicabilidad/No Aplicabilidad de Controles por Dominio según el Anexo A de la norma ISO/IEC 27001:2013	206
Figura 35: Relación de Controles Aplicables y no Aplicables de la ISO/IEC 27002:2013 .	206
Figura 36: Organigrama de la Estructura Organizacional del Sistema de Gestión de Seguridad de la Información (EOSGSI)	213
Figura 37: Porcentajes de Cumplimiento de Funciones Cubiertas del Comité de Gestión de Seguridad de la Información respecto a la Resolución Ministerial N° 166-2017-PCM	216

Índice de Tablas

Tabla 1: Indicadores y Métricas de logro de Objetivos Específicos.....	25
Tabla 2: Descripción y Alcance de Capítulos Abarcados en la Tesis	26
Tabla 3: Áreas Claves del Gobierno Corporativo.....	32
Tabla 4: Matriz de apoyo para la selección de categoría en el tratamiento de datos personales	44
Tabla 5: Descripción de los Niveles de Madurez usados por O-ISM3.....	52
Tabla 6: Categorización de Probabilidad de Ocurrencia de Amenazas.....	62
Tabla 7: Categorización de Probabilidad de Ocurrencia de Amenazas.....	62
Tabla 8: Definición del Marco de Seguridad y Privacidad en la Organización	89
Tabla 9: Implementación del Plan de Seguridad y Privacidad de la Información.....	94
Tabla 10: Monitoreo y mejoramiento continuo de la Seguridad de la Información – SGSI ..	97
Tabla 11: Definición del Marco de Seguridad y Privacidad en la Organización - SGSI	100
Tabla 12: Implementación del Plan de Seguridad y Privacidad de la Información – SGSI ..	100
Tabla 13: Monitoreo y mejoramiento continuo de la Seguridad de la Información – Fase de Verificación del SGSI	101
Tabla 14: Monitoreo y mejoramiento continuo de la Seguridad de la Información – Fase de Verificación del SGSI	101
Tabla 15: Tabla de Registro de Interesado del SGSI.....	103
Tabla 16: Tabla de la toma de requerimientos del Proyecto.....	105
Tabla 17: Datos/Información del Proyecto	105
Tabla 18: Listado de Aprobaciones del Proyecto	106
Tabla 19: Requerimientos del Proyecto	109
Tabla 20: Inventario de Activos de Información	119
Tabla 21: Valoración de Activos en base a los Pilares de la Seguridad de la Información..	122
Tabla 22: Definición de Severidad dentro del Rango	124
Tabla 23: Valor de Criticidad o Impacto sobre los Activos de Información	125
Tabla 24: Valores de Impacto del Activo de Información.....	127
Tabla 25: Valores de probabilidad del Riesgo sobre del Activo de Información.....	128
Tabla 26: Matriz del Riesgo sobre del Activo de Información.....	128

Tabla 27: Nivel de Aceptación del Riesgo	130
Tabla 28: Opciones de Tratamiento del Riesgo.....	131
Tabla 29: Inventario de Activos de Información	133
Tabla 30: Valoración de Activos de la Información según su Criticidad / Impacto.....	137
Tabla 31: Vulnerabilidad y Amenazas de Activos Valorados	147
Tabla 32: Tratamiento del Riesgo.....	156
Tabla 33: Plan de Tratamiento del Riesgo.....	159
Tabla 34: Declaración de Aplicabilidad – SOA	162
Tabla 35: Cantidad de Controles de Seguridad Aplicables	163
Tabla 36: Indicadores y Métricas de Logro de Objetivo I.....	173
Tabla 37: Matriz de Plan de Pruebas para el Objetivo Especifico I	174
Tabla 38: Ejecución de Pruebas de Escritorio para Objetivo Especifico I.....	177
Tabla 39: Activos de Información Valorizados	179
Tabla 40: Indicadores y Métricas de logro de Objetivo Específico II.....	182
Tabla 41: Matriz de Plan de Pruebas para el Objetivo Especifico II.....	184
Tabla 42: Matriz de Plan de Pruebas para el Objetivo Especifico II.....	187
Tabla 43: Riesgos y Nivel de Aceptación del Riesgo Resultante.....	192
Tabla 44: Indicadores y Métricas de logro de Objetivo Específico III.....	197
Tabla 45: Matriz de Plan de Pruebas para el Objetivo Especifico III.....	199
Tabla 46: Matriz de Nivel de Madurez de los Controles de Seguridad Adoptados.....	201
Tabla 47: Analisis del Nivel de Madurez de Controles por Dominio del Anexo A de la norma ISO/IEC 27001:2013	204
Tabla 48: Cantidad de Controles de Seguridad Aplicables	205
Tabla 49: Indicadores y Métricas de logro de Objetivo Específico IV	209
Tabla 50: Definición, Funciones e Integrantes de la Estructura Organizacional de la Gestión de la Seguridad de la Información	210
Tabla 51: Cuadro Comparativo de funciones según la Resolución Ministerial N° 166-2017- PCM y la Estructura Organizacional Propuesta.....	215

Índice de Anexos

ANEXO I: Implementación del Plan de Seguridad y Privacidad de la Información (40%) - Análisis GAP	227
ANEXO II: Vulnerabilidades y Amenazas de Activos Valorados	241
ANEXO III: Matriz de Riesgos	253
ANEXO IV: Tratamiento del Riesgo	256
ANEXO V: Plan de Tratamiento de Riesgos	261
ANEXO VI: Declaración de Aplicabilidad - SOA	310
ANEXO VII: Controles Técnicos Auxiliares	329
ANEXO VIII: Ejecución de Pruebas de Escritorio para Objetivo Específico I	337
ANEXO IX: Ejecución de Pruebas de Escritorio para Objetivo Específico II	339
ANEXO X: Roles, Responsabilidades y autoridades organizacionales especificados en la norma ISO/IEC 27001:2013	362
ANEXO XI: Resolución Ministerial N° 004-2016-PCM	364
ANEXO XII: Taller de Implementación de la norma ISO/IEC 27001	368
ANEXO XIII: Estructura Organizacional del SGSI-Curso UPC	370
ANEXO XIV: Inclusiones en la norma ISO/IEC 27001 respecto a su norma antecesora....	372
ANEXO XV: Resolución Ministerial N° 166-2017-PCM	373
ANEXO XVI : Encuesta sobre el desempeño de la Estructura Organizacional del Sistema de Gestión de Seguridad de la Información.....	375
ANEXO A: Manual del Sistema de Gestión de Seguridad de la Información	379
ANEXO B : Política de Seguridad de la Información	388
ANEXO C: Política de Control de Acceso	398
ANEXO D: Política de Uso Aceptable de los Sistemas de Información, Internet y Correo Electrónico	406
ANEXO E: Política de Puesto de Trabajo despejado y Bloqueo de Pantalla	414
ANEXO F: Política de Teletrabajo	417
ANEXO G : Política de Gestión de Incidentes de Seguridad de la Información.....	421
ANEXO H : Política y Procedimientos de intercambio de información	425

INTRODUCCIÓN

Es innegable mencionar que actualmente existe una gran necesidad de gestionar la seguridad de la información de los activos atribuidos a los procesos críticos de cada una de las organizaciones. Lo comentado, ya sea como un elemento diferenciador de negocios o como un elemento sustancial que permita atribuir procedimientos y lineamientos en la gestión de la seguridad de la información que contiene. En base a ello, el presente trabajo de grado describe y detalla los procedimientos, lineamientos y la metodología necesaria para poder diseñar un Sistema de Gestión de Seguridad de la Información de manera adecuada, preservando la confidencialidad, integridad y disponibilidad de los activos de información de un Integrador en Telecomunicaciones, específicamente referido a su proceso de Servicio Post-Venta.

Por ello, en el desarrollo de la presente tesis, para la consecución del logro del diseño comentado, nos apoyamos en la norma ISO/IEC 27001:2013, como base fundamental para el Sistema de Gestión de Seguridad de la Información (SGSI) propuesto, además de otras normas complementarias como la ISO/IEC 27002:2013 para la elección de controles de seguridad aplicables a los activos de información previamente valorados y controles técnicos auxiliares basados en buenas prácticas de la industria en materia de seguridad de la información.

Asimismo, es necesario mencionar que todo el levantamiento de información y pasos necesarios para llevar a cabo la metodología de Gestión de Riesgos propuesta se ejecutaron en varias sesiones de trabajo con el personal conocedor del proceso de Servicio Post-Venta y todo el personal de la organización que haya sido necesario en la misma, tales son: Alta Dirección, Gerencia General, Área Técnica, área Administrativa y Financiera y área Comercial. Ello permitió identificar y valorar los activos críticos de la organización, así como la identificación y evaluación de riesgos a los cuales estos estaban sometidos.

Por último, cabe precisar que el fin y alcance de la presente tesis no es la implementación, sino el diseño del SGSI, dejando a posterior a la organización la adopción del Sistema de Gestión con la consideración de todo el despliegue y consideraciones del presente trabajo.

CAPÍTULO 1: ESTRUCTURACIÓN DEL PLAN DE TESIS

1.1. Tema y Título

1.1.1. Tema

El presente Proyecto de Titulación comprende el Diseño de un Sistema de Gestión de Seguridad de la Información, por sus siglas SGSI, la cual se basa en el cumplimiento de sus Requisitos estipulados y la aplicabilidad de los Controles de Seguridad previamente seleccionados de un total de: Catorce (14) Clausulas, Treinta y cinco (35) Objetivos de Control y Ciento catorce (114) Controles, indicados en el Anexo A estructurados en la norma ISO/IEC 27001 en su versión 2013. Este diseño se encuentra enfocado específicamente al proceso de servicio de Post-Venta de un Integrador de Soluciones en Telecomunicaciones.

Por lo expuesto, el presente proyecto describe los conceptos involucrados en el diseño de un SGSI, dejando los lineamientos necesarios para su posterior puesta en marcha por parte de la organización cuando lo estime conveniente.

1.1.2. Título del Proyecto

“Diseño de un Sistema de Gestión de la Seguridad de la Información (SGSI), basada en la Norma ISO/IEC 27001:2013, para el proceso de servicio Post-Venta de un Integrador de Soluciones en Telecomunicaciones”.

1.2. Introducción - Motivación del Tema

En la actualidad es innegable que la Seguridad de la Información es clave para el correcto desenvolvimiento de la continuidad de los negocios, ya que la mayoría de estos procesos soportan su desempeño en sistemas informáticos, estos a su vez en sistemas de información, que apoyan la actividad gerencial y la toma de decisiones en las organizaciones. Por ello, el concepto de seguridad de la información pasa a ser un activo propio y fundamental dentro de la organización, el cual tenga un rol activo que genere valor y, para el caso de nuestro objeto

específico de estudio, trabaje como un elemento estratégico que sirva como diferenciador en su mercado, generando confianza en sus clientes, socios y demás interesados.

Por lo comentado, el presente proyecto describe los conceptos involucrados en el Diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) apoyada en la estructura de la norma ISO/IEC 27001:2013 al proceso de servicio Post-Venta de la organización. Aquello, motivado por la falta de lineamientos necesarios que preserven los principios fundamentales de la Seguridad de la Información: confidencialidad, integridad y disponibilidad de la información, lo cual genera pérdidas de información confidencial, tanto propia como de clientes, y posteriores consecuencias legales por su no correcto resguardo o protección. Por ello, la presente tesis asiste a la problemática causada en la empresa proponiendo un sistema de gestión que vele por la protección de la información confidencial de sus clientes y propia de la organización.

Por último, cabe indicar que un sin número de organizaciones están adoptando esta norma para poder crear lineamientos que fortalezcan los procesos de Seguridad de Información, no solo como un hecho de diferenciación por obtención de la norma, sino para el correcto uso, distribución y protección de los activos de información que se contemplan en el proceso específico que abarquen como objetos estudio y ejecución.

1.3. Organización Objetivo

La empresa en estudio es una organización nacional dedicada al rubro soluciones integrales de Telecomunicaciones con más de 22 años de experiencia, con miras a ampliar su cartera de negocios en países estratégicos de la región, tales como: Chile, Colombia y Ecuador. Entre sus principales servicios se contemplan:

- Implementación de Proyectos de Networking, Gestión de Ancho de Banda y Seguridad Informática.
- Implementación de Proyectos de Radiofrecuencia
- Implementación de Proyectos de Video Conferencia y Telepresencia
- Servicios Post-Venta de Implementación de Proyectos ejecutados
- Servicios Profesionales: Diseño, Consultoría y Auditoría de Proyectos Tecnológicos.

1.3.1. Visión

Ser reconocidos como la empresa líder en Latinoamérica en el manejo, control y seguridad de datos. Como consecuencia convertirse en el factor de referencia para clientes, empleados y proveedores.

1.3.2. Misión

Contribuir al logro de los objetivos de sus clientes al crear soluciones en sus necesidades de manejo, control y seguridad de datos, al usar tecnologías y servicios que agreguen valor a su negocio, proporcionando a sus empleados y accionistas bienestar y desarrollo personal.

Por otro lado, la constitución de la empresa es jerárquica y dividida en áreas funcionales con sus respectivas jefaturas, las cuales serán abordadas más adelante en la descripción de cada departamento que compone su organigrama.

1.3.3. Objetivos Estratégicos

Son los siguientes:

- Garantizar la sostenibilidad financiera de la empresa mediante la ejecución de estrategias comerciales y operativas, generando mayor rentabilidad y retorno de inversión.
- Crear alianzas con socios estratégicos del Sector de Telecomunicaciones para cubrir Proyectos de mayor envergadura a nivel nacional e internacional.
- Impulsar el desarrollo de estrategias internas que permitan la innovación de los colaboradores y orientarlo al campo de negocios del rubro de la empresa.
- Adoptar un Sistema de Gestión que ejerza un ciclo de mejora continua a los procesos establecidos en el área operativa, el cual brinde diferenciación y fortalezca la organización interna.

1.3.4. Estructura de la Empresa

La empresa u organización cuenta con el siguiente organigrama:

Figura 1: Organigrama de la Organización

Fuente: Elaboración propia

- **Directorio (Alta Dirección):** Se encuentra representado por la totalidad de sus accionistas, el cual se encuentra integrado por profesionales de larga trayectoria empresarial. Ellos son los encargados de la toma de las decisiones que definirán los objetivos de negocio y el alcance del rumbo de la empresa.
- **Gerencia General:** Es la máxima autoridad administrativa, encargada de la dirección gerencial de la empresa. Representa a la empresa en cualquier circunstancia, así como organizar el régimen interno de la empresa, usar el sello de la misma, cuidar de la contabilidad sea estable (este al día), fijar los sueldos y remuneraciones, además de celebrar contratos a nombre de la empresa.
- **Gerencia Técnica:** Esta área se encuentra ligada a la Gerencia Administrativa y Financiera y trabaja conjuntamente con el área de Proyectos, Desarrollo y Servicios Post-Venta.
 - **Proyectos:** Esta área se encarga de realizar un estudio de factibilidad y pre-factibilidad del proyecto (cálculos, estudio de campo, costos, diseños, entre otros) que indican la viabilidad del proyecto.
 - **Servicios Post-Venta:** Compuesta por el personal encargado de los servicios Post-venta de las soluciones en Telecomunicaciones ofrecidas. Esta área comprende

personal calificado para la resolución de incidentes y/o problemas que se pueda suscitar después de la implementación de los Proyectos ejecutados o Soporte a clientes con Infraestructura ya existente no instalada por la empresa. Tener en cuenta que esta área comprende también personal dedicado a la atención de llamadas para el registro de incidentes, problemas o dudas que puedan tener la totalidad de los clientes con contrato y sin contrato.

- **Desarrollo:** Compuesta por personal dedicado al desarrollo de nuevas aplicaciones asociadas a los productos que comercializa la empresa: APIS con soluciones de Video, Videoconferencia, Telefonía, entre otros.
- **Gerencia Administrativa y Financiera:** Tiene como función llevar a cabo los estados financieros, la parte legal y en general toda la parte administrativa que corresponde a procesos internos de la empresa y externos con otras entidades.
- **Contabilidad:** Encargada de la participación directa en el proceso contable de todos los módulos, aplicación de normas y entorno financiero.
- **Recursos Humanos:** Encargada de brindar información del aspecto social de la empresa, como información sobre convenios educativos, ceremonias, brindar un cronograma de vacaciones para los empleados, entre otros.
- **Gerencia Comercial:** Tiene a cargo el departamento de Pre -Ventas y Ventas, aquí se dan a conocer la bondades de los productos ofrecidos a los clientes, demostraciones de los equipos en tiempo real y asesoría en Telecomunicaciones, gestionando las ventas totales asociados a la empresa.

Con todo lo expuesto, la presente tesis se enfoca en los beneficios que traen consigo el diseño de la Norma ISO/IEC 27001:2013 al campo de acción del proceso de servicio Post-Venta. Lo comentado, debido a la ausencia de un sistema de gestión que implemente una Política de Seguridad de la Información, la cual ejecute procesos que alinee o sugiera: orden, planeamiento, monitoreo y resguardo de la información confidencial propia como también de clientes que maneja el área, actuando en forma inmediata ante alguna eventualidad o riesgo a la cual pueda estar inmersa.

1.4. Campo de Acción en la Organización Objetivo

El objeto de estudio de la presente tesis comprende el proceso de servicio Post-Venta de la organización. El campo de acción de este proceso abarca la ejecución de tareas diarias administrativas y de soporte, y la propia la interacción que existe con los clientes, prospectos de clientes y el personal de soporte de la organización. Por todo lo comentado, el proceso de servicio Post-Venta cuenta con las siguientes entradas o sub-procesos:

- Gestión de Venta o Renovación de Contratos de Mantenimiento
- Generación de Ticket para soporte remoto
- Generación de Ticket para soporte en sitio
- Atención de soporte en sitio en cliente
- Registro de Incidencias de soportes atendidos

1.4.1. Procesos

Como se comentó el proceso de Servicio Post-Venta integra las siguientes entradas descritas a continuación:

1.4.1.1. Gestión de Venta o Renovación de Contratos de Mantenimiento

Integra todo el flujo de servicio realizado para la adquisición de nuevos contratos de mantenimiento de clientes ya existentes. Aquí se revisa la base ya instalada de la Infraestructura Tecnológica con la que cuenta el cliente y la cual tiene que continuar ser soportada por un proveedor calificado.

1.4.1.2. Generación de Ticket para Soporte Remoto

Integra todo el flujo asociado desde el instante en que el cliente realiza la solicitud de requerimiento de servicio, el cual según la magnitud del problema y/o inconveniente puede ser atendido vía remota. Al igual que en la propia Gestión de Venta, este sub-proceso involucra el Sistema de Atención de Ticket. Este sistema estará asociado al Registro de Incidencias de soportes atendidos entregados mensualmente al cliente, dependiendo del SLA (Service Level Agreement) pactado entre la empresa y el cliente final.

1.4.1.3. Generación de Ticket para Soporte en Sitio

Integra todo el flujo asociado desde el instante que el cliente realiza la solicitud de requerimiento de servicio, el cual por la magnitud del problema o inconveniente debe ser

atendido en sitio, es decir en las instalaciones del propio cliente. Tal como en el sub-proceso anterior, todos estos soportes son ingresados al Sistema de Atención de Ticket para su posterior análisis en el Registro de Incidencias de soportes atendidos, esto en cumplimiento del SLA pactado entre la empresa y el cliente final.

1.4.1.4. Atención de Soporte en Sitio en Cliente

Integra todo el flujo para la asistencia y solución de inconvenientes asociados a la Infraestructura del Cliente. Este sub-proceso se apoya en la Generación de Ticket para soporte en sitio e involucra una asistencia presencial en las oficinas del cliente.

1.4.1.5. Registro de Incidencias de Soportes Atendidos

Busca contar con una bitácora de los soportes atendidos con el fin de crear métricas que ayuden al Jefe Técnico y a la propia administración definir alcances en los niveles de atención, niveles de urgencia, acciones ejecutadas y conclusiones por parte del propio soporte realizado. Asimismo, busca entregar recomendaciones para evitar problemas posteriores o la ejecución de un primer nivel de soporte realizado por el cliente final, acortando el impacto que pueda generar un inconveniente o problema en su Infraestructura Tecnológica.

Por todo lo expuesto, el objeto de estudio de la presente tesis, es reconocer los activos de información asociados a estas entradas al proceso de servicio Post-Venta y realizar una selección de los activos que impactan de mayor manera en el proceso para el cliente y aplicar los controles adecuados indicados en la norma ISO/IEC 27001 :2013

1.5. Situación Problemática y Problemas en el Campo de Acción

1.5.1. Situación Problemática

El crecimiento de la organización en cuanto a volumen de negocios ha obstruido de alguna manera la visión de la empresa en materia de seguridad de la información. En base a ello, en consecuencia, información de la organización y propia de clientes catalogada como confidencial fue extraída y robada en los últimos años. Esto se evidencia en tres situaciones particulares importantes en mencionar:

- Ausencia de archivos físicos y digitales de proyectos ejecutados por la organización: Tener en cuenta que dentro de la información de proyectos se encuentra: Información de contactos, versiones de software de equipos, configuraciones, topologías de red, estructura de datos, acuerdos de proyectos, actas de instalación, entre información de

distinta clase. Asimismo, un evento importante fue la disolución de contrato con una entidad privada de gran prestigio, ello por evidenciar mediante un enlace externo gran parte de los documentos y actas de la ejecución del proyecto de instalación de una solución de Comunicaciones. Esta situación en particular se atribuye a un ex-trabajador descontento que público información con la que interactuaba en su día a día.

- Evidencia en logs de Sistema de Gestión de Tickets de accesos no autorizado a módulos confidenciales del Sistema y archivos ejecutables ajenos al sistema alojado en la raíz de una de las particiones del disco del servidor. Ello fue verificado por una empresa externa mediante la presentación de su informe técnico del mantenimiento lógico preventivo del servidor.
- Ataques dirigidos a Sistemas Informáticos de la organización, específicamente el Sistema de Gestión de Ticket, el cual maneja muchos módulos claves para la organización. Ya que este sistema tiene un acceso público para una conexión remota, se han evidenciado ataques dirigidos en donde muchas veces han dejado el servicio indisponible, incluso en muchas ocasiones se ha optado por quitar la publicación de ese módulo dentro del Firewall Perimetral de la empresa.

1.5.2. Problemas a Resolver

Comentada ya la situación problemática de la organización en el ámbito del proceso en estudio y partiendo desde el desconocimiento de la propia información que se maneja en la organización y los propios activos que la soportan, se ha evidenciado los siguientes problemas:

- Continuos ataques a sus Sistemas Informáticos
- Pérdidas de información confidencial, tanto propia como de sus clientes.
- Ausencia de un inventario de activos de información asociados al proceso de Servicio Post-Venta. En consecuencia, no es posible realizar un análisis de los riesgos a los que se encuentran expuestos, minimizando la materialización de una amenaza sobre los mismos.
- Falta de una Estructura Organizacional de Seguridad de la Información en la cual recaiga la responsabilidad y obligación de los procesos de seguridad sobre los activos de información del proceso de Servicio Post-Venta.

- Carencia de procesos, lineamientos y políticas que propongan cambios a adoptar para evitar la incorrecta manipulación de información confidencial de clientes y propia de la organización.

En base a los problemas comentados, se ha considerado necesaria la adopción de un diseño de Sistema de Gestión de la Seguridad de la Información, comúnmente llamado SGSI, base de la norma ISO/IEC 27001 :2013 para la organización. El cual dentro de sus procedimientos y lineamientos internos permitan asegurar la confidencialidad, integridad y disponibilidad de la información de la misma.

1.6. Objetivos del Proyectos General y Específicos

1.6.1. Objetivos General

Diseñar un Sistema de Gestión de Seguridad de la Información (SGSI) que permita proteger la información asociada al proceso de Servicio Post-Venta de un Integrador de Telecomunicaciones.

1.6.2. Objetivos Específicos

Una vez ya definido el objetivo general del proyecto, se derivan de este los objetivos específicos citados a continuación:

- Clasificar los principales activos de información del proceso de Servicios Post-Venta en base a la metodología de evaluación de riesgos aplicada.
- Determinar el riesgo de seguridad de la información sobre los activos que soportan el proceso de Servicio Post-Venta.
- Proponer un Plan de Tratamiento de Riesgos que me permita determinar los controles de seguridad de la información requeridos para obtener un nivel de riesgo aceptable en la organización.
- Definir la estructura organizacional requerida para la operación del SGSI, estableciendo roles y responsabilidades del personal de la empresa.

1.7. Indicadores o Mecanismos del Logro de los Objetivos

Como sabemos no podemos evaluar el desarrollo de los objetivos previamente trazados sin tener métricas que cuantifiquen su progreso en el tiempo. Para ello, en base a los objetivos específicos se muestra el siguiente cuadro.

Tabla 1: Indicadores y Métricas de logro de Objetivos Específicos

Objetivo Específico	Indicador de logro de Objetivo	Métrica de logro de Objetivo
Clasificar los principales activos de información del proceso de Servicio Post-Venta en base a la metodología de evaluación de riesgos aplicada.	Clasificación de los activos de información en base a los pilares de la Seguridad de la Información, tales son: confidencialidad, integridad y su disponibilidad.	Porcentaje de activos de información con niveles de valoración de "Muy Altos" y "Altos" sobre el total de activos que componen el Inventario de Activos de Información
Determinar el riesgo de seguridad de la información sobre los activos que soportan el proceso de Servicio Post-Venta.	Principales vulnerabilidades de seguridad de la información identificadas y el impacto que tendría la ejecución de alguna amenaza sobre el activo de información valorizado en caso de materializarse.	Porcentaje de activos de información con Interpretación de Riesgo "Muy Alto" y "Alto", y Nivel de Aceptación del Riesgo "Importante" y "Considerable" sobre el total de activos de información que componen la Matriz de Riesgo realizada
Proponer un Plan de Tratamiento de Riesgos que me permita determinar los controles de seguridad de la información requeridos para obtener un nivel de riesgo aceptable en la organización.	Declaración de Aplicabilidad (SOA) que integre los controles de seguridad identificados y necesarios, seleccionados para cada nivel de riesgo asociado a cada activo de información valorizado.	Porcentaje de Controles seleccionados que aplican sobre los activos de información seleccionados sobre el Total de los 114 Controles de seguridad de la información indicados en la norma y controles Técnicos Auxiliares propuestos.
Definir la estructura organizacional requerida y sus integrantes para la operación del SGSI, estableciendo roles y responsabilidades del personal de la organización.	Organigrama de la en donde se indiquen los integrantes de la Estructura Organizacional del Sistema de Gestión de Seguridad de la Información.	Porcentaje de cumplimiento de las funciones del Comité de Gestión de Seguridad de la Información (CGSI) respecto a la NTP-ISO/IEC 27001:2014, RM N°166-2017-PCM

Fuente: Elaboración propia

1.8. Justificación del Proyecto

Al tener en cuenta el creciente aumento de amenazas asociadas a la extracción de información sensible de la información, ya sea con fines comerciales, operacionales o simplemente delictivos, y al no correcto manejo de la propia información, ya sea propia o de

terceros, es necesario contar con mecanismos que puedan apoyar la gestión de la seguridad de la información, implementando lineamientos que preserven la: Confidencialidad, Integridad y Disponibilidad de la misma.

En base a ello y al déficit indicado en la “**Situación Problemática**” de la empresa en estudio, esta contempla la adopción de un Sistema de Gestión de Seguridad de la Información, la cual ejerza un ciclo de mejora continua en el correcto resguardo y uso de los activos de información involucrados específicamente al proceso de servicios Post-Venta. Por ello, apoyada en la norma ISO/IEC 27001:2013 pretende:

- Establecer un compromiso importante con la Seguridad de la Información, aplicando los controles previamente seleccionados de la norma ISO/IEC 27001:2013
- Generar credibilidad y confianza a clientes y socios de la empresa mediante la adopción de la norma ISO/IEC 27001:2013
- Desarrollar una adecuada gestión de riesgos de los activos de información previamente seleccionados.
- Generar la sensibilización del personal asociado al proceso Servicios Post-Venta, y de la empresa en general, a la correcta manipulación y resguardo de la información de los distintos activos de información seleccionados.

1.9. Descripción del Contenido

Se muestra a continuación en el siguiente cuadro:

Tabla 2: Descripción y Alcance de Capítulos Abarcados en la Tesis

DESCRIPCIÓN DEL CONTENIDO	
Capítulo I : Estructuración del Plan de Tesis	Presentación y Justificación del Problema: Diseño de un Sistema de Gestión de la Seguridad de la Información (SGSI), basado en la Norma ISO/IEC 27001:2013, para el proceso de Servicio Post-Venta de un Integrador de Soluciones en Telecomunicaciones.
	Ventajas y Desventajas : Propuestas en el desarrollo del proyecto
	Aplicaciones : Propuestas en el desarrollo del proyecto
	Objetivos General y Específicos : Propuestas en el desarrollo del proyecto
Capítulo II : Estado del Arte y Marco Teórico	Estado del Arte : Sistema de Gestión de Seguridad de la Información (SGSI)
	Conceptos Generales de la Seguridad de la Información: Esto incluye introducción, definición, clasificación y otros.

	Relación de causa-efecto Riesgo - Activo de la Información.	
	Gestión de Riesgos: Incluye introducción, definición, fuentes de riesgo análisis y otros.	
	Sistema de Gestión de la Seguridad de la Información: Incluye introducción, objetivos, beneficios, estructura, despliegue, otros.	
	Norma ISO/IEC 27001:2013: Incluye introducción, antecedentes, familia de normas, alcance de la norma, objetivo, beneficios, estructura, despliegue, otros.	
	Descripción de los Controles de la Norma ISO/IEC 27001:2013: Incluye detalles de los 14 dominios de la norma, objetivos de control e implementación, otros.	
	Implementación de un SGSI basada en la norma ISO/IEC 27001:2013: Incluye la metodología y paso a seguir para la implantación de la norma en mención.	
	Descripción actual de la organización: Incluye rubro de trabajo, composición, estructura organizacional, otros.	
Capítulo III : Descripción del Hardware del Sistema Propuesto	Seguridad de la Información implementada actualmente en la organización: Incluye seguridad en la comunicaciones, aplicaciones, físicas, equipos necesarios para la protección de datos, otros.	
Capítulo IV : Descripción de la Etapa de Software del Sistema Propuesto	Diseño del SGSI basada en la norma ISO/IEC 27001 :2013 para la organización en estudio :	
	Fases del Proyecto	<p>1.- Fase de Inicio: Compromiso con la Dirección / Documentación del SGSI / Definición de Fechas y Registros de Interesados / Construcción de Estructura de desglose de Trabajo (EDT)</p> <p>2.- Fase de Planeamiento: Análisis de Brechas (Análisis GAP) / Definición de Alcance / Definición de Política de Seguridad / Definición de Estructura Organizacional del SGSI / Metodología de Evaluación de Riesgos / Identificación e Inventario de Activos de Información / Valoración de Activos / Análisis e Identificación de Vulnerabilidades / Análisis y Evaluación de Riesgos / Diseño de Matriz de Riesgos / Elaboración del Plan de Tratamiento de Riesgos / Declaración de Aplicabilidad (SOA)</p> <p>3.- Fase de Ejecución: Plan de Implementación del SGSI (No incluida dentro del Alcance del Diseño, posteriormente ejecutada por la organización).</p> <p>4.- Evaluación y Validación del Diseño de Gestión: Ensayos y Plan de Pruebas / Ejecución / Resultados / Plan de Mejoras</p>

		5.- Fase de Cierre: Conclusiones y Recomendaciones
Capítulo V: Prueba, resultados y validación	Pruebas, resultados y validación del diseño propuesto para una posterior implementación del proyecto en la organización. Incluye formatos de encuestas, niveles de alcance de los indicadores propuestos, otros.	

Fuente: Elaboración propia

1.10. Plan de Actividades y Cronograma

El cronograma de actividades para la ejecución del proyecto asciende a 228 días, tal lo indicado en cada tarea asignada al mismo a continuación:

Figura 2: Gantt de actividades del desarrollo de capítulos de la Tesis

Inicio del Proyecto	22 days	Thu 1/02/18	Fri 2/03/18
Definición del Problema en la Organización	5 days	Thu 1/02/18	Wed 7/02/18
Descripción y Sustentación de la Solución	2 days	Thu 8/02/18	Fri 9/02/18
Esquema de organización de cumplimiento de Requisitos de la norma	15 days	Mon 12/02/18	Fri 2/03/18
Planificación del Proyecto	16 days	Mon 5/03/18	Mon 26/03/18
Definición del Alcance del Proyecto del SGSI	2 days	Mon 5/03/18	Tue 6/03/18
Elaboración de Estructura de Desglose de Trabajo (EDT)	5 days	Wed 7/03/18	Tue 13/03/18
Asignación de Funciones y Responsabilidades	4 days	Wed 14/03/18	Mon 19/03/18
Entrega de Cronograma	5 days	Tue 20/03/18	Mon 26/03/18
Ejecución del Proyecto	155 days	Tue 27/03/18	Mon 29/10/18
Estructurar Propuesta de Política del Sistema de Gestión de Seguridad de la Información (SGSI)	5 days	Tue 27/03/18	Mon 2/04/18
Establecimiento de la Política del Sistema de Gestión de Seguridad de la Información (SGSI)	10 days	Tue 3/04/18	Mon 16/04/18
Definición de la Estructura Organizacional del Sistema de Gestión de Seguridad de la Información (SGSI)	10 days	Tue 17/04/18	Mon 30/04/18
Identificación de Activos de Información de Procesos asociados al Área de Servicio Post-Venta de la empresa	15 days	Tue 1/05/18	Mon 21/05/18
Inventario de Activos de Información	10 days	Tue 22/05/18	Mon 4/06/18
Valoración de Activos de la Información	15 days	Tue 5/06/18	Mon 25/06/18
Análisis e Identificación de Vulnerabilidades y Amenazas sobre los Activos de Información Valorizados	10 days	Tue 26/06/18	Mon 9/07/18
Análisis y Evaluación de Riesgos de los Activos de Información Valorizados	10 days	Tue 10/07/18	Mon 23/07/18
Diseño de la Matriz de Riesgo	10 days	Tue 24/07/18	Mon 6/08/18
Plan de Tratamiento de Riesgos	10 days	Tue 7/08/18	Mon 20/08/18
Redacción de la Declaración de Aplicabilidad	10 days	Tue 21/08/18	Mon 3/09/18
Redacción del Plan de Tratamiento de Riesgos	10 days	Tue 4/09/18	Mon 17/09/18
Documentación para evaluar determinación de medición de eficacia de Controles	5 days	Tue 18/09/18	Mon 24/09/18
Evaluación y Validación del Diseño de Gestión	25 days	Tue 25/09/18	Mon 29/10/18
Ensayos / Plan de Pruebas	8 days	Tue 25/09/18	Thu 4/10/18
Ejecución de Pruebas	6 days	Fri 5/10/18	Fri 12/10/18
Resultados Obtenidos	7 days	Mon 15/10/18	Tue 23/10/18
Plan de Mejoras	4 days	Wed 24/10/18	Mon 29/10/18
Cierre del Proyecto	10 days	Tue 30/10/18	Mon 12/11/18
Documentación para la posterior ejecución de pruebas y validación Post-Implementación del proyecto en la organización. Incluye formatos de encuestas, niveles de alcance de los indicadores propuestos, otros documentos y alcances.	8 days	Tue 30/10/18	Thu 8/11/18
Acta de Cierre de Proyecto	2 days	Fri 9/11/18	Mon 12/11/18

Fuente: Elaboración propia

CAPÍTULO 2: ESTADO DEL ARTE Y MARCO TEORICO

2.1. Estado del Arte

2.1.1. Introducción

En el Plan de Tesis desarrollado, dentro del apartado de “Situación Problemática y Problemas en el campo de acción” se identificó que el problema principal de la organización consiste en los continuos ataques y pérdidas de información clasificada como sensible, tanto propia como de sus clientes. Este problema principal, desencadenado por la ausencia de un inventario y análisis de riesgos de activos de información asociados al área en estudio y falta de una Estructura Organizacional de Seguridad de la Información en la cual recaiga la responsabilidad y obligación de los procesos de seguridad sobre los activos de información del área en mención, evidenció la necesidad de la organización de tomar en consideración algún modelo o sistema de gestión existente en el mercado mundial, que brinde una solución integral y permanente a los problemas presentados. Para ello, es fundamental en primer lugar realizar un estudio de los conceptos relacionados a la Seguridad de la Información, marcos legales asociados a la protección de datos personales y como estos interactúan dentro del campo de acción de un Integrador de Soluciones en Telecomunicaciones para el beneficio de la protección de activos de información involucrados en el alcance del presente proyecto.

2.1.2. Seguridad de la Información

Es intrínseco afirmar que hoy en día las organizaciones sostienen sus negocios en sistemas informáticos que apoyan su continuidad y por ende la consecución de sus objetivos trazados. En base a ello, el concepto de Seguridad de la Información toma un sentido de vital importancia para el correcto resguardo y manipulación de la información. Por ello, ISO e ISACA, dos grandes entidades relacionadas a Sistemas de Información, la conceptualizan como la preservación de la confidencialidad, integridad y disponibilidad de la información de

una organización, independiente del formato que tenga o se asocie, ya sea: físico, digital, electrónico, entre otras formas.

Por otro lado, otro término relacionado íntimamente con la Seguridad de la Información son los propios Activos de Información. Con ello, ¿Qué son los activos de Información? Para ello podemos citar el siguiente texto:

“Activo de información es algo a lo que una organización directamente le asigna un valor y, por lo tanto, la organización debe proteger...” (ISO/IEC 27001:2005, “Código de Práctica para la Gestión de Seguridad de la Información”)

Tomando en cuenta lo comentado, y en base a la literatura revisada, podemos decir que un activo de información representa aquel bien o servicio, ya sea tangible o intangible, el cual genera, procesa o almacena información. Asimismo, a este activo de información se le atribuye un grado de valor según su criticidad o asociación con los procesos del negocio. Tener en cuenta que en el caso específico del actual proyecto, serán los activos de información relacionados al proceso de servicio Post-Venta de un Integrador de soluciones en Telecomunicaciones.

2.1.3. ¿Seguridad de la Información o Ciberseguridad?

Es innegable no afirmar que la Seguridad de la Información y Ciberseguridad hoy en día son dos conceptos muy relacionados que incluso son asociados como equivalentes, pero de alcances diferentes. Por ello, ya habiendo conceptualizado la seguridad de la información como el conglomerado de medidas preventivas y reactivas que toma una organización para el cuidado, resguardo y protección de la información y los propios sistemas que la soportan en sus distintos niveles, es momento de centrarnos en sus diferencias con otros términos asociados para una mayor comprensión del proyecto.

2.1.3.1. Ciberseguridad

ISACA (Information Systems Audit and Control Association – Asociación de Auditoría y Control sobre los Sistemas de Información) la define como la protección de activos de información mediante el manejo y tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada (información digital) por los sistemas de información que se encuentran interconectados. A continuación, algunos ejemplos que comprenden su campo de acción:

- Traspaso de información de una Sede Principal a una Sede Remota mediante una VPN IPsec establecida entre Firewall perimetrales.
- Acceso no autorizado a un Servidor de Archivos publicado para el consumo de sus recursos.
- Ataque de “Hombre en el Medio” o “Man In The Middle” en una comunicación no cifrada, con el fin de obtener información confidencial y posteriormente alterarla con fines delictivos.
- Ataques de malware desconocido como un Ransomware para el cifrado de información de una organización. Ello, con la finalidad de solicitar rescate para la entrega de llave de des-encipción.

Con el concepto breve, pero conciso, pasamos en el siguiente punto a enumerar las diferencias entre la Ciberseguridad y la Seguridad de la Información.

2.1.3.2. Diferencias entre Ciberseguridad y Seguridad de la Información

Para contar con una diferenciación más marcada podemos mencionar las siguientes:

- La Seguridad de la Información tiene un alcance mayor que la Ciberseguridad, ya que esta busca proteger la información como un todo, cubriéndola de todo riesgo que pueda afectarla en sus diferentes presentaciones (digital o física), indistintamente si están mediante sistemas interconectados o no.
- El alcance de la Ciberseguridad se enfoca en la protección de la información en formato digital y los sistemas interconectados. Por ello, cuenta con una mayor relación y acercamiento con la seguridad informática.
- La Seguridad de la Información se sustenta en tecnología, metodologías, documentación técnica y otros elementos que soportan el alcance de la protección de la información, representada en sus distintas formas que adopta.
- Actualmente, existe una mayor demanda de alcances referidos a la Ciberseguridad, ello motivado por los avances tecnológicos que se incorporan en el día a día: Sistemas de Información, Infraestructura y procesos tecnológicos, entre otros.

Si bien es cierto, el objetivo principal de estos dos términos es proteger la información, considero que la Seguridad de la Información abarca un concepto más amplio y se ajusta

en la problemática de la organización objeto de estudio. Por ello, el sustento de su despliegue en el presente proyecto.

2.1.4. Gobierno de Seguridad de la Información

Para comprender los conceptos que comprende un Gobierno de Seguridad de la Información es necesario contemplar ciertos aspectos, los cuales son los siguientes:

2.1.5. Gobierno Corporativo

Gobierno Corporativo o “Corporate Governance”, según ISACA, es un marco de acción demostrable para operar una organización a niveles aceptables de riesgo. Asimismo, está relacionado en como la organización es direccionada y administrada dentro de su ambiente operativo. Según ello, entrando en detalle integra los siguientes atributos:

- El Gobierno Corporativo es el responsable del consejo de administración de la organización. Tiene como principal objetivo asegurar que la organización consiga los objetivos trazados previamente, mediante la interacción de la administración de la organización y la responsabilidad de la dirección de la misma.
- Entiende y defiende la estrategia de la organización en materia de gestión de riesgos y establece los mecanismos necesarios para establecer su evaluación.
- La naturaleza de las actividades realizadas por el gobierno corporativo es fundamental para enfocar a la administración de conocimiento y no hacia actividades operativas.

En base a lo comentado, a continuación, describimos las seis áreas claves que componen al Gobierno Corporativo, ello en base a sus dos grandes perspectivas: Dirección y Organización.

Tabla 3: Áreas Claves del Gobierno Corporativo

	Área	Contenido
Perspectiva de la Dirección	Conformación de la dirección	La estructura y composición de la junta y sus comités
	Ejecución y Efectividad de la dirección	La efectividad como la dirección demuestra sus tareas
	Estrategia, planeación y monitoreo	La forma como la dirección garantiza la responsabilidad financiera, la estructura de gestión y los planes futuros

Perspectiva de la Organización	Gestión de Riesgo y Cumplimiento	La forma en la que la dirección garantiza la fortaleza de los controles con un proceso robusto de cumplimiento y gestión de riesgo
	Transparencia y divulgación	Reporte transparente y divulgación de la información financiera y no financiera
	Interesados y la línea de fondo	Responsabilidad social, ética y ambiental, relación y comunicación de interesados externos

Fuente: ACIS- XI Jornada de Seguridad Informática

Si bien es cierto estas áreas nos indican el total de procesos que se ejecutan para llevar un acertado Gobierno Corporativo, para nuestro campo de acción del presente proyecto es necesario revisar específicamente el área de Gestión de Riesgo y Cumplimiento. En base a ello, es necesario que el área de Gestión de Riesgo y Cumplimiento reúna los siguientes requisitos:

- Una estructura de gestión de riesgo que abarque la totalidad, área o proceso de alcance de la organización, en la cual se definan los roles y responsabilidades necesarias.
- Un proceso de análisis de riesgo para identificar y evaluar los riesgos claves en las áreas claves de riesgo en la organización. En el caso concreto de nuestro proyecto un análisis de riesgos de los activos de información involucrados en el proceso de Servicio de Post-Venta.
- Garantizar que todos los riesgos identificados sean gestionados dentro del nivel de riesgo aceptado y asumido por la organización. Lo comentado, mediante la creación de políticas, estándares y procedimientos desarrollados dentro de la gestión del riesgo.
- Un proceso para el monitoreo constante del proceso de gestión de riesgos y la implementación de acciones correctivas que sean necesarias, así como un proceso para el reporte de riesgos que se proporcionen al personal interesado (Ejecutivos, Alta Dirección y/o los que aplique).
- Un proceso para comunicar de forma apropiada los riesgos de la información a los interesados en la organización, con retroalimentación del proceso de riesgos.

En base a los puntos descritos, es importante que una organización contemple y lleve a cabo una adecuada Gestión del Riesgo Corporativo. Este tema será abordado más adelante en el presente proyecto.

2.1.5.1. Gobierno de Seguridad de la Información

El Gobierno de Seguridad de la Información es un subconjunto del Gobierno Corporativo, revisado en el punto anterior. Cuenta con las siguientes características:

- Consiste en el liderazgo, estructura organizacional y los procesos inmersos que trabajan en conjunto para lograr proteger la información. Asociado a nuestro caso específico a los activos de Información inmersos en los procesos del área de la organización en estudio.
- Provee dirección estratégica para el manejo y monitoreo del programa de Seguridad de la Organización, con el fin de garantizar los objetivos establecidos y gestionar los riesgos de los activos de información de forma apropiada.
- Alinea sus estrategias y objetivos con las del propio negocio.
- Proporciona capacidad en la toma de decisiones estratégicas en la organización, en cumplimiento con las leyes y regulaciones actuales.

Cabe indicar que, dentro del Concepto de Gobierno de Seguridad de la Información, interactúa con un concepto adicional muy cercano: Gobierno de Tecnología de la Información. En la Figura 3 podemos observar su interacción:

Figura 3: Relación de Gobiernos de Protección de la Información

Fuente: Elaboración Propia

En base a ello, comentamos en forma resumida las funciones y características del gobierno de Tecnología de la Información en el siguiente apartado.

2.1.5.2. Gobierno de Tecnología de la Información (TI)

Podemos conceptualizar al Gobierno de TI como el agrupamiento de acciones que el área de Tecnologías de la Información (TI) realiza en coordinación constante con la Alta Dirección para alinear sus esfuerzos en la consecución de los objetivos de negocio. Asimismo, el alcance de los objetivos se logra mediante la ejecución un adecuado tratamiento de riesgos, ROI (retorno de la inversión) realizada en cuanto a materia de TI y la efectividad de los procesos de alcance.

Adicionalmente, el Gobierno de TI se componene de cinco áreas principales en las organizaciones, tales se muestran en el siguiente diagrama:

Figura 4: Áreas de Enfoque del Gobierno de TI

Fuente: ISACA Montevideo Chapter

Cada área juega un papel importante en el desempeño del Gobierno de TI. A continuación un breve alcance de las áreas comentadas:

- **Alineación Estratégica:** El Gobierno de TI debe actuar como intermediario entre los procesos de negocios y los procesos de TI para asegurar su trabajo en conjunto.
- **Agregar Valor:** El Gobierno de TI debe asegurar la mayor eficiencia y eficacia en la totalidad de procesos que atiende.
- **Administración del Riesgo:** El gobierno de TI debe permitir mostrar a los dueños del negocio y la propia organización los posibles riesgos a los que se encuentran expuestos. Asimismo, suministrar los mecanismos que sean necesarios para minimizarlos: Procesos, Metodologías, Gestión del Riesgo, otros.

- **Administración de los Recursos:** El Gobierno de TI debe asegurar que la gestión del recurso humano y los propios recursos tecnológicos (Infraestructura, servicios, entre otros) de la organización sea lo más optimizada.
- **Medición del Desempeño:** El Gobierno de TI debe apoyar su desempeño en la utilización de indicadores que sean necesarios, que avalen la medición de resultados y que tan alineados están a los objetivos y resultados que espera el negocio, la propia organización.

2.1.5.3. Marcos de Referencia

Los marcos de referencia del Gobierno de TI definen un conjunto de métodos y prácticas que permite a la organización establecer criterios de información que soporten los requisitos de TI alienados a la continuidad del negocio de la propia organización. Asimismo, permite identificar que recursos puedan ser necesarios en la organización, para que sirvan como modelo o guía para la integración de todas las operaciones relacionadas con las Tecnologías de Información. Con todo lo comentado, citemos el siguiente texto:

“El Gobierno de TI consiste en un completo marco de estructuras, procesos y mecanismos relacionales. Las estructuras implican la existencia de funciones de responsabilidad, como los ejecutivos y responsables de las cuentas de TI, así como diversos comités de TI. Los procesos se refieren a la monitorización y a la toma de decisiones estratégicas de TI. Los mecanismos relacionales incluyen las alianzas y la participación de la empresa/organización de TI, el diálogo en la estrategia y el aprendizaje compartido” (Jan Van Bon, Frameworks voor IT-management.2010)

Podemos evidenciar que en síntesis se comenta al Gobierno de TI como un marco de referencia que permita lineamientos para la correcta Gestión de los recursos y procesos de TI. Por ello, actualmente se manejan diversos marcos de referencia, las cuales cuentan con distintas metodologías orientadas al control de las organizaciones. Los marcos de Referencia para el Gobierno de TI son:

2.1.5.3.1. COBIT

“Control Objectives for Information and Related Technologies” o COBIT por sus siglas en Ingles, es un marco de referencia basado en las mejores prácticas de auditoría y control de procesos en sistemas de Información. En su última versión, COBIT 5, se enfoca

integralmente en la seguridad de la información, tomando en consideración, documento de mejores prácticas y guías detalladas para el resguardo de la información dentro y fuera de la organización en todos sus niveles.

Adicionalmente, COBIT 5 plantea y formula que la seguridad de la información es una disciplina integral y conjunta, por lo que considera aspectos de protección de datos en cada actividad y proceso desempeñado, tal lo mostrado en la siguiente figura:

Figura 5: Procesos para la Gestión de la Tecnología de la Información según COBIT 5

Fuente: ISACA Montevideo Chapter

De la misma, se desprenden los cinco dominios del modelo de referencia de procesos según COBIT, los cuales son siguientes:

- **Procesos Gobierno de TI - Gobernancia de TI:** Evaluar, dirigir y monitorear (supervisar), llamado EDM.
- **Procesos Gestión de TI - Administración de TI:** Alinear, planear y organizar, llamado APO.
- **Procesos Gestión de TI - Administración de TI:** Construir, adquirir e implantar, llamado BAI.
- **Procesos Gestión de TI - Administración de TI:** Entrega, servicio y soporte, llamado DSS
- **Procesos Gestión de TI - Administración de TI:** Monitorear (Supervisar), evaluar y valorar, llamado MEA.

Por último, Si bien no es el alcance del presente proyecto abarcar la gestión y ejecución de COBIT, cabe destacar que dentro de cada proceso se establecen prácticas, actividades, entradas y salidas entre los procesos, las cuales adjuntan metas y métricas específicas de logro de objetivos previamente trazados por la organización.

2.1.5.3.2. ISO/IEC 38500

En su versión 2008, la ISO/IEC 38500 es la norma ISO/IEC asociada al Gobierno de TI. En concreto, la norma fijar los estándares adecuados para un correcto gobierno de los procesos y decisiones de alto nivel que están relacionados con los servicios de TI. Estos servicios de TI se encuentran gestionados por especialistas en el área, ya sean internos o externos a la organización, pero que conocen a cabalidad los objetivos del negocio, es decir objetivos propios de la organización.

Adicionalmente, la norma define seis principios de un buen gobierno corporativo de TI, los cuales son:

- **Responsabilidad:** Claridad en el establecimiento de las responsabilidades sobre TI. En base a ello, todos (sin excepción) deben comprender y aceptar sus responsabilidades asociadas a TI.

- **Estrategia:** Fijar una estrategia de negocio en la organización tomando en consideración las capacidades actuales y futuras de TI. Debe existir una planificación de TI derivada de la estrategia de negocio, la cual brinde un mejor soporte a organización.
- **Adquisición:** Las adquisiciones de TI se deben hacer mediante un análisis previo de las necesidades de TI, las cuales den soporte a la estrategia de negocio en la organización. Es decir, revisar a cabalidad el ROI (Retorno de Inversión), riesgos y beneficios que traen a la estrategia de negocio comentada.
- **Rendimiento:** El área o departamento de TI debe estar consolidada, equipada y preparada para dar soporte a la organización, otorgando los servicios de manera adecuada e integra para cumplir con las necesidades actuales y futuras de la organización, alineados a la estrategia de TI.
- **Conformidad:** Cumplir con todas la normativa y legislación aplicables en el ámbito local y buenas prácticas asociadas en el exterior.
- **Conducta Humana:** La ejecución de las prácticas adoptadas por TI deben demostrar respeto por la conducta humana. Asimismo, deben considerar las necesidades actuales de la totalidad de colaboradores involucrada.

Por otro lado, el modelo de gestión para Gobierno de TI presentado por la ISO/IEC 38500 establece tres tareas principales, las cuales actúan como factor clave para brindar dirección y controlar los roles de gestión en la organización, tales son: Evaluar, dirigir y monitorear, tal lo mostrada el siguiente gráfico.

Figura 6: Modelo de Gobierno Corporativo de TI según ISO 38500

Fuente: ISACA.ORG

Por lo observado en el gráfico, en síntesis, el flujo inicia en la evaluación de la estrategia de TI y su propuesta de mejora el tiempo. Asimismo, es preponderante dirigir la preparación y posterior ejecución de los planes y políticas de TI en la cual se aseguren que el manejo y uso de los recursos de TI van alineado a los objetivos de negocio, propios de la organización. En la última etapa, como un recurso de feedback, se debe monitorear mediante recursos, los que sean necesarios, la medición del rendimiento de la gestión de TI, el cual vaya acorde a la estrategia establecida y planificada.

2.1.6. Ley de Protección de Datos Personales

Como un marco jurídico y de cumplimiento, es importante para la presente tesis comentar sobre la ley de Protección de Datos Personales. En base a ello, esta ley fue aprobada mediante Decreto Supremo N° 003-2013-JUS y tiene como tarea fundamental garantizar el derecho fundamental a la protección de datos personales y un adecuado tratamiento de los datos gestionados por las organizaciones, colaboradores, proveedores de servicios o cualquier otra entidad que maneje información confidencial de personas naturales, tal como se indica en la Constitución Política del Perú:

“Toda persona tiene derecho a que los servicios informativos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar...”
(Constitución Política del Perú, Artículo 2, inciso 6: “Derecho a la Autodeterminación Informativa”)

Un punto esencial en el despliegue y aplicabilidad de la ley es abordar el tratamiento de los bancos de datos personales, ya sea de carácter público o privado, pero: ¿Qué es un banco de datos personal? En el texto propio de la ley 29733 lo conceptualiza como “*Conjunto organización de datos personales, automatizados o no, independiente del soporte, sea este físico, magnético, digital, óptico u otros que se creen cualquiera fuera la forma o modalidad de su creación, formación, almacenamiento, organización y acceso*”.

Asimismo, según la ley comentada, estos bancos de datos personales deben ser inscritos en el Registro de Protección de Datos Personales (RNPD), el cual se encuentra a cargo de la Autoridad Nacional de Protección de Datos Personales (APDP). En base a ello, para una mejor comprensión, se muestra a continuación la estructura orgánica de la Autoridad Nacional de Protección de Datos Personales (APDP):

Figura 7: Estructura Orgánica de la Autoridad Nacional de Protección de Datos Personales (APDP)

Fuente: II Simposio Internacional Derecho, Economía y Ética, Protección de Datos Personales

Esta entidad, dentro su estructura cuenta como principales funciones:

- Emitir opinión técnica sobre los proyectos de normas asociadas a la Protección de Datos personales y orientar a los ciudadanos sobre el propio contenido, principios y alcance de la Ley en mención. Asimismo, supervisar el cumplimiento de la ley y aplicar sanción a quien la infrinja.
- Gestionar y mantener actualizado el Registro Nacional de Protección de Datos Personales (RNPD).

Ahora, entrando un poco más al detalle de las funciones por parte del Registro Nacional de Protección de Datos Personales (RNPD), en esencia podemos comentar lo siguiente:

- Realiza la inscripción del banco de datos personales de administración pública o privada a nivel nacional. Asimismo, da a conocer el alcance de inscripción realizada para la posterior consulta de las personas interesadas.
- Ejecuta las sanciones (cautelares o correctivas) impuestas por la Autoridad Nacional de Protección de Datos Personales al ente infractor.

La presente descripción no tiene como objetivo dar el detalle del procedimiento de inscripción de los bancos de datos personales, pero para un mayor detalle pueden revisar documentación indicada en la página Web del Ministerio de Justicia y Derechos Humanos y revisar específicamente: solicitud de inscripción y formulario de inscripción de banco de datos personales.

2.1.6.1. Directiva de Seguridad aplicada a la LDPDP

La Autoridad Nacional de Protección de Datos Personales (APDP) elaboró una directiva que sirve como documento facilitador en el cumplimiento de las normas de seguridad relacionadas al tratamiento del banco de datos personales. Si bien es cierto, aclaran que este documento no es obligatorio, sino el propio reglamento de la Ley 27933, es útil como documento de buenas prácticas para el correcto manejo de la seguridad de los bancos de datos personales, tal como lo indica a continuación:

“La presente directiva orienta sobre las condiciones, los requisitos y las medidas técnicas que se deben tomar en cuenta para el cumplimiento de la Ley N°29733 en materia de medidas de Seguridad de los bancos de datos personales”. (Directiva de Seguridad de la Autoridad Nacional de Protección de Datos Personales - APDP).

En base ello, podemos comentar lo siguiente:

- Las condiciones se refieren a recomendaciones que facilitan la implementación de requisitos.
- Los requisitos se refieren a condiciones que deben ser demostrables para considerar que se ha cumplido con la directiva.
- Las medidas técnicas son aquellas que se consideren coherentes para cumplir con los requisitos.

La directiva comprende un apartado inicial que considera, según el principio de proporcionalidad, descrito en el artículo 7 de la Ley, realizar la clasificación de categorías según el volumen de datos que contenga cada banco de datos personales. En base a ello, en la tabla mostrada a continuación podremos visualizar una matriz de apoyo para la selección de las categorías de tratamiento de datos personales:

Tabla 4: Matriz de apoyo para la selección de categoría en el tratamiento de datos personales

Item	Criterio	Básico	Simple	Intermedio	Complejo	Crítico
1	Volumen de registros, número de titulares de datos personales que consienten el tratamiento de sus datos. (Criterio utilizado para determinar las categorías).	Hasta 50	Hasta 100	Hasta 1000	Indeterminado	Indeterminado
2	Número de datos personales en banco de datos personales que no contienen datos sensibles. (Criterio utilizado para determinar el tipo básico).	Hasta 50	Más de 5	Más de 5	Más de 5	Más de 5
3	Finalidad del tratamiento de datos personales respaldada por ley o similar. (Criterio utilizado para determinar el tipo crítico).	No Aplica	No Aplica	No Aplica	No Aplica	Aplica
4	Periodo mayor a un (01) año o indeterminado para cumplir la finalidad (tiempo de tratamiento de los datos personales).	No Aplica	No Aplica	Aplica	Aplica	Aplica
5	Tipo de Titular del banco de datos personales: persona natural. (Criterio utilizado para determinar el tipo entre básico a intermedio).	Aplica	Aplica	Aplica	No Aplica	No Aplica
6	Tipo de Titular del banco de datos personales: persona jurídica. (Criterio utilizado para determinar la categoría entre simple a complejo).	No Aplica	Aplica	Aplica	Aplica	Aplica
7	Titular del banco de datos personales del tipo persona jurídica o entidad pública con múltiples localizaciones desde las cuales se tiene acceso al banco de datos personales o se realiza tratamiento de los datos personales.	No Aplica	No Aplica	No Aplica	Aplica	Aplica
8	El banco de datos personales puede incluir datos sensibles. (Criterio utilizado para determinar la categoría entre Intermedio a crítico).	No Aplica	No Aplica	Aplica	Aplica	Aplica

Fuente: Directiva de Seguridad – Autoridad Nacional de Protección de Datos Personales

Respecto a ello y referenciado al alcance de la presente tesis, dentro del ítem 1.3.1.6 de la Directiva indica el alineamiento a los requisitos según lo estipulado en la norma NTP-ISO/IEC 27001:2014. Es importante tener en cuenta que la NTP-ISO/IEC 27001:2014 es una adecuación de la norma ISO/IEC 27001:2013 para nuestro ámbito local. Asimismo, el ítem descrito indica que esta norma se debe incorporar de manera obligatoria dentro del alcance del Sistema de Gestión de Seguridad de la Información (SGSI) para el banco de datos personales que se clasifiquen como: Complejo y Crítico (Revisar la teblaa descrita líneas arriba). Asimismo, para el banco de datos personales que sean clasificados como: Básico, simple e intermedio son opcionales en implementación.

Asimismo, dentro del Anexo C de la directiva: “Orientación de Datos de Tipo Complejo o Crítico”, se indica que solo las entidades públicas pertenecientes al Sistema Nacional de Informática tienen la obligatoriedad de implementar la NTP-ISO/IEC 27001 (avalado en la Resolución Ministerial 129-2012-PCM), dejando a las personas jurídicas como opcional su despliegue dentro de la gestión de los bancos de datos personales.

Por todo lo expuesto, es indudable que esta Ley de Datos Personales N°29733 da un respaldo importante en el presente proyecto de tesis, más aun teniendo en cuenta lo indicado en el Anexo “C” sobre la aplicabilidad de la norma ISO/IEC 27001:2013 para la gestión de bancos de datos personales.

2.1.7. Metodologías de Gestión del Riesgo

Para poder conocer las metodologías vigentes para la Gestión del Riesgo, es necesario en primer lugar conocer los conceptos que se involucran dentro del riesgo asociado sobre un activo de la información. Si bien es cierto no es alcance específico del “Estado del Arte”, pero es necesario para comprensión de lo comentado en el presente apartado. Para ello se muestra la siguiente imagen:

Figura 8: Relación Causa-Efecto Riesgo-Activo de la Información

Fuente: INTECO, Interacción del Riesgo

Brevemente del gráfico podemos mencionar que los activos de información están expuestos a amenazas, además, de las vulnerabilidades que el mismo pueda presentar. Asimismo, el riesgo es la probabilidad que una amenaza explote una vulnerabilidad, con ello observamos que se concretiza el riesgo intrínseco, el cual es definido como el impacto determinado en un activo de la información. Para que este riesgo intrínseco pueda ser aceptado por la organización, esto dependiendo de su criticidad o importancia, se necesitan la ejecución de controles que permitan llevar el riesgo a su mínima expresión.

En base a lo comentado, es preciso indicar que la Gestión de riesgos es una pieza clave dentro de la implantación de un Sistema de Gestión de la Seguridad de la Información (fin del

presente proyecto), ya que en el mismo se manejan conceptos asociados a la propia evaluación y tratamiento de los riesgos que recaen sobre los activos de información. Esta evaluación y tratamiento de riesgos se sostienen sobre los recursos organizativos y tecnológicos que se demanden en la organización, los cuales permitan minimizar su impacto y dar continuidad al negocio, ello dependiendo de su alcance. Asimismo, esta Gestión de Riesgo se lleva a cabo en base a metodologías y normas asociadas a buenas prácticas, las cuales son mencionadas a continuación en los siguientes apartados.

2.1.8. ISO/IEC 27005

El ISO/IEC 27005:2011 es el estándar bandera de la ISO que se encarga de la Gestión de Riesgos de Seguridad de Información. Asimismo, sirve como apoyo a los requisitos del Sistema de Gestión de Seguridad de la Información (SGSI) indicada en la ISO/IEC 27001:2103. Muy breve podríamos decir que la norma identifica los requisitos de Seguridad de la Información en relación a los riesgos inherentes en la organización y el propio soporte efectivo de la propia gestión de riesgos en la misma.

En síntesis, su intención es manejar los riesgos que podrían comprometer la seguridad de la información de la organización y crear lineamientos que ejerzan controles para su correcta protección.

2.1.8.1. Proceso de Gestión de Riesgos de la ISO/IEC 27005

La norma ISO/IEC 27005 indica dentro de su estructura cuales son los procesos de gestión que la componen y cómo ellos interactúan entre sí para apoyar a la Gestión de Riesgos dentro del SGSI. La finalidad de la interacción de estos procesos es tratar la infinidad de posibles amenazas con un número limitado de recursos organizacionales, o lo que se estime conveniente según la gestión de riesgos realizada. En base a ello, los procesos de gestión de riesgos son los mostrados en la siguiente gráfica:

Figura 9: Proceso de gestión de riesgos de seguridad de la información ISO/IEC27005

Fuente: ISACA, Latín Amerca CACS

- **Establecimiento de Contexto:** Determina el alcance de la Gestión de Riesgos (criterios para evaluar, decidir el impacto y aceptar los riesgos). Asimismo, en esta fase se establece la estructura organizativa que soportará la gestión de riesgos.
- **Identificación del Riesgo:** Reconoce que activos de información se van a proteger, que amenazas y vulnerabilidades se encuentran expuestos y que consecuencias traería la materialización de una amenaza sobre el activo de información.
- **Estimación del Riesgo:** Se ejecuta la metodología de Gestión de Riesgos adoptada por la organización para estimar el nivel de riesgo sobre el activo de información. Es decir, evaluar a nivel cuantitativo y cualitativo la concretización de una amenaza sobre el activo.
- **Evaluación del Riesgo:** En base al resultado de los procesos anteriores en su conjunto se priorizan cuales son los riesgos a tratar por la organización.

- **Tratamiento del Riesgo:** Establece que controles de seguridad con necesarios implementar para evitar, disminuir o transferir los riesgos asociados a los activos de información seleccionados por la organización.
- **Comunicación del Riesgo / Monitorización del Riesgo:** Esta fase asegura una retroalimentación con el equipo de Gestión de Riesgos sobre la evolución y tendencia de los nuevos riesgos y/o cambios asociados a los riesgos de los activos de información seleccionados.

2.1.9. ISO 31000

Es la norma de Gestión de Riesgos de la ISO, pero a diferencia de la ISO/IEC 27005 da un alcance global. Es decir, no solo abarca la Gestión de Riesgos de activos asociados a la Seguridad de la Información, sino la totalidad de riesgos asociados a la propia organización. Adicionalmente, su estructura es dividida en tres grandes grupos, tal como se muestra en la gráfica a continuación:

Figura 10: Estructura ISO 31000

Fuente: ISO/FDIS 3100:2009(E)

Estos grupos abarcan:

- **Principios:** Once principios de Gestión del Riesgo indicados en la Cláusula 3 de la Norma, que resumen el alcance de la norma en términos de cumplimiento y despliegue dentro de la Gestión de Riesgos dentro de la organización.

- Marco de Trabajo: Abarca el flujo ejecutado para la Gestión del Riesgo indicado en la Cláusula 4 de la norma. Asimismo, cuenta con una metodología que cuenta como base la comprensión del contexto interno y externo de la organización, su evolución y su retroalimentación en referencia a la Gestión de Riesgos en la organización.
- Procesos: Se describen las fases de la gestión del riesgo indicado en la Cláusula 5 de la Norma. Es similar al flujo indicado en la norma ISO/IEC 27005, pero con la salvedad de un alcance global que no solo cubre la gestión de riesgos asociado a los activos de información.

2.1.10. Magerit

Se presenta como una metodología para el Análisis y Gestión de Riesgos que se derivan del uso de activos de información cubiertos dentro de los procesos tecnológicos que abarca la organización. Asimismo, permite, en base a su despliegue, contar con medidas de control necesarias para minimizar los riesgos asociados a los propios activos en estudio.

2.1.10.1. Características

Las principales son las siguientes:

- Crear conciencia de los riesgos sobre los activos de información, derivados del uso de TI, al grupo designado por la organización.
- Apoyar en la creación de un Plan de Tratamiento de Riesgos efectivo sobre los riesgos asociados a los activos de información.
- Dejar los lineamientos necesarios para posteriores procesos de acreditación o auditoría referida a la Gestión de Riesgos en la organización.

2.1.10.2. Método de Análisis de Riesgos

Las fases que componen el proceso de Análisis de Riesgo propuesto por MAGERIT comprenden lo siguiente:

- Identificar que activos de información son de mayor impacto en el proceso o alcance definido en la organización. Es decir, es muy importante definir el grado de criticidad del activo seleccionado.
- Identificar las amenazas asociadas a cada activo de información seleccionado, así como la estimación e impacto de la concretización de una amenaza sobre el mismo.

- Seleccionar o diseñar que controles de seguridad son necesarios para la protección o disminución del riesgo asociado y que tan efectivos son en el tiempo.

2.1.10.3. Otras Metodologías

Otras metodologías para la Gestión del Riesgo son las mencionadas a continuación:

- **OCTAVE:** “Operationally Critical Threat Asset and Vulnerability Evaluation” es una metodología de análisis y gestión del riesgo, que basa su despliegue en tres fases: Creación de perfiles de amenazas asociadas a los activos de información seleccionados, identificación de sus vulnerabilidades y desarrollo de estrategias necesarias para el control de seguridad sobre los activos en estudio.
- **MEHARI:** Metodología desarrollada por el Club Francés de la Seguridad de la Información (Clusif), la cual proporciona un método de evaluación y gestión de riesgos conforme a los requerimientos de ISO/IEC 27005:2013.

2.1.11. Metodologías de Seguridad de la Información

Por todo lo revisado, es necesario mencionar que en el mercado existen diversas perspectivas de sistemas que integran procedimientos para el control y protección de la información. Por ello, a continuación se mencionan los principales enfoques de metodologías asociadas a la seguridad de la información.

2.1.12. ISO/IEC 27001:2013

La familia de la norma ISO/IEC 27000 agrupa una serie de normas y estándares que se complementan entre si y llevan consigo un fin único hacia el despliegue de un Sistema de Gestión de Seguridad de la Información (SGSI). Para ello, cuenta con la norma base ISO/IEC 27001:2013, la cual incluye normativas sobre gestión de riesgos, métricas, auditoría, directrices, guías de implementación, entre otros aspectos relacionados a la implementación y mantenimiento de un SGSI. Dentro de sus características podemos comentar en resumen:

- La norma incluye dentro de su despliegue el uso de un Sistema de Gestión que se basa en un ciclo de mejora continua llamado PDCA “Plan-Do-Check-Act” (ver imagen líneas abajo), modelo de gestión que se ajusta a los requerimientos de la organización en estudio: Un Integrador de Soluciones en Telecomunicaciones.

Figura 11: Modelo de Gestión de Mejora Continua PDCA

Fuente: Círculo de Deming, Wikipedia

- Implementación de gestión de calidad y seguridad de la información ampliamente conocida, adoptada y aceptada mundialmente, es decir de amplio espectro.
- Los controles que la organización crea conveniente aplicar, en base a la postura de riesgo a asumir, deben documentarse y especificarse según los criterios de aplicabilidad de los controles y el alcance de su despliegue.

Adicionalmente, la norma ISO/IEC 27001:2013 incluye un su anexo A un código de buenas prácticas (Especificado en la norma ISO/IEC 27002:2013) la cual establece una estructura de dominios, objetivos de control y controles propiamente para la gestión de las salvaguardas asociadas a los activos de información previamente valorizados. Asimismo, la ISO/IEC 27001:2013 exige la realización de una evaluación de riesgos sobre los activos de información para dar a conocer las vulnerabilidades y amenazas a los que se encuentran expuestos e implementar con ello controles de seguridad necesarios para disminuir, evitar, transferir o eliminar los riesgos, según sea la postura de gestión de riesgos adoptada por la organización.

Tener en cuenta que la norma, sus especificaciones y anexos serán detallados en el Marco Teórico del presente proyecto.

2.1.13. O-ISM3

Debido al surgimiento de modelos de madurez, podemos mencionar al O-ISM3: “Open Information Security Management Maturity Model”, como un estándar de madurez para la seguridad de la información. Este modelo de madurez otorga un nuevo enfoque de los Sistemas de Gestión de Seguridad de la Información, ya que es resultado de la comparación y ejecución de diferenciales entre la norma ISO 9000 e ISO 27001, calidad y Sistema de

Gestión de la Seguridad de la Información respectivamente. Se conforma de cuatro niveles en su despliegue, lo cual facilita la mejora y alineación de las necesidades del negocio con los objetivos del SGSI.

Por otro lado, O-ISM3 ofrece un nuevo enfoque en el diseño e implementación de un SGSI, ello debido que tiene como finalidad proporcionar un marco para la gestión de seguridad, lo cual se puede utilizar tanto en niveles de entrada para organizaciones pequeñas, medianas o grandes, tomando en consideración los lineamientos asociados a un correcto Gobierno de TI, concepto revisado en apartados anteriores (revisar referencia de COBIT). Para ello, O-ISM3 se basa en cinco niveles de madurez estructurados tal como se muestran en la siguiente tabla:

Tabla 5: Descripción de los Niveles de Madurez usados por O-ISM3

Nivel de Madurez	Descripción
Nivel 0 O-ISM3	Nivel no recomendable, ello debido a su alcance en la reducción de amenazas técnicas sobre el alcance de Seguridad de la Información previamente definido.
Nivel 1 O-ISM3	Este nivel resulta en una reducción significativa de riesgos de amenazas técnicas, con una mínima inversión procesos de seguridad de la información. Se recomienda este nivel para organizaciones con bajos objetivos en Seguridad de la Información en entornos de bajo riesgo.
Nivel 2 O-ISM3	Este nivel resulta en una mayor reducción de riesgo de amenazas técnicas para una moderada inversión en procesos de seguridad de la información. Se recomienda este nivel para organizaciones con objetivos normales en Seguridad de la información en entornos normales de riesgo.
Nivel 3 O-ISM3	Este nivel resulta en una mayor reducción del riesgo de amenazas técnicas para una alta inversión en procesos de seguridad de la información. Se recomienda este nivel para organizaciones con objetivos altos en Seguridad de la información en entornos de alto riesgo.
Nivel 4 O-ISM3	Este nivel resulta en una mayor reducción del riesgo de las amenazas técnicas e internas para una alta inversión en procesos de seguridad de la información. Se recomienda este nivel para organizaciones afectadas por requisitos específicos, tales como: Servicios públicos, instituciones y organizaciones financieras, que compartan o mantengan información sensible, con objetivos altos en Seguridad de la información en entornos de normal o alto riesgo.

Fuente: Elaboración Propia

2.1.14. Comparativa ISO/IEC 27001:2013 y O-ISM3

De las metodologías de Gestión de Seguridad de la Información comentadas se procede describir sus ventajas y desventajas, las cuales sustenten su elección.

2.1.14.1. ISO/IEC 27001:2013

Las ventajas respecto a la norma ISO/IEC 27001:2013 son las mencionadas a continuación:

- Reducción de costos asociados a incidentes de seguridad presentados sobre los activos de información debido al modelo de gestión basado en controles.
- Ejecución de un análisis de riesgos identificando amenazas y vulnerabilidades sobre los distintos activos de la información previamente valorizados. Asimismo, la evaluación del impacto en la organización que puede generar la concretización de amenazas sobre el activo.
- Permite evaluar planes de continuidad del negocio en la organización. Esto será de vital importancia al analizar el ROI (Retorno de la Inversión) que la organización espera obtener al poner en práctica la norma y los beneficios que espera de su implementación y despliegue.
- Modelo de gestión mayormente adoptado es el basado en el ciclo PDCA, o también llamado ciclo de Deming. Esto generará un ciclo de mejora continua en la gestión de la seguridad de la información.
- Debido a que nuestro campo de estudio está referida a una organización prestadora de servicios en Telecomunicaciones, la adopción de la norma proporcionará un incremento en los niveles de confianza en los clientes, proveedores, accionista y asociados. Con ello, sin duda un aumento en el valor comercial y mejora de la imagen de la organización.
- Contribuye al cumplimiento de la legislación y normativa vigentes, tales como la Ley de Protección de Datos Personales en el Perú (Ley N°29733) y Seguridad de los distintos Activos de la Información.

Por otro lado, las desventajas que encontramos en la norma citada, podemos comentar:

- La norma específica que se deben incluir procedimientos y controles que respalden el SGSI, es decir la redacción de un documento para cada uno de los controles aplicados de un total de 114. Lo comentado puede resultar un problema para las organizaciones que pretenden su despliegue en un servicio, área o totalidad de la empresa, ya que existe una documentación considerable que se debe desarrollar y presentar, más aún si se pretende una certificación en la norma.

- Controles de seguridad ubicados en dominios equivocados y redundancia de requerimientos de documentación asociados a la formación y concienciación de empleados en materia de seguridad de la información, ello según algunos expertos en la materia.

2.1.14.2. O-ISM3

En cuanto a las ventajas que presenta este modelo de gestión basado en niveles de madurez podemos citar:

- Su estructura basada en niveles de madurez permite adaptarse a distintos recursos y requerimientos de la organización, dependiendo del alcance u objetivo de negocio que la organización desee cubrir.
- Complementa y fortalece en estructura a SGSI, incluso al propio ISO/IEC 27001.
- El modelo de madurez adoptado por O-ISM3 permite definir métricas de nivel de desempeño, ya que utiliza procesos en lugar de controles.

Por otro lado, respecto a su principal desventaja podemos mencionar:

- Su implementación generalmente es abordada para el fortalecimiento de un SGSI previamente implementado, no como un SGSI propiamente dicho.

Por lo comentado, respecto a los dos Sistemas de Gestión de Seguridad de la Información, si bien el O-ISM3 genera mayor expectativa debido a las ventajas que pueden traer en cuanto a la adopción del nivel adecuado de madurez, este modelo es generalmente adoptado como un sistema de fortalecimiento para SGSI previamente implementado, tal es el caso de la norma ISO/IEC 27001 en su versión 2013. Por otro lado, sin duda creemos también en la norma ISO/IEC 27001:2013 como un concepto ya maduro y adoptado mundialmente que enumera detalladamente sus fases para su elaboración y diseño, con toda la documentación necesaria para su ejecución y despliegue. Añadido a esto y a sus ventajas previamente enumeradas, y contemplando mi experiencia y conocimiento del despliegue de la norma, se optará para el desarrollo de la presente tesis.

2.2. MARCO TEÓRICO

2.2.1. Introducción

El concepto de Seguridad de la Información dentro de una organización ha tomado una importancia vital para la continuidad de sus procesos de negocio. Es decir, en otras palabras, se entiende a la información como un activo clave que debe ser custodiado de manera correcta, preservando su confidencialidad, integridad y disponibilidad. Para ello, no solo es necesario la adopción de sistemas informáticos que mitiguen las vulnerabilidades y concretización de amenazas, sino un sistema integrado de Gestión que cree directrices, políticas, procedimientos que alineen a sus colaboradores a los objetivos previamente identificados por la organización, esto en materia de seguridad de la información. Por ello, para la comprensión a cabalidad del presente proyecto, y en sí de la propia norma ISO/IEC 27001:2013, es necesario contar con la terminología necesaria para su correcta comprensión.

2.2.2. Definición de la Seguridad de la Información

Para dar una definición correcta de Seguridad de la Información, es necesario comentar en primera instancia los conceptos que abarcan los Principios Fundamentales de la Seguridad de la información, tales son: Confidencialidad, integridad y disponibilidad de la información, esto según lo mostrado en la figura líneas abajo. Por ello, se describen a continuación:

Figura 12: Principios Fundamentales de la Seguridad de la Información.

Fuente: www.widefense.com, Beneficios y la importancia de gestionar la seguridad de la información

- **Confidencialidad:** Esta referido a la disposición de la información o sistema de información, la cual solo debe estar restringida para su acceso al personal autorizado.
- **Integridad:** Especifica que la información no puede ser modificada en su envío/recepción, debe ser la misma de origen/destino.
- **Disponibilidad:** Indica que la información o sistema de información debe estar disponible cuando esta sea requerida.

Ahora, ya revisado los conceptos que encierran los Principios Fundamentales de la Seguridad de la Información o también llamados Pilares de la Seguridad de la Información, podemos definir la Seguridad de la Información como el conglomerado de medidas preventivas y reactivas que toma una organización para el cuidado, resguardo y protección de la información y sus sistemas que la soportan en sus distintos niveles, preservando en todo momento sus principios básicos. Lo comentado, permite un correcto manejo de la información y los procesos que la soportan, volviéndose en un activo de vital importancia que trabaje en beneficio de la consecución de los objetivos de negocio previamente definidos por la organización.

2.2.3. Definición de Activo de Información

Es indudable comentar que la finalidad expresa de actual proyecto en estudio está referida explícitamente al correcto resguardo de los activos de información que hayan sido seleccionados y las medidas de prevención que estas necesiten. Según esto, nos preguntamos, pero ¿Qué son Activos de Información? Para ello, podemos definir activo de información como aquel bien o servicio tangible o intangible, que genera, procesa o almacena información, en el cual se le atribuye un grado de valor según su criticidad o asociación con los procesos de negocio¹, los cuales están alineados a sus objetivos planteados. En consecuencia, estos activos de información requieren una adecuada protección, cuidado y respaldo.

2.2.3.1. Clasificación

Los activos de información pueden presentar diversas formas, tales como:

- **Documentos:** Divididos en confidencial o no confidencial, encontrados en documentos impresos o en distintos tipos de formatos. Ejemplos: Un contrato de

¹ Cfr. Díaz, Alzórriz, Sancristobal y Castro 2014: 34

servicios de consultoría con una empresa, un documento impreso donde se detallen las claves de acceso a un sistema, entre otros.

- **Datos/Información:** Principal activo que forma parte fundamental del Sistema de Gestión y en si de la organización. Todos los demás tipos de activos de información dan soporte a su continuidad, almacenamiento, entre otros.
- **Software:** Se refiere a las aplicaciones utilizadas por la organización o a los propios sistemas de información. Ejemplos: Sistemas Financieros, Sistemas Operativos, entre otros.
- **Personas / Recursos Humanos:** El personal humano es el activo más importante con el que cuenta la organización, son los principales generadores de la información que se transfiere sobre la organización.
- **Dispositivos físicos / Hardware:** Se refiere a medios físicos donde se almacena, procesa y transfiere información. Ejemplos comunes pueden ser memorias de almacenamiento (USB), computadores, etc.
- **Imagen y reputación de la empresa:** Referida a una marca patentada por la organización o la propia razón social.
- **Servicios:** Se refiere a los servicios internos o externos que brinda la empresa. Un ejemplo muy claro seria un servicio de seguridad gestionado de un proveedor, contratos de mantenimientos post-venta, entre otros.

Esta clasificación de activos de la información será tomada en cuenta cuando se realice la valoración de activos, ya que este definirá posteriormente la selección de la aplicabilidad de los controles necesarios, esto según el anexo A de la norma ISO/IEC27001:2013, o el código de buenas prácticas que se describe en la norma ISO/IEC 27002.

2.2.4. Definición de Riesgo

Por otro lado, el concepto de riesgo incluye dos términos muy importantes en su definición, que además crean una relación causa efecto según los grados de ausencia de control a la que estén sujetos. Estos términos son amenazas y vulnerabilidades. De manera concisa podemos decir lo siguiente:

- Amenaza es el potencial para causar un incidente no esperado o deseado, el cual pueda dañar o interrumpir la operación de activo de información o sistema de

información. Tener en cuenta que estas amenazas pueden ser intencionales o accidental, producto de hechos fortuitos inesperados. Entre los tipos de amenazas que podemos encontrar son: Desastres naturales, humanas y tecnológicas. Un ejemplo muy de moda en estos tiempos sería el despliegue de malware y específicamente ransomware dentro de una organización con la finalidad de encriptar la data de los servidores y pedir rescate por la llave de descryptación, previo a un depósito de pago.

- Vulnerabilidad es la ausencia de controles de seguridad implementados sobre los activos de información. Vale decir que por sí misma no causa daños, pero su descuido puede permitir concretizar una amenaza sobre el activo. Un ejemplo muy ilustrativo sería contar con Sistemas Operativos dados de baja por el fabricante en servidores de producción. En si, la operación del servidor se dará, pero debido a que no cuenta con soporte, ni parches de actualización de seguridad, puede ser atacado por un código malicioso que permota la comunicación con uns servidor de comanado y control y filtrar información sensible de la organización.

Al haber revisado de forma muy clara y concisa los conceptos de amenazas y vulnerabilidad, podemos decir que el riesgo es conceptuado como la probabilidad que una amenaza pueda explotar una vulnerabilidad en particular². Por ello, es importante la toma de medidas que sean necesarias para la disminución de los porcentajes de riesgos a la que nuestra información pueda estar expuesta, con ello podemos asegurar en gran medida que los procesos implementados seguirán su curso de manera adecuada y sin interrupciones, creando así un ambiente adecuado y próspero para la consecución de los objetivos previamente trazados.

Por otro lado, no podemos dejar de mencionar algunos otros conceptos que será de gran utilidad en la comprensión del despliegue de la presente tesis, tales como:

- Impacto es el resultado de la materialización de una amenaza sobre un activo o activo de información.
- Riesgo Intrínseco es definida como la probabilidad de que se produzca un impacto determinado en un activo o grupos de activos de información.
- Salvaguarda son las medidas adoptadas por las organizaciones para el manejo de los riesgos sobre los activos de la información, disminuyendo su impacto o probabilidad.

² Cfr. Peltier 2010: 6

- Riesgo Residual se llama al riesgo que queda después de aplicar las salvaguardas correspondientes y el cual la organización está de acuerdo a asumir.

2.3. Descripción de la relación causa-efecto en Riesgo-Activo de Información

Una vez revisado los conceptos de activo de la información, amenazas, vulnerabilidad y riesgo, tenemos las herramientas necesarias para comentar sus relaciones de causa-efectos y su interrelación de manera conjunta.

Figura 13: Relación Causa-Efecto Riesgo-Activo de la Información

Fuente: Security in Software Development, M.C Juan Carlos Olivares

Como se explico brevemente en el estado del arte, los activos de información están expuestos a vulnerabilidades que pueden ser explotadas por amenazas del medio que lo rodea. Para ello, es necesario la implementación de controles que reduzcan el riesgo, es decir la probabilidad que una amenaza explote una vulnerabilidad, minizando su impacto sobre el activo d información. Estos controles de seguridad están detallados en la norma ISO/IEC 27002 (Códigos de buenas prácticas). Sin embargo, su implantación compromete un costo, costo que debe ser asumido por la organización, revisando previamente si satisfacen necesidades de resguardo sobre el activo de alcance.

2.4. Gestión de Riesgos

2.4.1. Introducción

Es necesario comentar que la Gestión de riesgos es una pieza clave dentro de la implantación de un Sistema de Gestión de la Seguridad de la Información (SGSI). Debido a ello, la familia de normas de la ISO/IEC 27000 especifica una norma dedicada a lo comentado, tal es la norma ISO/IEC 27005, o la propia ISO31000, revisadas brevemente en el Estado del Arte, las cuales tienen en cuenta los procedimientos necesarios que se requieren para la gestión de riesgos. Por otro lado, existen otras, tales como la norma americana NISTP SP 800-30 o la propia AS/NZ 4360:2004, norma de Nueva Zelandia. Esto significa que existe una gran preocupación para formar metodologías correctas en Gestión de Riesgos que sean de gran utilidad en la consecución de objetivos que permitan la continuidad del negocio. Por otro lado, y centrándonos en la norma en estudio para el presente proyecto la ISO/IEC 27001:2013, en base a la evaluación de riesgos que se realicen se seleccionaran los controles asociados al Anexo A de la norma.

Por lo expuesto, es necesario que la organización en estudio se encuentre bien informada en cuanto a los niveles de riesgos a las que se encuentra expuesto, con ello seleccionar apropiadamente los controles necesarios y con alcanzar una óptima y eficaz gestión de control.

2.4.2. Análisis de Riesgo

En términos resumidos el Análisis de Riesgos consiste en la identificación de los riesgos de seguridad en la organización en estudio, determinando su magnitud e identificando las áreas en donde se requieren la implantación de procedimientos o mecanismos que reduzcan el riesgo, llevándolo a un nivel de riesgo residual asumible por la organización. Para ello, la organización debe ser capaz definir previamente el alcance de la norma ISO/IEC 27001:2013 y en base a ello, realizar la identificación de los activos de información que sean seleccionados para su posterior estudio a nivel de riesgos.

2.4.3. Proceso de Evaluación de Riesgos

El proceso de evaluación de riesgos se compone de seis fases, las cuales permiten a una organización estar en conformidad con los requerimientos que dispone la norma ISO/IEC

27001:2013. Estas 6 fases son presentadas en la siguiente gráfica, y las cuales serán detalladas brevemente individualmente.

Figura 14: Proceso de Evaluación de Riesgos

2.4.3.1. Identificación y Valoración de Activos

En esta primera etapa se establece que cada activo debe ser identificado y valorado significativamente, ello según su importancia dentro del proceso o área de alcance. Además, se debe definir su propietario y clasificarlo según sea la categoría de seguridad de la información a la que pertenezca.

2.4.3.2. Identificación de Requerimientos de Seguridad

La organización debe realizar una identificación de los requerimientos de seguridad en base a tres fuentes principales, descritas brevemente a continuación:

- La primera fuente es el resultado de realizar la valoración de riesgos comentada. Se identifica la exposición de amenazas sobre los activos, sus vulnerabilidades y la probabilidad de ocurrencia.
- La segunda fuente comprende la adopción de regulaciones y documentación necesaria para la satisfacción de los socios comerciales, contratistas y proveedores de servicios
- La tercera fuente contempla los procedimientos que deben ser adoptados por la organización para el correcto tratamiento de la información, ello en apoyo de las operaciones de negocio y sus procesos internos ejecutados.

Tener en cuenta que para la identificación de estos requerimientos de seguridad siempre se deben tener presente, como premisa los principios fundamentales de la Seguridad de la Información, tales son: confidencialidad, integridad y disponibilidad.

2.4.3.3. Evaluación de la posibilidad que las Amenazas y Vulnerabilidades ocurran

Aquí debemos recordar los conceptos revisados respecto a amenaza, vulnerabilidad y riesgos. Asimismo, se debe realizar previamente la identificación de amenazas y vulnerabilidades a las que se encuentran expuestos los activos de información. Adicionalmente, se debe evaluar mediante alguna metodología la probabilidad de ocurrencia de la amenaza y el impacto que ocasionaría de concretarse. A continuación, presentamos las tablas 6 y tabla 7 que cuantifican lo comentado.

Tabla 6: Categorización de Probabilidad de Ocurrencia de Amenazas

Probabilidad de Ocurrencia de Amenaza	
Alto (4)	Cuando la probabilidad de ocurrencia es frecuente. Ejemplo: al menos una vez al mes.
Medio (3)	Cuando la probabilidad de ocurrencia es regular. Ejemplo: al menos una vez al año.
Bajo (2)	Cuando la probabilidad de ocurrencia es baja. Ejemplo: al menos una vez cada 5 años.
Muy Bajo (1)	Cuando la probabilidad de ocurrencia es muy baja. Ejemplo: al menos una vez cada 20 años o más.

Tabla 7: Categorización de Probabilidad de Ocurrencia de Amenazas

Impacto	
Crítico (4)	Afecta irreversiblemente la operatividad, competitividad, rentabilidad o imagen de la organización.
Serio (3)	Afecta seriamente la operatividad, competitividad, rentabilidad o imagen de la organización.
Medio (2)	Afecta considerablemente la operatividad, competitividad, rentabilidad o imagen de la organización.
Mínimo (1)	No afecta considerablemente la operatividad, competitividad, rentabilidad o imagen de la organización.

2.4.3.4. Cálculos de los Riesgos de Seguridad

En una ecuación simple, el riesgo es calculado como el producto entre la probabilidad y el impacto que genera la materialización de una amenaza que aprovecha una vulnerabilidad sobre el activo de información. En base a ello, el propósito de la gestión de riesgos es la

identificación y evaluación de riesgos, estos últimos calculados como una combinación de valores de los activos y los niveles de requerimiento de seguridad deseados. Para ello, se debe tener en cuenta los siguientes aspectos:

- Las consecuencias que traen consigo el no cumplimiento de la seguridad de la información y como ello perjudica a la continuidad del negocio.
- La probabilidad de ocurrencia real en que estos fallos de seguridad se materialicen (materialización de una amenaza sobre la existencia de una vulnerabilidad), teniendo en cuenta los controles establecidos en la organización.
- Los resultados de esta etapa permitirán determinar una adecuada gestión de riesgos de seguridad de la información, basada en una adecuada gestión gerencial y técnica conformada por la organización.

Tener en cuenta que este proceso es un ciclo de mejora continua, en la cual se pueden establecer mejoras que contribuyan a la eficacia y eficiencia del Sistema de Gestión implantado. Por ello, es importante tener en cuenta cambios de requisitos y prioridades establecidas por organización, considerando nuevas amenazas, vulnerabilidades y confirmando que las medidas de control implantadas sean las apropiadas y eficientes.

2.4.3.5. Selección de Opciones de Tratamiento de Riesgo Apropriadas

De las fases anteriores, se deduce en una identificación y evaluación de los riesgos por parte de la organización. Con ello, la misma debe tomar las acciones que crean necesarias para el tratamiento de los riesgos, por ello la importancia de un Plan de Tratamiento de Riesgos (PTR). Para el SGSI, este PTR se consolida como un documento integral de vital importancia en su despliegue, y el cual tiene como principal objetivo la descripción de procedimientos que se realizarán para la disminución de los riesgos a niveles aceptables por la organización y recursos que se propondrán para cada uno de los procedimientos mencionados.

Por lo comentado, se disponen cuatro estrategias para el tratamiento de riesgos, los cuales se muestran a continuación:

2.4.3.5.1. Aceptación del Riesgo

Se da con las siguientes características:

- Cuando la organización no encuentra controles para mitigar el riesgo efectivo o su implementación tiene un costo superior que las consecuencias del riesgo en sí.
- Cuando las organizaciones optan por la aceptación del riesgo debe haber una documentación previa, en donde se indique los criterios utilizados para tal efecto.

2.4.3.5.2. Transferencia del Riesgo

Se da con las siguientes características:

- Cuando para la organización es complicado reducir o controlar el riesgo a nivel aceptable y la transferencia del riesgo a un tercero es más rentable.
- A pesar de que se realice la transferencia del riesgo a un tercero, la responsabilidad por la seguridad siempre recae sobre la organización.
- No elimina el Riesgo Residual en la organización.

2.4.3.5.3. Reducción del Riesgo

Se da con las siguientes características:

- Cuando la organización reduce los niveles de riesgo a niveles aceptables para la misma.
- Los controles a implementar pueden reducir el riesgo estimado en base a dos maneras: Reduciendo la probabilidad de ocurrencia de la amenaza que explota una vulnerabilidad identificada previamente o Minimizando el Impacto el cual podría causar si el riesgo llegar a concretarse sobre el activo o activo de información en estudio.
- Los controles a implementar por la organización deben ser acordes a los objetivos de negocio previamente identificados.

2.4.3.5.4. Evitar el Riesgo

Se da con las siguientes características:

- Algún plan que contemple algún control o acción propuesta por la organización el cual permita evitar la presencia del riesgo

- Las actividades contemplan, por ejemplo, evitando: Continuar desarrollando una actividad en particular, trasladar los activos o activos de información críticos a un lugar o zona insegura, entre otros.
- Los controles a implementar pueden reducir el riesgo estimado en base a dos maneras: Reduciendo la probabilidad de concretización de la amenaza sobre el activo o minimizando su impacto si el riesgo llegar a concretarse sobre el activo de información.
- Deben considerarse controles de seguridad a implementar acordes a los objetivos de negocio previamente identificados por la organización.

Tener en cuenta que la adopción de evitar el riesgo depende de algunos factores fundamentales, principalmente: Ubicación del activo, resguardo actual, instalaciones disponibles y nivel de exposición a la materialización de amenazas.

2.4.3.6. Selección de Controles para Reducir los Riesgos a un Nivel Aceptable

Luego de las etapas descritas anteriormente, es decir después de haber realizado la identificación y evaluación de las opciones para el tratamiento de los riesgos, es necesario que la organización seleccione los objetivos de control y los controles necesarios para realizar el tratamiento de los riesgos.

Por otro lado, tal como se ha mencionado a lo largo del proyecto, los controles pueden ser seleccionados en base al código de buenas prácticas, es decir los controles descritos en el Anexo A de la norma en estudio. Sin embargo, la propia norma establece que se pueden seleccionar objetivos de control y controles adicionales a la norma, los cuales sean requeridos según corresponda y que son considerados en la presente tesis como “Controles Técnicos Auxiliares”.

Ahora, es preciso determinar que controles se adoptaran en la organización, para ello, la organización debe tener en cuenta los siguientes:

- El control debe estar acorde y en línea al riesgo previamente identificado y al cual se desea dar un tratamiento adecuado.
- Observar si el control que se pretende dar al riesgo es el más adecuado para y cumple los requisitos necesarios para el correcto tratamiento del riesgo

- Aterrizar el costo que resultaría la implantación del control seleccionado y el impacto que tendría en objetivos de negocio de la organización.
- Tomar en consideración el tiempo el tiempo de implantación del control seleccionado, su eficiencia y los riesgos de seguridad que cubre sobre el activo de información.
- Tomar en consideración las exigencias legales y regulatorias, dependiendo de la organización y el escenario de alcance.
- Exigencias de controles a implementar por parte de socios comerciales o socios corporativos. Asimismo, evaluar entre ambas partes la mejor decisión que vaya en consecuencia de los objetivos de negocio previamente establecidos.

Por otro lado, es necesario comentar que existen tres tipos de controles que pueden ser implementados, tales como: del tipo Técnico, como un sistema de control de acceso, del tipo Documental, por ejemplo, una política de contratación de personal o del tipo Organizacional, como para la conformación para el Comité de Seguridad.

Además, podemos mencionar que la adopción de los controles permitirá tomar alguna acción de tratamiento de riesgo que permite a la organización la continuidad del negocio. Con ello, con su implementación es importante comentar que siempre habrá riesgos existentes, es decir su adopción permitirá reducir un riesgo específico a un nivel considerable, aceptable por la organización, lo que también es llamado Riesgo Residual ya revisado anteriormente.

2.5. Sistema de Gestión de Seguridad de la Información

2.5.1. Introducción

Actualmente es cotidiano toparnos con normas que sugieren modelos de procesos que se alinean para la consecución de un fin específico, esto en beneficio del cumplimiento de los objetivos de negocios trazados por la empresa y/u organización. Además, también se observan marcos de trabajo que conglomeran un listado ordenado, de gran utilidad y poco complicado a mi humilde entender, de buenas prácticas en la gestión de proyectos y servicios, tales como: PMBOK, ITIL y COBIT³. La integración de buenas prácticas mencionadas da un nuevo soporte a los procesos ya adoptados, y si la empresa u organización no los tiene, da una

³ PMBOK: *Project Management Body of Knowledge*, ITIL: *Information Technology Infrastructure Library*, COBIT: *Control Objectives for Information and related Technology*. Tiene en común la gestión de proyectos y servicios basados en procesos.

referencia enriquecedora que establece un antes y un después en la puesta en marcha de directrices probadas y sustentadas en el mercado laboral mundialmente. En consecuencia, nos proporciona un rendimiento y efectividad que en términos económicos es beneficioso para cualquier empresa y/u organización. Por lo expuesto, existe la necesidad de implementar sistemas integrados de gestión de procesos en las empresas y/u organizaciones, o en áreas funcionales de la misma en la cual se crea necesario por su criticidad e importancia.

Por todo lo comentado, se toma como referencia la adopción un Sistema de Gestión de Seguridad de la Información (SGSI) o *Information Security Managment System*, por sus siglas en inglés (ISMS), en la cual se detalla a continuación.

2.5.2. Definición del SGSI como herramienta de gestión de procesos

Para definir de manera cabal un SGSI, debemos partir de la premisa en la cual la información que se maneja en la organización vista de manera individual o global, es uno de los principales activos con los que esta cuenta. Las características a detalle de información y activo de información serán abordadas en el siguiente capítulo de esta monografía, pero básicamente podemos definir la información como el conglomerado de datos ordenados y organizados por la empresa, en la cual se le atribuye un valor dependiendo de su importancia. Esta información puede estar atribuida a datos valiosos de procesos productivos o tal vez, como en nuestro caso, un registro de información sensible de clientes de la empresa, por ende, la calificación de “importante” para la empresa es innegable, ya que se envuelve dentro de sus objetivos de negocio. Además, el SGSI se involucra en el tratamiento que se le da a la información y los sistemas que están asociados a ella. Por ello, un SGSI recoge un conjunto de procedimientos y políticas que tienen como objetivo conseguir y preservar los principios básicos de la seguridad de la información (confidencialidad, integridad y disponibilidad)⁴ ya comentados previamente.

Ahora que tenemos un concepto conciso y sustancial de qué es la información y lo que contribuye en un SGSI, no podemos dejar de mencionar el entorno de riesgo a la que pueda estar expuesta nuestra información o un sistema de información. Bien sabemos que no existe en el mundo un sistema totalmente seguro y un SGSI no es la excepción al caso. Por ello, podemos citar el siguiente texto:

⁴ Cfr. Aguilera 2010:10

“Es posible disminuir de forma significativa el impacto de los riesgos sin la necesidad de realizar grandes inversiones en software y sin cortar con una gran estructura de personal. Para ello se hace necesario conocer y afrontar de manera ordenada los riesgos a los que está sometida la información...” (INTECO 2014)

Por lo expuesto, coincidimos con la fuente que es necesario encontrar, conocer, verificar y dar un plan de respuesta a los riesgos en lo que estén expuestos nuestra información o activos de información, para llevarlos a un nivel de riesgo considerable que pueda ser asumido por la organización. Esto es adecuado y necesario ya que, de darse el evento, este no debe generar un gran impacto en los procesos que esté involucrado y en la cual la organización este en la capacidad de sobrellevarlo para poder dar una acción correctiva sin que altere o perjudique la continuidad del negocio. Tener en cuenta en la clasificación de esta clase de riesgos, el cual es llamado riesgo residual, y otras clases de riesgos, conceptos revisados anteriormente.

2.5.3. Importancia y características

Con lo expuesto en el apartado anterior, es claro que la puesta en marcha de un SGSI es muy importante para la organización, ya que trae consigo muchos beneficios para la misma. También se debe mencionar que la información y los procesos que la soportan, los sistemas de información y las propias redes, que funcionan como la capa principal de las tecnologías de la información y comunicación, son activos trascendentales para continuidad del negocio y los objetivos que esta persigue. Por ello, es necesario definir, realizar, mantener y mejorar, principios básicos del modelo de gestión PDCA o ciclo de mejora continua de Deming, la seguridad de la información para los siguientes fines⁵:

- Por la adopción de procesos y metodologías de gestión para el tratamiento de la seguridad de la información da un valor agregado y diferenciador a la organización, lo cual permite mantener y aumentar la competitividad de la empresa.
- Es de suma importancia trabajar en un entorno normado y clasificada como buena práctica de gestión en seguridad de la información para el cumplimiento legal de la normativa vigente a nivel nacional.

⁵ Cfr. INTECO 2014

- Determinar los principales riesgos en la que la información o activos de información que integren el total o parte de la organización están expuestos. Ello permite un conocimiento completo de la exposición de amenazas y vulnerabilidades de los mismos y las medidas correctivas que deben ser implementadas.
- Definir las responsabilidades y obligaciones en el manejo y cuidado de los distintos activos de la información por parte de la organización. Ello permitirá definir los roles necesarios para el correcto procedimiento de manejo de la información.
- Establecer una metodología de la gestión de la seguridad de la información que estandarice los procesos necesarios para un manejo claro, adecuado y eficiente de los activos de información.
- Las mencionadas son las causas más importantes para la inserción y puesta en marcha de un SGSI en una organización. Nuestro trabajo está enfocado a las tres últimas, las cuales tendrán un desarrollo a lo largo del mismo.

Antes de mencionar las características que componen a un SGSI, como ya se había mencionado de forma muy escueta en el estado del arte del presente proyecto, el SGSI adopta el modelo de gestión PDCA (Plan, Do, Check y Act) o también llamado ciclo de Deming⁶. Este modelo de gestión considera una mejora constante en un modelo de procesos ordenados e implementados y el mantenimiento de las distintas fases que la componen. Este ciclo es mencionado a continuación como un breve resumen para su entendimiento cuando se nombre las componentes de cada fase dentro del SGSI:

- **Plan (Planear):** Establece realizar inicialmente un plan de actividades programadas y ordenado, necesarios para la consecución de los objetivos previamente trazados. Esta etapa incluye realizar planes de pruebas simulando escenarios reales con los que finalmente se tendrán al frente. Es recomendable realizar todas las pruebas que sean necesarias para tener un porcentaje alto de efectividad cuando sea implementado.
- **Do (Hacer):** Después de las pruebas realizadas en la etapa anterior y con los resultados obtenidos, los cuales han debido ser favorables, se propone poner el plan en marcha la ejecución de plan establecido. Esta etapa incluye también la asignación de recursos, ya sea personal u otro activo de información, organización y dirección de la misma.

⁶ Cfr. Miranda, Chamorro y Rubio 2007: 35

- **Check (Chequeo):** Consiste en realizar la agrupación de los nuevos requerimientos que sean necesarios para mejorar el proceso o gestión ya implementada. Además, contempla el monitoreo constante de lo ya ejecutado para evitar daños, perjuicios o mal funcionamiento de los procesos o procedimientos ya implementados.
- **Act (Actuar):** Esta última etapa contempla las observaciones tomadas en la etapa de Check y ejecuta las acciones correctivas que sea necesaria. También incluye la modificación o inserción de un nuevo plan de ejecución si se detecta que el implementado no es el óptimo o no rinde los beneficios esperados.

A continuación, se muestra una imagen referida a lo comentado:

Figura 15: Ciclo de mejora continua del Ciclo de Deming o PDCA

Fuente: www.ntfs.es, Estrategía PDCA

Como se observa en el gráfico, se sobreentiende que el modelo de gestión de Deming es un ciclo de mejora continua que busca fortalecer el plan estratégico formulado y diseñado inicialmente por la organización, ejecutarlo y monitorear su desempeño, encontrando falencias o malos resultados que permitan actuar sobre ellos para obtener en cada cambio realizado el rendimiento máximo dentro del alcance establecido. En la siguiente imagen se muestra el SGSI adopta a sus necesidades las etapas del ciclo de mejora continua de Deming.

Figura 16: Ciclo de Deming aplicado a un SGSI

Fuente: www.iso27000.es, Ciclo de Deming

La gráfica resume el funcionamiento etapa por etapa del SGSI y el lazo de retroalimentación que se tiene entre la última (Act o Actuar) y primera (Plan o Planear) etapa. Comentaremos las características de cada etapa a detalle según desde el punto de vista de implementación de un SGSI⁷.

- **Planeamiento:** Podemos resumirlo como el establecimiento y gestión del SGSI. En esta etapa de planeamiento estratégico se definen las siguientes funciones:

⁷ Cfr. Díaz, Alzórriz y Sancristobal 2014: 206

- Definición del alcance y los límites que se pretende obtener en el establecimiento del SGSI.
- Definición de la política del SGSI la cual tiene como principal objetivo la dirección y soporte de la gestión de la seguridad de la información. Tener en cuenta que las bases de la política de información deben ser sobre la legislación nacional vigente y acorde a los objetivos de negocio trazados por la organización
- Realizar el alcance que muestre la gestión del riesgo, esto implica conocerlo, identificarlo, tratarlo y menguarlo a un nivel aceptable que no impacte negativamente en los procesos de negocio de la organización. En este punto se debe tener en cuenta en el Plan de Tratamiento de riesgos.
- En base al punto anterior definir el riesgo residual, es decir el riesgo que la organización está de acuerdo a afrontar ante alguna crisis surgida por la pérdida, robo, ataque o mala manipulación de un activo de la información. La alta dirección debe avalar y autorizar el porcentaje definido y ser documentada y archivada para cuando esta sea necesaria.
- En base a los controles que componen la Norma ISO/IEC 27001:2005, la organización debe seleccionar cuales controles serán aplicados dentro de los procesos a ejecutar. Esto es llamado comúnmente SOA o Declaración de Aplicabilidad y debe ser autorizado por la Alta Gerencia.
- **Hacer:** Comprende la etapa del “Do” y se encarga de la implementación y operación del SGSI. Esta etapa la podemos resumir en tres tareas coordinadas, las cuales son mostradas a continuación:
 - En base a los riesgos previamente identificados, debemos realizar la formulación e implementación del Plan de Tratamiento de Riesgos, comúnmente llamado PTR por sus siglas.
 - Implementar los controles de la norma ISO/IEC 27001:2005 previamente seleccionados. Además, de la gestión de operación y recursos del SGSI
 - Implementar los procedimientos y directrices necesarias para la toma rápida de acción ante algún inconveniente que pueda ser víctima algún activo de información previamente clasificado en base a su importancia y relación con los procesos de negocio.

- **Chequear:** Esta etapa está encargada del monitoreo y revisión del SGSI implementado y básicamente comprende el chequeo de los controles y procedimientos ejecutados en la fase anterior. Para resumir, podemos mencionar:
 - Revisiones programadas de la efectividad y rendimiento del SGSI. Es importante no olvidar que el SGSI persigue objetivos específicos marcados por la empresa y/o organización que deben cumplidos cabalmente.
 - Revisar si el riesgo residual asumido por la organización es el mismo a través del tiempo o puede modificarse según las nuevas tendencias de ataques y/o demás factores que se crean conveniente.
 - Tener un registro de las posibles acciones que puedan perjudicar el desempeño del SGSI implementado, esto como buena práctica para toma de decisiones en post de la mejora continua del sistema de gestión.
- **Actuar:** Esta etapa está encargada del mantenimiento y mejora continua del SGSI implementado. Se puede resumir en dos grandes campos:
 - En base a las fallas detectadas en la etapa de chequeo se debe tomar acción inmediata para la mejora del SGSI, si es necesario la reformulación del plan estratégico inicial que tenga en cuenta procedimientos que mitiguen o extingan los riesgos detectados.
 - Asegurar que las medidas correctivas que sean implementadas sean efectivas y cumplan su cometido.

Este modelo adoptado por el SGSI y las etapas que la integran son mencionadas en la norma ISO/IEC 27001:2013. Además, muestra procesos de la norma, objetivos de control y demás características que serán abarcados en el siguiente apartado.

2.6. Norma ISO/IEC 27001:2013

2.6.1. Familia de la norma ISO/IEC 27000

No es el objetivo del presente proyecto explicar las funciones y detalles de trabajo de la ISO (International Organization for Standardization o en español Organización Internacional de Estandarización) sino en modo concreto indicar que es un organismo encargado de establecer y promover normas internacionales en distintos ámbitos, tales como fabricación de productos y/o servicios, comercio y comunicación.

Para ello, la ISO se integra de organismos que participan en el desarrollo de Normas Internacionales a través de los llamados comités técnicos, esto con la finalidad de tratar campos particulares de actividad técnica. En este punto, es destacado mencionar que este organismo trabaja en colaboración con la IEC (International Electrotechnical Commission), la cual es la organización de normalización en los campos eléctrico, electrónico y tecnologías relacionadas.

Por otro lado, a lo largo de su historia este ente ha establecido normas que son mundialmente aceptadas y para decir de mejor modo dan un porcentaje diferenciador del resto de organizaciones que no las tiene. Por ello, es nuestro objeto de estudio la norma ISO/IEC 27001:2013, en la cual estableceremos la implementación de un SGSI en una organización en defensa del buen recaudo de los activos de la información, pero no sin antes haber mencionado el contenido de las normas que componen la familia ISO/IEC 27000.

Ahora, como ya se había comentado la familia de norma ISO/IEC 27000 se integra de una serie de estándares, esto según su paso en el tiempo. En base a ello, en la siguiente gráfica se muestra su evolución desde la norma BS 7799-1 en sus inicios hasta la ISO/IEC 27001 en su versión 2013 en la actualidad.

Figura 17: Historia de las normas de la familia ISO/IEC 27000

Fuente: blog.segu-info.com.ar, Bienvenida nueva ISO/IEC 27007:2017

Visto el grafico, se procede a continuación a mencionar brevemente cada una de ellas.

- **ISO/IEC 27000:** Da una visión general de la familia de estándares en relación a la Seguridad de la Información, da una introducción al concepto de SGSI y una descripción del ciclo de mejora continua. Publicada en abril del año 2009, da en resumen las generalidades de los sistemas de Gestión de Seguridad de la Información, sus fundamentos y vocabulario.
- **ISO/IEC 27001:2005:** Norma publicada el 15 de octubre del 2005, que especifica los requisitos necesarios para la implantación de un Sistema de Gestión de Seguridad de la Información (SGSI). Es la norma bandera de la familia 27000 y tiene sus orígenes en la norma británica BS 7799-2:2002, es la norma certificable a entidades y organizaciones que implementen y ejecuten un SGSI dentro de un proceso o área específica de las mimsas. Esta norma contiene en su estructura el anexo A, la cual enumera en forma resumida los objetivos de control y controles desarrollados en la norma
- **ISO/IEC 27001:2013:** Esta norma fue actualizada en el año 2013, en la cual se establecen cambios significativos con sus antecesora la ISO/IEC 27001:2005. Unos de los cambios saltantes es que se elimina el uso obligatorio del Sistema de Gestión PDCA, pudiendo tomar cualquier otro modelo de Gestión, ello acorde a las necesidades de la organización. Aunque este cambio no excluye la adopción del PDCA, se debe tener en cuenta que es normalmente aceptado, adoptado y reconocido, por lo cual sigue vigente en implementaciones de la Norma. Al igual que la ISO/IEC 27001:2005 cuenta con el anexo A, donde se da el alcance de los controles de seguridad aplicables a la organización.
- **ISO/IEC 27002:2005.** Tener en cuenta que no son obligatorios todos los controles, pero si la organización debe especificar la aplicabilidad y no aplicabilidad de los controles seleccionados y no seleccionados respectivamente. Entre los organismos acreditados más importante para la certificación se encuentran la AENOR, BSI, SGS y BRS.
- **ISO/IEC 27002:2013:** Publicada en el año 2013, esta norma es el código de buenas prácticas para la Gestión de la Seguridad de la Información. Esta guía de buenas prácticas describe a detalle los objetivos de control y controles necesarios para la seguridad de la información. Como ya se comentó, esta norma posee 14 cláusulas que

contienen 35 objetivos de control y 114 controles. Para evitar posible confusión, esta norma es la que corresponde al Anexo A de la norma ISO/IEC 27001:2013.

- **ISO/IEC 27003:** Compuesta en una guía para la implementación de SGSI y los distintos requerimientos del modelo de ciclo de mejora continua PDCA.
- **ISO/IEC 27004:** Publicada en diciembre del 2009, esta norma mide la eficacia de la implantación de un SGSI a través del desarrollo en la utilización de métricas, Por ello, ayuda a las organizaciones a medir, informar, y en consecuencia mejorar la eficacia de un Sistema de Gestión de Seguridad de la Información (SGSI)
- **ISO/IEC 27005:** Publicada en junio del 2008, esta norma se ocupa de la gestión del riesgo en la seguridad de la Información, apoyandose en los conceptos generales de la norma ISO/IEC 2700. Se puede revisar más información de la norma en el capítulo “Estado del Arte”, apartado 2.1.8.
- **ISO/IEC 27006:** Publicada en febrero del 2007, esta norma especifica los requisitos para la acreditación de las organizaciones que proporcionan la certificación de los Sistemas de Gestión de Seguridad de la Información. Como comentario, es una versión revisada de la norma ISO/IEC 17021, en la cual apoya en la interpretación de los criterios de acreditación de ISO/IEC 17021 cuando se aplican a entidades de certificación de ISO 27001.
- **ISO/IEC 27007:** La norma presenta una guía para los organismos de certificación acreditados, auditores internos, auditores externos y otros para la auditoria de un Sistema de Gestión de Seguridad de la Información (SGSI). Tener en cuenta que la norma se basa en la ISO/IEC 19011 (Norma de Calidad y auditoria de sistemas de gestión ambiental) y la ISO/IEC 17021 (Evaluación de la conformidad de requisitos para los organismos que realizan la auditoria y certificación de sistema de gestión de seguridad de la información).
- **ISO/IEC 27011:** Publicada en enero del 2008, esta norma comenta las directrices necesarias para la seguridad de la información en organizaciones de Telecomunicaciones utilizando la norma ISO/IEC 27002.
- **ISO/IEC 27031:** Publicada en marzo del 2011, esta norma proporciona un marco de métodos y procesos para la identificar y especificar todos los aspectos de mejora en la preparación de las TIC (Tecnología de la Información y Comunicación), con el fin de

garantizar la continuidad del negocio. Esta norma está en línea con la norma ISO 22301 (Continuidad del Negocio).

- **ISO/IEC 27032:** Publicada en el año 2012, esta norma proporciona orientación para mejorar el estado de la seguridad cibernética. En otras palabras, consiste en una guía relativa a la Ciberseguridad.
- **ISO/IEC 27033:** Norma relacionada a la norma ISO/IEC 18028, la cual muestra una metodología sistemática para la implementación de una red segura. Entre sus principales aspectos, comprende: Gestión de la seguridad de red, arquitectura de la seguridad de red, seguridad de las comunicaciones entre redes utilizando Gateway, seguridad de acceso remoto y seguridad de redes utilizando VPN.
- **ISO/IEC 27034:** Norma que consiste en una guía de seguridad de aplicaciones. Existen proyectos asociados, tal es el de OWASP, el cual establece un proyecto de controles asociados a la seguridad de las aplicaciones, en la cual se relacionan las mejores prácticas de OWASP Top 10 en los controles de seguridad de aplicaciones.
- **ISO 27799:** Publicada el 12 de junio de 2008, es la norma de Gestión de Seguridad de la Información Sanitaria utilizando la norma ISO/IEC 27002.

Una vez ya comentada las normas que componen la familia ISO/IEC 27000, es necesario revisar en detalle la norma ISO/IEC 27001:2013 para una familiarización de la norma y entendimientos del despliegue y ejecución del proyecto.

2.6.2. Evolución de la norma ISO/IEC 27001:2013

Si bien ya revisamos de forma rápida la evolución de la familia 27000, a continuación, se muestra específicamente la evolución de las normas para la Gestión de la Seguridad de la Información hasta llegar a la ISO/IEC 27001 en su versión 2013.

Figura 18: Historia de las normas de Seguridad de la Información

Fuente: www.pmg-ssi.com, la NCh ISO 27001

En la gráfica podemos observar la evolución de las normas asociadas a seguridad de la información, tal como se incluye la normativa BS (British Standards), creada a comienzos del año 95, hasta la actual ISO/IEC 27001:2013, la cual es nuestro tema de estudio. Todas las creadas siempre han tenido en cuenta la adopción de sistemas de gestión que se basen en procedimientos y directrices que soporten el resguardo de la información en todos sus ámbitos. En base a ello, la descripción de la norma ISO/IEC 27001:2013 la mencionamos en el siguiente apartado.

2.6.3. Definición de la norma ISO/IEC 27001:2013

La norma ISO/IEC 27001 en su versión publicada en el año 2013, pertenece a la familia de normas ISO 27000, en la cual establece la implementación de un sistema de gestión de seguridad de la información basada generalmente en el ciclo de mejora continua PDCA o ciclo de Deming. Por ello, como ya se ha comentado, esto comprende el establecimiento, implementación, monitoreo, mantenimiento y mejora continua del SGSI bajo un enfoque basado en procesos. Esta norma se apoya en la ISO/IEC 27002, la cual establece los dominios, controles y objetivos de control de se debe ejecutar para la toma de decisiones y acción respecto a la seguridad de los activos de información dentro y fuera de la organización. Esta última también es llamada código de buenas prácticas, ya que se enumeran 14 cláusulas, 35 objetivos de control y 114 controles, en donde se describe a detalle los escenarios que debemos tener en cuenta para el resguardo y buen manejo de los activos de información.

2.6.4. Importancia y Características

Como ya se ha comentado, el enfoque basado en procesos en el cual se basa la norma ISO/IEC 27001:2013, permite e integra a todo el personal de la organización, no solo a los responsables de la custodia de los activos de información, sino al conjunto de sus colaboradores. Por ello, es importante que todo el personal está inmerso de las directivas a implementar y la política de SGSI ejecutada, la conozcan y entiendan a cabalidad sus objetivos para que el proceso sea exitoso. En palabras resumidas el modelo basado en procesos estimulará al personal a seguir el ciclo de mejora continúa comentado en párrafos anteriores. Con lo comentado, pasaremos a mencionar los controles establecidos en el Anexo A de la norma ISO/IEC 27001:2013, o comúnmente llamada ISO/IEC 27002:2013.

Figura 19: Dominios, objetivos de control y controles establecidos por la norma ISO/IEC 27002:2013

Fuente: Magazcitur, ISO/IEC 27001:2013 ¿Qué hay de nuevo?

Como se muestra en la gráfica anterior, los controles especificados en la norma ISO/IEC 27002, se sub-dividen en cuatro áreas fundamentales. Descritas anteriormente, tales son del tipo Técnicos, control, organizaciones y físicos.

Ahora, es preciso comentar que la norma ISO/IEC 27001:2013 se avala en la documentación necesaria, en la cual toda medida de protección que se haya implantada debe ser documentada. Esta documentación está dividida de la siguiente manera:

- **Políticas:** Tiene como propósito sentar las bases de seguridad, en donde se especifican los objetivos generales y las implantaciones que ha realizado la organización en esfuerzo de la consecución de la seguridad de la información. Esto sirve de muestra para información de los objetivos mencionados a todo el personal de la organización.
- **Procedimientos:** Aquí se detallan a niveles técnicos como se proponen alcanzar los objetivos propuestos mencionados en la política de seguridad de la información.
- **Instrucciones:** Básicamente estructuran el desarrollo de los procedimientos y que ejecuciones son necesarias para su puesta en marcha.
- **Registros:** De modo concreto muestran que efectiva es la implantación del SGSI y el cumplimiento de los requisitos. Para ello, la importancia de indicadores y métricas

que nos muestren que tan cerca o lejos estamos en cuantos a los objetivos en materia de seguridad de la información han sido trazados.

Para culminar el presente capítulo, se ha tomado los conceptos y definiciones de los actores principales que se establecen en la norma ISO/IEC 27001:2013, los cuales son: SGSI, PDCA (ciclo de Deming o de mejora continua) e ISO/IEC 27002 (código de buenas prácticas que incluye dominios, objetivos de control y controles). Estas definiciones serán fundamentales para la comprensión del objeto de la norma y los beneficios que traen consigo en la implementación de la misma para la organización en estudio.

CAPÍTULO 3: DEFINICIÓN DEL PROBLEMA Y TOMA DE REQUERIMIENTOS

3.1. Introducción

Es importante mencionar que el avance tecnológico de los últimos años ha traído consigo falencias en materia de Seguridad, ya sea a nivel de procedimientos o a nivel técnico. Esto se refleja en las estadísticas arrojadas en los Reportes de Seguridad de distintos fabricantes, en donde se evidencia que, entre otras clases de amenazas, las violaciones de datos en las grandes y pequeñas organizaciones tuvieron un incremento considerable comparado con años anteriores. Estas violaciones de datos, las cuales pueden ser desde ataques internos, fraudes, robo de información confidencial, entre otras, impactan de gran manera la continuidad del negocio y a la vez la imagen de las organizaciones, peor aún si nos centramos en empresa prestadoras de Servicios, ya sean Servicios de Salud, Administrativos, Técnicos, entre otros. En base a lo comentado, es necesario mostrar algunas estadísticas mencionadas en el Informe de Amenazas a la Seguridad de Internet (Volumen 21, Abril del 2016), proporcionado por el fabricante Symantec, líder de Soluciones en Seguridad. Dentro del apartado “Violaciones de Datos y Privacidad”, evidencia cifras de como los incidentes en las violaciones de datos se han desarrollado durante el 2015 y que Sectores sufrieron violaciones por el número de identidades expuestas e incidentes de Seguridad.

Figura 20: Línea del Tiempo de Violaciones de Datos

Fuente: Symantec, Informe de Amenazas a la Seguridad de Internet 2016

Como se puede apreciar en la imagen, existen aproximadamente 195 millones de Identidades Expuestas en diciembre del 2015 y 41 millones de número de incidentes de Seguridad como pico más alto ocurrido en el mes de junio. Como un alto número, estas son cifras alarmantes al tener en cuenta que todo este conglomerado de amenazas sobre activos de información dentro de las organizaciones, lo cual se puede considerar como información sensible o confidencial, han sido materializadas.

En el mismo sentido de lo comentado, el fabricante nos da evidencias de cuales han sido los principales sectores, clases o tipos de organizaciones que han sido víctimas de pérdida de información sensible y confidencial:

Figura 21: Principales Sectores que sufrieron Violaciones por Número de Identidades Expuestas e Incidentes

Fuente: Symantec, Informe de Amenazas a la Seguridad de Internet 2016

Como se observa en la gráfica N°2, el Sector de Servicios (Salud, Administrativos, Tecnológicos, entre otros) ha sido el más afectado en el 2015 y por las tendencias de materialización de amenazas en las organizaciones, el crecimiento en el porcentaje es casi un hecho si no se toman medidas al respecto. Por ello, si bien se considera que la información es uno de los activos más importantes dentro de las organizaciones, podemos evidenciar que son muy pocas las que adoptan medidas de prevención contra este tipo de incidentes. Ello no significa solo estar al día con los últimos equipamientos tecnológicos, lo cual es un gran apoyo, sino también contemplar un Sistema de Gestión que permita a la organización prepararse de una manera integral, considerando controles tecnológicos, políticas, procedimientos, capacitación y entrenamiento del personal, para proteger los activos de información que se encuentran involucrados en sus procesos de negocio.

En base a todo lo comentado, este capítulo aborda la problemática de una empresa Integradora de Servicios de Telecomunicaciones y como un Sistema de Gestión de Seguridad de la Información puede contribuir con preservar la confidencialidad, integridad y disponibilidad de la información que soporta al proceso de servicios Post-Venta de la empresa.

3.2. Análisis del Problema

Los problemas identificados en la organización fueron:

- Continuos ataques a Sistemas Informáticos de la organización, específicamente el servidor de Gestión de Tickets. Ello evidenciado en registros de eventos o logs desde redes externas (Internet) y redes Internas (Redes locales mediante ataques de hombre en el medio, entre otros). Tener en cuenta que a pesar de que la organización cuenta con equipos de Seguridad dentro de Infraestructura de Red, las evidencias de ataques no son analizadas y no existe un plan de acción de remediación. Adicionalmente, no cuentan con procedimientos para el acceso y manejo de la información en todos sus ámbitos.
- Pérdidas de información confidencial, tanto propia como de sus clientes. Esta información se encuentra ubicada en un Servidor de Archivos sin niveles de acceso restringido y ninguna jerarquización o clasificación del tipo de información. Entre el tipo de información alojada en el servidor podemos mencionar: Backup de implementaciones, información de contactos, versiones de software de equipos, configuraciones, topologías de red, estructura de datos, informes de trabajos, informes de proyectos, análisis financiero de proyectos, entre otros. Cabe indicar que la organización no cuenta actualmente con un sistema de respaldo de esta información confidencial.
- Ausencia de un inventario de activos de información asociados al Proceso de Servicio Post-Venta de la organización. En consecuencia, no es posible realizar un análisis de los riesgos a los que se encuentran expuestos, minimizando la materialización de una amenaza sobre los mismos.
- Falta de una Estructura Organizacional de Seguridad de la Información en la cual recaiga la responsabilidad y obligación de los procesos de seguridad sobre los activos de información del proceso Servicio Post-Venta de la organización.

- Carencia de procesos, lineamientos y políticas que propongan cambios a adoptar para evitar la incorrecta manipulación de información sensible de clientes y propia de la organización.

3.3. Impacto del Problema en la Organización

El objeto central de estudio es el proceso de Servicio Post-Venta de la organización. En base a ello, el impacto que genera los problemas comentados en el Integrador de Telecomunicaciones son los siguientes:

- Impacto en la continuidad del servicio ofrecido por el área debido a pérdida de información confidencial de clientes y propia de la organización. No contar con la información de accesos a Infraestructura Tecnológica del cliente, la cual cuenta con contrato de Soporte, retrasa la resolución de problemas o servicios solicitados por los clientes finales, creando insatisfacción en los clientes de la organización.
- Impacto en la productividad del servicio ofrecido por área, específicamente el proceso de Servicio Post-Venta. En este punto tenemos que tener en cuenta que el Sistema de Gestión de Tickets es un sistema que integra módulos logísticos, técnicos y administrativos, lo cual su inoperatividad trae como consecuencia la inadecuada gestión de los requerimientos del cliente, creando caos en la asignación de recursos, ya sea a nivel de personal calificado u herramientas de soporte necesarias para la atención de los requerimientos.
- Impacto económico por pérdidas de ingresos/facturación y oportunidades de negocios para la organización. Ello debido a la pérdida de información confidencial y sensible de clientes y propia de la organización. Los retrasos en los tiempos de atención a los requerimientos del cliente, excedidos a los acordados en los niveles de servicio (SLA), trajo como consecuencia la ejecución de penalidades descritas en el contrato firmado entre ambas partes. Asimismo, añadido al monto asumido por la organización por la penalidad sancionada, la misma tuvo que asumir en muchas ocasiones los montos de traslados, viáticos y pagos de horas extras al personal que ejecutaron las labores. Esto generó un alto valor de pérdida de ganancias dentro del contrato establecido.
- Impacto en la imagen de la empresa y en las relaciones de confianza establecidas con los clientes por pérdida de información confidencial. Algunos clientes de la organización optaron por no continuar con el vínculo contractual entre ambas partes

con la organización, dejando fuera ingresos anuales seguros, a través del tiempo, en la misma.

- Impacto legal y penal por pérdidas de información confidencial, y muchas veces catalogada como información “sensible” de clientes. En este punto debemos tener en cuenta que con la aprobación del Reglamento de Ley 29733: Ley de Protección de Datos Personales, es obligatorio su ejecución en entidades públicas y privadas. Si bien es cierto se debe realizar un análisis de la información que contiene la organización, la cual pueda ser considerada como datos personales, es necesaria su cumplimiento dentro de la organización. Por último, es necesario resaltar que, aunque pudieron hacerlo, los clientes no presentaron ningún recurso legal por pérdida de información confidencial.

3.4. Causas Origen del Problema

Las principales causas detectadas que origina la problemática mencionada en la organización son:

- Falta de controles de accesos a Sistemas de Información críticos en la organización, tales como servidores de archivos, Sistemas de Gestión de Ticket, entre otros.
- No existen cargos, ni castigos que penalicen el acceso de información confidencial de clientes y propia de la organización a personal no autorizado.
- No existe una clasificación de la información dentro de los activos de información, catalogada como privada, confidencial y pública.
- No existe un inventario de activos de información que estén asociados e involucrados al proceso de Servicio Post-Venta de la organización.
- No existe un control de las vulnerabilidades a lo que estos activos pueden estar expuestos. Asimismo, los riesgos asociados a la concretización de una amenaza sobre los activos mencionados.
- Ausencia de un Sistema de Gestión en donde se estipulen políticas y procedimientos en relación a la protección de los activos de información en la organización.

3.5. Solución al Problema

Debido a los problemas en materia de Seguridad de la Información expuestos al proceso de Servicio Post-Venta de la Organización, se vio necesario la adopción de algún modelo o sistema existente en el mercado mundial, que brinde una solución integral y permanente a los problemas presentados. En base a ello, la organización cree conveniente la adopción de un Sistema de Gestión de Seguridad de la Información, por sus siglas SGSI, base de la norma ISO/IEC 27001 en su última versión (2013). Este SGSI, dentro de sus procedimientos y lineamientos internos permitirán a la organización:

- Clasificar lo principales activos de información involucrados en el proceso de servicios Post-venta de la organización.
- Determinar los riesgos de Seguridad a los que se encuentran expuestos los activos de información asociados a los procesos del área de servicios Postventa de la empresa y proponer un Plan de Tratamiento de Riesgos de los mismos.
- Definir la Estructura Organizacional del SGSI, estableciendo roles y responsabilidades en el manejo de la Seguridad de los activos de información que integran el proceso de Servicios Post-Venta de la organización.

3.6. Resultados esperados

Son los siguientes:

- Lograr la clasificación de los activos de información en base a los pilares de la Seguridad de la Información, tales son: confidencialidad, integridad y su disponibilidad.
- Determinar las principales vulnerabilidades de seguridad de la información identificada y el impacto que tendría la ejecución de alguna amenaza sobre el activo de información valorizado en caso de materializarse.
- Establecer un Plan de Tratamiento de Riesgos (PTR) para la gestión necesaria de los riesgos asociados a los activos de información valorizados.
- Establecer la Declaración de Aplicabilidad (SOA) que integre los controles de seguridad identificados y necesarios, seleccionados para cada nivel de riesgo asociado a cada activo de información valorizado.

- Establecer los roles, responsabilidades, funciones y obligaciones asignadas según la clasificación de la Estructura Organizacional de la Gestión de la Seguridad de la Información.

3.7. Análisis actual de Seguridad de la Información en la Organización (Análisis de Brechas - GAP Analysis)

En este apartado realizamos el Análisis de Brechas o Gap Analysis en el cual una organización identifica la distancia entre la situación actual de Seguridad de la Información y las buenas prácticas más reconocidas en la industria. Cabe decir que durante su ejecución se realiza entrevistas con las diferentes áreas de la organización, ello con el fin de identificar la situación actual de la misma en materia de seguridad, comparándola contra las mejores prácticas o normativas vigentes respecto a la seguridad de la información, en nuestro caso específico lo indicado en la norma ISO/IEC 27001 en su versión 2013.

Las actividades involucradas en la misma son:

- Identificación de la brecha existente entre las prácticas de seguridad actuales dentro de la organización y las mejores prácticas existentes en la industria.
- Análisis de la distancia entre las prácticas actuales de la organización y aquellas requeridas por las normas vigentes. En nuestro caso la norma ISO/IEC 27001 en su versión 2013.
- Punto de partida para un análisis de Seguridad de la Información actual en la organización y que grado de cumplimiento tiene respecto a lo indicado en la norma.
- Proponer prácticas para mejorar el nivel actual de seguridad de la compañía.

Para nuestro caso de proyecto, se realizó el Análisis de Brechas o GAP Analysis mediante la clasificación de tres (03) grandes logros, los cuales son los siguientes:

- Definición del Marco de Seguridad y Privacidad en la Organización
- Implementación del Plan de Seguridad y Privacidad de la Información
- Monitoreo y mejoramiento continuo

Los logros serán revisados uno a uno a continuación.

3.7.1. Definición del Marco de Seguridad y Privacidad en la Organización

En este logro se realizan consultas asociadas al estado actual de seguridad y privacidad en la organización. Dentro de ellas, se definen tres estados de cumplimiento según lo indicado en la norma ISO/IEC 27001 en su versión 2013. Los estados son conceptualizados de la siguiente manera:

- **Cumple satisfactoriamente:** La organización lo ha adoptado y mantiene una gestión sobre ello. Asimismo, se encuentra documentado y es conocido por el personal asociado al SGSI. Adicionalmente, su ejecución va en cumplimiento de la norma ISO27001:2013. Finalmente, su cumplimiento es del 100%.
- **Cumple parcialmente:** Su ejecución va en cumplimiento parcial con los requerimientos de la norma estipulados en la norma ISO27001:2013. Asimismo, a pesar que se aprobó por el personal relacionado a la gestión de la Seguridad de la Información, no se encuentra gestionado, ni documentado.
- **No cumple:** No existe, ni se está ejecutando.

Según lo comentado, las consultas realizadas fueron las siguientes:

Tabla 8: Definición del Marco de Seguridad y Privacidad en la Organización

PLANEAR				
ITEM	PREGUNTA	VALORACIÓN	EVIDENCIA	RECOMENDACIÓN
1	¿Cuenta la organización con un plan de proyecto donde se incluyen las prioridades y objetivos para la implementación del SGSI?	Cumple parcialmente	La organización tiene planeado adoptar un Sistema de Gestión de Seguridad de la Información (SGSI), pero aún no lo lleva en marcha. Tiene definido objetivo principal, pero aún no está documentado. Tomará como base el diseño del presente proyecto.	Crear un plan inicial del proyecto que incluya prioridades y objetivos y estructura del SGSI.
2	¿La organización contó con la aprobación de la Alta Dirección para el inicio la adopción del SGSI?	Cumple parcialmente	La Alta Dirección: Directorio y Gerencia General tienen aprobado el inicio de un Sistema de Gestión de Seguridad de Información (SGSI) en la Organización, pero aún no se gestiona.	Debe existir un documento preliminar de aprobación firmado por parte de la dirección donde se aprueba el inicio del proyecto.
3	¿Cuenta la organización con una autoevaluación que mida el avance en el establecimiento, implementación, mantenimiento y mejora continua del SGSI?	No cumple	No existe actualmente un Sistema de Gestión de Seguridad de la Información (SGSI) implementado en la Organización en estudio.	Una vez implementado el SGSI, se sugiere ejecutar una autoevaluación del mismo.
4	¿La organización ha identificado los aspectos internos y externos que pueden afectar en el desarrollo de la implementación del SGSI?	Cumple parcialmente	La Organización ha evaluado que aspectos pueden impactar en la puesta en marcha del Sistema de Gestión de Seguridad de la Información, específicamente en los procesos asociados al proceso de Servicios Post-Venta, pero no existe un documento formal que contenga los puntos revisados.	Se deben formalizar en un documento revisado por la Alta Gerencia y personal involucrado en el proyecto los aspectos internos y externos que impactan en el desarrollo de la implementación del SGSI.
5	¿La organización ha documentado la asociada al Sistema de Gestión de Seguridad de la Información?	No cumple	No existe actualmente en la Organización documentación asociada a un Sistema de Gestión de Seguridad de la Información (SGS), aún no se encuentra implementado el SGSI.	Toda la documentación generada del Sistema de Gestión de Seguridad de la Información debe estar debidamente documentada, ello al momento de su implementación y despliegue.

PLANEAR				
ITEM	PREGUNTA	VALORACIÓN	EVIDENCIA	RECOMENDACIÓN
6	¿La organización ha identificado las partes interesadas, necesidades y expectativas que contempla la implementación del SGSI?	Cumple parcialmente	A pesar de que la organización cuenta como parte Interesada a la Alta Dirección: Directorio y Gerencia General, también la Gerencia Técnica, aún no define documentación al respecto, ni ha creado aún un plan de necesidades y expectativas por el momento.	Se requiere que se identifiquen las partes interesadas tanto internas como externas, detallando cuáles son sus necesidades y expectativas en la implantación del SGSI.
7	¿La organización ha evaluado los objetivos y las necesidades asociadas a la correcta gestión de la Seguridad de la Información?	Cumple parcialmente	La organización ha evaluado el objetivo general y objetivos específicos de la puesta en marcha de un Sistema de Gestión de Seguridad de la Información (SGSI), pero aún no está documentado.	Reaizar la documentación formal del objetivo general y objetivos específicos del SGSI.
8	¿Existe un Comité de Seguridad de la Información dentro de la organización?	No cumple	No existe aún una clasificación jerárquica en donde se definan roles y obligaciones asociadas a la Seguridad de la Información en la Organización.	Definir la Estructura Organizacional del Sistema de Gestión de Seguridad de la Información, documentarla y hacerla expresa a todos los colaboradores de la organización.
9	¿La organización ha definido el alcance y los límites del Sistema de Gestión de Seguridad de la Información?	Cumple parcialmente	La organización tiene como alcance del Sistema de Gestión de Seguridad de la Información (SGSI) al proceso de Servicio de Post-Venta. Sin embargo, aún no existe documentación al respecto.	Crear un documento formal donde se estipule el alcance a nivel organizativo del SGSI.

PLANEAR				
ITEM	PREGUNTA	VALORACIÓN	EVIDENCIA	RECOMENDACIÓN
10	¿Existe una Política de Seguridad de la Información aprobada por la Alta Dirección?	No cumple	No hay reunión existente en donde se haya revisado la implementación de una Política de Seguridad de la Información que este asociado al SGSI. No existe documentación al respecto.	Crear un documento que defina la política general de Seguridad de la Información y sus respectivos alcances.
11	¿Existe un documento formal donde se detalle los roles, responsabilidades y autoridades en materia de seguridad de la información?	No cumple	No hay reunión existente en donde se haya revisado definir los roles, responsabilidades y autoridades asociados a la Seguridad de la Información. No existe documentación al respecto.	Definir la Estructura Organizacional del Sistema de Gestión de Seguridad de la Información, documentarla y hacerla expresa a todos los colaboradores de la organización
12	¿La organización tiene establecido algún proceso para identificar, analizar, valorar y tratar los riesgos de seguridad sobre los activos de información?	Cumple parcialmente	La organización tiene como alcance del Sistema de Gestión de Seguridad de la Información (SGSI) al proceso de Servicio Post-Venta. Las entradas o sub-procesos involucrados en el mismo son: Gestión de Venta o Renovación de Contratos de Mantenimiento, Generación de Ticket para soporte remoto, Generación de Ticket para soporte en sitio, Atención de soporte en sitio en cliente y Registro de Incidencias de soportes atendidos. Sin embargo, aún no existe documentación al respecto.	La organización debe adoptar una metodología para gestionar los riesgos, ya sea reconocida en el mercado o propia. En ello, describir en una matriz de riesgos los resultados de acuerdo a los criterios de aceptación de riesgos asumidos por la organización.
13	¿La organización ha realizado un SOA (Declaración de aplicabilidad) que contenga los controles de seguridad necesarios en la organización?	No cumple	No existe un SOA (Declaración de Aplicabilidad) en donde se especifiquen que controles son necesarios adoptar y ejecutar para la Gestión de Riesgos en los activos de información.	Crear documento de declaración de aplicabilidad donde se justifique la inclusión y exclusión de controles del Anexo A de la norma ISO27001 versión 2013.

PLANEAR				
ITEM	PREGUNTA	VALORACIÓN	EVIDENCIA	RECOMENDACIÓN
14	¿Se ha definido un modelo de comunicaciones internas y externas asociada a la seguridad de la información?	No cumple	No existe un modelo de comunicaciones internas, ni externas en donde se dé información de los avances o estatutos asociados al Sistema de Gestión de Seguridad de la Información (SGSI) o de la propia Seguridad de Información.	Se debe desarrollar un modelo que indique el contenido de la comunicación y su trazabilidad e el tiempo.
15	¿La organización ha evaluado las competencias de sus colaboradores a su cargo que afecten el desempeño de la seguridad de la Información?	No cumple	No existe una evaluación de competencias de colaboradores o trabajadores de la organización que estén asociadas a Seguridad de la Información.	Se debe verificar las competencias del personal que se encuentre involucrado con la seguridad de la información dentro de la organización. Asimismo, de no tenerlas, se debe definir un plan de capacitación con el fin de que dichas personas adquieran las competencias respectivas.

Fuente: Versión adaptada y modificada de <http://tic.bogota.gov.co>, Autodiagnóstico del SGSI

3.7.2. Implementación del Plan de Seguridad y Privacidad de la Información

En este logro se revisan que controles de la norma ISO/IEC 27002 se encuentran actualmente en ejecución en la organización. Dentro de ello, se definen cuatro estados de cumplimiento según lo indicado en la norma ISO/IEC 27001 en su Anexo “A”, es decir la norma ISO/IEC 27002. Los estados son conceptualizados de la siguiente manera:

- **Cumple satisfactoriamente:** La organización lo ha adoptado y mantiene una gestión sobre ello. Asimismo, se encuentra documentado y es conocido por el personal asociado al SGSI. Adicionalmente, su ejecución va en cumplimiento de la norma ISO27001:2013. Finalmente, su cumplimiento es del 100%.
- **Cumple parcialmente:** Su ejecución va en cumplimiento parcial con los requerimientos de la norma estipulados en la norma ISO27001:2013. Asimismo, a pesar que se aprobó por el personal relacionado a la gestión de la Seguridad de la Información, no se encuentra gestionado, ni documentado.
- **No cumple:** No existe, ni se está ejecutando.
- **No aplica:** El control no es aplicable para la organización.

Según lo comentado, la tabla de aplicabilidad de controles actualmente en la organización se puede observar y revisar en detalle en el “**Anexo I**”, adjunto al presente proyecto. De todos modos, se muestra el desarrollo de los primeros controles de prueba, según su estatus de cumplimiento en la organización:

Tabla 9: Implementación del Plan de Seguridad y Privacidad de la Información

ANEXO			ESTADO	EVIDENCIA
A5	POLÍTICAS DE LA SEGURIDAD DE LA INFORMACION			
A5.1	Orientación de la dirección para la gestión de la seguridad de la información			
Objetivo: Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes				
A5.1.1	Políticas para la seguridad de la información	Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.	No cumple	No existe documentación o ejecución de control comentado.
A5.1.2	Revisión de las políticas para la seguridad de la información.	Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.	No cumple	No existe documentación o ejecución de control comentado.
A6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION			
A6.1	Organización interna			
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.				

ANEXO			ESTADO	EVIDENCIA
A6.1.1	Roles y responsabilidades para la seguridad de la información	Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	No cumple	No existe documentación o ejecución de control comentado.
A6.1.2	Separación de deberes	Control: Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización	No cumple	No existe documentación o ejecución de control comentado.
A6.1.3	Contacto con las autoridades	Control: Se deben mantener contactos apropiados con las autoridades pertinentes.	No cumple	No existe documentación o ejecución de control comentado.
A6.1.4	Contacto con grupos de interés especial	Control: Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad	No cumple	No existe documentación o ejecución de control comentado
A6.1.5	Seguridad de la información en la gestión de proyectos.	Control: La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.	No cumple	No existe documentación o ejecución de control comentado.

Fuente: Versión adaptada y modificada de <http://tic.bogota.gov.co>, Autodiagnóstico del SGSI

3.7.3. Monitoreo y Mejoramiento continuo

En este logro se revisan que las dos últimas fases del ciclo de mejora continuo del ciclo de Deming o PDCA: Verificar y Actuar. Si bien es cierto aún no está implementada la norma, esto queda como un documento valorable dentro de la organización, ya que permitirá revisar su evolución y desempeño una vez sea implementada la norma. Dentro de ello, se definen tres estados de cumplimiento según lo indicado en la norma ISO/IEC 27001 en su Anexo “A”, es decir la norma ISO/IEC 27002. Los estados son conceptualizados de la siguiente manera:

- **Cumple satisfactoriamente:** La organización lo ha adoptado y mantiene una gestión sobre ello. Asimismo, se encuentra documentado y es conocido por el personal asociado al SGSI. Adicionalmente, su ejecución va en cumplimiento de la norma ISO27001:2013. Finalmente, su cumplimiento es del 100%.
- **Cumple parcialmente:** Su ejecución va en cumplimiento parcial con los requerimientos de la norma estipulados en la norma ISO27001:2013. Asimismo, a pesar que se aprobó por el personal relacionado a la gestión de la Seguridad de la Información, no se encuentra gestionado, ni documentado.
- **No cumple:** No existe, ni se está ejecutando.

Según lo comentado, las consultas realizadas fueron las siguientes:

Tabla 10: Monitoreo y mejoramiento continuo de la Seguridad de la Información – SGSI

VERIFICAR				
ITEM	PREGUNTA	VALORACIÓN	EVIDENCIA	RECOMENDACIÓN
1	¿La organización cuenta con una metodología, propia o adoptada, para dar seguimiento, medición y análisis continuo al desempeño de la Seguridad de la Información?	No cumple	No existe un Sistema de Gestión de Seguridad de la Información (SGSI) implementado.	La organización debe considerar que se desea medir, cuando y quien realizará la medición, y cuando se analizaran los resultados obtenidos.
2	¿La organización ha ejecutado auditorías internas al Sistema de Gestión de Seguridad de la Información?	No cumple	No existe un Sistema de Gestión de Seguridad de la Información (SGSI) implementado.	La organización debe programar auditorías en un intervalo de tiempo establecido con el fin de evaluar y verificar la eficacia del SGSI.
3	¿La organización cuenta con programas de auditorías aplicables al SGSI donde se verifique su desempeño y cumplimiento?	No cumple	No existe un Sistema de Gestión de Seguridad de la Información (SGSI) implementado.	La organización debe planificar, establecer, implementar y mantener algún programa de auditoría donde se incluye verificación de su desempeño y cumplimiento.
4	¿La Alta Dirección programa y ejecuta revisiones periódicas al Sistema de Gestión de Seguridad de la Información?	No cumple	No existe un Sistema de Gestión de Seguridad de la Información (SGSI) implementado.	La Alta Dirección debe programar revisiones establecidas del SGSI y evaluar su desempeño.
5	¿En las revisiones realizadas al sistema por la Alta Dirección hay procesos de feedback sobre el desempeño de la seguridad de la información?	No cumple	No existe un Sistema de Gestión de Seguridad de la Información (SGSI) implementado.	La organización, específicamente la Alta Dirección, debe contar con procesos de feedback donde se especifique el rendimiento del SGSI.

6	¿Hay documentación formal de las revisiones realizadas por la Alta Dirección al Sistema de Gestión de Seguridad de la Información?	No cumple	No existe un Sistema de Gestión de Seguridad de la Información (SGSI) implementado.	Se debe documentar las revisiones realizadas por la Alta Dirección con el fin de verificar el estado del sistema de seguridad de la información.
ACTUAR				
ITEM	PREGUNTA	VALORACIÓN	EVIDENCIA	RECOMENDACIÓN
7	¿La organización da respuesta a las no conformidades evidenciadas en los planes de auditoría del SGSI?	No cumple	No existe un Sistema de Gestión de Seguridad de la Información (SGSI) implementado	La organización debe tomar las medidas necesarias para suprimir las causas de las no conformidades, ello con la finalidad de que no vuelvan a ocurrir.
8	¿La organización ha implementado acciones a las no conformidades del SGSI?	No cumple	No existe un Sistema de Gestión de Seguridad de la Información (SGSI) implementado	Toda la información de acciones realizadas al Sistema de Gestión de Seguridad de la Información debe ser documentada.
9	¿La organización verifica la eficacia de las acciones correctivas implementadas por la presencia de una no conformidad de seguridad de la información?	No cumple	No existe un Sistema de Gestión de Seguridad de la Información (SGSI) implementado	Se debe evaluar la eficacia de las acciones correctivas con la finalidad de que no vuelvan a ocurrir. Asimismo, todo este proceso debe estar documentado.
10	¿La organización realiza cambios al Sistema de Gestión de Seguridad de la Información después de las acciones correctivas implementadas?	No cumple	No existe un Sistema de Gestión de Seguridad de la Información (SGSI) implementado	Toda la información de cambios al Sistema de Gestión de Seguridad de la Información debe ser documentada.

11	¿La organización documenta la información referente a las acciones correctivas implementadas en materia de seguridad de la información?	No cumple	No existe un Sistema de Gestión de Seguridad de la Información (SGSI) implementado	Toda la información de cambios al Sistema de Gestión de Seguridad de la Información debe ser documentada.
12	¿La organización ejecuta procesos de mejora continua para el Sistema de Gestión de Seguridad de la Información?	No cumple	No existe un Sistema de Gestión de Seguridad de la Información (SGSI) implementado	La organización debe evaluar una mejora continua del SGSI, identificando nuevos alcances definidos por la propia organización.

Fuente: Versión adaptada y modificada de <http://tic.bogota.gov.co>, Autodiagnóstico del SGSI

3.7.4. Análisis de Seguridad actual en la Organización

El fin del análisis de los tres logros es medir de alguna manera el estado actual de seguridad de la información en la organización. En base a ello, tenemos los siguientes resultados:

- **Definición del Marco de Seguridad y Privacidad en la Organización:** Corresponde a la Fase de Planeamiento, en la cual se le asigna el 30% del avance de un Sistema de Gestión de Seguridad de la Información.

Tabla 11: Definición del Marco de Seguridad y Privacidad en la Organización - SGSI

Definición del Marco de Seguridad y Privacidad en la Organización (30%) - Fase de Planeamiento		
Ítem	Total de Clasificación	Porcentaje
Cumple Satisfactoriamente	0	0.00%
Cumple Parcialmente	7	46.67%
No cumple	8	53.33%
Total	15	100.00%

Fuente: Elaboración propia

- **Implementación del Plan de Seguridad y Privacidad de la Información:** Corresponde a la Fase de Ejecución, en la cual se le asigna el 40% del avance de un Sistema de Gestión de Seguridad de la Información. Aquí se revisa que controles se están ejecutando en la organización, esto en base al Anexo “A” de la norma ISO/IEC 27001:2013.

Tabla 12: Implementación del Plan de Seguridad y Privacidad de la Información – SGSI

Implementación del Plan de Seguridad y Privacidad de la Información (40%) - Fase de Ejecución		
Ítem	Total de Clasificación	Porcentaje
Cumple Satisfactoriamente	0	0.00%
Cumple Parcialmente	2	1.75%
No cumple	103	90.35%
No Aplica	9	7.89%
Total	114	100.00%

Fuente: Elaboración propia

- **Monitoreo y mejoramiento continuo:** Corresponde a la Fase de Verificación y Actuar en el desempeño de un SGSI. Si bien no se encuentra implementada aun en la organización, este formato quedará para medir el grado de desempeño del SGSI una vez implementado.

Tabla 13: Monitoreo y mejoramiento continuo de la Seguridad de la Información – Fase de Verificación del SGSI

Monitoreo y Mejoramiento Continuo (15%) - Fase de Verificación		
Ítem	Total de Clasificación	Porcentaje
Cumple Satisfactoriamente	0	0.00%
Cumple Parcialmente	0	0.00%
No cumple	6	100.00%
Total	6	100.00%

Fuente: Elaboración propia

Tabla 14: Monitoreo y mejoramiento continuo de la Seguridad de la Información – Fase de Verificación del SGSI

Monitoreo y Mejoramiento Continuo (15%) - Fase de Actuar (Mejora)		
Ítem	Total de Clasificación	Porcentaje
Cumple Satisfactoriamente	0	0.00%
Cumple Parcialmente	0	0.00%
No cumple	6	100.00%
Total	6	100.00%

Fuente: Elaboración propia

3.7.5. Resultados del Análisis de Seguridad actual en la Organización

Dentro de Análisis realizado, las evidencias en medidas porcentuales nos describen el estado actual de la organización en cuanto a Seguridad de la Información. Teniendo en cuenta para los dos primeros puntos de análisis son los más representativos para la etapa de diseño del presente proyecto, podemos concluir en lo siguiente:

- **Definición del Marco de Seguridad y Privacidad en la Organización:**

El objetivo de análisis es obtener la información necesaria para evaluar nivel de madurez de las cláusulas que soportan la norma ISO/IEC 27001:2013.

Asimismo, identificar las necesidades de implantación de la norma ISO 27001. En base a ello, los resultados obtenidos arrojan:

- **Cumple Satisfactoriamente:** 0%
- **Cumple Parcialmente:** 46.67%
- **No Cumple:** 53.33%

Estas cifras arrojan que antes de la adopción de la norma en la organización, un 46.67% del total de 14 cláusulas, son manejadas por la organización de manera parcial, ya que se ejecutan algunos procedimientos y lineamientos indicados en la norma, pero no está documentado, ni tampoco se tiene un control o seguimiento de las mismas.

- **Implementación del Plan de Seguridad y Privacidad de la Información:**

El objetivo de esta segunda parte de la evaluación es conocer el estado actual de la organización a nivel de medidas de seguridad, no sólo técnicas, sino también organizativas, legales y procedimentales. Es decir, evaluar el cumplimiento de los controles descritos en el Anexo “A” de la norma, dividido en 114 Controles de seguridad, repartidos en 35 Objetivos de Control.

- **Cumple Satisfactoriamente:** 0%
- **Cumple Parcialmente:** 1.75%
- **No Cumple:** 90.35%
- **No Aplica:** 7.89%

Estas cifras arrojan que antes de la adopción de la norma, un 90.35% del total de 114 controles de seguridad, no son tomadas en cuenta o no son ejecutadas en la organización. Esta es una cifra muy alarmante, ya que el Anexo “A” de la norma, establece un catálogo de buenas prácticas, el cual determina, desde la experiencia, una serie de objetivos de control y controles que se integran dentro de todos los requisitos de la norma en relación con el tratamiento de los riesgos.

Por último, una vez ya definido la situación actual de la organización en materia de seguridad de la información, es necesario realizar el análisis de riesgos de los activos de información asociados al proceso de Servicio Post-Venta. Esto será llevado a cabo en base a la metodología de gestión necesaria, la cual se sustenta en el diseño de un Sistema de Gestión de Seguridad de la Información, desarrollado en el siguiente capítulo “Diseño del Sistema Propuesto”.

3.8. Registro de Interesados

El registro de Interesados en el presente proyecto es:

Tabla 15: Tabla de Registro de Interesado del SGSI

Interesado	Organización a que pertenece	Cargo	Categoría de interesado	Nivel interés (Bajo, Medio, Alto)	Nivel influencia (Bajo, Medio, Alto)
Antonio Raúl Paredes Lujan	Integrador de Telecomunicaciones	Alta Dirección	Patrocinador	Alto	Alto
Augusto Jose Jara Lopez	Integrador de Telecomunicaciones	Gerente Técnico	Cliente Final	Alto	Medio
Martha Elena Ascencio Tang	Integrador de Telecomunicaciones	Alta Dirección	Cliente Final	Alto	Alto
Martin Renzo Torres León	Empresa Consultora	Consultor	Proveedor	Alto	Alto
Martin Renzo Torres León	Empresa Consultora	Consultor	Director Proyecto	Alto	Alto
Luis Ariel Manco Ruiz	Empresa Consultora	Consultor	Miembro proyecto	Medio	Medio

Fuente: Elaboración Propia

3.9. Toma de Requerimientos

Los requerimientos que aplican al presente proyecto se describen a continuación:

- **Compromiso de la Dirección:** Tal como se indica en la Cláusula N°5 de la norma ISO/IEC 27001:2013 “Liderazgo y compromiso”, involucrar a la Alta Dirección es sin duda el factor más importante para la implementación de un SGSI. Si bien es cierto el fin del proyecto no es realizar la implantación del SGSI, si lo es su diseño. Por ello para un diseño exitoso debe haber un compromiso de la Alta Dirección en el establecimiento de todas las fases que supone el Sistema de Gestión de Seguridad de la información (SGSI). Dentro de ello, la dirección tendrá como funciones:
 - Autorizar el diseño del SGSI por parte de la Alta Dirección.

- Formular y aprobar la política del SGSI. Difundirla a la totalidad de los miembros de la organización, así como, en su caso, a proveedores y clientes.
- Asignar los roles y responsabilidades en materia de Seguridad de la Información.
- Proporcionar los recursos necesarios para el programa del SGSI. Esto permitirá asegurar que se implantan programas de concienciación, formación y capacitación en materia de seguridad de información en la organización.
- Decidir los criterios de aceptación del riesgo y los niveles aceptables de riesgo.
- **Documentación del SGSI:** En estos requerimientos se enumeran los principales documentos y registros que deben generarse y mantenerse en el establecimiento del SGSI. En base a ello, se debe exigir como la siguiente documentación:
 - Alcance del Sistema de Gestión de Seguridad de la Información (SGSI)
 - Declaraciones de Política de Seguridad de la Información (SGSI) y los objetivos que persigue.
 - Estructura Organizacional del Sistema de Gestión de Seguridad de la Información.
 - Identificación de Activos de Información del proceso de Servicio Post-Venta
 - Valoración de Activos de Información
 - Análisis e Identificación de Vulnerabilidades y Amenazas
 - Análisis y Evaluación de riesgos
 - Matriz de Riesgos
 - Plan de Tratamiento de Riesgos
 - Declaración de aplicabilidad (SOA)
- **Definición de Fechas y Responsables:** Dentro de la ejecución del proyecto, específicamente en su fase de inicio es necesario las fechas y responsables de cada actividad embebida en el mismo. Cada responsable, los cuales están descritos en la tabla de registro de interesados, tendrá de manera específica asignadas tareas, roles y funciones dentro de cada actividad a ejecutar. Asimismo, dentro de ello los plazos a ejecutarse.

A continuación, se muestra un resumen del registro de interesado:

Tabla 16: Tabla de la toma de requerimientos del Proyecto

Requerimiento	Descripción / Resumen	Interesado	Prioridad
Compromiso de la Dirección	Solicitar el apoyo de la Alta Dirección para que asuma el rol principal en la gestión del cambio de cultura en la organización, referida a la concienciación de la Seguridad de la Información.	Martha Elena Ascencio Tang (Alta Dirección) / Antonio Raúl Paredes Lujan (Alta Dirección)	Alta
Documentación del SGSI	Desarrollar el diseño del Sistema de Gestión de Seguridad de la Información (SGSI)	Antonio Raúl Paredes Lujan (Alta Dirección) / Martin Renzo Torres León (Consultor)	Alta
Definición de Fechas y Responsables	Generar la planeación del Diseño del Sistema de Gestión de Seguridad de la Información (SGSI)	Antonio Raúl Paredes Lujan (Alta Dirección) / Martin Renzo Torres León (Consultor)	Alta

Fuente: Elaboración Propia

3.10. Estructura de Desglose de Trabajo

Se elaboró la Estructura de Desglose de Trabajo (EDT), tal lo mostrado a continuación:

3.10.1. Información del Proyecto

Tabla 17: Datos/Información del Proyecto

Empresa / Organización	
Proyecto	Diseño de un Sistema de Gestión de Seguridad de la Información, basado en la norma ISO/IEC 27001:2013, para el proceso de Servicio Post-Venta
Fecha de preparación	26/10/2017
Cliente	Integrador de Servicios de Telecomunicaciones
Patrocinador principal	Antonio Raúl Paredes Lujan

Director de proyecto	Martin Renzo Torres León
Descripción	Debido a la problemática actual de la organización: Continuos ataques a Servidor de Atención y Gestión de Ticket, pérdidas de información confidencial y sensible, tanto propia como de sus clientes y total desinformación y desinterés en materia de Seguridad de la Información por gran parte de los colaboradores de la Organización, la misma ha creído conveniente la adopción de un Sistema de Gestión de Seguridad de la Información (SGSI) la cual ejerza un ciclo de mejora continua en el correcto resguardo y uso de los activos de información involucrados específicamente al proceso de Servicio Post-Venta. El diseño propuesto se apoya en la norma ISO/IEC 27001:2013

Fuente: Elaboración Propia

3.10.2. Aprobaciones

Tabla 18: Listado de Aprobaciones del Proyecto

Aprobador	Fecha	Firma
Antonio Raúl Paredes Lujan (Patrocinador)	26/10/2017	
Augusto Jose Jara Lopez (Gerencia Técnica)		

3.10.3. Vista Jerárquica

1. Diseño de un SGSI para un Integrador de Telecomunicaciones
 - 1.1. Fase de Inicio
 - 1.1.1. Compromiso con la Alta Dirección
 - 1.1.2. Documentación del SGSI
 - 1.1.3. Definición de Fechas y Registros de Interesados
 - 1.1.4. Construcción de la Estructura de Desglose de Trabajo (EDT)
 - 1.2. Fase de Planeamiento
 - 1.2.1. Análisis de Brechas (Análisis GAP)
 - 1.2.2. Definición del Alcance
 - 1.2.3. Definición de la Política de Seguridad
 - 1.2.4. Definición de la Estructura Organizacional del SGSI
 - 1.2.5. Identificación de Activos de Información

- 1.2.6. Inventario de Activos de Información
- 1.2.7. Valoración de Activos
- 1.2.8. Análisis e Identificación de Vulnerabilidades
- 1.2.9. Análisis y Evaluación de Riesgos
- 1.2.10. Diseño de Matriz de Riesgos
- 1.2.11. Declaración de Aplicabilidad (SOA)
- 1.3. Fase de Ejecución
 - 1.3.1. Elaboración del Plan de Tratamiento de Riesgos
- 1.4. Fase de Especificaciones y Desarrollo
 - 1.4.1. Manual del Sistema de Gestión de Seguridad de la Información
- 1.5. Fase de Cierre
 - 1.5.1. Entrega de documentación de análisis realizado en la etapa de Planeamiento
 - 1.5.2. Acta de cierre del proyecto

3.10.4. Mapas de Procesos - EDT

Figura 22: Mapa de Procesos – EDT

Fuente: Elaboración propia

Nota: Tener en cuenta que debido a que el alcance del presente proyecto de tesis es Diseño del SGSI, la fase de ejecución contemplará la elaboración y entrega del Manual del Sistema de Gestión de Seguridad de la Información

CAPÍTULO 4: PLANTEAMIENTO DE PROPUESTA DE SOLUCIÓN

4.1. Introducción

Dentro de las actividades de negocio referidas a una organización es innegable mencionar que los objetivos que persigue deben llevar detrás un sustento que soporte su desempeño, el cual acompañe hacia el logro de sus metas. Por ello, la Gestión de la Seguridad de la Información se integra a los procesos de negocio implementados de la organización, entendiendo la información como un activo importante y trascendental que debe ser custodiado de manera correcta, preservando siempre su confidencialidad, integridad y disponibilidad. Lo comentado no solo es resultado de la adopción de sistemas informáticos que mitiguen o disminuyan las vulnerabilidades, fallas y/o brechas de seguridad que puedan contener sus sistemas informáticos, sino manejar y actuar en un sistema integrado de gestión que cree directrices, políticas y procedimientos que alineen a sus colaboradores a trabajar en conjunto hacia la consecución de objetivos previamente identificados por la organización, todo aquello especificado en materia de seguridad de la información.

4.2. Elaboración de especificaciones

Las especificaciones a desarrollar son en cumplimiento de los requerimientos estipulados en el capítulo anterior. Según ello, se elaboró la siguiente tabla resumen:

Tabla 19: Requerimientos del Proyecto

Requerimientos del Proyecto	
Compromiso de la Dirección	Autorizar el diseño del SGSI
	Formular y aprobar la política del SGSI
	Asignar los roles y responsabilidades en materia de Seguridad de la Información
	Proporcionar los recursos necesarios para el programa de SGSI
	Formación y concientización en materia de Seguridad de la Información
	Decidir los criterios de aceptación del riesgo y los niveles aceptables de riesgo

Documentación del SGSI	Alcance del Sistema de Gestión de Seguridad de la Información
	Declaración de Política del Sistema de Gestión de Seguridad de la Información
	Estructura Organizacional del Sistema de Gestión de Seguridad de la Información
	Identificación de Activos de Información del proceso de servicio Post-Venta
	Valoración de Activos de Información
	Análisis e Identificación de Vulnerabilidades y Amenazas
	Análisis y Evaluación de riesgos
	Matriz de Riesgos
	Plan de Tratamiento de Riesgos
	Declaración de aplicabilidad (SOA)
	Manual del Sistema de Gestión de Seguridad de la Información (SGSI)
Definición de Fechas y Responsables	Definición de roles y funciones dentro de cada actividad a ejecutar dentro de la etapa de Inicio del Proyecto. Asimismo, dentro de ello los plazos a ejecutarse, estipulados en el cronograma de trabajo

Fuente: Elaboración propia

En base a ello, a continuación, se describirá los tres requerimientos indicados y el conjunto de acciones que las integran.

4.3. Compromiso de la Dirección

La figura de la Alta Dirección debe estar contemplado siempre desde el punto de vista del alcance del SGSI. Por ello, dentro del presente proyecto la alta dirección tiene asignada las siguientes responsabilidades:

- **Autorizar el diseño del SGSI:** Debe haber de por medio un documento expreso en donde se presente el plan de trabajo que contemple el diseño del SGSI, para el cual la Alta Dirección analizará cada punto de despliegue, tomando en cuenta todos los alcances necesarios. En base a ello, es fundamental que la Alta Dirección apruebe el plan de trabajo o Proyecto de Diseño de SGSI, autorizando su puesta en marcha, asumiendo sus responsabilidades dentro del alcance y asignando los recursos que sean necesarios en el mismo. Básicamente, este plan de trabajo está asociado al cronograma de actividades del proyecto y los alcances que contiene cada actividad dentro del mismo.
- **Formular y aprobar la política del SGSI:** Este punto lo veremos a detalle dentro del apartado de “Documentación del SGSI”, pero podemos comentar brevemente que este

documento de contenido genérico establece el compromiso de la Alta Dirección y el enfoque de la organización en la gestión de la Seguridad de la Información.

- **Asignar los roles y responsabilidades en materia de Seguridad de la Información:** Estos roles y responsabilidades serán asignados dentro de la Estructura Organizacional del Sistema de Gestión de Seguridad de la Información (SGSI).
- **Proporcionar los recursos necesarios para el programa de SGSI:** Para que todas las actividades asociadas al SGSI se desarrollen es fundamental y necesario que la Alta Dirección asigne los recursos necesarios. Por ello, es responsabilidad de la Alta dirección garantizar que cuentan con los suficientes recursos para:
 - Establecer, implementar, operar, monitorizar, revisar y mantener el Sistema de Gestión de Seguridad de la Información. Esto asociado al Ciclo de mejora continua PDCA o ciclo de Deming. Aquí es necesario acotar que el presente trabajo solo tiene como alcance el diseño de un SGSI, por la cual existen tareas asociadas a algunas fases que no se encuentran dentro del mismo.
 - Garantizar que todos los procedimientos de seguridad de la información que integren el SGSI apoyen a los requerimientos de negocio y que vayan acorde a los objetivos generales y específicos definidos en el presente proyecto.
 - Identificar todos los requerimientos necesarios para cumplir con la legislación vigente. En el caso actual ir acorde de la Ley N° 29733 “Ley de Protección de Datos Personales”, en beneficio de la confidencialidad de los datos de clientes manejados por la propia organización.
 - Tener conocimiento y estar involucrados en la declaración de aplicabilidad (SOA) donde se definan los controles de Seguridad necesarias para la protección de los activos de información seleccionados.
 - Cumplir un rol auditor dentro de la organización y realizar todas las revisiones del SGSI cuando sea necesario, por lo menos una revisión del SGSI una vez al año. Si bien es cierto que este punto no aplica al presente proyecto por alcance del mismo, es necesario tenerlo en cuenta cuando la organización crea conveniente su implementación.
 - Mejorar la eficacia del Sistema de Gestión de Seguridad de la Información (SGSI) mediante un ciclo de retroalimentación, específicamente PDCA.

- **Formación y concientización en materia de Seguridad de la Información:** La formación y la concienciación en Seguridad de la Información son elementos fundamentales en la consecución del éxito de un Sistema de Gestión de Seguridad de la Información. Por ello, la Alta Dirección debe asegurar que se cumpla con las funciones de la Estructura Organizacional del Sistema de Gestión de Seguridad de la Información (SGSI) y que en general todo el personal de la organización tenga conocimientos de las directrices de seguridad establecidas en la misma. En base a ello, la Alta Dirección tendrá como responsabilidad:
 - Determinar las competencias necesarias que debe tener cada persona de la organización en función de las tareas que vaya a desempeñar.
 - Satisfacer las necesidades de Seguridad de la Información en la organización mediante planes de formación y concientización.
 - Evaluar la eficacia de las acciones tomadas en materia de Seguridad de la Información.
 - Mantener todos los registros de estudios, formación, habilidades, experiencia y cualificación del personal en materia de Seguridad de la Información, que sirva como base a definir posibles roles y funciones dentro de la Estructura Organizacional del Sistema de Gestión de Seguridad de la Información (SGSI)
 - Asegurar que todo el personal relevante se encuentre concienciado con la importancia de sus actividades en materia de Seguridad de la Información y de cómo contribuye a la consecución de los objetivos del Sistema de Gestión de Seguridad de la Información.
- **Decidir los criterios de aceptación del riesgo y los niveles aceptables de riesgo:** Los Criterios de Aceptación de Riesgos (CAR) y los Niveles de Aceptación del Riesgo (NAR) se encuentran definidos en la metodología de Gestión de Riesgos utilizada en el presente proyecto, el cual la Alta Dirección debe contribuir activamente en la participación del desarrollo y despliegue de la misma. Este punto será desarrollado a cabalidad en el apartado “Documentación del SGSI”, revisado más adelante.

4.4. Documentación del SGSI

En este requerimiento se realiza todo el despliegue de los pasos indicados en la norma ISO/IEC 27001 en su versión 2013 y en si es el propio Diseño del Sistema de Gestión de

Seguridad de la Información (SGSI). Los acápites que lo conforman son detalles a continuación en los siguientes apartados.

4.4.1. Alcance del Sistema de Gestión de Seguridad de la Información

El diseño del Sistema de Gestión de Seguridad de la Información (SGSI) en nuestro actual proyecto aborda las directrices estipuladas en la norma ISO/IEC 27001:2013. Con lo comentado, según el modelo de mejora continua que tiene como referencia la norma, tal es la del PDCA (Plan, Do, Check y Act), debemos iniciar el desarrollo del mismo en la fase o etapa de Planeamiento, especificado en las fases incluidas en el EDT (Estructura de Desglose de Trabajo). Por ello, es importante definir previamente cual es el alcance y los límites que tendrá el diseño del SGSI planificado para su implementación posterior al proceso de Servicio de Post-Venta de la organización.

Por lo expuesto, en la etapa de planificación el alcance del Sistema de Gestión de Seguridad de la Información es incluido al proceso en estudio, los cuales son comentados a continuación:

- Comprensión de la cultura organizacional de la organización, específicamente el proceso de servicio Post-Venta.
- Identificación de los recursos tecnológicos disponibles asociados al proceso de servicio Post-Venta y los distintos procesos que interactúan con la misma. Asimismo, la identificación de activos de información que formaran parte del presente proyecto de investigación.
- Definir la metodología de valoración de riesgos de activos de información a utilizar, en nuestro caso adoptado de buenas prácticas en seguridad de la información.
- Analizar y evaluar el impacto que los riesgos identificados sobre cada activo de información puedan materializarse. Esto incluye un cálculo de ocurrencia del riesgo y si la concretización del mismo es aceptable o no por la organización.
- Determinar las opciones a adoptar para minimizar la materialización de los riesgos ya identificados. De materializarse, que acciones son necesarias para realizar un adecuado tratamiento de riesgos sobre los activos de información involucrados.
- Definir de tratamiento del riesgo de los activos de información seleccionados.

- En base a los objetivos de negocio que la organización persigue se debe determinar que controles la organización debe adoptar. La selección de los controles de seguridad adoptados serán tomados del Anexo “A” de la norma o la norma ISO/IEC 27002 y controles Técnicos Auxiliares propuestos. Su ejecución permitirá minimizar la exposición de los riesgos al activo de información en estudio.

4.4.2. Estructura Organizacional del Sistema de Gestión de Seguridad de la Información

Tal como lo indica la norma ISO/IEC 27001:2013 en su requisito N° 5 denominado “Liderazgo” y en su apartado número 5.3 denominado “Roles, responsabilidades y autoridades organizacionales”, la alta dirección debe asegurar las responsabilidades y la autoridad necesaria relacionadas a Seguridad de la Información en la asignación de roles y responsabilidades en el desempeño del Sistema de Gestión de Seguridad de la Información. Para mayor información revisar “Anexo X” “Roles, Responsabilidades y autoridades organizacionales especificados en la norma ISO/IEC 27001:2013”.

Asimismo, complementando la norma su similar en la versión peruana, es decir la NTP ISO/IEC 27001:2014, resuelve mediante Resolución Ministerial N° 004-2016-PCM en su Artículo 5, denominado: “Del Comité de Gestión de Seguridad de la Información”, que cada organización designará un Comité de Gestión de Seguridad de la Información, el cual se encuentre conformado por personal encargado de llevar la Gestión de Negocio o la Gestión Organizacional, en donde la propia organización deberá establecer las funciones que desempeñará el Comité de Gestión de Seguridad de la Información. Para mayor detalle revisar “Anexo XI” “Resolución Ministerial N° 004-2016-PCM”.

Adicionalmente, es preciso comentar que múltiples organizaciones contemplan roles y responsabilidades adicionales a las del Comité de Gestión de Seguridad de la Información (CGSI), ello con la finalidad de lograr disgregar funciones y ser más efectivos en materia de seguridad de la información. Teniendo ese preámbulo, y tomando en cuenta artículos específicos de la ONGEI (Oficina Nacional de Gobierno Electrónico e Informática), PCM (Presidencia de Consejo de Ministros), cursos sobre Seguridad de la Información y nuevas incorporaciones de la propia norma ISO/IEC 27001:2013, se logró determinar una estructura organizacional modelada en el siguiente trabajo. Para un mayor detalle revisar “Anexo XII” “Taller de Implementación de la norma ISO/IEC 27001”, “Anexo XIII” “Estructura

Organizacional SGSI-Curso UPC” y “Anexo XIV” “Inclusiones en la norma ISO/IEC 27001 respecto a su norma antecesora”.

Ante todo lo comentado, es necesario revisar en primer lugar el organigrama de la organización y como se distribuyen sus áreas.

Figura 23: Organigrama de la Organización

Fuente: Elaboración propia

La composición de áreas dentro del organigrama y sus propios integrantes, serán los que compongan la Estructura Organizacional del Sistema de Gestión de Seguridad. Asimismo, cabe mencionar que la norma no indica un perfil del personal que integrará los cargos dentro de la Estructura Organizacional del SGSI de la Información, más si indica que la Alta Dirección (cabeza de la organización) tomará la función de elegir al personal que la componen. Para un mayor entendimiento se puede revisar las Resoluciones Ministeriales N° 004-2016-PCM y N°166-2017-PCM.

Por lo comentando, los roles y responsabilidades de los componentes de la Estructura Organizacional del Sistema de Gestión de Seguridad de la Información (EOSGSI) se describe a continuación:

4.4.2.1. Comité de Gestión de Seguridad de la Información (CGSI)

Dentro de la empresa u organismo es el ente máximo que tendrá las principales funciones:

- Procederá a revisar y proponer la máxima autoridad para la ejecución de la Política de Gestión de Seguridad de la Información y la delegación de funciones en materia de Seguridad de la Información, alineados a los objetivos de negocio.
- Ser gestor responsable de todo lo relacionado a la implementación del SGSI, verificación de su continuidad y evaluación de su desempeño.
- Ser ente líder en la difusión de la importancia del SGSI dentro de la organización.
- Asignar roles y responsabilidades en materia de seguridad de información a cada área, esto según los procesos organizacionales en estudio.
- Promover la difusión y apoyo de la seguridad de la información dentro de la organización, creando un ambiente seguro y compacto que genere bienestar e identificación con las políticas y procedimientos establecidos.

Para el caso específico de la organización, los integrantes del Comité de Gestión de Seguridad de la Información (CGSI) serán: El Gerente General, Gerente Técnico, Gerente Comercial, Gerente Administrativo y Financiero, y Gerente de Recursos Humanos.

4.4.2.2. Grupo Interdisciplinario de Seguridad de la Información (GISI)

Dentro de la empresa u organismo aseguran que las actividades de Seguridad de la Información sean ejecutadas en conformidad con la Política de Gestión de Seguridad de la Información, aprobando metodologías y procesos que permitan al personal de la organización a expresar sus dudas e inquietudes en materia de Seguridad de la información, generando confianza y concientización en los estatutos y procedimientos indicados en la Política de SGSI.

Para el caso específico de la organización, los integrantes del Grupo Interdisciplinario de Seguridad de la Información (GISI) serán los Jefes que integran la Gerencia Técnica: Jefes de Proyectos, Jefe de Servicios Post-Venta y Desarrollo.

4.4.2.3. Oficial de Seguridad de la Información (OSI)

Dentro de la empresa u organismo, el Oficial de la Información propone metodologías, procedimientos, estatutos, herramientas, planes, programas y procesos para la seguridad de la información, y en sí para el cumplimiento de controles que rigen para el cumplimiento de la misma. En adición a lo comentado, administrar los incidentes y vulnerabilidades de los

distintos activos de información para identificar los controles a implementar, elaborando y actualizando el plan de Seguridad de la Información.

Adicionalmente, tiene como responsabilidad el monitoreo constante de incidentes relativos a la seguridad de la información, estableciendo parámetros de mejora en base a análisis previamente realizados.

Para el caso específico de la organización, para la elección del Oficial de la Seguridad de la Información, se tomaron rigurosas pruebas en referencia al conocimiento, experiencia en diseño e implementación de la norma ISO /IEC 27001:2013. El oficial de Seguridad de la Información será el Jefe de servicios Post-Venta de la organización.

4.4.2.4. Dueño del Riesgo

La norma ISO/IEC 27001 en su versión 2013 establece la figura de Dueño del Riesgo la persona(s) responsable (s) de gestionar los riesgos asociados a los activos de información valorizados. Es decir, gestionar de manera correcta las actividades y recursos necesarios para evitar la materialización de amenazas sobre las vulnerabilidades existentes en los activos de información. El rol no implica necesariamente que sea la persona que finalmente ejecuta los controles, sino alguien que se responsabiliza de que realmente los controles aplicables sobre los activos de información se están llevando a cabo acorde a lo establecido.

Adicionalmente, el dueño del riesgo deberá monitorear cambios significativos en los riesgos que afectan los activos de información previamente identificados, esto frente a las amenazas más relevantes que afecten o puedan afectar los activos de información seleccionados.

El Dueño del Riesgo será designado según sea el activo de información y el control de seguridad asociado al mismo.

4.4.2.5. Propietarios de Activos de la Información

Son los responsables de clasificar los activos de información con el grado de confidencialidad y criticidad necesario. Añadido a lo comentado, deberán documentar y mantener actualizadas la clasificación de activos de información realizada y definir que usuarios tiene o no acceso a los distintos activos de información que tiene bajo su custodia. Para el caso específico de la organización, para la elección de los Propietarios de Activos de la Información serán tomados en cuenta los Gerentes que representen cada área que disponga los múltiples activos de información que hayan sido seleccionados. Por nombrar un ejemplo, los contratos de

Mantenimiento de Servicios Post-Venta de los distintos clientes con los que cuenta la organización será propiedad del Gerente Técnico de la organización y así sucesivamente.

4.4.2.6. Custodio de los Activos de Información

Administran y resguardan los activos de información, al monitorear el cumplimiento de controles de seguridad en los activos que se encuentren bajo su administración. En pocas palabras es el nexo entre el Propietario de la Información y el usuario de los activos de información.

Para el caso específico de la organización, los custodios de los activos de información serán los Jefes del Área Técnica: Jefe de Proyectos, Jefe de Post-Venta y Jefe de Desarrollo.

4.4.2.7. Usuario de activos de Información

Son los usuarios finales que hacen uso del activo de información para la ejecución de sus deberes. Para el caso específico de la organización, los usuarios de los activos de Información son todas las personas que tengan a su cargo cualquier activo (bien, proceso, servicio, entre otro) que sea asignado bajo un documento formal y explícito, en mutuo acuerdo entre ambas partes.

Figura 24: Interacción entre componentes de la Estructura Organizacional de Seguridad de la Información

Fuente: Elaboración propia

4.4.3. Metodología de Evaluación de Riesgos

Para el Integrador de Telecomunicaciones, la organización que aplica al presente proyecto, se utiliza una metodología propia para valorar los riesgos de la Seguridad de la Información. Esta metodología tiene en consideración los siguientes aspectos.

4.4.3.1. Identificación de Activos de Información

La identificación se realiza en base al flujo del proceso involucrado en el alcance del presente proyecto, ello con la finalidad de valorarlos e identificar los riesgos de seguridad asociados al mismo. Tener en cuenta que el proceso involucrado es el Servicio Post-Venta. Asimismo, dentro del ejercicio de la valoración de activos utilizamos la siguiente clasificación:

Tabla 20: Inventario de Activos de Información

Tipo de Activo	Descripción / Detalle
Datos / Información	Almacenada en equipos o soportes de información, los cuales normalmente se encuentran agrupados como directorios o BD, o en su defecto transferidos de un lugar a otro por medios extraíbles o de un lugar a otro. Ejemplos: Ficheros de datos, respaldo de datos, credenciales, datos de control de acceso, datos de configuración, entre otros asociados.
Dispositivo Físico / Hardware	Medios físicos que soportan directa o indirectamente los servicios que presta la organización: Medios de Almacenamiento temporal o permanente de datos, Soporte en la ejecución de las aplicaciones informáticas o responsables del procesado o transmisión de datos. Ejemplos: Servidores, laptop, desktop, dispositivos móviles, equipos de Networking, impresoras, entre otros asociados.
Software / Aplicaciones Informáticas	Medios que gestionan, analizan y transforman los datos, permitiendo la explotación de la información para la prestación de los servicios. Ejemplos: Aplicaciones propietarias o no propietarias, desarrollos, programas, correo electrónico, servidor de aplicaciones, sistemas operativos, entre otros asociados.
Servicios	Funciones conjuntas que permiten atender una necesidad específica o conjunta a un grupo de usuarios. Contempla las redes de comunicaciones, los cuales son instalaciones dedicadas como servicios de comunicaciones contratados a terceros o como medios de transporte de información o datos de un sitio a otro. Ejemplos: Páginas web, correo electrónico, internet, líneas dedicadas, LAN, WAN, Infraestructura de clave pública, entre otros asociados.

Personas Recurso Humano	/	Ejemplos: Conjunto de: usuarios internos o externos, proveedores, administradores de sistemas, entre otros asociados.
Imagen Reputación	/	Representa la presencia de la organización ante el público, clientes, personas, otras organizaciones, mostrando la identidad y competencia con la cual se diferencia de otras. Ejemplos: Imagen de una organización, reputación, diferenciación entre organización, entre otros asociados.

Adicionalmente, el formato utilizado para el inventario de activos contiene los ítems mostrados en la siguiente gráfica:

Figura 25: Ítem de Identificación de Activos de Información

IDENTIFICACIÓN DEL ACTIVO							
No	Nombre del Activo	Descripción	Tipo de Activo	Clasificación	Propietario	Usuarios del Activo	Ubicación

Fuente: Elaboración propia

A continuación, se describe los ítems involucrados:

- **No:** Número de Activo de Información seleccionado del proceso de Servicio Post Venta de la organización.
- **Nombre del Activo:** Nombre del Activo de Información seleccionado del proceso de Servicio Post Venta de la organización.
- **Descripción:** Descripción y detalles específicos del Activo de Información seleccionado del proceso de Servicio Post Venta de la organización.
- **Tipo de Activo:** Clasificación del activo de información. Ejemplo: Software, Datos/Información, Servicios, otros.
- **Propietario:** Rol asignado a un personal de la organización con la responsabilidad de velar sobre la seguridad del activo de información.
- **Usuarios del Activo:** Usuarios y/o usuarios dentro o fuera de la organización que hacen uso del activo de la información.
- **Ubicación:** Ubicación dentro de la organización del Activo de la Información.

4.4.3.2. Valoración de Activos de Información

Posteriormente a la identificación de los activos de información, el siguiente paso es la valorización de los mismos. Con ello, determinaremos cual es valor que cada activo tiene para la organización para después reconocer cuál sería el impacto que tendría dentro de la misma si llegara a concretizarse una amenaza. Por ello, para realizar dicha valorización, se determinó una escala cualitativa, aquello debido a que no es posible cuantificar en valores monetarios todos los activos envueltos dentro del proceso en estudio. Para ello, se ha evaluado realizar la valoración en base a los principios fundamentales de la Seguridad de la Información, tales son: Confiabilidad, Integridad y Disponibilidad. Según ello, se definen valores que corresponden a criterios establecidos por nuestra metodología, los cuales varían desde: Muy Bajo, Bajo, Medio, Alto y Muy Alto. Para cada criterio se establece un valor numérico que cruza con cada elemento de confidencialidad, integridad y disponibilidad. El detalle de lo comentado y la descripción de cada criterio en base a su confidencialidad, integridad y disponibilidad se muestran a continuación:

Tabla 21: Valoración de Activos en base a los Pilares de la Seguridad de la Información

VALORACIÓN DE LA SEGURIDAD				
CRITERIOS		CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
MUY BAJO	1	El conocimiento o divulgación no autorizada de la información que gestiona el activo o el propio activo de la información no tiene ningún impacto en los procesos o en la propia organización.	La pérdida de exactitud y completitud del activo de información o la propia información que gestiona el activo no genera ningún impacto en los procesos o en la propia organización.	La falta o no disponibilidad del activo o la propia información que gestiona el activo no genera ningún impacto en los procesos o en la propia organización.
BAJO	2	El conocimiento o divulgación no autorizada de la información que gestiona el activo o el propio activo de la información tiene un impacto bajo en los procesos o en la propia organización.	La pérdida de exactitud y completitud del activo de información o la propia información que gestiona el activo genera un impacto bajo en los procesos o en la propia organización.	La falta o no disponibilidad del activo o la propia información que gestiona el activo genera un impacto bajo en los procesos o en la propia organización.
MEDIO	3	El conocimiento o divulgación no autorizada de la información que gestiona el activo o el propio activo de la información tiene un impacto moderado en los procesos o en la propia organización.	La pérdida de exactitud y completitud del activo de información o la propia información que gestiona el activo genera un impacto moderado en los procesos o en la propia organización.	La falta o no disponibilidad del activo o la propia información que gestiona el activo genera un impacto moderado en los procesos o en la propia organización.
ALTO	4	El conocimiento o divulgación no autorizada de la información que gestiona el activo o el propio activo de la información tiene un impacto alto en los procesos o en la propia organización.	La pérdida de exactitud y completitud del activo de información o la propia información que gestiona el activo genera un impacto alto en los procesos o en la propia organización.	La falta o no disponibilidad del activo o la propia información que gestiona el activo genera un impacto alto en los procesos o en la propia organización.

VALORACIÓN DE LA SEGURIDAD				
CRITERIOS		CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
MUY ALTO	5	El conocimiento o divulgación no autorizada de la información que gestiona el activo o el propio activo de la información tiene un impacto alto y negativo en los procesos o en la propia organización.	La pérdida de exactitud y completitud del activo de información o la propia información que gestiona el activo genera un impacto alto y negativo en los procesos o en la propia organización.	La falta o no disponibilidad del activo o la propia información que gestiona el activo genera un impacto alto y negativo en los procesos o en la propia organización.

Los criterios de valoración de los distintos activos de la información están clasificados en cinco niveles, tales son: Muy bajo, Bajo, Medio, Alto y Muy Alto. Según el valor numérico que represente la suma de los valores de Confidencialidad, Integridad y Disponibilidad del Activo de la Información se definirá la severidad dentro del rango sobre el activo. Acto seguido, esta suma dará el criterio de criticidad que determinará que activos son o no determinantes para su elección dentro de su valoración. Lo comentado se muestra a continuación:

Tabla 22: Definición de Severidad dentro del Rango

Clasificación	Valor de Impacto Sobre el Activo	Rango de Severidad	Definición de Severidad dentro del Rango
Muy Bajo	1	1	Impacto muy bajo sobre el activo con severidad baja.
		2	Impacto muy bajo sobre el activo con severidad media
		3	Impacto muy bajo sobre el activo con severidad alta.
Bajo	2	4	Impacto bajo sobre el activo con severidad baja.
		5	Impacto bajo sobre el activo con severidad media
		6	Impacto bajo sobre el activo con severidad alta.
Medio	3	7	Impacto medio sobre el activo con severidad baja.
		8	Impacto medio sobre el activo con severidad media
		9	Impacto medio sobre el activo con severidad alta.
Alto	4	10	Impacto alto sobre el activo con severidad baja.
		11	Impacto alto sobre el activo con severidad media
		12	Impacto alto sobre el activo con severidad alta.
Muy Alto	5	13	Impacto muy alto el sobre activo con severidad baja.
		14	Impacto muy alto el sobre activo con severidad media
		15	Impacto muy alto el sobre activo con severidad alta.

Tabla 23: Valor de Criticidad o Impacto sobre los Activos de Información

VALORES DE CRITICIDAD DEL ACTIVO		
MUY BAJO	1	1-3
BAJO	2	4-6
MEDIO	3	7-9
ALTO	4	10-12
MUY ALTO	5	13-15

Según la tabla mostrada, podemos describir en lo siguiente:

- **Muy Bajo (1):** Para la sumatorio total de los valores de confidencialidad, criticidad y disponibilidad obtenido, que varíen en un rango de 1-3 unidades, significa que el activo de información referenciado tiene un valor de impacto “Muy Bajo” dentro del proceso de Seguridad de la Información previamente identificado.
- **Bajo (2):** Para la sumatorio total de los valores de confidencialidad, criticidad y disponibilidad obtenido, que varíen en un rango de 4-6 unidades, significa que el activo de información referenciado tiene un valor de impacto “Bajo” dentro del proceso de Seguridad de la Información previamente identificado.
- **Medio (3):** Para el sumatorio total de los valores de confidencialidad, criticidad y disponibilidad obtenido, que varíen en un rango de 7-9 unidades, significa que el activo de información referenciado tiene un valor de impacto “Medio” dentro del proceso de Seguridad de la Información previamente identificado.
- **Alto (4):** Para la sumatoria total de los valores de confidencialidad, criticidad y disponibilidad obtenido, que varíen en un rango de 10-12 unidades, significa que el activo de información referenciado tiene un valor de impacto “Alto” dentro del proceso de Seguridad de la Información previamente identificado.
- **Muy Alto (5):** Para la sumatoria total de los valores de confidencialidad, criticidad y disponibilidad obtenido, que varíen en un rango de 13-15 unidades, significa que el activo de información referenciado tiene un valor de impacto “Muy Alto” dentro del proceso de Seguridad de la Información previamente identificado.

Tener en cuenta que para nuestro campo de estudio del presente proyecto, se seleccionaran los activos de información que se encuentren dentro del criterio de criticidad o de impacto de “Muy Alto” y “Alto” para la valoración de los activos.

4.4.3.3. Análisis e Identificación de Vulnerabilidades y Amenazas

Las vulnerabilidades se consideran factores de riesgos sobre los activos de información. Asimismo, también las causas o amenazas que puedan determinar la materialización de un evento no favorable sobre el mismo. Por ello, es importante conocer los riesgos asociados a los activos de información y crear planes para el manejo de riesgos que soporten y manejen de alguna manera el impacto de la materialización de alguna amenaza sobre el activo de información, lo cual permita su continuidad y por ende a la continuidad del negocio.

En base a lo comentado, para conocer las vulnerabilidades y amenazas sobre los activos de información se realiza, en esencia, mediante la documentación de fuentes como:

- Entrevistas no estructuradas con las personas que interactúan día a día con los activos de información sobre su operatividad, desempeño y el flujo de trabajo dentro de los procesos en estudio.
- Fuentes estadísticas y tendencias de los riesgos de seguridad y privacidad de los activos, basados en buenas prácticas e información relevante sobre seguridad de activos de información.
- Observaciones de expertos y analistas, y sobre todo opinión de personal involucrado en el desempeño y utilización del activo de información.
- Estudio de los procedimientos, guías y diagramas de información asociados al activo de información.
- Establecimiento de la criticidad del activo y su tratamiento por parte de las personas, los procesos y la tecnología, gestión de riesgos realizados anteriormente

4.4.3.4. Análisis y Evaluación de Riesgos

En esta etapa del SGSI se analizan y se evalúan los riesgos asociados a los activos de información valorados. Posteriormente, se realiza la estimación del riesgo para el activo (estimación de impacto y riesgo), para pasar a la fase de Tratamiento de Riesgos. Todo lo mencionado se indica en el siguiente gráfico:

Figura 26: Integración del Análisis y Evaluación del Riesgo

Al igual como ya se había definido en la valoración de activos, en los valores de impacto de riesgo en los activos de información se cuantificarán en base a la clasificación de: “Muy Bajo”, “Bajo”, “Medio”, “Alto” y “Muy Alto”. El rango de puntuación, así como su ponderación se muestra a continuación:

Tabla 24: Valores de Impacto del Activo de Información

VALORES DE CRITICIDAD O IMPACTO		
RANGO	ESCALA	VALOR
MUY BAJO	1-3	1
BAJO	4-6	2
MEDIO	7-9	3
ALTO	10-12	4
MUY ALTO	13-15	5

Esta tabla de valor de criticidad o impacto es el resultado de la valoración de activos de información, en donde se evalúa la confidencialidad, integridad y disponibilidad del activo en criterio de escalas de impacto: “Muy Bajo”, “Bajo”, “Medio”, “Alto” y “Muy Alto”.

Asimismo, en base a la metodología seleccionada, definimos los valores de probabilidad a los que estarán sujetos los riesgos sobre los activos de información. Para ello, en base a la clasificación realizada: “Muy Bajo”, “Bajo, Medio”, “Alto” y “Muy Alto”) se deberá cuantificar escalas de puntuación y porcentajes definidos de probabilidad de ocurrencia del riesgo. Lo comentado se muestra a continuación:

Tabla 25: Valores de probabilidad del Riesgo sobre del Activo de Información

VALORES DE PROBABILIDAD DEL RIESGO			
RANGO	ESCALA	VALOR	DESCRIPCIÓN
MUY BAJO	1-20	1	La probabilidad de riesgo sobre el activo de información fluctúa entre 1% a 10%, es decir la probabilidad de ocurrencia es muy baja.
BAJO	21 -40	2	La probabilidad de riesgo sobre el activo de información fluctúa entre 11% a 30%, es decir la probabilidad de ocurrencia es baja.
MEDIO	41 - 60	3	La probabilidad de riesgo sobre el activo de información fluctúa entre 31% a 65%, es decir la probabilidad de ocurrencia es media.
ALTO	61 -80	4	La probabilidad de riesgo sobre el activo de información fluctúa entre 66% a 85%, es decir la probabilidad de ocurrencia es alta.
MUY ALTO	81 - 100	5	La probabilidad de riesgo sobre el activo de información fluctúa entre 86% a 100%, es decir la probabilidad de ocurrencia es muy alta.

Con las dos tablas mostradas, debemos realizar el cruce de las mismas para hallar la matriz de Valoración del Riesgo a los activos de la información.

Tabla 26: Matriz del Riesgo sobre del Activo de Información

VALORACIÓN DEL RIESGO						
IMPACTO		PROBABILIDAD				
		MUY BAJO	BAJO	MEDIO	ALTO	MUY ALTO
		1	2	3	4	5
MUY BAJO	1	1	2	3	4	5
BAJO	2	2	4	6	8	10
MEDIO	3	3	6	9	12	15
ALTO	4	4	8	12	16	20
MUY ALTO	5	5	10	15	20	25

Como se muestra en la tabla, la cuantificación o puntuación de cada cruce de nivel de impacto y probabilidad de riesgo sobre el activo resulta en un producto entre ambos. Por ejemplo, para un impacto de riesgos sobre el activo medio, con una probabilidad de riesgo sobre el activo Muy Alto, daría como producto un valor de 15 (3x5). Con ello, generalizamos lo comentado en la siguiente formula de valoración de riesgo:

$$\text{Valoración de Riesgo} = \text{Impacto del Riesgo} \times \text{Probabilidad del Riesgo}$$

Por lo comentado, con el producto indicado del Impacto del riesgo y la Probabilidad de riesgo sobre los activos de información previamente clasificados, resultara en una valoración de Riesgo y en un nivel de aceptación del riesgo por la organización. Los niveles de aceptación del riesgo para la misma son clasificados como Insignificante, Considerable e Importante. La definición de cada uno de ellos se comenta a continuación:

- **Insignificante:** Es el resultado del producto de Impacto de Riesgo y probabilidad de riesgo, el cual arroja un valor dentro de una escala de 1-6 unidades, valorables de 1 a 2 unidades. Este tipo de clasificación de riesgos es definido como un riesgo totalmente aceptable por la empresa u organización y en la cual la misma no debe tomar ninguna acción de remediación sobre el riesgo resultante.
- **Considerable:** Es el resultado del producto de Impacto de Riesgo y probabilidad de riesgo, el cual arroja un valor dentro de una escala de 7-16 unidades, valorables de 3 a 4 unidades. Este tipo de clasificación de riesgos es definido como un riesgo no aceptable por la empresa u organización, en la cual la misma hará uso de algún control para la reducción del riesgo resultante. La intervención del control toma en cuenta algún control incluido dentro de la norma ISO/IEC 27002 y controles Técnicos Auxiliares propuestos.
- **Importante:** Es el resultado del producto de Impacto de Riesgo y probabilidad de riesgo, el cual arroja un valor dentro de una escala de 17-26 unidades, valorables en 5 unidades. Este tipo de clasificación de riesgos es definido como un riesgo no aceptable por la empresa u organización, en la cual la misma hará uso de algún control para la reducción del riesgo resultante. La intervención del control toma en cuenta algún control incluido dentro de la norma ISO/IEC 27002 y controles Técnicos Auxiliares propuestos.

Todo lo comentado se muestra en la siguiente tabla:

Tabla 27: Nivel de Aceptación del Riesgo

VALORES DE RIESGO				
ESCALA		VALOR	NIVEL DE ACEPTACIÓN DEL RIESGO	
MUY BAJO	1-2	1	INSIGNIFICANTE	RIESGO ACEPTABLE PARA LA EMPRESA U ORGANIZACIÓN.
BAJO	3-6	2	INSIGNIFICANTE	RIESGO ACEPTABLE PARA LA EMPRESA U ORGANIZACIÓN.
MEDIO	7-9	3	CONSIDERABLE	RIESGO INACEPTABLE PARA LA EMPRESA U ORGANIZACIÓN, SE NECESITA LA EJECUCIÓN DE UN CONTROL DE SGURIDAD
ALTO	10-16	4	CONSIDERABLE	RIESGO INACEPTABLE PARA LA EMPRESA U ORGANIZACIÓN, SE NECESITA LA EJECUCIÓN DE UN CONTROL DE SGURIDAD
MUY ALTO	17-25	5	IMPORTANTE	RIESGO INACEPTABLE PARA LA EMPRESA U ORGANIZACIÓN, SE NECESITA LA EJECUCIÓN DE UN CONTROL DE SGURIDAD

4.4.3.5. Matriz de Riesgos

La matriz de riesgos contiene el consolidado de los ítems y criterios de evaluación vistos anteriormente. En base a ello, podemos mostrar la siguiente gráfica.

Figura 27: Componentes de la Matriz de Riesgos

RIESGOS		VULNERABILIDADES	Σ PROBABILIDAD	PROBABILIDAD	INTERPRETACIÓN DE LA PROBABILIDAD	NIVEL DE RIESGO (IMPACTO * PROBABILIDAD)	INTERPRETACIÓN DEL RIESGO	NIVEL DE ACEPTACIÓN DEL RIESGO	TIENE CONTROLES	FACTOR DE EFECTIVIDAD DEL CONTROL
ACTIVO	IMPACTO DEL ACTIVO	INTERPRETACIÓN DEL IMPACTO								

En la matriz de riesgos se combinan los siguientes criterios:

- Clasificación de los activos de información en base a escalas de Confidencialidad, Integridad y Disponibilidad. Ello dará como suma el impacto sobre el activo valorado.
- Valores de Impacto sobre el activo de Información valorado y su respectiva interpretación.
- Valores de Probabilidad de ocurrencia de una amenaza aproveche una vulnerabilidad sobre el activo de información valorado para causar algún daño. Sumatoria de los valores de probabilidad y su respectiva interpretación.

- Valoración del nivel riesgo sobre los activos de información valorados como resultado de la probabilidad de ocurrencia de una amenaza versus el impacto que tuviera sobre el activo y su respectiva interpretación.
- Nivel de aceptación del riesgo, definido en escalas de: Insignificante, considerable e importante
- Verificación de Controles de Seguridad Asociados a los activos de información valorados en la presente matriz de riesgos.

4.4.3.6. Apetito del Riesgo

En base al análisis anterior y en base a nuestro campo de estudio, dentro de la Estructura de Gestión de Seguridad de la Información su Comité, Grupo Interdisciplinario y el propio Oficial de Seguridad de la Información seleccionarán los activos de información que cuenten con un “Nivel de Aceptación del Riesgo” calificados como “Considerables” o “Importantes” serán analizados por la organización en cuanto a la asignación de controles de seguridad necesarios.

4.4.3.7. Opciones de Tratamiento de Riesgos

Una vez realizada la matriz de riesgos con los datos recolectados, se deberá identificar quien o quienes son los responsables del tratamiento de riesgos y evaluar los tipos de tratamiento que sean más apropiados para la organización. Lo comentado se muestra en la siguiente tabla:

Tabla 28: Opciones de Tratamiento del Riesgo

Tratamiento	Opciones de Tratamiento del Riesgo
Reducción del Riesgo	Reducir los riesgos mediante la implementación de controles que reduzcan el riesgo a un nivel aceptable para la organización.
Aceptación del Riesgo	La organización decide no tratar el riesgo debido que no ha identificado controles adecuados para el tratamiento de los riesgos, o el costo de implementar algún control es mayor a los beneficios que se obtendrán.
Transferencia del Riesgo	La organización toma como alternativa más económica transferir el control del riesgo a un tercero, más no la responsabilidad del riesgo.
Eliminación del Riesgo	Implica la eliminación de un activo, proceso o área de negocio que es fuente del riesgo para un activo o grupo de activos.

4.4.3.8. Riesgo Residual

En este apartado hay que tener en cuenta que dentro de la Estructura Organizacional del Sistema de Gestión de Seguridad de la Información, dentro de las funciones del Oficial de

Seguridad de la Información es realizar un seguimiento continuo de los controles implementados en la organización. Ello con la finalidad de revisar y asegurar que sean efectivos y que verdaderamente reduzcan la probabilidad de materialización de una amenaza sobre los activos de información valorizados.

Por otro lado, como tiempo establecido dentro de este proyecto de Diseño de SGSI, se estima evaluar los riesgos residuales en un periodo no mayor a un año. Con ello, revisar las medidas preventivas/correctivas que la organización considere necesario para la salvaguarda de los activos de información que pertenecen a la misma.

4.4.4. Identificación de Activos de Información

En base a la metodología descrita, el proceso en estudio es el de Servicio Post-Venta. En ello, se identificaron los siguientes activos de información:

- Sistema de Gestión de Tickets
- Contratos de Servicios, Instalación, entre otros.
- Carpeta de Proyectos
- Carpeta de Licitaciones
- Carpetas de Áreas Administrativas y Contabilidad
- Equipos de computo
- Correo Electrónico
- Internet / Servicios Dedicados
- Sistema de Gestión de Movilidad
- File Server (Servidor de Archivos)
- Infraestructura de Comunicaciones
- Personal
- Imagen de la Organización

En base a ello, respecto a la metodología de gestión de activos utilizada se elaboró la siguiente tabla:

Tabla 29: Inventario de Activos de Información

IDENTIFICACIÓN DEL ACTIVO							
No	Nombre del Activo	Descripción	Tipo de Activo	Clasificación	Propietario	Usuarios del Activo	Ubicación
1	Sistema de Gestión de Tickets	Sistema de gestión de boletas de atención de averías y/o servicios solicitados por los distintos clientes que cuenta o no con contrato de Servicios de Mantenimiento, Instalación y otros con la organización.	Software	Privada	Gerencia Técnica	Directorio / Gerencias / Jefaturas / Personal autorizado de las distintas áreas	Servidor dedicado
2	Contratos de Servicios, Instalación, entre otros	Documentación física de contratos firmados con los distintos clientes con los que cuenta la organización.	Datos / Información	Confidencial	Gerencia Técnica / Gerencia Comercial / Gerencia de Administración y Finanzas	Directorio / Gerencias / Jefaturas / Personal autorizado de las distintas áreas	Armarios ubicados en las distintas área de la organización
3	Carpetas de proyectos	Contiene información del planeamiento, desarrollo, ejecución y cierre de los distintos proyectos que ejecuta la organización. El tipo de documentación está referida a: reuniones pactadas, correos de coordinación, fases de proyectos, cronogramas, informes, actas, diseños de red, topologías, datos de contactos/clientes y demás información del desarrollo del proyecto.	Datos / Información	Privada	Gerencia Técnica / Jefes de Proyectos	Directorio / Gerencia General / Gerencia y Jefatura Técnica / Gerencia y Jefatura Comercial / Personal autorizado del área técnica y comercial	File Server ubicado en Data Center

IDENTIFICACIÓN DEL ACTIVO							
No	Nombre del Activo	Descripción	Tipo de Activo	Clasificación	Propietario	Usuarios del Activo	Ubicación
4	Carpeta de Licitaciones	Contiene la información del desarrollo y ejecución de las propuestas comerciales con entidades privadas y estatales. El tipo de documentación incluye: documentos contractuales, Informes, Comunicados, Actas, datos de contactos/clientes y demás información del desarrollo del proyecto.	Datos / Información	Privada	Gerencia Comercial / Gerencia Técnica	Directorio / Gerencias / Jefaturas / Personal autorizado de las distintas áreas	File Server ubicado en Data Center
5	Carpeta de Áreas Administrativas y Contabilidad	Contiene información referida a procesos administrativos y contables de la organización, este tipo de documentación comprende: planes de negocio, documentación contable, documentación financiera, acuerdos bancarios, entre otros.	Datos / Información	Privada	Gerencia de Administración y Finanzas	Directorio / Gerencia General / Gerencia Técnica / Gerencia y Jefatura Administrativa y Financiera / Gerencia y Jefatura Comercial / Personal autorizado del área administrativa y financiera, y comercial	File Server ubicado en Data Center
6	Equipos de Computo	Referida a equipos portátiles y equipos de escritorio, entre ellos: laptop, desktop, proyectores, teclados, monitores, modem, mouses, entre otros.	Dispositivo Físico / Hardware	Privada	Gerencia Técnica / Gerencia de Administración y Finanzas	Directorio / Gerencias / Jefaturas / Personal autorizado de las distintas áreas	Distintos ambientes de la organización
7	Correo Electrónico	Servicio de correo electrónico para los distintos colaboradores de la organización.	Software / Servicio	Confidencial	Gerencia Técnica	Directorio / Gerencias / Jefaturas / Personal autorizado de las distintas áreas	Servidor de Correos ubicado en el Data Center

IDENTIFICACIÓN DEL ACTIVO							
No	Nombre del Activo	Descripción	Tipo de Activo	Clasificación	Propietario	Usuarios del Activo	Ubicación
8	Internet / Servicios Dedicados	Servicio dedicado de Internet y Servicios dedicados de interconexión hacia las distintas Sedes	Servicio	Pública	Gerencia Técnica	Directorio / Gerencias / Jefaturas / Personal autorizado de las distintas áreas	Virtual / Conexión de Proveedor de Servicios de Internet y Líneas dedicadas
9	Sistema de Gestión de movilidad	Sistema de gestión de movilidad que centraliza las movilizaciones realizadas por todo el personal técnico y no técnico de la organización.	Software	Privada	Gerencia Técnica	Directorio / Gerencias / Jefaturas / Personal autorizado de las distintas áreas	Servidor dedicado
10	File Server (Servidor de Archivos)	Servidor de archivos que contiene los diversos directorios de las distintas áreas de la organización / Servicio de FTP dentro del propio servidor	Dispositivo Físico / Hardware / Software	Privada	Gerencia Técnica	Directorio / Gerencias / Jefaturas / Personal autorizado de las distintas áreas	Servidor dedicado
11	Infraestructura de Comunicaciones	Comprende equipamiento de infraestructura de comunicaciones, tales como: Router, modem, switches, servidores, aceleradores de ancho de banda, central telefónica, firewall, entre otros.	Dispositivo Físico / Hardware	Privada	Gerencia Técnica	Directorio / Gerencias / Jefaturas / Personal de las distintas áreas	En los distintos ambientes de la organización (comprende gabinetes, Data Center, etc)
12	Personal	Personal que desarrolla las distintas actividades dentro y fuera de la organización.	Personas / Recursos Humanos	No Aplica	Gerencia Administrativa y Financiera / Recursos Humanos	No aplica	No aplica
13	Imagen de la Organización	Imagen vista de la organización frente a otras de distintos o mismo rubro.	Imagen y Reputación de la Empresa	No Aplica	Directorio / Gerencia General	Colaboradores de la organización	No aplica

4.4.5. Valoración de Activos de Información

En base a los criterios de valoración de activos descritos en la metodología utilizada, se elaboró una tabla con el detalle de la puntuación de los pilares fundamentales de la Seguridad de la Información (Confidencialidad, integridad y disponibilidad) y el nivel de criticidad de los mismos en el proceso en estudio. En base a ello se muestra la valoración de activos comentada:

Tabla 30: Valoración de Activos de la Información según su Criticidad / Impacto

IDENTIFICACIÓN DEL ACTIVO			VALORACIÓN DEL ACTIVO					
No	Nombre del Activo	Descripción	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	Σ PILARES DE LA SEGURIDAD DE LA INFORMACIÓN	CRITICIDAD	VALORACIÓN DEL ACTIVO
1	Sistema de Gestión de Tickets	Sistema de gestión de boletas de atención de averías y/o servicios solicitados por los distintos clientes que cuenta o no con contrato de Servicios de Mantenimiento, Instalación y otros con la organización.	5	5	5	15	5	MUY ALTO
2	Contratos de Servicios, Instalación, entre otros	Documentación física de contratos firmados con los distintos clientes con los que cuenta la organización.	4	5	4	13	5	MUY ALTO
3	Carpetas de proyectos	Contiene información del planeamiento, desarrollo, ejecución y cierre de los distintos proyectos que ejecuta la organización. El tipo de documentación está referida a: reuniones pactadas, correos de coordinación, fases de proyectos, cronogramas, informes, comunicados, actas en sus distintas variedades, diseños de red, topologías, datos de contactos/clientes y demás información del desarrollo del proyecto.	5	5	4	14	5	MUY ALTO

IDENTIFICACIÓN DEL ACTIVO			VALORACIÓN DEL ACTIVO					
No	Nombre del Activo	Descripción	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	Σ PILARES DE LA SEGURIDAD DE LA INFORMACIÓN	CRITICIDAD	VALORACIÓN DEL ACTIVO
4	Carpeta de Licitaciones	Contiene la información del desarrollo y ejecución de las propuestas comerciales con entidades privadas y estatales. El tipo de documentación incluye: documentos contractuales, Informes, Comunicados, Actas, datos de contactos/clientes y demás información del desarrollo del proyecto.	5	5	5	15	5	MUY ALTO
5	Carpetas de Áreas Administrativas y Contabilidad	Contiene información referida a procesos administrativos y contables de la organización, este tipo de documentación comprende: planes de negocio, documentación contable, documentación financiera, acuerdos bancarios, entre otros.	5	5	5	15	5	ALTO
6	Equipos de Computo	Referida a equipos portátiles y equipos de escritorio, entre ellos: laptop, desktop, proyectores, teclados, monitores, modem, mouses, entre otros.	4	4	3	11	4	ALTO
7	Correo Electrónico	Servicio de correo electrónico para los distintos colaboradores de la organización.	5	4	4	13	5	MUY ALTO
8	Internet / Servicios Dedicados	Servicio dedicado de Internet y Servicios dedicados de interconexión hacia las distintas Sedes	4	4	3	11	4	ALTO

IDENTIFICACIÓN DEL ACTIVO			VALORACIÓN DEL ACTIVO					
No	Nombre del Activo	Descripción	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	Σ PILARES DE LA SEGURIDAD DE LA INFORMACIÓN	CRITICIDAD	VALORACIÓN DEL ACTIVO
9	Sistema de Gestión de movilidad	Sistema de gestión de movilidad que centraliza las movilizaciones realizadas por todo el personal técnico y no técnico de la organización.	2	3	2	7	3	MEDIO
10	File Server (Servidor de Archivos)	Servidor de archivos que contiene los diversos directorios de las distintas áreas de la organización / Servicio de FTP dentro del propio servidor	5	4	5	14	5	MUY ALTO
11	Infraestructura de Comunicaciones	Comprende equipamiento de infraestructura de comunicaciones, tales como: Router, modem, Switches, servidores, aceleradores de ancho de banda, central telefónica, firewall, entre otros.	5	4	4	13	5	MUY ALTO
12	Personal	Personal que desarrolla las distintas actividades dentro y fuera de la organización.	5	4	4	13	5	MUY ALTO
13	Imagen de la Organización	Imagen vista de la organización frente a otras de distintos o mismo rubro.	3	3	3	9	3	MEDIO

Para el campo de estudio del presente proyecto, para la valoración de activos se tomaran en cuenta los activos de información que se encuentren dentro del criterio de criticidad de “Muy Alto” y “Alto”. Por ello, de la clasificación realizada, los activos de información seleccionados son:

- Sistema de Gestión de Tickets
- Contratos de Servicios, Instalación, entre otros
- Carpetas de Proyectos
- Carpeta de Licitaciones
- Carpetas de áreas Administrativas y Contabilidad
- Equipos de Cómputo
- Correo Electrónico
- Internet / Servicios Dedicados
- File Server (Servidor de Archivos)
- Infraestructura de Comunicaciones
- Personal

Tener en cuenta que la Valoración de Activos desarrollada será crucial para el posterior desarrollo de la matriz de riesgos a realizar. Asimismo, en base a lo discriminado, se realizara el análisis e identificación de vulnerabilidades y amenazas.

4.4.6. Análisis e Identificación de Vulnerabilidades y Amenazas

Una vez ya definidos los activos de información, debemos realizar una identificación de las vulnerabilidades y amenazas a las que se encuentra expuestos. Con ello, podremos realizar posteriormente el análisis y evaluación de riesgo mediante la matriz de valor de riesgos y los posteriores controles de seguridad necesarios para su manejo y protección. En base a ello, las principales amenazas y vulnerabilidades identificadas dentro del proceso de servicio Post-Venta de la organización se detallan en los siguientes puntos.

4.4.6.1. Vulnerabilidades

Las vulnerabilidades detectadas en los activos de información son los siguientes:

- Falta de cierre de inicio de sesión en cada logueo realizado.
- No existe definición de roles de usuarios. Es decir, el mismo usuario además de crear boletas de atención, puede observar módulos contables no autorizados, entre otros.
- Servicios innecesarios para los usuarios que acceden al sistema.
- Contraseñas de acceso definidas son de un nivel de protección o durabilidad muy baja.
- Fallas en tomas de alimentación eléctrica estabilizada de servidor que aloja aplicación o software (inestabilidad de alimentación eléctrica / no conectada en tomas de acceso a UPS)
- Aplicación no cuenta con un sistema de respaldo en otro servidor dedicado teniendo en cuenta la criticidad del mismo.
- Ausencia de Mantenimiento de servidor que aloja aplicación o software de Gestión de Tickets.
- Ausencia de Mantenimiento de servidor que aloja aplicación o software de Correo Electrónico
- Falta de logs de la aplicación o software para posteriores auditorias.
- Transmisión de contraseñas de acceso por teléfono o vía correo.
- Ausencia de Responsable de acceso y/o modificación de aplicativo
- Falta de actualizaciones en servidor donde se aloja las aplicaciones y de la propia aplicación.
- Falta de gestión de paquetes de actualización o parches de Sistemas Operativos de equipos de cómputo o de los equipos que componen la Infraestructura de Comunicaciones
- Acceso a información se encuentra en un armario de total acceso a usuarios no autorizados, no existen candado ni llaves para su acceso.
- Ausencia del responsable de acceso a la documentación física
- Control de accesos a equipos, sistemas y aplicaciones mediante mecanismos técnicos.

- No existe definición de procedimientos para el movimiento o traslado del activo dentro y fuera de la oficina.
- Falta de mecanismos de backup para la documentación Física
- No existen controles para su acceso a nivel de acceso y seguridad de carpetas a pesar de comunicado difundido
- Ausencia del responsable de acceso a carpeta.
- Ausencia de backup o respaldo de documentación de carpeta.
- Uso inadecuado de contenido de la carpeta
- Ausencia de controles contra modificación o alteración de contenido de carpeta.
- Algunos equipos no se encuentran ingresadas en el dominio, no cumpliendo los estándares de seguridad aplicados por la organización.
- No existe controles de desinstalación de programas/aplicaciones auditables instaladas por la organización
- Ausencia o falta de backup o respaldos de documentación interna de los equipos o de la información más relevante.
- Falta de mecanismos de autenticación de usuarios sobre los equipos de cómputo asignados.
- Ausencia de protección física para el retiro de equipos a clientes.
- Ausencia de hardware de backup
- Ausencia de responsable del bien
- Ausencia de controles de retiro de equipos para labores a realizar en los distintos clientes
- Ausencia de políticas y/o procedimientos para envío de correos (tamaño, destinatario, adjunto, etc).
- Mala gestión de Contraseñas
- Ausencia de backup o respaldo de la información Extensiones .pst)
- Falta de gestión de logs en servidor de correo para seguimiento o auditoria.

- Falta de gestión de logs en consumo de recursos de navegación en Internet para seguimiento o auditoria.
- Falta de disponibilidad del servicio por parte del proveedor o ISP.
- Falta de Mantenimiento de equipamiento de Infraestructura
- Red perimetral de la organización carece de mecanismos de defensa ante a ataques de día cero (Zero days), malware conocido o específicamente código malicioso.
- Ausencia de mecanismos de protección contra correo del tipo SPAM
- Ausencia de mecanismos de protección y concientización al usuario sobre ataques de Ingeniería Social y Phishing
- Falta de Mantenimiento de equipamiento de acceso a Internet otorgado por el Proveedor o ISP
- Acceso a Data Center no definido mediante documentación y/o asignación de responsabilidades.
- Ausencia de mantenimiento a servidor de archivos
- Falta de gestión de logs en equipos de Infraestructura de comunicaciones para seguimiento o auditoria.
- Falta de gestión de logs en servidor de archivos para seguimiento o auditoria (recursos del equipo).
- Falta de gestión de logs de accesos y contenido de recursos de datos alojados en carpetas de File Server (Servidor de Archivos).
- Ausencia de backup o respaldo de la información interna.
- Control de accesos no definidos mediante documentación o asignación de responsabilidades.
- Control de accesos de navegación a Internet no definidos mediante documentación o asignación de perfiles.
- Falta de inducción, capacitación y sensibilización sobre riesgos.
- Renuncias y/o despidos del personal

- Ausencia de documento donde se especifique que el personal que accede a la documentación de la organización debe preservar la confidencialidad, integridad y de ser el caso la disponibilidad de la misma.
- Ausencia de documento donde se especifique que el personal que accede a la aplicación debe preservar la confidencialidad, integridad y de ser el caso la disponibilidad de la misma.
- Ausencia de documento donde se especifique que el personal que accede al servidor debe preservar la confidencialidad, integridad y de ser el caso la disponibilidad de la misma.
- Manejo inadecuado de software o herramientas brindadas por la organización.
- Ausencia de orden en asignación de servicios a los distintos clientes de la empresa u organización.
- Red cableada expuesta a acceso no autorizado.
- Equipos que componen la Infraestructura de Comunicaciones que soportan los sistemas y servicios críticos no cuentan con equipos alternos en ubicaciones alternas que permitan la continuidad del negocio.

4.4.6.2. Amenazas

En base a las vulnerabilidades detectadas, se evidenciaron las siguientes amenazas para la totalidad de activos de información valorizados:

- Manipulación de la información
- Procesamiento ilegal de los datos
- Espionaje de contraseñas
- Ataques de diccionario
- Mal funcionamiento de software y/o aplicación
- Destrucción de la propia aplicación
- Abuso de derechos
- Abuso de confidencialidad de datos
- Abuso de confidencialidad, integridad y disponibilidad de la información

- Sniffer de Información
- Robo de información
- Robo o pérdida de información ingresada
- Robo o pérdida de documentación ingresada
- Robo de equipo
- Perdidas de comunicación por manipulación
- Pérdida de actividad de labores
- Destrucción del equipo
- Destrucción de la propia aplicación
- Destrucción de equipo o propia aplicación
- Inoperatividad del equipo y/o equipos
- Inoperatividad del sistema o servicio
- Fallas en el funcionamiento de equipo y/o equipos
- Falla en el suministro eléctrico
- Correos con contenidos maliciosos y/o SPAM
- Saturación del circuito de Internet
- Acceso a destinos de alto riesgo de infección
- Infección de Código malicioso: Virus, Spyware, Ransomware, entre otros en la red interna
- Desastre natural
- Falla masiva
- No resolución de problemas tecnológicos
- Negligencia en trabajos asignados
- Clientes insatisfechos
- Ataques de Phishing
- Ingeniería Social

- Apropiación indebida de activos
- Ataque de cualquier tipo que atente contra la continuidad del negocio
- Incumplimiento de normas establecidas respecto a Seguridad de la Información
- Acceso no autorizado al sistema
- Acceso no autorizado al equipo

En base a lo comentado, en referencia a las vulnerabilidades y amenazas detectadas se elaboró el cuadro de “Vulnerabilidades y Amenazas de Activos Valorados”, el cual se puede observar de manera íntegra y detallada en el “Anexo II” adjunto al presente proyecto. A modo de ejemplo se muestra parte del detalle para el activo de información “Sistema de Gestión de Tickets”:

Tabla 31: Vulnerabilidad y Amenazas de Activos Valorados

No	Nombre del Activo	Descripción	Vulnerabilidades	Amenazas
1	Sistema de Gestión de Tickets	Sistema de gestión de boletas de atención de averías y/o servicios solicitados por los distintos clientes que cuenta o no con contrato de Servicios de Mantenimiento, Instalación y otros con la organización.	Falta de cierre de inicio de sesión en cada logueo realizado.	Manipulación de la Información
			No existe definición de roles de usuarios. Es decir, el mismo usuario además de crear boletas de atención, puede observar módulos contables no autorizados, entre otros.	Abuso de derechos
			Servicios innecesarios para los usuarios que acceden al sistema.	Abuso de derechos / Procesamiento ilegal de los datos
			Contraseñas de acceso definidas son de un nivel de protección o durabilidad muy baja.	Espionaje de Contraseñas / Ataques de diccionario / Acceso no autorizado al Sistema
			Fallas en tomas de alimentación eléctrica estabilizada de servidor que aloja aplicación o software (inestabilidad de alimentación eléctrica / no conectada en tomas de acceso a UPS)	Inoperatividad del Sistema
			Aplicación no cuenta con un sistema de respaldo en otro servidor dedicado, teniendo en cuenta la criticidad del mismo.	Robo o pérdida de documentación ingresada
			Ausencia de Mantenimiento de servidor que aloja aplicación o software de Gestión de Tickets.	Inoperatividad del Sistema / Destrucción de la propia aplicación

4.4.7. Análisis y Evaluación de Riesgos

Después de haber analizado las vulnerabilidades y amenazas sobre los activos de información valorizados, es necesario analizar y evaluar los riesgos en base a la metodología descrita. En base a ello, se elaboró la matriz de riesgos en la cual se revisa cálculos de la probabilidad que una amenaza aproveche una vulnerabilidad para causar daños sobre el activo y el impacto sobre el activo en base a los tres pilares de la seguridad de la información: confidencialidad, disponibilidad e integridad, realizado en su valoración. En base a lo comentado, a continuación se muestra matriz de riesgos diseñada, la cual puede revisarse al detalle en el “**Anexo III**” adjunto al presente proyecto.

Figura 28: Matriz de Riesgos

RIESGOS		VULNERABILIDADES									
			Falta de cierre de inicio de sesión en cada logueo realizado.	No existe definición de roles de usuarios. Es decir, el mismo usuario además de crear boletas de atención, puede observar módulos contables no autorizados, entre otros.	Servicios innecesarios para los usuarios que acceden al sistema.	Contraseñas de acceso definidas son de un nivel de protección o durabilidad muy baja.	Fallas en tomas de alimentación eléctrica estabilizada de servidor que aloja aplicación o software (inestabilidad de alimentación eléctrica / no conectada en tomas de acceso a UPS)	Aplicación no cuenta con un sistema de respaldo en otro servidor dedicado teniendo en cuenta la criticidad del mismo.	Ausencia de Mantenimiento de servidor que aloja aplicación o software de Gestión de Tickets.	Ausencia de Mantenimiento de servidor que aloja aplicación o software de Correo Electrónico	Falta de logs de la aplicación o software para posteriores auditorías.
ACTIVO	IMPACTO DEL ACTIVO	INTERPRETACIÓN DEL IMPACTO									
Sistema de Gestión de Tickets	5	MUY ALTO	5	5	4	4	5	3	3		3
Contratos de Servicios, Instalación, entre otros	5	MUY ALTO									
Carpeta de Proyectos	5	MUY ALTO									
Carpeta de Licitaciones	5	MUY ALTO									
Carpetas de Areas Administrativas y Contabilidad	5	MUY ALTO									
Equipos de Computo	4	ALTO	5			4					
Correo Electrónico	5	MUY ALTO	5			5	5	4		3	
Internet / Servicios dedicados	4	ALTO					5				
File Server (Servidor de Archivos)	5	MUY ALTO					5				
Infraestructura de Comunicaciones	5	MUY ALTO					5				
Personal	5	MUY ALTO									

RIESGOS		VULNERABILIDADES										
			Transmisión de contraseñas de acceso por teléfono o vía correo.	Ausencia de Responsable de acceso y/o modificación de aplicativo	Falta de actualizaciones en servidor donde se aloja la aplicación y de la propia aplicación.	Acceso a información se encuentra en un armario de total acceso a usuarios no autorizados, no existen candado ni llaves para su acceso.	Ausencia de Responsable de acceso a documentación física	No existe definición de procedimientos para el movimiento o traslado del activo dentro y fuera de la oficina.	Falta de mecanismos de backup para la documentación Física	No existen controles para su acceso a nivel de acceso y seguridad de carpetas a pesar de comunicado difundido	Ausencia de Responsable de acceso a carpeta.	Ausencia de backup o respaldo de documentación de carpeta.
ACTIVO	IMPACTO DEL ACTIVO	INTERPRETACIÓN DEL IMPACTO										
Sistema de Gestión de Tickets	5	MUY ALTO	2	4	3							
Contratos de Servicios, Instalación, entre otros	5	MUY ALTO				5	5	5	5			
Carpeta de Proyectos	5	MUY ALTO								5	5	5
Carpeta de Licitaciones	5	MUY ALTO								5	5	5
Carpetas de Areas Administrativas y Contabilidad	5	MUY ALTO								5	5	5
Equipos de Computo	4	ALTO	4					4				
Correo Electrónico	5	MUY ALTO	5		4							
Internet /Servicios dedicados	4	ALTO										
File Server (Servidor de Archivos)	5	MUY ALTO										
Infraestructura de Comunicaciones	5	MUY ALTO										
Personal	5	MUY ALTO										

RIESGOS		VULNERABILIDADES	AMENAZAS DETECTADAS									
			Uso inadecuado de contenido de la carpeta	Ausencia de controles contra modificación o alteración de contenido de carpeta.	Algunos equipos no se encuentran ingresados en el dominio, no cumpliendo los estándares de seguridad aplicados por la organización.	No existe controles de desinstalación de programas/aplicaciones auditable instaladas por la organización	Ausencia o falta de backups o respaldos de documentacion interna de los equipos o de la información mas relevante.	Falta de mecanismos de autenticación de usuarios sobre los equipos de cómputo asignados.	Ausencia de protección física para el retiro de equipos a clientes.	Ausencia de hardware de backup	Ausencia de responsable del bien	Ausencia de controles de retiro de equipos para labores a realizar en los distintos clientes
ACTIVO	IMPACTO DEL ACTIVO	INTERPRETACIÓN DEL IMPACTO	PROBABILIDAD: PROBABILIDAD QUE UNA AMENAZA APROVECHE UNA VULNERABILIDAD PARA CAUSAR UN DAÑO EN									
Sistema de Gestión de Tickets	5	MUY ALTO									4	
Contratos de Servicios, Instalación, entre otros	5	MUY ALTO									5	
Carpeta de Proyectos	5	MUY ALTO	5	5							5	
Carpeta de Licitaciones	5	MUY ALTO	5	5							5	
Carpetas de Areas Administrativas y Contabilidad	5	MUY ALTO	5	5							5	
Equipos de Computo	4	ALTO			5	4	4	4	4		4	3
Correo Electrónico	5	MUY ALTO									5	
Internet / Servicios dedicados	4	ALTO									5	
File Server (Servidor de Archivos)	5	MUY ALTO		5						5	4	
Infraestructura de Comunicaciones	5	MUY ALTO					4			5	4	
Personal	5	MUY ALTO										

RIESGOS		VULNERABILIDADES											
			Ausencia de políticas y/o procedimientos para envío de correos (tamaño, destinatario, adjunto, etc).	Mala gestión de Contraseñas	Ausencia de backup o respaldo de la información Extensiones .pst)	Falta de gestión de logs en servidor de correo para seguimiento o auditoria.	Falta de gestión de logs en consumo de recursos de Navegación en Internet para seguimiento o auditoria.	Falta de disponibilidad del servicio por parte del proveedor o ISP.	Falta de Mantenimiento de equipamiento de Infraestructura	Falta de Mantenimiento de equipamiento de acceso a Internet otorgado por el Proveedor o ISP	Acceso a Data Center no definido mediante documentación y/o asignación de responsabilidades.	Ausencia de mantenimiento a servidor de archivos	Falta de gestión de logs en equipos de Infraestructura de comunicaciones para seguimiento o auditoria.
ACTIVO	IMPACTO DEL ACTIVO	INTERPRETACIÓN DEL IMPACTO	EL ACTIVO DE INFORMACIÓN										
Sistema de Gestión de Tickets	5	MUY ALTO		4									
Contratos de Servicios, Instalación, entre otros	5	MUY ALTO											
Carpeta de Proyectos	5	MUY ALTO											
Carpeta de Licitaciones	5	MUY ALTO											
Carpeta de Areas Administrativas y Contabilidad	5	MUY ALTO											
Equipos de Computo	4	ALTO		4									
Correo Electrónico	5	MUY ALTO	5	5	5	5							
Internet / Servicios dedicados	4	ALTO					5	5		5	5		
File Server (Servidor de Archivos)	5	MUY ALTO										4	
Infraestructura de Comunicaciones	5	MUY ALTO		4					4				4
Personal	5	MUY ALTO											

RIESGOS		VULNERABILIDADES									
			Falta de gestión de logs en servidor de archivos para seguimiento o auditoría (recursos del equipo)	Falta de gestión de logs de accesos y contenido de recursos de datos alojados en carpetas de File Server (Servidor de Archivos)	Ausencia de backup o respaldo de la información interna.	Control de accesos no definidos mediante documentación o asignación de responsabilidades.	Control de accesos de navegación a Internet no definidos mediante documentación o asignación de perfiles.	Falta de inducción, capacitación y sensibilización sobre riesgos.	Renuncias y/o despidos del personal	Ausencia de documento donde se especifique que el personal que accede a la documentación de la organización debe preservar la confidencialidad, integridad y de ser el caso la disponibilidad de la misma.	Ausencia de documento donde se especifique que el personal que accede a la aplicación debe preservar la confidencialidad, integridad y de ser el caso la disponibilidad de la misma.
ACTIVO	IMPACTO DEL ACTIVO	INTERPRETACIÓN DEL IMPACTO									
Sistema de Gestión de Tickets	5	MUY ALTO				4					5
Contratos de Servicios, Instalación, entre otros	5	MUY ALTO				5				5	
Carpeta de Proyectos	5	MUY ALTO		5		5				5	
Carpeta de Licitaciones	5	MUY ALTO		5		5				5	
Carpetas de Areas Administrativas y Contabilidad	5	MUY ALTO		5		5				5	
Equipos de Computo	4	ALTO			3	3					
Correo Electrónico	5	MUY ALTO									5
Internet / Servicios dedicados	4	ALTO					5				
File Server (Servidor de Archivos)	5	MUY ALTO	5		5	5					
Infraestructura de Comunicaciones	5	MUY ALTO				5					
Personal	5	MUY ALTO						5	4		

RIESGOS		VULNERABILIDADES				
			Ausencia de documento donde se especifique que el personal que accede al servidor debe preservar la confidencialidad, integridad y de ser el caso la disponibilidad de la misma.	Manejo inadecuado de software o herramientas brindadas por la organización.	Ausencia de orden en asignación de servicios a los distintos clientes de la empresa u organización.	Red cableada expuesta a acceso no autorizado.
ACTIVO	IMPACTO DEL ACTIVO	INTERPRETACIÓN DEL IMPACTO				
Sistema de Gestión de Tickets	5	MUY ALTO		3		
Contratos de Servicios, Instalación, entre otros	5	MUY ALTO				
Carpeta de Proyectos	5	MUY ALTO				
Carpeta de Licitaciones	5	MUY ALTO				
Carpetas de Areas Administrativas y Contabilidad	5	MUY ALTO				
Equipos de Computo	4	ALTO				4
Correo Electrónico	5	MUY ALTO		3		
Internet / Servicios dedicados	4	ALTO				
File Server (Servidor de Archivos)	5	MUY ALTO	5			5
Infraestructura de Comunicaciones	5	MUY ALTO				5
Personal	5	MUY ALTO	5	4	5	

RIESGOS		VULNERABILIDADES	Σ PROBABILIDAD DEL RIESGO	PROBABILIDAD DEL RIESGO	INTERPRETACIÓN DE LA PROBABILIDAD DEL RIESGO	NIVEL DE RIESGO (IMPACTO * PROBABILIDAD)	INTERPRETACIÓN DEL RIESGO	NIVEL DE ACEPTACIÓN DEL RIESGO	TIENE CONTROLES
ACTIVO	IMPACTO DEL ACTIVO	INTERPRETACIÓN DEL IMPACTO							
Sistema de Gestión de Tickets	5	MUY ALTO	61	4	ALTO	20	MUY ALTO	IMPORTANTE	NO
Contratos de Servicios, Instalación, entre otros	5	MUY ALTO	35	2	BAJO	10	ALTO	CONSIDERABLE	NO
Carpeta de Proyectos	5	MUY ALTO	45	3	MEDIO	15	ALTO	CONSIDERABLE	NO
Carpeta de Licitaciones	5	MUY ALTO	45	3	MEDIO	15	ALTO	CONSIDERABLE	NO
Carpetas de Areas Administrativas y Contabilidad	5	MUY ALTO	45	3	MEDIO	15	ALTO	CONSIDERABLE	NO
Equipos de Computo	4	ALTO	59	3	MEDIO	12	ALTO	CONSIDERABLE	NO
Correo Electrónico	5	MUY ALTO	64	4	ALTO	20	MUY ALTO	IMPORTANTE	NO
Internet / Servicios dedicados	4	ALTO	35	2	BAJO	8	MEDIO	CONSIDERABLE	NO
File Server (Servidor de Archivos)	5	MUY ALTO	48	3	MEDIO	15	ALTO	CONSIDERABLE	NO
Infraestructura de Comunicaciones	5	MUY ALTO	40	2	BAJO	10	ALTO	CONSIDERABLE	NO
Personal	5	MUY ALTO	23	2	BAJO	10	ALTO	CONSIDERABLE	NO

Esta matriz de riesgos nos permitirá realizar Plan de Tratamiento de riesgos y estimar las acciones necesarias en cuanto a las opciones de tratamiento de riesgos que serán asumidas por la organización.

4.4.8 Plan de Tratamiento de Riesgos

Luego de definir los niveles de riesgos respecto a las vulnerabilidades de cada activo y las amenazas que puedan afectar a cada uno de los pilares de la seguridad de la información, tales son: integridad, confidencialidad o disponibilidad, se definió un criterio de aceptación del riesgo el cual determina si el riesgo es aceptable o si requiere de algún tratamiento. En base a ello, el tratamiento del riesgo resultante de la matriz de riesgos ejecutada se muestra en el “**Anexo IV**” adjunto al presente proyecto. De igual manera el formato de la tabla en base al activo de información Sistema de Gestión de Tickets a modo de ejemplo es:

Tabla 32: Tratamiento del Riesgo

Ítem	Activo de Información	Interpretación del Riesgo	Nivel de Aceptación de Riesgos	Amenaza / Riesgo	Opción de Tratamiento del Riesgo	Dueño del Riesgo
1	Sistema de Gestión de Tickets	Muy Alto	Importante	Manipulación de Información	Reducción del Riesgo	Gerente Técnico
				Abuso de derechos		
				Procesamiento ilegal de los datos		
				Espionaje de Contraseñas		
				Ataques de diccionario		
				Acceso no autorizado al Sistema		
				Inoperatividad del Sistema		

Fuente: Elaboración propia

Donde:

- **Ítem:** Número de activo de información seleccionado.
- **Activo de Información:** Se refiere al activo de información seleccionado para el plan de tratamiento de riesgos respectivo. Tener en cuenta que son 11 activos de información valorizados e indicados en la tabla.

- **Interpretación del Riesgo:** Es la valoración del riesgo sobre los activos de información, después del cruce del impacto y la probabilidad de ocurrencia de una amenaza sobre el activo de información. Los valores resultantes son: “Muy Bajo”, “Bajo”, “Medio” “Alto” y “Muy Alto”.
- **Nivel de Aceptación del Riesgo:** Es la categorización que se da al riesgo sobre un activo de información y como la organización lo asume. Es decir, si es aceptable o no aceptable para la organización y según ello si es necesario la adopción de un control de seguridad para su salvaguarda.
- **Amenaza / Riesgo:** Es la relación que permite a la organización saber que riesgos están expuestos a cada activo de información con la concretización de una amenaza sobre el activo.
- **Opción de Tratamiento del Riesgo:** Son las opciones que la organización toma para manejar el riesgo sobre los activos de información. Las opciones son: reducción, aceptación, transferencia y eliminación del riesgo.
- **Dueño del Riesgo:** Personal encargado responsable de gestionar los riesgos asociados a los activos de información valorizados
- Asimismo, después de describir los ítems de la tabla mostrada, en la resultante del mismo se puede observar que el nivel de aceptación de riesgos cuenta con valores aproximados de:
 - 18% para Nivel de Riesgo Importante
 - 82% para Nivel de Riesgos Considerable
 - 0% para Nivel de Riesgo Insignificante

De la información indicada se elaboró el siguiente grafico del Nivel de Aceptación del Riesgo

Figura 29: Nivel de Aceptación del Riesgo

Fuente: Elaboración propia

Por otro lado, en el Plan de tratamiento de los riesgos se detalla cuáles son los riesgos a los que están sujetos los activos de información y los controles que son necesarios para la acción de los mismos. Aquí cabe indicar que no solo se ha considerado la adopción de los controles del “Anexo A” de la norma ISO/IEC 27001:2013, sino también Controles Auxiliares (TA), los cuales son controles técnicos que la organización debe adoptar para complementar los controles administrativos indicados en la norma. Este Plan de Tratamiento de Riesgo se encuentra desarrollado en el “**Anexo V**” adjunto al presente proyecto. De igual manera el formato de la tabla en base al activo de información Sistema de Gestión de Tickets a modo de ejemplo es:

Tabla 33: Plan de Tratamiento del Riesgo

ITEM	ACTIVO	AMENAZA / RIESGO	OPCIONES DE TRATAMIENTO DEL RIESGO	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR	DUEÑO DEL RIESGO	RESPONSABLE DEL CONTROL	ESTADO DEL CONTROL
1	Sistema de Gestión de Tickets	Manipulación de Información / Abuso de derechos / Procesamiento ilegal de los datos / Espionaje de Contraseñas / Ataques de diccionario / Acceso no autorizado al Sistema	Reducción del riesgo	A 5.1.1 CONJUNTO DE POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN / A 5.1.2 REVISIÓN DE LAS POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN	Norma ISO/IEC 27002:2013	Mantener implementados los lineamientos de la Política de Seguridad de la Información y las normas de seguridad dentro de la organización.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Inoperatividad del Sistema / Destrucción de la propia aplicación	Transferencia del riesgo	TA 5. MIGRACIÓN DEL SISTEMA DE GESTIÓN DE TICKETS EN UN SERVICIO EN LA NUBE MEDIANTE IAAS	Técnico Auxiliar	La organización debe contemplar la aplicación y ejecución de uno de los modelos de Cloud Computing, es decir Infraestructura como Servicio (IaaS) y llevar el Servicio del Sistema de Gestión de Tickets a la nube, evitando gastos de capital y reduciendo los costos corrientes, por un pago mensual o anual según convenga.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado

Donde:

- **Ítem:** Número de activo de información seleccionado.
- **Activo:** Se refiere al activo de información seleccionado para el plan de tratamiento de riesgos respectivo. Tener en cuenta que son 11 activos de información valorizados e indicados en la tabla.
- **Amenaza / Riesgo:** Es la relación que permite a la organización saber que riesgos están expuestos a cada activo de información con la concretización de una amenaza sobre el activo.
- **Opciones de Tratamiento del Riesgo:** Son las opciones que la organización toma para manejar el riesgo sobre los activos de información. Las opciones son: reducción, aceptación, transferencia y eliminación del riesgo.
- **Control:** Control de seguridad indicado en el “Anexo A” de la norma ISO/IEC 27001:2013 y controles Técnicos auxiliares (TA) propuestos para complementar los controles administrativos indicados en la norma.
- **Tipo de Control:** Indicado en el “Anexo A” de la norma ISO/IEC 27002:2013 o Control Técnico Auxiliar (TA).
- **Descripción / Acciones a tomar:** Descripción de las acciones a ejecutar con la adopción del control de seguridad sobre el activo de información.
- **Dueño del Riesgo:** Personal encargado responsable de gestionar los riesgos asociados a los activos de información valorizados.
- **Responsable del Control:** Personal a cargo de la gestión del Control de Seguridad.
- **Estado del Control:** Estado del control propuesto: Implementado o no Implementado.

4.4.9. Declaración de Aplicabilidad

Este punto se abarca los criterios de aplicabilidad de controles para cada activo de la información según lo indicado en el “Anexo A” de la norma ISO/IEC 27002:2013 y controles Técnicos Auxiliares propuestos. El detalle de los controles seleccionados de la norma, su justificación y los propios controles Técnicos Auxiliares se encuentran a detalle en el “**Anexo VI**” y “**Anexo VII**” adjuntos en el presente proyecto respectivamente, tal como se muestra a continuación:

Tabla 34: Declaración de Aplicabilidad – SOA

CLÁUSULA	OBJETIVOS DE CONTROL	CONTROLES	APLICABILIDAD	JUSTIFICACIÓN
A.5 POLÍTICAS DE SEGURIDAD	A 5.1 DIRECTRICES DE LA DIRECCIÓN EN LA SEGURIDAD DE LA INFORMACIÓN	A 5.1.1 CONJUNTO DE POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN	SI	Se ha identificado los riesgos de información en la organización. Por ello, es necesario establecer una política de seguridad de la información para informar y concientizar a todos los colaboradores y partes interesadas sobre los riesgos a los que se encuentran expuestos. Asimismo, informar e indicar los controles implementados para evitar la materialización de estos riesgos.
A.6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	A 6.1 ORGANIZACIÓN INTERNA	A 6.1.1 ASIGNACIÓN DE RESPONSABILIDADES PARA LA SEGURIDAD DE LA INFORMACIÓN	SI	La organización mediante su Política de Seguridad de la Información debe establecer el compromiso y asignación de responsabilidades para su cumplimiento en materia de seguridad de la información. Asimismo, velar por mantener protegida su información mediante la revisión del sistema de gestión de seguridad de la información (SGSI), la firma de los acuerdos de confidencialidad, manteniendo contacto con las autoridades y con grupos de interés especiales.
		A 6.1.2 SEGREGACIÓN DE TAREAS	SI	
		A 6.1.3 CONTACTO CON LAS AUTORIDADES	NO	No contemplado para la organización
		A 6.1.4 CONTACTO CON GRUPOS DE INTERÉS ESPECIAL	NO	No contemplado para la organización

Tener en cuenta que en base a la tabla revisada en este punto el total de controles aplicados seleccionados por la norma para reducir el riesgo y contrarrestar las amenazas, ya descritas para cada activo de la información, asciende a un total de 64 de 114 en total descrito por la norma.

Tabla 35: Cantidad de Controles de Seguridad Aplicables

CLÁUSULA	APLICAB.	NO APLICAB
A.5 POLITICAS DE SEGURIDAD	2	0
A.6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	3	4
A.7 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	5	1
A.8 GESTION DE ACTIVOS	8	2
A.9 CONTROL DE ACCESOS	11	3
A.10 CIFRADO / CRIPTOGRAFIA	0	2
A. 11 SEGURIDAD FISICA Y AMBIENTAL	11	4
A.12 SEGURIDAD DE LAS OPERACIONES	6	8
A. 13 SEGURIDAD EN LAS TELECOMUNICACIONES	6	1
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	1	12
A.15 RELACIONES CON LOS PROVEEDORES / SUMINISTRADORES	1	4
A.16 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION	3	4
A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO	3	1
A. 18 CUMPLIMIENTO	3	5
Total Controles	64	50

Por otro lado, en cuanto a los controles Técnicos Auxiliares (TA) propuestos para complementar los indicados en la norma ISO/IEC 27002:2013 asciende a 32 controles. El listado de los controles que aplican a los activos de información valorizados y su respectiva descripción son:

- **TA1. Ejecución de procedimientos para el uso de contraseñas fuertes:** Ejecutar procedimientos técnicos para evitar el Espionaje de contraseñas, ataques de contraseñas o métodos de cracking. El procedimiento es indicado dentro de la Política de Control de Acceso, en el apartado "Gestión de Contraseñas de Usuario", propuesto en el presente proyecto.
- **TA2. Limitar el número de acceso a contraseñas inválidas:** Ejecutar procedimientos técnicos para evitar el Espionaje de contraseñas, ataques de contraseñas o métodos de cracking. El procedimiento es indicado dentro de la Política de Control de Acceso, en el apartado "Gestión de Contraseñas de Usuario", propuesto en el presente proyecto.
- **TA3. Implementación de software de monitoreo de estado de salud y rendimiento de la aplicación:** La organización debe adquirir un software de monitoreo para la revisión de logs y recursos del sistema. Asimismo, este software permitirá evaluar el rendimiento de la aplicación mediante parámetros técnicos asociadas a su estructura.
- **TA4. Implementación de un Data Loss Prevention (DLP):** La organización debe contemplar la adopción de una solución de DLP (Data Loss Prevention) para la clasificación de Información y manejo adecuado de la misma dentro y fuera de la organización, ello en cumplimiento de las reglas o directrices indicadas por la misma.
- **TA5. Migración del Sistema de Gestión de Tickets en un servicio en la nube mediante IAAS:** La organización debe contemplar la aplicación y ejecución de uno de los modelos de Cloud Computing, es decir Infraestructura como Servicio (IaaS) y llevar el Servicio del Sistema de Gestión de Tickets a la nube, evitando gastos de capital y reduciendo los costos corrientes (energía, aire acondicionado, otros), por un pago mensual o anual según convenga.
- **TA6. Migración de copias legalizadas a proveedor de custodia de archivos:** La organización deberá tener en cuenta realizar copias físicas y digitales de contratos y/o archivos asociados a los Contratos de Servicios, Instalación, entre otros en custodia de un proveedor tercero, tal como: Hermes, Prosegur, entre otros que se encuentren disponibles en el mercado.
- **TA7. Implementación de software de auditoria de uso de datos de Carpeta de Proyectos:** La organización debe considerar la adopción de un software de auditoria

de uso de los datos contenidos dentro de la carpeta de proyectos. Esto incluye: uso, acceso, horario de acceso, entre otros datos relevantes para la auditoria.

- **TA8. Migración de la carpeta de proyectos bajo un servicio en la nube mediante IAAS:** La organización debe contemplar la aplicación y ejecución de uno de los modelos de Cloud Computing, es decir Infraestructura como Servicio (IaaS) y llevar el servidor FTP que contiene la Carpeta de Proyectos Servicio a la nube, evitando gastos de capital y reduciendo los costos corrientes (energía, aire acondicionado, otros), por un pago mensual o anual según convenga.
- **TA9. Despliegue de una solución de repositorio en la nube de acceso específico:** La organización debe contemplar una solución en donde pueda pasar los datos de la Carpeta de Proyectos a un repositorio en la nube y en ello categorizar su acceso mediante alternativas de acceso: confidencial, privada y pública de usuarios de la organización, para accesos dentro y fuera de la organización. Estas soluciones pueden ser tipo: Check Point Workspace u otras soluciones como CASB (Cloud Access Security Broker) para aplicaciones o recursos publicados propietarios.
- **TA10. Implementación de software de auditoria de uso de datos de Carpeta de Licitaciones:** La organización debe considerar la adopción de un software de auditoria de uso de los datos contenidos dentro de la carpeta de licitaciones. Esto incluye: uso, acceso, horario de acceso, entre otros datos relevantes para la auditoria.
- **TA11. Migración de la Carpeta de Licitaciones bajo un servicio en la nube mediante IAAS:** La organización debe contemplar la aplicación y ejecución de uno de los modelos de Cloud Computing, es decir Infraestructura como Servicio (IaaS) y llevar el servidor FTP que contiene la Carpeta de Licitaciones a la nube, evitando gastos de capital y reduciendo los costos corrientes (energía, aire acondicionado, otros), por un pago mensual o anual según convenga.
- **TA12. Implementación de software de auditoria de uso de datos de Carpetas de áreas Administrativas y Contabilidad:** La organización debe considerar la adopción de un software de auditoria de uso de los datos contenidos dentro de la Carpetas de Áreas Administrativas y Contabilidad. Esto incluye: uso, acceso, horario de acceso, entre otros datos relevantes para la auditoria.
- **TA13. Migración de la carpetas de áreas Administrativas y Contabilidad bajo un servicio en la nube mediante IAAS:** La organización debe contemplar la aplicación

y ejecución de uno de los modelos de Cloud Computing, es decir Infraestructura como Servicio (IaaS) y llevar el servidor FTP que contiene la Carpetas de Áreas Administrativas y Contabilidad a la nube, evitando gastos de capital y reduciendo los costos corrientes (energía, aire acondicionado, otros), por un pago mensual o anual según convenga.

- **TA14. Ingreso lógico de cada equipo de cómputo por medio del Directorio Activo:** Cada equipo de cómputo deberá ser unido al dominio de la organización vía el soporte del Active Directory. Ello para contar con una administración de despliegue de política de seguridad, despliegue de paquetes de actualización, accesos a carpetas de archivos seleccionados y otras funcionalidades de manera centralizada.
- **TA15. Implementación de una suite o solución de Endpoint para prevenir ataques de firmas comunes y de Día Cero:** La organización debe implementar una suite o solución de Endpoint para la protección y prevención contra ataques comunes y ataques de Día Cero (Zero Days). Esta solución deberá contar con módulos de seguridad como: AV, Antibot, IPS, Antimalware (prevención y protección contra ataques de día cero) y otros Blades o módulos de seguridad embebidos.
- **TA16. Implementación de una solución de respaldo de Endpoint o estaciones de trabajo y/o servidores:** La organización debe considerar la implementación de una solución de respaldo de estaciones finales de trabajo o Endpoint, esto mediante un agente instalado en el computador, apuntando el respaldo a un Storage local o en nube: Soluciones como Barracuda Backup, Veeam Backup, Veritas, entre otras. Todas las PC's asociadas a la plana de Gerentes, Jefes y usuarios finales deben tener un respaldo del contenido del computador sin excepción, esto para fines de recuperación y auditoría.
- **TA17. Implementación de un servidor centralizado para instalación de parches de seguridad:** La organización debe implementar un servidor centralizado para la instalación de parches de seguridad, esto programado de manera automática o ejecutada de manera manual. Con ello, evitar o disminuir fallas de seguridad asociadas a versiones de Sistema Operativos, específicamente Windows (Servidor centralizado WSUS) debido a que es el Sistema Operativo utilizado en la organización.

- **TA18. Implementación de una solución de Endpoint Encryption:** La organización debe contemplar implementar una solución de Endpoint Encryption (Encriptación de Endpoint o dispositivos finales) la cual ofrezca cifrado eficaz de disco completo y soportes extraíbles. Lo comentado mediante una administración centralizada para proteger la información confidencial y asegurar el cumplimiento normativo dentro de la organización.
- **TA19. Alquiler de equipos de cómputo:** La organización debe evaluar el alquiler de equipos de cómputo para transferir el riesgo de pérdida del equipo (80% aproximado en laptop, 20% aproximado en PC de escritorio), inoperatividad o fallas en su funcionamiento. Asimismo, los acuerdos con la empresa que alquila los equipos debe cubrir cambio ante fallas, pérdidas (seguro o póliza que aplique), fallas en su funcionamiento, cambio de piezas o partes del computador, cambio por obsolescencia, entre otros acuerdos.
- **TA20. Implementación de software de auditoria de uso del servicio de Correo Electrónico:** La organización debe considerar la adopción de un software de auditoria de uso o flujo de correos enviados y recibidos por los usuarios internos. Esto incluye: uso, acceso, envíos de correo, recepción de correos, horario de acceso, entre otros datos relevantes para la auditoria.
- **TA21. Implementación de un servicio o appliance de AntiSpam:** La organización debe considerar la adopción de un servicio o appliance dedicado para AntiSpam. Ello para el manejo de correos spam (basura o no deseados), así como también su uso para la protección contra código malicioso embebido dentro de los correos electrónicos, ya sea como adjunto, direccionamiento mediante un link de acceso, código malicioso incrustado dentro del cuerpo de correo, entre otras amenazas.
- **TA22. Migración del servicio de correo electrónico a la nube mediante SAAS:** La organización debe contemplar la aplicación y ejecución de uno de los modelos de Cloud Computing, es decir el Software como Servicio (SaaS) y llevar el Servicio del Correo Electrónico a la nube, evitando gastos de capital y reduciendo los costos corrientes (energía, aire acondicionado, otros), por un pago mensual o anual según convenga.
- **TA23. Implementación de software de monitoreo del consumo de internet:** La organización debe adquirir un software de monitoreo para la revisión y análisis del

consumo de Internet. Con ello, revisar en base a los reportes, quienes son los destinos más concurridos y su categorización de seguridad. Con ello, ajustar los accesos y disminuir el riesgo de infección o ataques de día cero provenientes de destinos previamente identificados como malignos.

- **TA24. Implementación de software de monitoreo del consumo de Internet:** La organización debe adquirir un software de monitoreo para la revisión y análisis del consumo de Internet. Con ello, revisar en base a los reportes, quienes son los destinos más concurridos y su categorización de seguridad. Con ello, ajustar los accesos y disminuir el riesgo de infección o ataques de día cero provenientes de destinos previamente identificados como malignos.
- **TA25. Implementación de una suite o Solución Perimetral para prevenir ataques de Día Cero:** La organización debe implementar una suite o solución de perimetral para la protección y prevención contra ataques de Dia Cero (Zero Days). Esta solución deberá contar con módulos de seguridad de antimalware, ya sea en un despliegue de appliance físico o un análisis ejecutado en la nube del fabricante.
- **TA26. Implementación de software de auditoria de uso de los contenidos de los equipos de Infraestructura de Comunicaciones:** La organización debe considerar la adopción de un software de auditoria de uso de los datos contenidos dentro de los equipos que componen la Infraestructura de Comunicaciones (Incluye servidores). Esto incluye: uso, acceso, horario de acceso, entre otros datos relevantes para la auditoria.
- **TA27. Ingreso lógico del Servidor de Archivos por medio del Directorio Activo:** El servidor de archivos deberá ser unido al dominio de la organización vía el soporte del Active Directory. Ello para contar con una administración de despliegue de política de seguridad, despliegue de paquetes de actualización, accesos a carpetas de archivos seleccionados y otras funcionalidades de manera centralizada.
- **TA28. Migración del servicio de FTP bajo un servicio en la nube mediante IAAS:** La organización debe contemplar la aplicación y ejecución de uno de los modelos de Cloud Computing, es decir Infraestructura como Servicio (IaaS) y llevar el servidor FTP que contiene las distintas carpetas de datos con información de la organización a la nube, evitando gastos de capital y reduciendo los costos corrientes (energía, aire acondicionado, otros), por un pago mensual o anual según convenga.

- **TA29. Ingreso lógico del Servidor de Archivos por medio del Directorio Activo:** Los servidores que componen la Infraestructura de Comunicaciones deberán ser unido al dominio de la organización vía el soporte del Active Directory. Ello para contar con una administración de despliegue de política de seguridad, despliegue de paquetes de actualización, accesos a carpetas de archivos seleccionados y otras funcionalidades de manera.
- **TA30. Evaluación e implementación de un data center alternativo:** La organización debe evaluar un Site Alternativo o Data Center Alternativo en el cual se pueda sostener la operación de los servicios más críticos que dan continuidad al negocio, esto ante alguna eventualidad de para de continuidad de labores, desastre natural, ataque cibernético o cualquier ataque que atente contra la continuidad del negocio.
- **TA31. Adopción de sistema de simulación de ejecución de Phishing:** La organización debe adoptar un sistema de preparación contra Phishing para evaluar a los empleados respecto a la que acciones tomar ante esta clase de ataques cibernéticos. Para ello, es necesario para establecer una línea base que permita implementar un programa eficaz de preparación contra el Phishing. Tomar como referencia el "Phishing Readiness Services" del fabricante Symantec.
- **TA32. Programas de información sobre técnicas de ataques de Ingeniería Social:** La organización debe plantear programas de capacitación al personal de la empresa en donde se explique y detalle las técnicas de ataques de Ingeniería Social utilizadas por los delincuentes informáticos.

El análisis del SOA en cuanto a la distribución de controles de la norma y propuestos serán expuestos en el siguiente capítulo: "Evaluación y Validación de Resultados".

4.4.10. Manual del Sistema de Gestión de Seguridad de la Información

4.4.10.1. Objetivo

El Manual del Sistema de Gestión de Seguridad de la Información es mostrar las directivas, acciones, lineamientos y políticas a seguir para la posterior implementación de un Sistema de Gestión de Seguridad de la Información. Lo comentado, con el objetivo principal de minimizar las vulnerabilidades y amenazas de seguridad de la información presentes sobre los activos de información de la organización.

4.4.10.2. Alcance del Manual de Seguridad de la Información

El alcance del presente manual, el cual se basa en los lineamientos solicitados por la norma ISO/IEC 27001:2013 tiene como alcance el proceso de Servicio Post-Venta de la organización. Asimismo, el contenido del presente manual como información e instructivo, aplica a todo el personal o colaboradores de la organización. El desarrollo, estructura y desglose del documento se encuentra en al “**Anexo A**”, adjunto al presente proyecto. Ello, puede ser revisado a cabalidad para los fines que sean pertinentes.

CAPÍTULO 5: EVALUACIÓN Y VALIDACIÓN DE LA PROPUESTA

5.1. Introducción

El presente capítulo introduce a las pruebas y los medios necesarios utilizados para comprobar que los objetivos específicos planteados logren satisfacer sus indicadores de logro de objetivos trazados. Asimismo, mostrar y evidenciar que las métricas planteadas en estos objetivos al inicio del proyecto sean coherentes con los valores fijados inicialmente.

5.2. Flujo de trabajo para la evaluación y validación de la propuesta

Para poder cumplir con los objetivos, indicadores y métricas planteadas en los objetivos del presente proyecto, se propone un flujo de trabajo en donde se da secuencia a las fases y componentes necesarios para su éxito. El flujo de trabajo es mostrado a continuación:

Figura 30: Flujo de trabajo para Evaluación y Validación de la Propuesta

Fuente: Elaboración propia

Del gráfico podemos mostrar lo siguiente:

- **Plan de Pruebas:** En esta primera fase se selecciona el método de validación necesario para hacer frente al objetivo específico en estudio. Asimismo, se mencionan que actividades y recursos son necesarios para poder realizar la evaluación respectiva. Por último, se fija una fecha de ejecución de las actividades a ejecutar con la finalidad de que

la organización disponga de los elementos necesarios con anticipación para el éxito de las pruebas posteriores.

- **Ejecución:** En esta fase se da actividad y ejecución al método de validación seleccionado. Como la razón de ser del presente proyecto es diseñar un Sistema de Gestión de Seguridad de la Información, no se incluye la implementación de los controles indicados en el “Anexo A” de la norma ISO/IEC 27001:2013, ni los controles Técnicos Auxiliares (TA) propuestos. En base a ello, el método de validación utilizado será “Pruebas de escritorio” para la gestión de pruebas de activos de información y la determinar de riesgo de seguridad de la información sobre los activos que soportan el proceso de Servicio Post-Venta. En ello se realizará entrevistas no estructuradas entre los integrantes de:
 - Alta Dirección
 - Gerencia General
 - Estructura Organizacional de Sistema de Gestión de Seguridad de la Información
 - Personal que interactúa constantemente con los activos de información y conocedores del proceso de Servicio Post-Venta
- **Resultados y Validación:** En esta fase se revisan los resultados obtenidos de las pruebas realizadas y se valida con los indicadores y métricas de logro de objetivo trazados.
- **Plan de Mejoras:** En esta fase, la cual realimenta a la fase de Plan de Pruebas ya que puede ser usado como un ciclo de mejora continua para las pruebas y validación, se proponen mejoras respecto a los objetivos específicos analizados (de aplicarse).

5.3. Análisis de los Objetivos específicos trazados y métricas asociadas

En este apartado se analiza, en base al flujo de trabajo para la evaluación y validación de la propuesta, cada uno de los cinco (05) objetivos específicos mencionados en la sección 1.6.2 del Capítulo I: “Estructuración del Plan de Tesis”. Lo comentado se desarrolla a continuación:

5.3.1. Objetivo Específico I

El Objetivo Especifico I se muestra en la siguiente tabla:

Tabla 36: Indicadores y Métricas de Logro de Objetivo I

Objetivo Específico	Indicador de logro de Objetivo	Métrica de logro de Objetivo
Clasificar los principales activos de información del proceso de Servicios Post-Venta en base a la metodología de evaluación de riesgos aplicada.	Clasificación de los activos de información en base a los pilares de la Seguridad de la Información, tales son: confidencialidad, integridad y su disponibilidad.	Porcentaje de activos de información con niveles de valoración de "Muy Altos" y "Altos" sobre el total de activos que componen el Inventario de Activos de Información.

Fuente: Elaboración propia

5.3.1.1. Plan de Pruebas

En el capítulo anterior se desarrolló el Inventario de Activos de Información en base a la metodología de Gestión de Riesgos utilizada, en el cual se determinó trece (13) activos de información dentro del inventario de activos realizados. En base a ello, este objetivo tiene como finalidad la clasificación de los principales activos de información asociados al proceso de servicios Post-Venta de la organización en base a los pilares de la Seguridad de Información, es decir la valoración de los mismos. En base a ese inventario, su flujo trabajo para su evaluación y validación se muestra en la siguiente tabla:

Tabla 37: Matriz de Plan de Pruebas para el Objetivo Especifico I

Objetivo Específico	Método de Validación	Integrantes	Actividades a Desarrollar	Preguntas de Rigor	Recursos Necesarios	Fecha de Ejecución
OE1: Clasificar los principales activos de información del proceso de Servicios Post-Venta en base a la metodología de evaluación de riesgos aplicada	Pruebas de Escritorio: Revisión y verificación de la valoración de los Activos de Información en base a los pilares de Seguridad de la Información, tales son: Confidencialidad, Integridad y Disponibilidad de los activos de información del proceso de Servicio Post-Venta. Lo comentado, en base a la metodología de Gestión y Evaluación de Riesgos utilizada	Alta Dirección, Gerencia General, integrantes de la Estructura Organizacional de Sistema de Gestión de Seguridad de la Información y personal que interactúa constantemente con los activos de información y conocedores del proceso de Servicio Post-Venta	Actividad #1: Entrevistas no estructuradas (libre y con preguntas abiertas) entre los participantes sobre la operatividad, desempeño y el flujo de trabajo del activo de información dentro del proceso de Servicio Post-Venta	¿Cuál es el rol del activo de información dentro del proceso de Servicio Post-Venta? ¿Qué tan importante o crítico es el activo de información dentro del proceso de Servicio Post-Venta?	- Revisión del rol del activo de información dentro del proceso de Servicio Post-Venta	Rango de días entre el 18 y 22 de diciembre del 2017
		Alta Dirección, Gerencia General, integrantes de la Estructura Organizacional de Sistema de Gestión de Seguridad de la Información y personal que interactúa constantemente con los activos de información y conocedores del proceso de Servicio Post-Venta	Actividad #2: Entrevistas no estructuradas (libre y con preguntas abiertas) sobre qué tan importante es la confidencialidad de los datos que contiene el activo de información o el propio activo de información dentro del proceso de Servicio Post-Venta, en consecuencia dentro de la organización	En una escala de puntuación del 1 al 5 donde los valores representativos son: 1: Muy Bajo. 2: Bajo 3: Medio 4: Alto 5: Muy Alto ¿Cuál es la puntuación para la integridad de los datos o el propio activo de información dentro del proceso de servicio Post-Venta?	- Revisión de Mapas de Procesos Internos del flujo de operación del activo (de aplicar) - Autorización de reunión para ejecutar las pruebas correspondientes - Cuarto de Reunión para ejecutar las Pruebas de Escritorio	Rango de días entre el 18 y 22 de diciembre del 2018

Objetivo Específico	Método de Validación	Integrantes	Actividades a Desarrollar	Preguntas de Rigor	Recursos Necesarios	Fecha de Ejecución
		Alta Dirección, Gerencia General, integrantes de la Estructura Organizacional de Sistema de Gestión de Seguridad de la Información y personal que interactúa constantemente con los activos de información y conocedores del proceso de Servicio Post-Venta	Actividad #3: Entrevistas no estructuradas (libre y con preguntas abiertas) sobre qué tan importante es la confidencialidad de los datos que contiene el activo de información o el propio activo de información dentro del proceso de Servicio Post-Venta, en consecuencia dentro de la organización	En una escala de puntuación del 1 al 5 donde los valores representativos son: 1: Muy Bajo. 2: Bajo 3: Medio 4: Alto 5: Muy Alto ¿Cuál es la puntuación para la integridad de los datos o el propio activo de información dentro del proceso de servicio Post-Venta?		Rango de días entre el 18 y 22 de diciembre del 2019
		Alta Dirección, Gerencia General, integrantes de la Estructura Organizacional de Sistema de Gestión de Seguridad de la Información y personal que interactúa constantemente con los activos de información y conocedores del proceso de Servicio Post-Venta	Actividad #4: Entrevistas no estructuradas (libre y con preguntas abiertas) sobre qué tan importante es la disponibilidad de los datos que contiene el activo de información o el propio activo de información dentro del proceso de Servicio Post-Venta, en consecuencia dentro de la organización	En una escala de puntuación del 1 al 5 donde los valores representativos son: 1: Muy Bajo. 2: Bajo 3: Medio 4: Alto 5: Muy Alto ¿Cuál es la puntuación para la disponibilidad de los datos o el propio activo de información dentro del proceso de servicio Post-Venta?		Rango de días entre el 18 y 22 de diciembre del 2020

Fuente: Elaboración propia

5.3.1.2. Ejecución

Dentro del Plan de Pruebas propuesto interactúan los siguientes integrantes:

- **A:** Alta Dirección
- **B:** Gerencia General
- **C:** Integrantes de la Estructura Organizacional de Sistema de Gestión de Seguridad de la Información
- **D:** Personal que interactúa constantemente con los activos de información y conocedores del proceso de Servicio Post-Venta

En base a ello, se da puntajes a los activos de información del proceso. El detalle de esta ejecución de pruebas puede revisarse en el “**Anexo VIII**”: Ejecución de Pruebas de Escritorio para Objetivo Especifico I, el mismo que se muestra a continuación:

Tabla 38: Ejecución de Pruebas de Escritorio para Objetivo Especifico I

IDENTIFICACIÓN DEL ACTIVO		PRUEBAS DE ESCRITORIO	VALORACIÓN DEL ACTIVO						
No	Nombre del Activo	Integrantes	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	á IMPACTO	IMPACTO	INTERPRETACIÓN IMPACTO	IMPACTO RESULTANTE
1	Sistema de Gestión de Tickets	A	5	5	5	15	5	MUY ALTO	MUY ALTO
		B	5	5	5	15	5	MUY ALTO	
		C	5	5	5	15	5	MUY ALTO	
		D	5	5	5	15	5	MUY ALTO	
2	Contratos de Servicios, Instalación, entre otros	A	5	5	5	15	5	MUY ALTO	MUY ALTO
		B	5	5	5	15	5	MUY ALTO	
		C	4	4	4	12	4	ALTO	
		D	5	5	5	15	5	MUY ALTO	
3	Carpetas de proyectos	A	5	5	5	15	5	MUY ALTO	MUY ALTO
		B	5	5	5	15	5	MUY ALTO	
		C	5	5	5	15	5	MUY ALTO	
		D	4	5	5	14	5	MUY ALTO	
4	Carpeta de Licitaciones	A	5	5	5	15	5	MUY ALTO	MUY ALTO
		B	5	5	5	15	5	MUY ALTO	
		C	5	5	5	15	5	MUY ALTO	
		D	4	5	5	14	5	MUY ALTO	
5	Carpetas de Áreas Administrativas y Contabilidad	A	5	5	5	15	5	MUY ALTO	MUY ALTO
		B	5	5	5	15	5	MUY ALTO	
		C	5	5	5	15	5	MUY ALTO	
		D	5	5	5	15	5	MUY ALTO	
6	Equipos de Computo	A	4	4	4	12	4	ALTO	ALTO
		B	3	4	5	12	4	ALTO	
		C	5	5	3	13	5	MUY ALTO	
		D	4	4	3	11	4	ALTO	
7	Correo	A	5	5	5	15	5	MUY ALTO	MUY ALTO

IDENTIFICACIÓN DEL ACTIVO		PRUEBAS DE ESCRITORIO	VALORACIÓN DEL ACTIVO						
	Electrónico	B	5	5	5	15	5	MUY ALTO	
		C	5	5	5	15	5	MUY ALTO	
		D	5	4	4	13	5	MUY ALTO	
8	Internet / Servicios Dedicados	A	3	3	5	11	4	ALTO	ALTO
		B	4	4	4	12	4	ALTO	
		C	4	4	4	12	4	ALTO	
		D	4	4	3	11	4	ALTO	
9	Sistema de Gestión de movilidad	A	5	5	5	15	5	MUY ALTO	MEDIO
		B	1	1	4	6	2	BAJO	
		C	3	3	3	9	3	MEDIO	
		D	2	3	2	7	3	MEDIO	
10	File Server (Servidor de Archivos)	A	4	4	4	12	4	ALTO	MUY ALTO
		B	4	4	4	12	4	MUY ALTO	
		C	5	5	5	15	5	MUY ALTO	
		D	5	4	5	14	5	MUY ALTO	
11	Infraestructura de Comunicaciones	A	5	4	4	13	5	MUY ALTO	MUY ALTO
		B	4	4	4	12	4	ALTO	
		C	5	5	5	15	5	MUY ALTO	
		D	5	4	4	13	5	MUY ALTO	
12	Personal	A	5	5	5	15	5	MUY ALTO	MUY ALTO
		B	5	5	5	15	5	MUY ALTO	
		C	5	5	5	15	5	MUY ALTO	
		D	5	4	4	13	5	MUY ALTO	
13	Imagen de la Organización	A	4	4	4	12	4	ALTO	MEDIO
		B	4	4	4	12	4	ALTO	
		C	2	2	2	6	2	BAJO	
		D	3	3	3	9	3	MEDIO	

5.3.1.3. Resultados y Validación

Tal como se observa en la última columna de la tabla anterior, se muestra el impacto resultante respecto a la confidencialidad, integridad y disponibilidad de cada activo de información inventariado. El resultado se analiza según lo mostrado a continuación:

$$IR_t = (IIA + IIB + IIC + IID) / 4$$

Donde:

- **IRt:** Impacto Resultante total sobre el activo de Información
- **IIA:** Interpretación del Impacto sobre el activo de según la puntuación establecida por A (Alta Dirección)
- **IIB:** Interpretación del Impacto sobre el activo de según la puntuación establecida por B (Gerencia General)
- **IIC:** Interpretación del Impacto sobre el activo de según la puntuación establecida por C (Estructura Organizacional del Sistema de Gestión de Seguridad de la Información)
- **IID:** Interpretación del Impacto sobre el activo de según la puntuación establecida por D (Personal que interactúa con el activo de información y conoce el proceso de Servicio Post-Venta)
- **Nota:** Tener en cuenta las puntuaciones según la metodología de gestión de riesgos para los valores de Impacto del Activo de Información.

En base a ello, en resumen para cada activo de información se obtiene el siguiente resultado:

Tabla 39: Activos de Información Valorizados

IDENTIFICACIÓN DEL ACTIVO		PRUEBAS DE ESCRITORIO	RESULTADOS	
No	Nombre del Activo	Integrantes	INTERPRETACIÓN IMPACTO	IMPACTO RESULTANTE
1	Sistema de Gestión de Tickets	A	MUY ALTO	MUY ALTO
		B	MUY ALTO	
		C	MUY ALTO	
		D	MUY ALTO	
2	Contratos de Servicios, Instalación, entre otros	A	MUY ALTO	MUY ALTO
		B	MUY ALTO	
		C	ALTO	
		D	MUY ALTO	

IDENTIFICACIÓN DEL ACTIVO		PRUEBAS DE ESCRITORIO	RESULTADOS	
3	Carpetas de proyectos	A	MUY ALTO	MUY ALTO
		B	MUY ALTO	
		C	MUY ALTO	
		D	MUY ALTO	
4	Carpeta de Licitaciones	A	MUY ALTO	MUY ALTO
		B	MUY ALTO	
		C	MUY ALTO	
		D	MUY ALTO	
5	Carpetas de Áreas Administrativas y Contabilidad	A	MUY ALTO	MUY ALTO
		B	MUY ALTO	
		C	MUY ALTO	
		D	MUY ALTO	
6	Equipos de Computo	A	ALTO	ALTO
		B	ALTO	
		C	MUY ALTO	
		D	ALTO	
7	Correo Electrónico	A	MUY ALTO	MUY ALTO
		B	MUY ALTO	
		C	MUY ALTO	
		D	MUY ALTO	
8	Internet / Servicios Dedicados	A	ALTO	ALTO
		B	ALTO	
		C	ALTO	
		D	ALTO	
9	Sistema de Gestión de movilidad	A	MUY ALTO	MEDIO
		B	BAJO	
		C	MEDIO	
		D	MEDIO	
10	File Server (Servidor de Archivos)	A	ALTO	MUY ALTO
		B	MUY ALTO	
		C	MUY ALTO	
		D	MUY ALTO	
11	Infraestructura de Comunicaciones	A	MUY ALTO	MUY ALTO
		B	ALTO	
		C	MUY ALTO	
		D	MUY ALTO	
12	Personal	A	MUY ALTO	MUY ALTO
		B	MUY ALTO	
		C	MUY ALTO	
		D	MUY ALTO	
13	Imagen de la Organización	A	ALTO	MEDIO
		B	ALTO	
		C	BAJO	
		D	MEDIO	

De los resultados obtenidos, se desprenden las siguientes cifras:

- **Activos de Información de criticidad o impacto “Muy Alto”:** 9, el cual representa el 70% aproximadamente.
- **Activos de Información de criticidad o impacto “Alto”:** 2, el cual representa el 15% aproximadamente.
- **Activos de Información de criticidad o impacto “Medio”:** 2, el cual representa el 15% aproximadamente.
- **Activos de Información de criticidad o impacto “Bajo”:** 0, el cual representa el 0%.
- **Activos de Información de criticidad o impacto “Muy Bajo”:** 0, el cual representa el 0%.

De la identificación y valoración de activos y en concordancia con la métrica de logro de objetivo se obtiene el porcentaje de activos valorados en criticidad o impacto como “Altos” y “Muy Altos”, tal como se muestra a continuación:

Figura 31: Porcentaje de Activos según su criticidad o impacto

Fuente: Elaboración propia

5.3.1.4. Plan de Mejoras:

Debido a que el presente trabajo no incluye la implementación del SGSI, sino su diseño, no se incluye mejoras de implementación. Sin embargo, dentro de las pruebas de escritorio realizadas, mientras la organización no decida implementar el SGSI, se recomienda realizar en plazos de 03-04 nuevas pruebas a las ya realizadas, esto debido a que puede haber algún

activo de información que en el tiempo varió su criticidad o impacto en el negocio o para la misma organización es más crítico después del análisis ya realizado.

5.3.2. Objetivo Específico II

El Objetivo Especifico II se muestra en la siguiente tabla:

Tabla 40: Indicadores y Métricas de logro de Objetivo Específico II

Objetivo Específico	Indicador de logro de Objetivo	Métrica de logro de Objetivo
Determinar el riesgo de seguridad de la información sobre los activos que soportan el proceso de Servicio Post-Venta.	Principales vulnerabilidades de seguridad de la información identificadas y el impacto que tendría la ejecución de alguna amenaza sobre el activo de información valorizado en caso de materializarse.	Porcentaje de activos de información con Interpretación de Riesgo "Muy Alto" y "Alto", y Nivel de Aceptación del Riesgo "Importante" y "Considerable" sobre el total de activos de información que componen la Matriz de Riesgo realizada

Fuente: Elaboración propia

5.3.2.1 Plan de Pruebas

Dentro del Plan de Pruebas previo ejecutado para los activos de información inventariados, se realizaron las pruebas correspondientes para establecer los niveles de criticidad o impacto sobre los mismos. Lo comentado, es parte fundamental para hallar los niveles de riesgos sobre los activos de información, ello teniendo en cuenta que el riesgo es el resultado de la probabilidad de la materialización de una amenaza y el impacto que generaría sobre el mismo.

Por otro lado, tal como se comentó en el apartado 4.4.3.3 “Análisis e Identificación de Vulnerabilidades y Amenazas”, para conocer las vulnerabilidades y amenazas sobre los activos de información se toma en consideración lo siguiente:

- Entrevistas no estructuradas con las personas que interactúan día a día con los activos de información sobre su operatividad, desempeño y el flujo de trabajo dentro de los procesos en estudio.

- Fuentes estadísticas y tendencias de los riesgos de seguridad y privacidad de los activos, basados en buenas prácticas e información relevante sobre seguridad de activos de información.
- Observaciones de expertos y analistas, y sobre todo opinión de personal involucrado en el desempeño y utilización del activo de información.
- Estudio de los procedimientos, guías y diagramas de información asociados al activo de información.
- Establecimiento de la criticidad del activo y su tratamiento por parte de las personas, los procesos y la tecnología, gestión de riesgos realizados anteriormente

En base a ello, ya contando con las vulnerabilidades y amenazas de seguridad sobre los activos de información, las cuales pueden revisarse en detalle el apartado 4.4.6.1 “Vulnerabilidades” y 4.4.6.2 “Amenazas”, o recurrir al Anexo II: “Cuadro de Vulnerabilidades y Amenazas”, el flujo trabajo para su evaluación y validación del presente Objetivo Especifico se muestra en la siguiente tabla:

Tabla 41: Matriz de Plan de Pruebas para el Objetivo Especifico II

Objetivo Especifico	Método de Validación	Integrantes	Actividades a Desarrollar	Preguntas de Rigor	Recursos Necesarios	Fecha de Ejecución
OE2: Determinar el riesgo de seguridad de la información sobre los activos que soportan el proceso de Servicio Post-Venta.	<p>Pruebas de Escritorio que incluyen:</p> <ul style="list-style-type: none"> - Revisión y verificación de las vulnerabilidades y amenazas a las que están expuestos los activos de información inventariados y valorizados del proceso de Servicio Post-Venta. - Analizar los cálculos de probabilidad del riesgo de la materialización de una amenaza sobre el activo de información. - Cuantificar los valores de riesgo total sobre el activo de información para definir el nivel de aceptación del riesgo. 	Alta Dirección, Gerencia General, integrantes de la Estructura Organizacional de Sistema de Gestión de Seguridad de la Información y personal que interactúa constantemente con los activos de información y conocedores del proceso de Servicio Post-Venta	Actividad #1: Toma de datos de los resultados del Plan de Pruebas realizado en la valoración de Activos de Información anterior. Ello respecto a los niveles de puntuación de confidencialidad, integridad y disponibilidad sobre el activo de información, es decir su criticidad o impacto sobre el activo	No aplica el procedimiento ya fue realizado en el Plan de Pruebas del Objetivo Especifico I (OEI)	<ul style="list-style-type: none"> - Revisión del rol del activo de información dentro del proceso de Servicio Post-Venta - Revisión de Mapas de Procesos Internos del flujo de operación del activo (de aplicar) - Importancia del activo de información dentro del proceso de negocio 	Rango de días entre el 25 y 29 de diciembre del 2017
		Alta Dirección, Gerencia General, integrantes de la Estructura Organizacional de Sistema de Gestión de Seguridad de la Información y personal que interactúa constantemente con los activos de información y conocedores del proceso de Servicio Post-Venta	Actividad #2: Después de haber identificado las vulnerabilidades y amenazas sobre los Activos de Información se realizarán preguntas grupales sobre cuáles creen que es el valor de probabilidad de cada riesgo sobre los datos que contiene el activo de información o el propio activo de información dentro del proceso de Servicio Post-Venta, en consecuencia dentro de la organización	En una escala de puntuación del 1 al 5 donde los valores representativos son: 1: Muy Bajo. 2: Bajo 3: Medio 4: Alto 5: Muy Alto ¿Cuál es la puntuación para la probabilidad de cada riesgo sobre los datos o el propio activo de información dentro del proceso de servicio Post-Venta?	<ul style="list-style-type: none"> - Listado de vulnerabilidades y amenazas sobre el activo de información - Autorización de reunión para ejecutar las pruebas correspondientes - Cuarto de Reunión para ejecutar las Pruebas de Escritorio 	Rango de días entre el 25 y 29 de diciembre del 2017

Objetivo Específico	Método de Validación	Integrantes	Actividades a Desarrollar	Preguntas de Rigor	Recursos Necesarios	Fecha de Ejecución
		Alta Dirección, Gerencia General, integrantes de la Estructura Organizacional de Sistema de Gestión de Seguridad de la Información y personal que interactúa constantemente con los activos de información y conocedores del proceso de Servicio Post-Venta	Actividad #3: Realizar la suma total de cada uno de los riesgos asociados a la materialización de una amenaza sobre cada activo de información. La sumatoria será revisada en la opción de "Escala" de la Tabla 25 para verificar su rango de riesgos total sobre el mismo, ello en denominaciones de "Bajo" "Muy Bajo", "Medio", "Alto" y "Muy Alto".	De cada activo de información analizado en base a sus riesgos asociados ¿Cuál es la sumatorio total de los riesgos individuales? Según la puntuación, El resultado determinará la interpretación de la probabilidad del riesgo sobre el Activo de Información.		Rango de días entre el 25 y 29 de diciembre del 2017
		Alta Dirección, Gerencia General, integrantes de la Estructura Organizacional de Sistema de Gestión de Seguridad de la Información y personal que interactúa constantemente con los activos de información y conocedores del proceso de Servicio Post-Venta	Actividad #4: Realizar el producto del impacto o criticidad sobre el activo de información versus la probabilidad de riesgo de la materialización de una amenaza sobre el activo de información. El resultante del producto se revisará en la Tabla 27 y se verificará su valor de riesgo total y su nivel de aceptación de riesgos para la organización.	De cada activo de información analizado en base al producto del impacto o criticidad del activo versus la probabilidad de riesgo total sobre el activo ¿Cuál es su nivel de aceptación del Riesgo? Los resultados variaran en el rango de: Insignificante, considerable o importante para la organización.		Rango de días entre el 25 y 29 de diciembre del 2017

Fuente: Elaboración propia

5.3.2.2. Ejecución

Dentro del Plan de Pruebas propuesto interactúan los siguientes integrantes:

- **A:** Alta Dirección
- **B:** Gerencia General
- **C:** Integrantes de la Estructura Organizacional de Sistema de Gestión de Seguridad de la Información
- **D:** Personal que interactúa constantemente con los activos de información y conocedores del proceso de Servicio Post-Venta

En base a ello, se da puntajes a los activos de información del proceso. El detalle de esta ejecución de pruebas puede revisarse en el “**Anexo IX**”: Ejecución de Pruebas de Escritorio para Objetivo Específico II, el mismo que se muestra a continuación:

Tabla 42: Matriz de Plan de Pruebas para el Objetivo Especifico II

RIESGOS			YULNERABILIDADES	Σ PROBABILIDAD DEL RIESGO	PROBABILIDAD DEL RIESGO	INTERPRETACIÓN DE LA PROBABILIDAD DEL RIESGO	NIVEL DE RIESGO (IMPACTO * PROBABILIDAD)	INTERPRETACIÓN DEL RIESGO	NIVEL DE ACEPTACIÓN DEL RIESGO
ACTIVO	INTEGRANTE	IMPACTO DEL ACTIVO	INTERPRETACIÓN DEL IMPACTO						
Sistema de Gestión de Tickets	A	5	MUY ALTO	63	4	ALTO	20	MUY ALTO	IMPORTANTE
	B	5	MUY ALTO	67	4	ALTO	20	MUY ALTO	IMPORTANTE
	C	5	MUY ALTO	67	4	ALTO	20	MUY ALTO	IMPORTANTE
	D	5	MUY ALTO	61	4	ALTO	20	MUY ALTO	IMPORTANTE
Contratos de Servicios, Instalación, entre otros	A	5	MUY ALTO	30	2	BAJO	10	ALTO	CONSIDERABLE
	B	5	MUY ALTO	31	2	BAJO	10	ALTO	CONSIDERABLE
	C	4	ALTO	32	2	BAJO	8	MEDIO	CONSIDERABLE
	D	5	MUY ALTO	35	2	BAJO	10	ALTO	CONSIDERABLE
Carpeta de Proyectos	A	5	MUY ALTO	42	3	MEDIO	15	ALTO	CONSIDERABLE
	B	5	MUY ALTO	41	3	MEDIO	15	ALTO	CONSIDERABLE
	C	5	MUY ALTO	41	3	MEDIO	15	ALTO	CONSIDERABLE
	D	5	MUY ALTO	45	3	MEDIO	15	ALTO	CONSIDERABLE

RIESGOS			VULNERABILIDADES	Z PROBABILIDAD DEL RIESGO	PROBABILIDAD DEL RIESGO	INTERPRETACIÓN DE LA PROBABILIDAD DEL RIESGO	NIVEL DE RIESGO (IMPACTO * PROBABILIDAD)	INTERPRETACIÓN DEL RIESGO	NIVEL DE ACEPTACIÓN DEL RIESGO
ACTIVO	INTEGRANTE	IMPACTO DEL ACTIVO	INTERPRETACIÓN DEL IMPACTO						
Carpeta de Licitaciones	A	5	MUY ALTO	42	3	MEDIO	15	ALTO	CONSIDERABLE
	B	5	MUY ALTO	42	3	MEDIO	15	ALTO	CONSIDERABLE
	C	5	MUY ALTO	42	3	MEDIO	15	ALTO	CONSIDERABLE
	D	5	MUY ALTO	45	3	MEDIO	15	ALTO	CONSIDERABLE
Carpetas de Áreas Administrativas y Contabilidad	A	5	MUY ALTO	41	3	MEDIO	15	ALTO	CONSIDERABLE
	B	5	MUY ALTO	41	3	MEDIO	15	ALTO	CONSIDERABLE
	C	5	MUY ALTO	42	3	MEDIO	15	ALTO	CONSIDERABLE
	D	5	MUY ALTO	45	3	MEDIO	15	ALTO	CONSIDERABLE
Equipos de Computo	A	4	ALTO	60	3	MEDIO	12	ALTO	CONSIDERABLE
	B	4	ALTO	60	3	MEDIO	12	ALTO	CONSIDERABLE
	C	5	MUY ALTO	68	4	ALTO	20	MUY ALTO	IMPORTANTE
	D	4	ALTO	59	3	MEDIO	12	ALTO	CONSIDERABLE
Correo Electrónico	A	5	MUY ALTO	60	3	MEDIO	15	ALTO	IMPORTANTE
	B	5	MUY ALTO	62	4	ALTO	20	MUY ALTO	IMPORTANTE
	C	5	MUY ALTO	61	4	ALTO	20	MUY ALTO	IMPORTANTE
	D	5	MUY ALTO	64	4	ALTO	20	MUY ALTO	IMPORTANTE

RIESGOS			VULNERABILIDADES	Σ PROBABILIDAD DEL RIESGO	PROBABILIDAD DEL RIESGO	INTERPRETACIÓN DE LA PROBABILIDAD DEL RIESGO	NIVEL DE RIESGO (IMPACTO * PROBABILIDAD)	INTERPRETACIÓN DEL RIESGO	NIVEL DE ACEPTACIÓN DEL RIESGO
ACTIVO	INTEGRANTE	IMPACTO DEL ACTIVO	INTERPRETACIÓN DEL IMPACTO						
Internet / Servicios dedicados	A	4	ALTO	32	2	BAJO	8	MEDIO	CONSIDERABLE
	B	4	ALTO	30	2	BAJO	8	MEDIO	CONSIDERABLE
	C	4	ALTO	31	2	BAJO	8	MEDIO	CONSIDERABLE
	D	4	ALTO	35	2	BAJO	8	MEDIO	CONSIDERABLE
File Server (Servidor de Archivos)	A	4	ALTO	45	3	MEDIO	12	ALTO	CONSIDERABLE
	B	5	MUY ALTO	45	3	MEDIO	15	ALTO	CONSIDERABLE
	C	5	MUY ALTO	45	3	MEDIO	15	ALTO	CONSIDERABLE
	D	5	MUY ALTO	48	3	MEDIO	15	ALTO	CONSIDERABLE
Infraestructura de Comunicaciones	A	5	MUY ALTO	40	2	BAJO	10	ALTO	CONSIDERABLE
	B	4	ALTO	40	2	BAJO	8	MEDIO	CONSIDERABLE
	C	5	MUY ALTO	39	2	BAJO	10	ALTO	CONSIDERABLE
	D	5	MUY ALTO	40	2	BAJO	10	ALTO	CONSIDERABLE
Personal	A	5	MUY ALTO	24	2	BAJO	10	ALTO	CONSIDERABLE
	B	5	MUY ALTO	22	2	BAJO	10	ALTO	CONSIDERABLE
	C	5	MUY ALTO	22	2	BAJO	10	ALTO	CONSIDERABLE
	D	5	MUY ALTO	23	2	BAJO	10	ALTO	CONSIDERABLE

5.3.2.3. Resultados y Validación

Dentro de las operaciones realizadas en la Matriz de Gestión de Riesgos, se realiza el siguiente cálculo:

- **La Interpretación del Riesgo Resultante:** El resultado se analiza según lo mostrado a continuación:

$$\text{IRrT} = (\text{IRrA} + \text{IRrB} + \text{IRrC} + \text{IRrD}) / 4$$

Donde:

- **IRrT:** Interpretación del Riesgo Resultante Total sobre el activo de Información analizado
- **IRrA:** Interpretación del Riesgo Resultante sobre el activo de Información analizado según la puntuación establecida por A (Alta Dirección)
- **IRrB:** Interpretación del Riesgo Resultante sobre el activo de Información analizado según la puntuación establecida por B (Gerencia General)
- **IRrC:** Interpretación del Riesgo Resultante sobre el activo de Información analizado según la puntuación establecida por C (Estructura Organizacional del Sistema de Gestión de Seguridad de la Información)
- **IRrD:** Interpretación del Riesgo Resultante sobre el activo de Información analizado según la puntuación establecida por D (Personal que interactúa con el activo de información y conoce el proceso de Servicio Post-Venta)
- **El Nivel de Aceptación del Riesgo Resultante:** El resultado se analiza según lo mostrado a continuación:

$$\text{NARrT} = (\text{NARrA} + \text{NARrB} + \text{NARrC} + \text{NARrD}) / 4$$

Donde:

- **NARrT:** Nivel de Aceptación del Riesgo Resultante Total sobre el activo de Información analizado

- **NARrA:** Nivel de Aceptación del Riesgo Resultante Total sobre el activo de Información analizado según la puntuación establecida por A (Alta Dirección)
- **NARrB:** Nivel de Aceptación del Riesgo Resultante Total sobre el activo de Información analizado según la puntuación establecida por B (Gerencia General)
- **NARrC:** Nivel de Aceptación del Riesgo Resultante Total sobre el activo de Información analizado según la puntuación establecida por C (Estructura Organizacional del Sistema de Gestión de Seguridad de la Información)
- **NARrD:** Nivel de Aceptación del Riesgo Resultante Total sobre el activo de Información analizado según la puntuación establecida por D (Personal que interactúa con el activo de información y conoce el proceso de Servicio Post-Venta)

Nota: Tener en cuenta las puntuaciones según la metodología de gestión de riesgos para los valores de Impacto del Activo de Información.

En base a ello, en resumen de la interacción entre los integrantes en la evaluación de riesgos (Matriz de Gestión de Riesgos) para cada activo de información se obtiene el siguiente resultado:

Tabla 43: Riesgos y Nivel de Aceptación del Riesgo Resultante

RIESGOS			VULNERABILIDADES	INTERPRETACIÓN DEL RIESGO	INTERPRETACIÓN DEL RIESGO RESULTANTE	NIVEL DE ACEPTACIÓN DEL RIESGO	NIVEL DE ACEPTACIÓN DEL RIESGO RESULTANTE
ACTIVO	INTEGRANTE	IMPACTO DEL ACTIVO	INTERPRETACIÓN DEL IMPACTO				
Sistema de Gestión de Tickets	A	5	MUY ALTO	MUY ALTO	MUY ALTO	IMPORTANTE	IMPORTANTE
	B	5	MUY ALTO	MUY ALTO		IMPORTANTE	
	C	5	MUY ALTO	MUY ALTO		IMPORTANTE	
	D	5	MUY ALTO	MUY ALTO		IMPORTANTE	
Contratos de Servicios, Instalación, entre otros	A	5	MUY ALTO	ALTO	ALTO	CONSIDERABLE	CONSIDERABLE
	B	5	MUY ALTO	ALTO		CONSIDERABLE	
	C	4	ALTO	MEDIO		CONSIDERABLE	
	D	5	MUY ALTO	ALTO		CONSIDERABLE	
Carpeta de Proyectos	A	5	MUY ALTO	ALTO	ALTO	CONSIDERABLE	CONSIDERABLE
	B	5	MUY ALTO	ALTO		CONSIDERABLE	
	C	5	MUY ALTO	ALTO		CONSIDERABLE	
	D	5	MUY ALTO	ALTO		CONSIDERABLE	

RIESGOS			VULNERABILIDADES	INTERPRETACIÓN DEL RIESGO	INTERPRETACIÓN DEL RIESGO RESULTANTE	NIVEL DE ACEPTACIÓN DEL RIESGO	NIVEL DE ACEPTACIÓN DEL RIESGO RESULTANTE
ACTIVO	INTEGRANTE	IMPACTO DEL ACTIVO	INTERPRETACIÓN DEL IMPACTO				
Carpeta de Licitaciones	A	5	MUY ALTO	ALTO	ALTO	CONSIDERABLE	CONSIDERABLE
	B	5	MUY ALTO	ALTO		CONSIDERABLE	
	C	5	MUY ALTO	ALTO		CONSIDERABLE	
	D	5	MUY ALTO	ALTO		CONSIDERABLE	
Carpetas de Areas Administrativas y Contabilidad	A	5	MUY ALTO	ALTO	ALTO	CONSIDERABLE	CONSIDERABLE
	B	5	MUY ALTO	ALTO		CONSIDERABLE	
	C	5	MUY ALTO	ALTO		CONSIDERABLE	
	D	5	MUY ALTO	ALTO		CONSIDERABLE	
Equipos de Computo	A	4	ALTO	ALTO	ALTO	CONSIDERABLE	CONSIDERABLE
	B	4	ALTO	ALTO		CONSIDERABLE	
	C	5	MUY ALTO	MUY ALTO		IMPORTANTE	
	D	4	ALTO	ALTO		CONSIDERABLE	
Correo Electrónico	A	5	MUY ALTO	ALTO	MUY ALTO	IMPORTANTE	IMPORTANTE
	B	5	MUY ALTO	MUY ALTO		IMPORTANTE	
	C	5	MUY ALTO	MUY ALTO		IMPORTANTE	
	D	5	MUY ALTO	MUY ALTO		IMPORTANTE	

RIESGOS			VULNERABILIDADES	INTERPRETACIÓN DEL RIESGO	INTERPRETACIÓN DEL RIESGO RESULTANTE	NIVEL DE ACEPTACIÓN DEL RIESGO	NIVEL DE ACEPTACIÓN DEL RIESGO RESULTANTE
ACTIVO	INTEGRANTE	IMPACTO DEL ACTIVO	INTERPRETACIÓN DEL IMPACTO				
Internet / Servicios dedicados	A	4	ALTO	MEDIO	MEDIO	CONSIDERABLE	CONSIDERABLE
	B	4	ALTO	MEDIO		CONSIDERABLE	
	C	4	ALTO	MEDIO		CONSIDERABLE	
	D	4	ALTO	MEDIO		CONSIDERABLE	
File Server (Servidor de Archivos)	A	4	ALTO	ALTO	ALTO	CONSIDERABLE	CONSIDERABLE
	B	5	MUY ALTO	ALTO		CONSIDERABLE	
	C	5	MUY ALTO	ALTO		CONSIDERABLE	
	D	5	MUY ALTO	ALTO		CONSIDERABLE	
Infraestructura de Comunicaciones	A	5	MUY ALTO	ALTO	ALTO	CONSIDERABLE	CONSIDERABLE
	B	4	ALTO	MEDIO		CONSIDERABLE	
	C	5	MUY ALTO	ALTO		CONSIDERABLE	
	D	5	MUY ALTO	ALTO		CONSIDERABLE	
Personal	A	5	MUY ALTO	ALTO	ALTO	CONSIDERABLE	CONSIDERABLE
	B	5	MUY ALTO	ALTO		CONSIDERABLE	
	C	5	MUY ALTO	ALTO		CONSIDERABLE	
	D	5	MUY ALTO	ALTO		CONSIDERABLE	

Fuente: Elaboración propia

De los resultados obtenidos, se desprenden las siguientes cifras:

- **Activos de Información con Interpretación del Riesgo Resultante “Muy Alto”:** 2, el cual representa el 18% aproximadamente.
- **Activos de Información con Interpretación del Riesgo Resultante “Alto”:** 8, el cual representa el 73% aproximadamente.
- **Activos de Información con Interpretación del Riesgo Resultante “Medio”:** 1, el cual representa el 9% aproximadamente.
- **Activos de Información con Interpretación del Riesgo Resultante “Muy Bajo”:** 0, el cual representa el 0%.
- **Activos de Información con Interpretación del Riesgo Resultante “Bajo”:** 0, el cual representa el 0%.

De la evaluación de riesgos sobre los activos de información y en concordancia con la métrica de logro de objetivo se obtiene el porcentaje de activos respecto a su interpretación del riesgo valorados como “Muy Altos” (18% aproximadamente) y “Altos” (73% aproximadamente). El total de los resultados se muestra a continuación:

Figura 32: Porcentaje de Activos de Información Vs Interpretación del Riesgo Resultante

Fuente: Elaboración propia

Por otro lado, respecto al nivel de aceptación del riesgo resultante, se desprenden las siguientes cifras:

- **Activos de Información con Nivel de Aceptación del Riesgo Resultante “Importante”:** 2, el cual representa el 18% aproximadamente.
- **Activos de Información con Nivel de Aceptación del Riesgo Resultante “Considerable”:** 9, el cual representa el 82% aproximadamente.
- **Activos de Información con Nivel de Aceptación del Riesgo Resultante “Insignificante”:** 0, el cual representa el 0%.

De la evaluación de riesgos sobre los activos de información y en concordancia con la métrica de logro de objetivo se obtiene el porcentaje de activos respecto a su nivel de aceptación del riesgo valorados como “Importante” (18% aproximadamente) y “Considerable” (82% aproximadamente). El total de los resultados se muestra a continuación:

Figura 33: Porcentaje de Activos de Información Vs Nivel de Aceptación del Riesgo

Fuente: Elaboración propia

5.3.2.4. Plan de Mejoras:

Debido a que el presente trabajo no incluye la implementación del SGSI, sino su diseño, no se incluye mejoras de implementación. Sin embargo, dentro de las pruebas de escritorio realizadas, mientras la organización no decida implementar el SGSI, se recomienda realizar

en plazos de 03-04 meses nuevas pruebas a las ya realizadas, esto debido a que puede haber algún activo de información que en el tiempo varió su criticidad o impacto, probabilidad de materialización de una amenaza o existen nuevas vulnerabilidades o amenazas sobre el mismo después del análisis realizado.

5.3.3. Objetivo Específico III

El Objetivo Especifico III se muestra en la siguiente tabla:

Tabla 44: Indicadores y Métricas de logro de Objetivo Específico III

Objetivo Específico	Indicador de logro de Objetivo	Métrica de logro de Objetivo
Proponer un Plan de Tratamiento de Riesgos que me permita determinar los controles de seguridad de la información requeridos para obtener un nivel de riesgo aceptable en la organización.	Declaración de Aplicabilidad (SOA) que integre los controles de seguridad identificados y necesarios, seleccionados para cada nivel de riesgo asociado a cada activo de información valorizado.	Porcentaje de Controles seleccionados que aplican sobre los activos de información seleccionados sobre el total de los 114 Controles de seguridad de la información indicados en la norma y controles Técnicos Auxiliares propuestos.

Fuente: Elaboración propia

Respecto al desarrollo del presente objetivo específico, es importante mencionar en primera instancia lo siguiente:

- En el desarrollo del capítulo IV del presente trabajo de tesis, se definió la valoración de activos de información, la cual daría el punto de partida para la asignación de posibles impactos o criticidad a la que se encuentra sujeta, esto tomando en consideración la confidencialidad, integridad y disponibilidad de los datos del activo o el propio activo de información.
- Se definieron las posibles vulnerabilidades y amenazas a las que se encuentra expuestas los activos de información. Con ello, se definieron tablas donde se le asigna un valor numérico a los valores de impacto y a la probabilidad de riesgos sobre cada uno de los once (11) activos de información seleccionados o valorados como “Altos” y “Muy Altos”.

- En base a ello, se realiza la Valoración de Riesgos sobre los activos de información, la cual es una resultante entre el producto de los niveles de Impacto y la Probabilidad de riesgos sobre el activo de información.
- De lo anterior, se realizó una Matriz de Riesgos que conglomeró los puntos comentados, en la cual se calculan la Probabilidad de Riesgo, Valoración de Riesgos, su interpretación y el Nivel de Aceptación del Riesgo.
- Una vez realizada la Matriz de Riesgos, los activos de Información que componen el Plan de Tratamiento de Riesgos son los resultantes de un Nivel de Aceptación del Riesgo “Considerable” e “Importante”.
- En este estudio del Plan de Tratamiento de Riesgos se seleccionan los controles del Anexo A de la norma ISO/IEC 27001:2013 y los Controles Técnicos Auxiliares propuestos.
- Establecimiento del SOA (Declaración de Aplicabilidad). Este punto abarca los criterios de aplicabilidad y justificación de los controles, esto para cada activo de la información según lo indicado en la norma ISO/IEC 27002:2013.

Por todo lo comentado, ha sido importante describir la secuencia de pasos ejecutados para justificar y dar paso a lo comentado en el Plan de Pruebas, teniendo en cuenta que el alcance del presente proyecto es el Diseño de un SGSI, no implementación del mismo.

5.3.3.1. Plan de Pruebas

No aplica un plan de pruebas para el presente Objetivo Específico, debido a que el presente proyecto tiene como alcance el Diseño de un Sistema de Gestión de Seguridad de la Información, no la implementación de controles de seguridad seleccionados, ya sean del Anexo A de la norma ISO/IEC 27001:2013 o los propios Controles Técnicos Auxiliares propuestos. Sin embargo, a pesar de que no existe la implementación de controles de seguridad sobre los activos de información, se propone un método de nivel de madurez sobre los controles propuestos. Es decir, el nivel de madurez propuesto tiene como objetivo dejar lineamientos de revisión de estado actual, desarrollo y mejora sobre los controles de seguridad implementados. En base a lo comentado, se muestra la siguiente tabla:

Tabla 45: Matriz de Plan de Pruebas para el Objetivo Especifico III

Objetivo Específico	Método de Validación	Integrantes	Actividades a Desarrollar	Preguntas de Rigor	Recursos Necesarios	Fecha de Ejecución
OE3: Proponer un Plan de Tratamiento de Riesgos que me permita determinar los controles de seguridad de la información requeridos para obtener un nivel de riesgo aceptable en la organización.	No Aplica.	Personal que interactúa constantemente con los activos de información y conocedores del proceso de Servicio Post-Venta (Dentro de ello se incluye mi persona, autor del presente proyecto)	Actividad #1: Enumeración de todos los controles del anexo A de la norma ISO/IEC 27001:2013 que aplican en el Plan de Tratamiento de Riesgos para la salvaguarda de riesgos sobre los activos de información valorados.	¿Qué controles de Seguridad de la Información del Anexo A de la norma ISO/IEC 27001:2013 aplican sobre los activos de información valorados?	Revisión de los controles de seguridad de la norma ISO/IEC 27001:2013	Después de Implementar Controles de Seguridad de la norma y Técnicos Auxiliares propuestos
	- Debido a que el presente proyecto tiene como alcance el Diseño de un Sistema de Gestión de Seguridad de la Información, no incluye la implementación de controles de seguridad seleccionados, ya sean del Anexo A de la norma ISO/IEC 27001:2013 o los propios Controles Técnicos Auxiliares propuestos.	Integrantes de la Estructura Organizacional del Sistema de Gestión de Seguridad de la Información			Revisión de los controles Técnicos Auxiliares propuestos	
	- A pesar que no existe la implementación de controles de seguridad sobre los activos de información, se propone un método de nivel de madurez sobre los controles propuestos.	Personal que interactúa constantemente con los activos de información y conocedores del proceso de Servicio Post-Venta (Dentro de ello se incluye mi persona, autor del presente proyecto)	Actividad #2 Enumeración de todos los controles Técnicos Auxiliares propuestos, complementado los del anexo A de la norma ISO/IEC 27001:2013, los cuales aplican en el Plan de Tratamiento de Riesgos para la salvaguarda de riesgos sobre los activos de información valorados.	¿Qué controles de Seguridad de la Información Técnicos Auxiliares Propuestos aplican sobre los activos de información valorados?	Entendimiento del nivel de madurez de los controles de seguridad de la información seleccionados y propuestos	Después de Implementar Controles de Seguridad de la norma y Técnicos Auxiliares propuestos
	- El nivel de madurez propuesto	Integrantes de la Estructura Organizacional del Sistema de Gestión de Seguridad de la Información				

Objetivo Específico	Método de Validación	Integrantes	Actividades a Desarrollar	Preguntas de Rigor	Recursos Necesarios	Fecha de Ejecución
	tiene como objetivo dejar lineamientos de revisión de estado actual, desarrollo y mejora sobre los controles de seguridad implementados.	Personal que interactúa constantemente con los activos de información y conocedores del proceso de Servicio Post-Venta (Dentro de ello se incluye mi persona, autor del presente proyecto) Integrantes de la Estructura Organizacional del Sistema de Gestión de Seguridad de la Información	Actividad #3: Dejar los lineamientos necesarios para ejecutar y revisar el nivel de madurez propuesto sobre el estado actual, desarrollo y mejora de los controles de seguridad implementados posteriormente por la organización.	¿Cuáles son los valores de nivel de madurez sobre el estado actual, desarrollo y mejora de los controles de seguridad implementados? ¿Qué representa cada valor asignado a cada control de seguridad? ¿Existe una conformidad de la operación y desempeño del control de seguridad analizado?		Después de Implementar Controles de Seguridad de la norma y Técnicos Auxiliares propuestos

Fuente: Elaboración propia

5.3.3.2. Ejecución

El nivel de madurez será realizado por el personal que interactúa constantemente con los activos de información y conocedores del proceso de Servicio Post-Venta (Dentro de ello se incluye mi persona, autor del presente proyecto). Asimismo, como dentro del Diseño incluye la conformación de los integrantes de la Estructura Organizacional del Sistema de Gestión de Seguridad de la Información, se deberá tener en cuenta para las posteriores evaluaciones del desempeño del control de seguridad sobre el activo de información.

Por otro lado, los niveles de madurez propuestos están contemplados en la siguiente tabla:

Tabla 46: Matriz de Nivel de Madurez de los Controles de Seguridad Adoptados

Nivel de Madurez	Estado de Madurez	Efectividad del Control	Descripción del Estado de Madurez	Grado de Cumplimiento
0	Inicial	0% de efectividad del Control de Seguridad seleccionado	No existe evidencia o registros donde se indique que el control de seguridad seleccionado este operativo o en ejecución.	No Conformidad Mayor (NCM). No hay conformidad de la operatividad o ejecución del control de seguridad seleccionado
1	Muy Bajo	Rango variable de efectividad del Control de Seguridad Implementado entre 0% y 25%: $0\% < EC < 25\%$	El control de seguridad seleccionado está parcialmente operativo o parcialmente en ejecución, pero la evidencia o registro sobre la operatividad o ejecución del mismo no existe.	No Conformidad Mayor (NCM). El control seguridad esta implementado, pero parcialmente. No hay documentación que avale su desempeño
2	Bajo	Rango variable de efectividad del Control de Seguridad Implementado entre 25% y 50%: $25\% < EC < 50\%$	El control de seguridad seleccionado está parcialmente operativo o parcialmente en ejecución, pero la evidencia o registro sobre la operatividad del mismo es muy pobre o existen	No Conformidad Leve (NCL). El control seguridad esta implementado, pero parcialmente. Existe documentación que avale su desempeño, pero es muy pobre o escasa.

Nivel de Madurez	Estado de Madurez	Efectividad del Control	Descripción del Estado de Madurez	Grado de Cumplimiento
			deficiencias en la gestión sobre el mismo.	
3	Medio	Rango variable de efectividad del Control de Seguridad Implementado entre 50% y 75%: $50\% < EC < 75\%$	El control de seguridad seleccionado está operativo o en ejecución y existe evidencia o registro sobre la operatividad del mismo. Sin embargo, no se explotan las métricas asociadas al desempeño del control de seguridad	Estado de observación y monitoreo (EOM). El control seguridad está en ejecución y operativo, existe documentación específica que avale su operación y desempeño, pero no se toman en cuenta sus métricas para tener un ciclo de mejora continua.
4	Alto	Rango variable de efectividad del Control de Seguridad Implementado entre 75% y 100%: $75\% < EC < 100\%$	El control de seguridad seleccionado está operativo o en ejecución y existe evidencia o registro sobre la operatividad del mismo. Asimismo, la organización, específicamente la Estructura de Gestión de Seguridad de la Información explotan las métricas asociadas al desempeño del control de seguridad	Conformidad. El control seguridad está en ejecución y operativo, existe documentación específica que avale su operación y desempeño, y se toman en cuenta sus métricas para tener un ciclo de mejora continua.

Fuente: Elaboración propia

Lo propuesto dentro del presente proyecto es que la organización lleve los niveles de madurez sobre los controles de seguridad seleccionados como mínimo en:

- **Valores de 3:** Nivel de madurez medio, con efectividad del control no menor a 75%.
A pesar de que no hay una conformidad de la operación y ejecución del control de seguridad implementado, es el estado ideal para levantar observaciones y pasar al

estado de conformidad. Se espera tener este resultado en un plazo no menor a 01 o 02 meses de implementado el SGSI

- **Valores de 4:** Nivel de madurez alto, con efectividad del control variable entre 75% y 100%, llegando a niveles óptimos. Este es el estado ideal del control, en donde se indica que el control está operativo, se tienen registros que avalen su desempeño y se están tomando en cuenta sus métricas de operación. Tener en cuenta que este es un ciclo de mejora continua, así que el proceso es cíclico y retroalimentado en el tiempo.

A continuación, se muestra un ejemplo de cómo debería hacerse el despliegue del modelo de madurez de controles de seguridad, según los lineamientos indicados:

Tabla 47: Analisis del Nivel de Madurez de Controles por Dominio del Anexo A de la norma ISO/IEC 27001:2013

	PORCENTAJE	0%	0%<EC<25%	25%<EC<50%	50%<EC<75%	75%<EC<100%	EVALUACIÓN DE LA MADUREZ	
CLAUSULA / CONTROLES	CANTIDAD DE CONTROLES	INICIAL	MUY BAJO	BAJO	MEDIO	ALTO	MADUREZ POR CLAUSULA	GRADO DE CUMPLIMIENTO
A.5 POLITICAS DE SEGURIDAD	2	0	0	0	1	1	75%<EC<100%	CONFORMIDAD
A 5.1.1 CONJUNTO DE POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN	1	NA	NA	NA	NA	4	75%<EC<100%	CONFORMIDAD
A 5.1.2 REVISIÓN DE LAS POLITICAS PARA LA SEGURIDAD DE LA INFORMACIÓN	1	NA	NA	NA	NA	4	75%<EC<100%	CONFORMIDAD

Fuente: Elaboración propia

5.3.3.3. Resultados y Validación

Una vez ya recomendado un nivel de madurez para los controles de seguridad adoptado, es necesario comentar a continuación que controles de seguridad son adoptados en el SOA: Controles del Anexo A de la norma ISO/IEC 27001:2013 y Técnicos auxiliares propuestos.

5.3.3.3.1. Controles del Anexo A de la norma ISO/IEC 27001:2013

De la Tabla mostrada a continuación (Tabla N°43) se indica una gráfica donde se evidencia la relación de controles aplicados y el total de controles indicados por la norma ISO/IEC 27002:2013. Tener en cuenta en este punto que el total de controles aplicados seleccionados para mitigar y contrarrestar las amenazas, ya descritas para cada activo de la información, asciende a un total de 64 de 114 en total descrito por la norma. Se muestra lo comentado:

Tabla 48: Cantidad de Controles de Seguridad Aplicables

CLÁUSULA	APLICAB.	NO APLICAB
A.5 POLITICAS DE SEGURIDAD	2	0
A.6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	3	4
A.7 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	5	1
A.8 GESTION DE ACTIVOS	8	2
A.9 CONTROL DE ACCESOS	11	3
A.10 CIFRADO / CRIPTOGRAFIA	0	2
A. 11 SEGURIDAD FISICA Y AMBIENTAL	11	4
A.12 SEGURIDAD DE LAS OPERACIONES	6	8
A. 13 SEGURIDAD EN LAS TELECOMUNICACIONES	6	1
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	1	12
A.15 RELACIONES CON LOS PROVEEDORES / SUMINISTRADORES	1	4
A.16 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION	3	4
A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO	3	1
A. 18 CUMPLIMIENTO	3	5
Total Controles	64	50

En base a este nivel de aplicabilidad de controles se realizó la siguiente gráfica:

Figura 34: Relación de Aplicabilidad/No Aplicabilidad de Controles por Dominio según el Anexo A de la norma ISO/IEC 27001:2013

Fuente: Elaboración propia

Asimismo, de la totalidad de controles de seguridad aplicables y no aplicables del Anexo “A” o ISO/IEC 27002:2013, se muestra la siguiente gráfica:

Figura 35: Relación de Controles Aplicables y no Aplicables de la ISO/IEC 27002:2013

Fuente: Elaboración propia

Según lo observado en el gráfico se observa los siguientes resultados:

Controles de Seguridad aplicables del Anexo A de la norma ISO/IEC 27002:2013: 56%

Controles de Seguridad no aplicables del Anexo A de la norma ISO/IEC 27002:2013: 44%

5.3.3.3.2. Controles Técnicos Auxiliares propuestos a la norma ISO/IEC 27001:2013

Por otro lado, en cuanto a los controles Técnicos Auxiliares (TA) propuestos, vales decir que la norma establece que se pueden adoptar controles adicionales a los indicados en el Anexo A de la misma, ello para complementar la salvaguarda y protección de los controles de seguridad sobre los activos de información. En el caso del presente proyecto se adoptaron treinta y dos (32) controles Técnicos Auxiliares (TA), los cuales se pueden revisar a detalle en el “Anexo VII”, adjunto al presente proyecto. De todos modos, los controles adoptados son los siguientes:

- TA1. Ejecución de procedimientos para el uso de contraseñas fuertes
- TA2. Limitar el número de acceso a contraseñas inválidas
- TA3. Implementación de software de monitoreo de estado de salud y rendimiento de la aplicación
- TA4. Implementación de un Data Loss Prevention (DLP)
- TA5. Migración del Sistema de Gestión de Tickets en un servicio en la nube mediante IAAS
- TA6. Migración de copias legalizadas a proveedor de custodia de archivos:
- TA7. Implementación de software de auditoria de uso de datos de Carpeta de Proyectos
- TA8. Migración de la carpeta de proyectos bajo un servicio en la nube mediante IAAS
- TA9. Despliegue de una solución de repositorio en la nube de acceso específico
- TA10. Implementación de software de auditoria de uso de datos de Carpeta de Licitaciones
- TA11. Migración de la Carpeta de Licitaciones bajo un servicio en la nube mediante IAAS

- TA12. Implementación de software de auditoria de uso de datos de Carpetas de áreas Administrativas y Contabilidad
- TA13. Migración de las carpetas de áreas Administrativas y Contabilidad bajo un servicio en la nube mediante IAAS
- TA14. Ingreso lógico de cada equipo de cómputo por medio del Directorio Activo
- TA 15. Implementación de una suite o solución de Endpoint para prevenir ataques de firmas comunes y de Día Cero
- TA16. Implementación de una solución de respaldo de Endpoint o estaciones de trabajo y/o servidores
- TA17. Implementación de un servidor centralizado para instalación de parches de seguridad
- TA18. Implementación de una solución de Endpoint Encryption
- TA19. Alquiler de equipos de cómputo
- TA20. Implementación de software de auditoria de uso del servicio de Correo Electrónico
- TA21. Implementación de un servicio o appliance de AntiSpam
- TA22. Migración del servicio de correo electrónico a la nube mediante SAAS
- TA23. Implementación de software de monitoreo del consumo de internet
- TA 24. Implementación de software de monitoreo del consumo de Internet
- TA25. Implementación de una suite o Solución Perimetral para prevenir ataques de Día Cero
- TA26. Implementación de software de auditoria de uso de los contenidos de los equipos de Infraestructura de Comunicaciones
- TA27. Ingreso lógico del Servidor de Archivos por medio del Directorio Activo
- TA28. Migración del servicio de FTP bajo un servicio en la nube mediante IAAS
- TA29. Ingreso lógico del Servidor de Archivos por medio del Directorio Activo
- TA30. Evaluación e implementación de una data center alternativo

- TA31. Adopción de sistema de simulación de ejecución de Phishing
- TA32. Programas de información sobre técnicas de ataques de Ingeniería Social

5.3.3.4. Plan de Mejoras

Debido a que el presente trabajo no incluye la implementación del SGSI, sino su diseño, no se incluye mejoras de implementación. Sin embargo, una vez implementado el Sistema de Gestión de Seguridad de la Información (SGSI), con los controles que comprenden el Anexo A de la norma ISO/IEC 27001:2013 y los controles Técnicos Auxiliares, se recomienda la adopción de la ejecución de la medición de madurez del total de controles seleccionados.

5.3.4. Objetivo Específico IV

El Objetivo Especifico IV se muestra en la siguiente tabla:

Tabla 49: Indicadores y Métricas de logro de Objetivo Específico IV

Objetivo Específico	Indicador de logro de Objetivo	Métrica de logro de Objetivo
Definir la estructura organizacional requerida y sus integrantes para la operación del SGSI, estableciendo roles y responsabilidades del personal de la organización.	Organigrama de la en donde se indiquen los integrantes de la Estructura Organizacional del Sistema de Gestión de Seguridad de la Información.	Porcentaje de cumplimiento de las funciones del Comité de Gestión de Seguridad de la Información (CGSI) respecto a la NTP-ISO/IEC 27001:2014, RM N°166-2017-PCM

Fuente: Elaboración propia

Tal como lo indica la norma ISO/IEC 27001:2013 en su apartado 5.3 “Roles, responsabilidades y autoridades organizacionales”, en donde se manifiesta que la Alta Dirección debe asegurar que las responsabilidades y la autoridad para los roles relevantes a la seguridad de la información estén asignadas y comunicadas”, este objetivo tiene como finalidad definir la Estructura Organizacional del Sistema de Gestión de Seguridad de la Información, estableciendo roles y responsabilidades en el manejo de la seguridad de los activos e información seleccionados en el proceso de Servicio Post-Venta de la organización.

En base a ello, en el capítulo VI, específicamente en el apartado 4.4.2, se definieron los roles y responsabilidades de la Estructura Organizacional del Sistema de Gestión de Seguridad de la Información, tal como se muestra a continuación:

Tabla 50: Definición, Funciones e Integrantes de la Estructura Organizacional de la Gestión de la Seguridad de la Información

Clasificación	Definición	Funciones	Integrantes
Comité de Gestión de Seguridad de la Información (CGSI)	Máximo órgano consultivo de carácter no técnico sobre la seguridad de la información. Deberá reunirse por lo menos una vez, de ser el caso, al mes para evaluar la situación institucional en materia de seguridad de la información y el plan de acción para la mejora continua	Revisar y proponer la máxima autoridad para la ejecución de la Política de Gestión de Seguridad de la Información y la delegación de funciones en materia de Seguridad de la Información, alineados a los objetivos de negocio.	El Gerente General, Gerente Técnico, Gerente Comercial, Gerente Administrativo y Financiero, y Gerente de Recursos Humanos.
		Ser gestor responsable de todo lo relacionado a la implementación del SGSI, verificación de su continuidad y evaluación de su desempeño.	
		Ser ente líder en la difusión de la importancia del SGSI dentro de la organización.	
		Asignar roles y responsabilidades en materia de seguridad de información a cada área, esto según los procesos organizacionales en estudio.	
		Promover la difusión y apoyo de la seguridad de la información dentro de la organización, creando un ambiente seguro y compacto que genere bienestar e identificación con las políticas y procedimientos establecidos.	
Grupo Interdisciplinario de Seguridad de la Información (GISI)	Grupo homogéneo organizacional que vela por el cumplimiento de los estipulado en la Política de SGSI	Asegurar dentro de la Organización que las actividades de Seguridad de la Información sean ejecutadas en conformidad con la Política de Gestión de Seguridad de la Información.	Jefes de Proyectos, Jefe de Servicios Post-Venta y Desarrollo.

Clasificación	Definición	Funciones	Integrantes
		Aprobar metodologías y procesos que permitan al personal de la organización a expresar sus dudas e inquietudes en materia de Seguridad de la información	
		Generar confianza y concientización en los estatutos y procedimientos indicados en la Política de SGSI.	
Oficial de Seguridad de la Información (OSI)	Responsable de diseñar, desarrollar, implantar y mantener el Sistema de Gestión de Seguridad de la Información (SGSI) en la organización	Proponer metodologías, procedimientos, estatutos, herramientas, planes, programas y procesos para la seguridad de la información, para el cumplimiento de controles adoptados por la organización.	Jefe de Servicios Post-Venta
		Monitoreo constante de incidentes relativos a la seguridad de la información, estableciendo parámetros de mejora en base a análisis previamente realizados.	
		Administrar los incidentes y vulnerabilidades de los distintos activos de información para identificar los controles a implementar, elaborando y actualizando el plan de Seguridad de la Información.	
Dueño del Riesgo	Es la persona responsable de gestionar los riesgos asociados a los activos de información valorizados	Gestionar de manera correcta las actividades y recursos necesarios para evitar la materialización de amenazas sobre las vulnerabilidades existentes en los activos de información.	Varía según el activo de información en cuestión (designado según sea el activo de información y el control de seguridad)

Clasificación	Definición	Funciones	Integrantes
		<p>Monitorear cambios significativos en los riesgos que afectan los activos de información previamente identificados, esto frente a las amenazas más relevantes que afecten o puedan afectar los activos de información seleccionados.</p> <p>El rol no implica necesariamente que sea la persona que finalmente ejecuta los controles, sino alguien que se responsabiliza de que realmente los controles aplicables sobre los activos de información se estén llevando a cabo acorde a lo establecido.</p>	asociado al mismo)
Propietarios de Activos de la Información	Es la persona o entidad que tiene la responsabilidad gerencial aprobada sobre los activos de información que se generan y se utilizan en las Unidades u Oficinas administrativas	<p>Clasificar los activos de información con el grado de sensibilidad y criticidad necesario.</p> <p>Documentar y mantener actualizada la clasificación de activos de información realizada y definir qué usuarios tiene o no acceso a los distintos activos de información que tiene bajo su custodia.</p>	Gerentes que representen a cada área que disponga los múltiples activos de información que hayan sido seleccionados
Custodio de los Activos de Información	Nexo entre el Propietario de la Información y el usuario de los activos de información.	Administrar y resguardar los activos de información, monitoreando el cumplimiento de controles de seguridad en los activos que se encuentren bajo su administración.	Jefe de Proyectos, Jefe de Post-Venta y Jefe de Desarrollo
Usuario de Activos de Información	Personal permanente, personal temporal, consultores y proveedores de bienes y/o servicios, que utilizan los activos de información de la organización como parte de sus actividades diarias	Usar el activo de información para la ejecución de sus deberes.	Todas las personas que tengan a su cargo cualquier activo (bien, proceso, servicio, entre otro) que sea asignado bajo un documento formal y explícito, en mutuo acuerdo entre ambas partes

Fuente: Elaboración propia

5.3.4.1. Organigrama

El organigrama establecido para la Estructura de la Organización del Sistema de Gestión de Seguridad de la información se muestra a continuación:

Figura 36: Organigrama de la Estructura Organizacional del Sistema de Gestión de Seguridad de la Información (EOSGSI)

Fuente: Elaboración propia

Adicionalmente, complementando el objetivo específico y para dar valor a la métrica asociada, dentro de las investigaciones realizadas y asociadas al trabajo actual, el año pasado fue promulgada la Resolución Ministerial N° 166-2017-PCM, en la cual modifican el artículo N°5 de la Resolución Ministerial N°004-2016-PCN, ello en referencia a las funciones del Comité de Gestión de Seguridad de la Información (Para mayor profundidad revisar “Anexo XV” “Resolución Ministerial N° 166-2017-PCM”). Si bien es cierto que la norma ISO/IEC 27001:2013 es autónoma, tiene su símil (traducción literal y toma de requisitos y lineamientos establecidos en la propia ISO/IEC 27001:2013) y es representada en el Perú mediante la NTP-ISO/IEC 27001:2014.

En base a todo lo comentado, se ha elaborado un cuadro comparativo en donde se evidencia el porcentaje de cumplimiento de las funciones o responsabilidades asignadas específicamente al Comité de Gestión de Seguridad de la Información, el cual es el máximo

órgano consultivo de carácter no técnico sobre la seguridad de la información, específicamente el SGSI. Se muestra el cuadro comparativo:

Tabla 51: Cuadro Comparativo de funciones según la Resolución Ministerial N° 166-2017-PCM y la Estructura Organizacional Propuesta

CÓMITE DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN			
FUNCIÓN	RESOLUCIÓN MINISTERIAL N° 166-2017-PCM	ESTRUCTURA ORGANIZACIONAL DEL SGSI PROPUESTO	CUMPLIMIENTO
A	Proponer la política y objetivos de seguridad de la información alineados con el Plan Estratégico Institucional, con la Política Nacional de Gobierno Electrónico y regulación en el ámbito de seguridad de la información.	Revisar y proponer la máxima autoridad para la ejecución de la Política de Gestión de Seguridad de la Información y la delegación de funciones en materia de Seguridad de la Información, alineados a los objetivos de negocio.	100%
B	Promover y gestionar la implementación del Sistema de Gestión de Seguridad de la Información.	Ser gestor responsable de todo lo relacionado a la implementación del SGSI, verificación de su continuidad y evaluación de su desempeño.	100%
C	Promover la gestión de seguridad de la información en los procesos y cultura organizacional.	Ser ente líder en la difusión de la importancia del SGSI dentro de la organización.	100%
D	Gestionar la asignación del personal y recursos necesarios para la implementación del Sistema de Gestión de Seguridad de la Información.	Asignar roles y responsabilidades en materia de seguridad de información a cada área, esto según los procesos organizacionales en estudio.	100%
E	Difundir la importancia de una efectiva gestión de seguridad de la información a las partes interesadas, en conformidad con los requisitos del Sistema de Gestión de Seguridad de la Información.	Ser ente líder en la difusión de la importancia del SGSI dentro de la organización.	100%
F	Evaluar el desempeño del Sistema de Gestión de Seguridad de la Información.	Ser gestor responsable de todo lo relacionado a la implementación del SGSI, verificación de su continuidad y evaluación de su desempeño.	100%
G	Otras funciones que se le asigne en el ámbito de su competencia y aquellas concordantes con la materia.	Promover la difusión y apoyo de la seguridad de la información dentro de la organización, creando un ambiente seguro y compacto que genere bienestar e identificación con las políticas y procedimientos establecidos.	100%

Fuente: Elaboración propia

En base a la tabla comparativa, se evidencian los siguientes resultados de funciones cubiertas para el Comité de Gestión de Seguridad de la Información:

Figura 37: Porcentajes de Cumplimiento de Funciones Cubiertas del Comité de Gestión de Seguridad de la Información respecto a la Resolución Ministerial N° 166-2017-PCM

Fuente: Elaboración propia

Como se puede observar todas las funciones indicadas en la Resolución Ministerial N° 166-2017-PCM, respecto a la Estructura Organizacional del SGSI propuesta son cubiertas al 100%.

5.3.4.2. Plan de Mejoras

Se elaboró una encuesta llamada: “Encuesta sobre el Desempeño de la Estructura Organizacional del Sistema de Gestión de Seguridad de la Información”, la cual será utilizada una vez ya implementado el Sistema de Gestión de Seguridad de la Información. El contenido de la encuesta mencionado a continuación:

5.3.4.3. Encuesta sobre el desempeño de la Estructura Organizacional del Sistema de Gestión de Seguridad de la Información (EOSGSI)

Esta encuesta está dirigida a personal Administrativo, Operativo y Consultivo de la Organización, la cual tiene como objetivos:

- Conocer si el personal que integra la organización conoce la existencia de la Estructura Organizacional del Sistema de Gestión de Seguridad de la Información
- Conocer si el personal que integra la organización conocen las labores y funciones de la Estructura Organizacional del Sistema de Gestión de Seguridad de la Información
- Conocer como personal de la organización percibe el desempeño de las labores y funciones de la Estructura Organizacional del Sistema de Gestión de Seguridad de la Información
- Evaluar el desempeño de las labores y funciones de la Estructura Organizacional del Sistema de Gestión de Seguridad de la Información

El detalle de la encuesta puede revisarse en el “**Anexo XVI**”: “Encuesta sobre el desempeño de la Estructura Organizacional del Sistema de Gestión de Seguridad de la Información (EOSGSI)”, adjunto en el presente proyecto.

CAPÍTULO 6: CONCLUSIONES Y RECOMENDACIONES

6.1. Introducción

En el presente capítulo se revisan las conclusiones y recomendaciones correspondiente al Diseño de un Sistema de Gestión de Seguridad de la Información, basada en la norma ISO/IEC 27001:2013, aplicado al proceso de Servicio Post-Venta de un Integrador de Telecomunicaciones.

6.2. Conclusiones

Partiendo de la problemática de la organización, los cuales en esencia son:

- Continuos ataques a sus Sistemas Informáticos
- Pérdidas de información confidencial, tanto propia como de sus clientes.
- Ausencia de un inventario de activos de información asociados al proceso de Servicio Post-Venta.
- Falta de una Estructura Organizacional de Seguridad de la Información
- Carencia de procesos, lineamientos y políticas de seguridad de la información.

Las conclusiones del presente proyecto son:

- Se logró realizar un inventario, clasificación y valoración de los Activos de Información que se encuentran involucrados en el proceso de Servicio Post-Venta, ello en base a la metodología de Evaluación de Riesgos propuesta.
- Se logró identificar las principales vulnerabilidades y amenazas a las que se encuentran expuestas los distintos activos de la información seleccionados.
- Se logró evaluar los riesgos de seguridad en los distintos activos de información valorados, esto en base al Plan de Tratamiento de Riesgos ejecutado.

- Se logró identificar y ejecutar los niveles de aplicabilidad de controles que indica la norma ISO/IEC 27002:2013 y controles Auxiliares Técnicos propuestos, ello para la correcta salvaguarda de los activos de información valorados.
- Se realizó el diseño de una Política de Seguridad de la Información la cual proporciona una guía y apoyo para el correcto manejo la seguridad de la información en la Organización, aquello en relación a los objetivos y requisitos de negocio previamente trazados.
- Se logró establecer una Estructura Organizacional del Sistema de Gestión de Seguridad de la Información, permitiendo establecer roles, responsabilidades y obligaciones en el manejo y cuidado de la Seguridad de la Información en la organización.
- En base a todas las conclusiones indicadas en conjunto, se logró Diseñar un Sistema de Gestión de Seguridad de la Información, enfocado al proceso de Servicio Post-Venta de un Integrador de Telecomunicaciones, basado en la norma ISO/IEC 27001:2013.

6.3. Recomendaciones

Son las siguientes:

- Se recomienda realizar la implementación del Sistema de Gestión de la Seguridad de la Información diseñado en la presente tesis en la organización en estudio.
- Tener un ciclo de mejora continua y revisar la eficacia de la Política de Seguridad de la Información en base a los lineamientos de Seguridad de la Información previamente trazados.
- Una vez ya implementado el SGSI, se recomienda poner en marcha la evaluación de la efectividad de los controles seleccionados mediante el modelo de madurez propuesto.
- Revisar constantemente nuevas vulnerabilidades y amenazas de seguridad de la información sobre los activos de información valorados.

7. RECOMENDACIONES PARA TRABAJOS FUTUROS

Después de la posterior implementación del Sistema de Gestión de Seguridad de la Información (SGSI) se recomienda a la organización en estudio como trabajos futuros, contemplar procesos adicionales al de Soporte Post-Venta dentro del alcance del mismo. Ello tendrá como resultado, abarcar más procesos o áreas del negocio y gestionar de manera global la seguridad de los activos de información de la organización.

Es altamente recomendable para la organización evaluar y desarrollar posteriormente un Plan de Recuperación ante Desastres (DRP), tal como se indica dentro de la descripción de los controles de seguridad adoptados del Anexo A de la norma ISO/IEC 27001:2013 (A17.1.1 Planificación de la Continuidad de la Seguridad de la Información y A17.1.2 Implantación de la continuidad de la Seguridad de la Información), ello como medidas de recuperación y continuidad del negocio.

8. BIBLIOGRAFÍA

1. DÍAZ ORUETA, Gabriel, ALZÓRRIZ ARMENDÁRIZ, Ignacio, SANCRISTÓBAL RUIZ, Elio, CASTRO GIL, Manuel Alonso (2014) Procesos y Herramientas para la Seguridad de Redes. Madrid: UNED.
2. PELTIER, R. Thomas (2010) Information Security Risk Analysis. Third Edition. Florida: Auerbach.
3. INTECO(2014)(http://www.inteco.es/Formacion/SGSI/Conceptos_Basicos/Concepto_SGSI) Sitio web oficial del Instituto Nacional de Tecnologías de las Información de España; contiene información sobre conceptos, buenas prácticas, implementación y otros sobre Sistemas de Gestión de Seguridad de la Información (consulta: lunes 26 de octubre de 2017)
4. OFICINA NACIONAL DE GOBIERNO ELECTRONICO E INFORMATICA (ONGEI)(http://www.gobiernodigital.gob.pe/docs/ISO_27001_v011.pdf) Sitio web de la Presidencia del Consejo de Ministros (PCM) y la Secretaria de Gobierno Digital (SGD) sobre el Taller de Implementación de la Norma ISO/IEC 27001:2013 (consulta: martes 02 de noviembre del 2017)
5. PMG-SGSI (<https://www.pmg-ssi.com/2016/07/iso-27001-2013-los-riesgos-y-las-oportunidades>) Sitio web especializado en Sistema de Gestión de Seguridad de la Información. Revisión de las nuevas incorporaciones y novedades de la norma ISO/IEC 27001:2013 respecto a su antecesora ISO/IEC 27001: (consulta: martes 01 de enero del 2018)
6. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO) (2005), Norma ISO/IEC 27001:2005: Tecnología de la Información - Técnicas de seguridad – Sistemas de Gestión de Seguridad de la Información – Requisitos.
7. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO) (2014)(<http://www.iso.org/iso/home/standards/managementstandards/iso27001.htm>) Sitio web oficial de la ISO; contiene información sobre la norma y enlaces de interés (consulta: 05 de marzo)
8. ALTA CONSEJERÍA DISTRITAL DE TIC (2017)([http:// ticbogota.gov.co/](http://ticbogota.gov.co/)) Sitio web oficial de la Alta Consejería Distrital de TIC de Colombia; contiene información sobre proyectos, despliegues y buenas practicas asociados a Tecnología de la Información (TIC) (consulta: martes 27 octubre de 2017)
9. ISO 27000 (2012) (<http://www.iso27000.es/sgsi.html>) Sitio web que contiene un repositorio sobre documentación de implementación de un SGSI. (Consulta 10 de mayo)
10. ISO TOOLS EXCELLENCE (2013) (<http://www.isotools.org/2013/12/05/eninventario-de-activos-en-la-implementacion-de-la-norma-iso-27001/>) Sitio web que contiene información relacionada con la implementación de un SGSI y todos los componentes que comprende (Consulta 01/06/2014)

11. MERINO BADA, Cristina, CAÑIZARES SALES, Ricardo (2011) Implantación de un Sistema de Gestión de Seguridad de la Información según ISO 27001. Edición 2001. Madrid: FC Editorial.
12. MIRANDA GONZÁLES, Francisco, CHAMORRO MERA, Antonio, RUBIO LACOB, Sergio (2007) Introducción a la Gestión de la Calidad. Madrid: Delta.

9. GLOSARIO

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma que tenga valor para la organización

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización

Respaldo: Comúnmente llamado backup o copia adicional de los archivos de la computadora que generalmente se guarda en un lugar físicamente separado de los originales.

COBIT: Es un modelo utilizado para valorar los sistemas de información de una entidad, tomado en cuenta como modelo de madurez.

10. SIGLARIO

- PMBOK: Project Management Body of Knowledge
- ITIL: Information Technology Infrastructure Library
- COBIT: Control Objectives for Information and related Technology
- INTECO: Instituto Nacional de Tecnologías de la Comunicación
- PDCA: Plan, Do, Check, Act (Siglas en español que hacen referencia al ciclo de Deming o el Planear, Hacer, Chequear y Actuar)
- OISM3: Open Information Security Management Maturity Model
- SGSI: Sistema de Gestión de Seguridad de la Información
- ISMS: Information Security Management System
- NIST: National Institute of Standards and Technology
- PTR: Plan de Tratamiento de Riesgos
- ISO: International Organization for Standardization
- IEC: International Electrotechnical Commission
- AS/NZS 4360: Australia/New Zealand 4360 (Norma)
- BSI: British Standards Institution
- BS 7799-1: British Standards 7799-1 (Norma)
- TIC: Tecnología de la Información y Comunicación
- OWASP: Open Web Application Security Project
- EOSGSI: Estructura Organizacional del Sistema de Gestión de Seguridad de la Información
- CGSI: Comité de Gestión de Seguridad de la Información
- GISI: Grupo Interdisciplinario de Seguridad de la Información
- OSI: Oficial de Seguridad de la Información
- SAT: Sistema de Atención de Tickets

- UPS: Uninterruptible Power Supply
- SGT: Sistema de Gestión de Tickets
- TA: Técnico Auxiliar
- IRR: Interpretación del Riesgo Resultante
- NARRT: Nivel de Aceptación del Riesgo Resultante Total

11. ANEXOS

ANEXO I: Implementación del Plan de Seguridad y Privacidad de la Información (40%) - Analisis GAP

Por favor, conteste la siguiente encuesta, de acuerdo con el instructivo.

ESTADO	DESCRIPCIÓN
Cumple satisfactoriamente	Existe, es gestionado, se está cumpliendo con lo que la norma solicita, está documentado, es conocido y aplicado por todos los involucrados en el SGSI. Cumple 100%.
Cumple parcialmente	Lo que la norma requiere se está haciendo de manera parcial, se está haciendo diferente, no está documentado, se definió pero no se gestiona.
No cumple	No existe y/o no se está haciendo.
No aplica	El control no es aplicable para la entidad. En el campo evidencia por favor indicar la justificación respectiva de su no aplicabilidad.

ANEXO			ESTADO	EVIDENCIA
A5	POLÍTICAS DE LA SEGURIDAD DE LA INFORMACION			
A5.1	Orientación de la dirección para la gestión de la seguridad de la información			
Objetivo: Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes				
A5.1.1	Políticas para la seguridad de la información	Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.	No cumple	No existe documentación o ejecución de control comentado.
A5.1.2	Revisión de las políticas para la seguridad de la información.	Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.	No cumple	No existe documentación o ejecución de control comentado.
A6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION			
A6.1	Organización interna			
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.				
A6.1.1	Roles y responsabilidades para la seguridad de la información	Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	No cumple	No existe documentación o ejecución de control comentado.
A6.1.2	Separación de deberes	Control: Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización	No cumple	No existe documentación o ejecución de control comentado.
A6.1.3	Contacto con las autoridades	Control: Se deben mantener contactos apropiados con las autoridades pertinentes.	No cumple	No existe documentación o ejecución de control comentado.
A6.1.4	Contacto con grupos de interés especial	Control: Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad	No cumple	No existe documentación o ejecución de control comentado

ANEXO			ESTADO	EVIDENCIA
A6.1.5	Seguridad de la información en la gestión de proyectos.	Control: La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.	No cumple	No existe documentación o ejecución de control comentado.
A6.2	Dispositivos móviles y teletrabajo			
Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles				
A6.2.1	Política para dispositivos móviles	Control: Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	No cumple	No existe documentación o ejecución de control comentado.
A6.2.2	Teletrabajo	Control: Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	No cumple	No existe documentación o ejecución de control comentado.
A7	SEGURIDAD DE LOS RECURSOS HUMANOS			
A7.1	Antes de asumir el empleo			
Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.				
A7.1.1	Selección	Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso y a los riesgos percibidos.	No cumple	No existe documentación o ejecución de control comentado.
A7.1.2	Términos y condiciones del empleo	Control: Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	No cumple	No existe documentación o ejecución de control comentado.
A7.2	Durante la ejecución del empleo			
Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.				
A7.2.1	Responsabilidades de la dirección	Control: La dirección debe exigir a todos los empleados y contratista la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	No cumple	No existe documentación o ejecución de control comentado.
A7.2.2	Toma de conciencia, educación y formación en la seguridad de la información.	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.	No cumple	No existe documentación o ejecución de control comentado.
A7.2.3	Proceso disciplinario	Control: Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	No cumple	No existe documentación o ejecución de control comentado.
A7.3	Terminación y cambio de empleo			

ANEXO			ESTADO	EVIDENCIA
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo				
A7.3.1	Terminación o cambio de responsabilidades de empleo	Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de empleo de deben definir, comunicar al empleado o contratista y se deben hacer cumplir.	No cumple	No existe documentación o ejecución de control comentado.
A8	GESTION DE ACTIVOS			
A8.1	Responsabilidad por los activos			
Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección adecuadas.				
A8.1.1	Inventario de activos	Control: Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	No cumple	No existe documentación o ejecución de control comentado.
A8.1.2	Propiedad de los activos	Control: Los activos mantenidos en el inventario deben tener un propietario.	No cumple	No existe documentación o ejecución de control comentado.
A8.1.3	Uso aceptable de los activos	Control: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	No cumple	No existe documentación o ejecución de control comentado.
A8.1.4	Devolución de activos	Control: Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	No cumple	No existe documentación o ejecución de control comentado.
A8.2	Clasificación de la información			
Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.				
A8.2.1	Clasificación de la información	Control: La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	No cumple	No existe documentación o ejecución de control comentado.
A8.2.2	Etiquetado de la información	Control: Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	No cumple	No existe documentación o ejecución de control comentado.
A8.2.3	Manejo de activos	Control: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	No cumple	No existe documentación o ejecución de control comentado.
A8.3	Manejo de medios			
Objetivo: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios				
A8.3.1	Gestión de medio removibles	Control: Se deben implementar procedimientos para la gestión de medio removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	No cumple	No existe documentación o ejecución de control comentado.

ANEXO			ESTADO	EVIDENCIA
A8.3.2	Disposición de los medios	Control: Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	No cumple	No existe documentación o ejecución de control comentado.
A8.3.3	Transferencia de medios físicos	Control: Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	No cumple	No existe documentación o ejecución de control comentado.
A9	CONTROL DE ACCESO			
A9.1	Requisitos del negocio para el control de acceso			
Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.				
A9.1.1	Política de control de acceso	Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información.	No cumple	No existe documentación o ejecución de control comentado.
A9.1.2	Acceso a redes y a servicios en red	Control: Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	No cumple	No existe documentación o ejecución de control comentado.
A9.2	Gestión de acceso de usuarios			
Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.				
A9.2.1	Registro y cancelación del registro de usuarios	Control: Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	No cumple	No existe documentación o ejecución de control comentado.
A9.2.2	Suministro de acceso de usuarios	Control: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.	No cumple	No existe documentación o ejecución de control comentado.
A9.2.3	Gestión de derechos de acceso privilegiado	Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	No cumple	No existe documentación o ejecución de control comentado.
A9.2.4	Gestión de información de autenticación secreta de usuarios	Control: La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	No cumple	No existe documentación o ejecución de control comentado.
A9.2.5	Revisión de los derechos de acceso de usuarios	Control: Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	No cumple	No existe documentación o ejecución de control comentado.
A9.2.6	Retiro o ajuste de los derechos de acceso	Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	No cumple	No existe documentación o ejecución de control comentado.
A9.3	Responsabilidades de los usuarios			
Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.				
A9.3.1	Uso de información de autenticación secreta	Control: Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	No cumple	No existe documentación o ejecución de control comentado.

ANEXO			ESTADO	EVIDENCIA
A9.4	Control de acceso a sistemas y aplicaciones			
Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.				
A9.4.1	Restricción de acceso a la información	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	No cumple	No existe documentación o ejecución de control comentado.
A9.4.2	Procedimiento de ingreso seguro	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	No cumple	No existe documentación o ejecución de control comentado.
A9.4.3	Sistema de gestión de contraseñas	Control: Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	No cumple	No existe documentación o ejecución de control comentado.
A9.4.4	Uso de programas utilitarios privilegiados	Control: Se debe restringir y controlar estrictamente el usos de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	No cumple	No existe documentación o ejecución de control comentado.
A9.4.5	Control de acceso a códigos fuente de programas	Control: Se debe restringir el acceso a los códigos fuente de los programas.	No cumple	No existe documentación o ejecución de control comentado.
A10	CRIPTOGRAFIA			
A10.1	Controles criptográficos			
Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o la integridad de la información				
A10.1.1	Política sobre el uso de controles criptográficos	Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	No cumple	No existe documentación o ejecución de control comentado.
A10.1.2	Gestión de llaves	Control: Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.	No cumple	No existe documentación o ejecución de control comentado.
A11	SEGURIDAD FISICA Y DEL ENTORNO			
A11.1	Áreas seguras			
Objetivo: Prevenir el acceso físico no autorizado, el daño e la interferencia a la información y a las instalaciones de procesamiento de información de la organización.				
A11.1.1	Perímetro de seguridad física	Control: Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o critica, e instalaciones de manejo de información.	No cumple	No existe documentación o ejecución de control comentado.
A11.1.2	Controles de acceso físicos	Control: Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.	No cumple	No existe documentación o ejecución de control comentado.
A11.1.3	Seguridad de oficinas, recintos e instalaciones.	Control: Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones.	No cumple	No existe documentación o ejecución de control comentado.

ANEXO			ESTADO	EVIDENCIA
A11.1.4	Protección contra amenazas externas y ambientales.	Control: Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	No cumple	No existe documentación o ejecución de control comentado.
A11.1.5	Trabajo en áreas seguras.	Control: Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	No cumple	No existe documentación o ejecución de control comentado.
A11.1.6	Áreas de carga, despacho y acceso público	Control: Se deben controlar los puntos de acceso tales como las áreas de despacho y carga y otros puntos por donde pueden entrar personas no autorizadas y, si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	No cumple	No existe documentación o ejecución de control comentado.
A11.2	Equipos			
Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.				
A11.2.1	Ubicación y protección de los equipos	Control: Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	No cumple	No existe documentación o ejecución de control comentado.
A11.2.2	Servicios de suministro	Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	No cumple	No existe documentación o ejecución de control comentado.
A11.2.3	Seguridad en el cableado.	Control: El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.	No cumple	No existe documentación o ejecución de control comentado.
A11.2.4	Mantenimiento de los equipos.	Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	No cumple	No existe documentación o ejecución de control comentado.
A11.2.5	Retiro de activos	Control: Los equipos, información o software no se deben retirar de su sitio sin autorización previa	No cumple	No existe documentación o ejecución de control comentado.
A11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Control: Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	No cumple	No existe documentación o ejecución de control comentado.
A11.2.7	Disposición segura o reutilización de equipos	Control: Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobrescrito en forma segura antes de su disposición o reúso.	No cumple	No existe documentación o ejecución de control comentado.
A11.2.8	Equipos de usuario desatendido	Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	No cumple	No existe documentación o ejecución de control comentado.

ANEXO			ESTADO	EVIDENCIA
A11.2.9	Política de escritorio limpio y pantalla limpia	Control: Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	No cumple	No existe documentación o ejecución de control comentado.
A12	SEGURIDAD DE LAS OPERACIONES			
A12.1	Procedimientos operacionales y responsabilidades			
Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.				
A12.1.1	Procedimientos de operación documentados	Control: Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.	No cumple	No existe documentación o ejecución de control comentado.
A12.1.2	Gestión de cambios	Control: Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	No cumple	No existe documentación o ejecución de control comentado.
A12.1.3	Gestión de capacidad	Control: Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.	No cumple	No existe documentación o ejecución de control comentado.
A12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Control: Se deben separar los ambientes de desarrollo, pruebas y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	No cumple	No existe documentación o ejecución de control comentado.
A12.2	Protección contra códigos maliciosos			
Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.				
A12.2.1	Controles contra códigos maliciosos	Control: Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	Cumple parcialmente	Existen Equipos de Seguridad Perimetral que previenen estos ataques, pero no hay documentación en donde se explique a los usuarios cómo actuar ante un posible ataque.
A12.3	Copias de respaldo			
Objetivo: Proteger contra la pérdida de datos				
A12.3.1	Respaldo de la información	Control: Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	Cumple parcialmente	Existe Sistemas de respaldo (físicos y lógicos), pero que no se encuentran documentados.
A12.4	Registro y seguimiento			
Objetivo: Registrar eventos y generar evidencia				
A12.4.1	Registro de eventos	Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	No cumple	No existe documentación o ejecución de control comentado.

ANEXO			ESTADO	EVIDENCIA
A12.4.2	Protección de la información de registro	Control: Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	No cumple	No existe documentación o ejecución de control comentado.
A12.4.3	Registros del administrador y del operador	Control: Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.	No cumple	No existe documentación o ejecución de control comentado.
A12.4.4	Sincronización de relojes	Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	No cumple	No existe documentación o ejecución de control comentado.
A12.5	Control de software operacional			
Objetivo: Asegurarse de la integridad de los sistemas operacionales				
A12.5.1	Instalación de software en sistemas operativos	Control: Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	No cumple	No existe documentación o ejecución de control comentado.
A12.6	Gestión de la vulnerabilidad técnica			
Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas				
A12.6.1	Gestión de las vulnerabilidades técnicas	Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	No cumple	No existe documentación o ejecución de control comentado.
A12.6.2	Restricciones sobre la instalación de software	Control: Se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios.	No cumple	No existe documentación o ejecución de control comentado.
A12.7	Consideraciones sobre auditorias de sistemas de información			
Objetivo: Minimizar el impacto de las actividades de auditoria sobre los sistemas operativos				
A12.7.1	Controles de auditorías de sistemas de información	Control: Los requisitos y actividades de auditoria que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	No cumple	No existe documentación o ejecución de control comentado.
A13	SEGURIDAD DE LAS COMUNICACIONES			
A13.1	Gestión de la seguridad de las redes			
Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.				
A13.1.1	Controles de redes	Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	No cumple	No existe documentación o ejecución de control comentado.
A13.1.2	Seguridad de los servicios de red	Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	No cumple	No existe documentación o ejecución de control comentado.
A13.1.3	Separación en las redes	Control: Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	No cumple	No existe documentación o ejecución de control comentado.
A13.2	Transferencia de información			

ANEXO			ESTADO	EVIDENCIA
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.				
A13.2.1	Políticas y procedimientos de transferencia de información	Control: Se debe contar con políticas, procedimientos y controles de transferencia información formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.	No cumple	No existe documentación o ejecución de control comentado.
A13.2.2	Acuerdos sobre transferencia de información	Control: Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.	No cumple	No existe documentación o ejecución de control comentado.
A13.2.3	Mensajería Electrónica	Control: Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	No cumple	No existe documentación o ejecución de control comentado.
A13.2.4	Acuerdos de confidencialidad o de no divulgación	Control: Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	No cumple	No existe documentación o ejecución de control comentado.
A14	Adquisición, desarrollo y mantenimiento de sistemas			
A14.1	Requisitos de seguridad de los sistemas de información			
Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes.				
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Control: Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	No cumple	No existe documentación o ejecución de control comentado.
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	Control: La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	No cumple	No existe documentación o ejecución de control comentado.
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones.	Control: La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.	No cumple	No existe documentación o ejecución de control comentado.
A14.2	Seguridad en los procesos de Desarrollo y de Soporte			
Objetivo: Asegurar que la seguridad de la información este diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.				

ANEXO			ESTADO	EVIDENCIA
A.14.2.1	Política de desarrollo seguro	Control: Se debe establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.	No aplica	La organización no es una entidad dedicada al desarrollo o producción de Software, es un Integrador de Servicios de Telecomunicaciones.
A.14.2.2	Procedimientos de control de cambios en sistemas	Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.	No aplica	La organización no es una entidad dedicada al desarrollo o producción de Software, es un Integrador de Servicios de Telecomunicaciones.
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Control: Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	No aplica	La organización no es una entidad dedicada al desarrollo o producción de Software, es un Integrador de Servicios de Telecomunicaciones.
A.14.2.4	Restricciones en los cambios a los paquetes de software	Control: Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	No aplica	La organización no es una entidad dedicada al desarrollo o producción de Software, es un Integrador de Servicios de Telecomunicaciones.
A.14.2.5	Principio de Construcción de los Sistemas Seguros.	Control: Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	No aplica	La organización no es una entidad dedicada al desarrollo o producción de Software, es un Integrador de Servicios de Telecomunicaciones.
A.14.2.6	Ambiente de desarrollo seguro	Control: Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	No aplica	La organización no es una entidad dedicada al desarrollo o producción de Software, es un Integrador de Servicios de Telecomunicaciones.
A.14.2.7	Desarrollo contratado externamente	Control: La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	No aplica	La organización no es una entidad dedicada al desarrollo o producción de Software, es un Integrador de Servicios de Telecomunicaciones.

ANEXO			ESTADO	EVIDENCIA
A.14.2.8	Pruebas de seguridad de sistemas	Control: Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.	No aplica	La organización no es una entidad dedicada al desarrollo o producción de Software, es un Integrador de Servicios de Telecomunicaciones.
A.14.2.9	Prueba de aceptación de sistemas	Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.	No aplica	La organización no es una entidad dedicada al desarrollo o producción de Software, es un Integrador de Servicios de Telecomunicaciones.
A14.3	Datos de prueba			
Objetivo: Asegurar la protección de los datos usados para pruebas.				
A.14.3.1	Protección de datos de prueba	Control: Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.	No cumple	No existe documentación o ejecución de control comentado.
A15	RELACIONES CON LOS PROVEEDORES			
A15.1	Seguridad de la información en las relaciones con los proveedores.			
Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.				
A15.1.1	Política de seguridad de la información para las relaciones con proveedores	Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.	No cumple	No existe documentación o ejecución de control comentado.
A15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Control: Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	No cumple	No existe documentación o ejecución de control comentado.
A15.1.3	Cadena de suministro de tecnología de información y comunicación	Control: Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	No cumple	No existe documentación o ejecución de control comentado.
A15.2	Gestión de la prestación de servicios de proveedores			
Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores				
A15.2.1	Seguimiento y revisión de los servicios de los proveedores	Control: Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	No cumple	No existe documentación o ejecución de control comentado.

ANEXO			ESTADO	EVIDENCIA
A15.2.2	Gestión del cambio en los servicios de los proveedores	Control: Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y las mejoras de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos de negocio involucrados, y la revaluación de los riesgos.	No cumple	No existe documentación o ejecución de control comentado.
A16	GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION			
A16.1	Gestión de incidentes y mejoras en la seguridad de la información			
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.				
A16.1.1	Responsabilidades y procedimientos	Control: Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	No cumple	No existe documentación o ejecución de control comentado.
A16.1.2	Reporte de eventos de seguridad de la información	Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.	No cumple	No existe documentación o ejecución de control comentado.
A16.1.3	Reporte de debilidades de seguridad de la información	Control: Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	No cumple	No existe documentación o ejecución de control comentado.
A16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Control: Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.	No cumple	No existe documentación o ejecución de control comentado.
A16.1.5	Respuesta a incidentes de seguridad de la información	Control: Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	No cumple	No existe documentación o ejecución de control comentado.
A16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o impacto de incidentes futuros.	No cumple	No existe documentación o ejecución de control comentado.
A16.1.7	Recolección de evidencia	Control: La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	No cumple	No existe documentación o ejecución de control comentado.
A17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO			
A17.1	Continuidad de Seguridad de la información			
Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.				
A17.1.1	Planificación de la continuidad de la seguridad de la información	Control: La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	No cumple	No existe documentación o ejecución de control comentado.

ANEXO			ESTADO	EVIDENCIA
A17.1.2	Implementación de la continuidad de la seguridad de la información	Control: La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	No cumple	No existe documentación o ejecución de control comentado.
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Control: La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.	No cumple	No existe documentación o ejecución de control comentado.
A17.2	Redundancias			
Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.				
A17.2.1	Disponibilidad de instalaciones de procesamiento de información	Control: Las instalaciones de procesamientos de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	No cumple	No existe documentación o ejecución de control comentado.
A18	CUMPLIMIENTO			
A18.1	Cumplimiento de requisitos legales y contractuales			
Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.				
A18.1.1	Identificación de la legislación aplicable.	Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.	No cumple	No existe documentación o ejecución de control comentado.
A18.1.2	Derechos propiedad intelectual (DPI)	Control: Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.	No cumple	No existe documentación o ejecución de control comentado.
A18.1.3	Protección de registros	Control: Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	No cumple	No existe documentación o ejecución de control comentado.
A18.1.4	Privacidad y protección de información de datos personales	Control: Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige e la legislación y la reglamentación pertinentes, cuando sea aplicable.	No cumple	No existe documentación o ejecución de control comentado.
A18.1.5	Reglamentación de controles criptográficos.	Control: Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	No cumple	No existe documentación o ejecución de control comentado.
A18.2	Revisiones de seguridad de la información			

ANEXO			ESTADO	EVIDENCIA
Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.				
A18.2.1	Revisión independiente de la seguridad de la información	Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información), se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	No cumple	No existe documentación o ejecución de control comentado.
A18.2.2	Cumplimiento con las políticas y normas de seguridad	Control: Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.	No cumple	No existe documentación o ejecución de control comentado.
A18.2.3	Revisión del cumplimiento técnico	Control: Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	No cumple	No existe documentación o ejecución de control comentado.

ANEXO II: Vulnerabilidades y Amenazas de Activos Valorados

No	Nombre del Activo	Descripción	Vulnerabilidades	Amenazas
1	Sistema de Gestión de Tickets	Sistema de gestión de boletas de atención de averías y/o servicios solicitados por los distintos clientes que cuenta o no con contrato de Servicios de Mantenimiento, Instalación y otros con la organización.	Falta de cierre de inicio de sesión en cada logueo realizado.	Manipulación de la Información
			No existe definición de roles de usuarios. Es decir, el mismo usuario además de crear boletas de atención, puede observar módulos contables no autorizados, entre otros.	Abuso de derechos
			Servicios innecesarios para los usuarios que acceden al sistema.	Abuso de derechos / Procesamiento ilegal de los datos
			Contraseñas de acceso definidas son de un nivel de protección o durabilidad muy baja.	Espionaje de Contraseñas / Ataques de diccionario / Acceso no autorizado al Sistema
			Fallas en tomas de alimentación eléctrica estabilizada de servidor que aloja aplicación o software (inestabilidad de alimentación eléctrica / no conectada en tomas de acceso a UPS)	Inoperatividad del Sistema
			Aplicación no cuenta con un sistema de respaldo en otro servidor dedicado, teniendo en cuenta la criticidad del mismo.	Robo o pérdida de documentación ingresada
			Ausencia de Mantenimiento de servidor que aloja aplicación o software de Gestión de Tickets.	Inoperatividad del Sistema / Destrucción de la propia aplicación
			Falta de logs de la aplicación o software para posteriores auditorias.	Abuso de derechos / Procesamiento ilegal de los datos
			Transmisión de contraseñas de acceso por teléfono o vía correo.	Abuso de derechos / Procesamiento ilegal de los datos / Manipulación de la Información

No	Nombre del Activo	Descripción	Vulnerabilidades	Amenazas
			Ausencia de Responsable de acceso y/o modificación de aplicativo	Manipulación de la Información / Abusos de derechos
			Falta de actualizaciones en servidor donde se aloja la aplicación y de la propia aplicación.	Mal funcionamiento de Software y/o aplicación / Inoperatividad del Sistema
			Ausencia de responsable del bien	Abuso de derechos / Robo o pérdida de documentación ingresada
			Mala gestión de Contraseñas	Abuso de derechos
			Control de accesos no definidos mediante documentación o asignación de responsabilidades.	Abuso de derechos / Robo o pérdida de documentación ingresada
			Ausencia de documento donde se especifique que el personal que accede a la aplicación debe preservar la confidencialidad, integridad y de ser el caso la disponibilidad de la misma.	Abuso de derechos / Robo o pérdida de documentación ingresada
			Manejo inadecuado de software o herramientas brindadas por la organización.	Abuso de derechos / Robo de Información / Manipulación de la Información
			Red cableada expuesta a acceso no autorizado.	Sniffer de Información / Perdidas de comunicación por manipulación
2	Contratos de Servicios, Instalación, entre otros	Documentación física de contratos firmados con los distintos clientes con los que cuenta la organización.	Acceso a información se encuentra en un armario de total acceso a usuarios no autorizados, no existen candado ni llaves para su acceso.	Manipulación de la Información / Abusos de derechos
			Ausencia de Responsable de acceso a documentación física	Robo o pérdida de documentación ingresada
			No existe definición de procedimientos para el movimiento o traslado del activo dentro y fuera de la oficina.	Manipulación de la Información / Abusos de derechos
			Falta de mecanismos de backup para la documentación física.	Robo o pérdida de documentación ingresada

No	Nombre del Activo	Descripción	Vulnerabilidades	Amenazas
			Ausencia de responsable del bien	Abuso de derechos / Robo o pérdida de documentación ingresada
			Control de accesos no definidos mediante documentación o asignación de responsabilidades.	Abuso de derechos / Robo o pérdida de documentación ingresada
			Ausencia de documento donde se especifique que el personal que accede a la documentación de la organización debe preservar la confidencialidad, integridad y de ser el caso la disponibilidad de la misma.	Abuso de derechos / Robo o pérdida de documentación ingresada
3	Carpetas de proyectos	Contiene información del planeamiento, desarrollo, ejecución y cierre de los distintos proyectos que ejecuta la organización. El tipo de documentación está referida a: reuniones pactadas, correos de coordinación, fases de proyectos, cronogramas, informes, comunicados, actas en sus distintas variedades, diseños de red, topologías, datos de contactos/clientes y demás información del desarrollo del proyecto.	No existen controles para su acceso a nivel de acceso y seguridad de carpetas a pesar de comunicado difundido.	Manipulación de la Información
			Ausencia de responsable de acceso a carpeta	Manipulación de la Información / Abusos de derechos
			Ausencia de backup o respaldo de documentación de carpeta	Robo o pérdida de documentación ingresada
			Uso inadecuado del contenido de la carpeta.	Manipulación de la Información
			Ausencia de controles contra modificación o alteración de contenido de carpeta.	Robo o pérdida de documentación ingresada
			Ausencia de responsable del bien.	Abuso de derechos / Robo o pérdida de documentación ingresada
			Control de accesos no definidos mediante documentación o asignación de responsabilidades.	Abuso de derechos / Robo o pérdida de documentación ingresada
			Ausencia de documento donde se especifique que el personal que accede a la documentación de la organización debe preservar la confidencialidad, integridad y de ser el caso la disponibilidad de la misma.	Abuso de derechos / Robo o pérdida de documentación ingresada
			Red cableada expuesta a acceso no autorizado.	Sniffer de Información / Perdidas de comunicación por manipulación

No	Nombre del Activo	Descripción	Vulnerabilidades	Amenazas
4	Carpeta de Licitaciones	Contiene la información del desarrollo y ejecución de las propuestas comerciales con entidades privadas y estatales. El tipo de documentación incluye: documentos contractuales, Informes, Comunicados, Actas, datos de contactos/clientes y demás información del desarrollo del proyecto.	No existen controles para su acceso a nivel de acceso y seguridad de carpetas a pesar de comunicado difundido.	Manipulación de la Información
			Ausencia de responsable de acceso a carpeta	Manipulación de la Información / Abusos de derechos
			Ausencia de backup o respaldo de documentación de carpeta	Robo o pérdida de documentación ingresada
			Uso inadecuado del contenido de la carpeta.	Manipulación de la Información
			Ausencia de controles contra modificación o alteración de contenido de carpeta.	Robo o pérdida de documentación ingresada
			Ausencia de responsable del bien.	Abuso de derechos / Robo o pérdida de documentación ingresada
			Control de accesos no definidos mediante documentación o asignación de responsabilidades.	Abuso de derechos / Robo o pérdida de documentación ingresada
			Ausencia de documento donde se especifique que el personal que accede a la documentación de la organización debe preservar la confidencialidad, integridad y de ser el caso la disponibilidad de la misma.	Abuso de derechos / Robo o pérdida de documentación ingresada
			Red cableada expuesta a acceso no autorizado.	Sniffer de Información / Perdidas de comunicación por manipulación
5	Carpetas de Áreas Administrativas y Contabilidad	Contiene información referida a procesos administrativos y contables de la organización, este tipo de documentación comprende: planes de negocio, documentación contable, documentación financiera, acuerdos bancarios, entre otros.	No existen controles para su acceso a nivel de acceso y seguridad de carpetas a pesar de comunicado difundido.	Manipulación de la Información
			Ausencia de responsable de acceso a carpeta	Manipulación de la Información / Abusos de derechos
			Ausencia de backup o respaldo de documentación de carpeta	Robo o pérdida de documentación ingresada
			Uso inadecuado del contenido de la carpeta.	Manipulación de la Información
			Ausencia de controles contra modificación o alteración de contenido de carpeta.	Robo o pérdida de documentación ingresada

No	Nombre del Activo	Descripción	Vulnerabilidades	Amenazas
			Ausencia de responsable del bien.	Abuso de derechos / Robo o pérdida de documentación ingresada
			Control de accesos no definidos mediante documentación o asignación de responsabilidades.	Abuso de derechos / Robo o pérdida de documentación ingresada
			Ausencia de documento donde se especifique que el personal que accede a la documentación de la organización debe preservar la confidencialidad, integridad y de ser el caso la disponibilidad de la misma.	Abuso de derechos / Robo o pérdida de documentación ingresada
			Red cableada expuesta a acceso no autorizado.	Sniffer de Información / Perdidas de comunicación por manipulación
6	Equipos de Computo	Referida a equipos portátiles y equipos de escritorio, entre ellos: laptop, desktop, proyectores, teclados, monitores, modem, mouses, entre otros.	Falta de cierre de inicio de sesión en cada logueo realizado.	Manipulación de la Información
			Contraseñas de acceso definidas son de un nivel de protección o durabilidad muy baja.	Espionaje de Contraseñas / Ataques de diccionario / Acceso no autorizado al Sistema / Acceso no autorizado al equipo
			Transmisión de contraseñas de acceso por teléfono o vía correo.	Abuso de derechos / Procesamiento ilegal de los datos / Manipulación de la Información
			No existe definición de procedimientos para el movimiento o traslado del activo dentro y fuera de la oficina.	Manipulación de la Información / Abusos de derechos / Robo de equipo / Inoperatividad del equipo y/o equipos / Fallas en el funcionamiento de equipo y/o equipos
			Algunos equipos no se encuentran ingresadas en el dominio, no cumpliendo los estándares de seguridad aplicados por la organización.	Abuso de derechos

No	Nombre del Activo	Descripción	Vulnerabilidades	Amenazas
			No existe controles de desinstalación de programas/aplicaciones auditables instaladas por la organización	Abusos de derechos
			Ausencia o falta de backup o respaldos de documentación interna de los equipos o de la información más relevante.	Robo o pérdida de documentación ingresada
			Falta de mecanismos de autenticación de usuarios sobre los equipos de cómputo asignados.	Abuso de derechos
			Ausencia de protección física para el retiro de equipos a clientes.	inoperatividad del equipo y/o equipos / Robo de Equipo
			Ausencia de responsable del bien	Abuso de derechos / Robo o pérdida de documentación ingresada
			Ausencia de controles de retiro de equipos para labores a realizar en los distintos clientes	Abuso de derechos / Robo o pérdida de documentación ingresada / Inoperatividad del equipo y/o equipos / Robo de Equipo
			Mala gestión de contraseñas	Abuso de derechos
			Ausencia de backup o respaldo de la información interna.	Robo o pérdida de documentación ingresada / Inoperatividad del equipo y/o equipos / Fallas en el funcionamiento de equipo y/o equipos
			Control de accesos no definidos mediante documentación o asignación de responsabilidades.	Abuso de derechos / Inoperatividad del equipo y/o equipos
7	Correo Electrónico	Servicio de correo electrónico para los distintos colaboradores de la organización.	Red cableada expuesta a acceso no autorizado.	Sniffer de Información
			Falta de cierre de inicio de sesión en cada logueo realizado.	Manipulación de la Información
			Contraseñas de acceso definidas son de un nivel de protección o durabilidad muy baja.	Espionaje de Contraseñas / Ataques de diccionario / Acceso no autorizado al Sistema

No	Nombre del Activo	Descripción	Vulnerabilidades	Amenazas
			Fallas en tomas de alimentación eléctrica estabilizada de servidor que aloja aplicación o software (inestabilidad de alimentación eléctrica / no conectada en tomas de acceso a UPS)	Inoperatividad del sistema o servicio
			Aplicación no cuenta con un sistema de respaldo en otro servidor dedicado, teniendo en cuenta la criticidad del mismo.	Robo o pérdida de documentación ingresada
			Ausencia de Mantenimiento de servidor que aloja aplicación o software de Correo Electrónico	Inoperatividad del Sistema / Destrucción de equipo o propia aplicación
			Transmisión de contraseñas de acceso por teléfono o vía correo.	Abuso de derechos / Procesamiento ilegal de los datos / Manipulación de la Información
			Falta de actualizaciones en servidor donde se aloja la aplicación y de la propia aplicación.	Mal funcionamiento de Software y/o aplicación / Inoperatividad del Sistema
			Ausencia de responsable del bien	Abuso de derechos / Robo o pérdida de documentación ingresada
			Ausencia de políticas y/o procedimientos para envío de correos (tamaño, destinatario, adjunto, etc).	Abuso de derechos
			Mala gestión de Contraseñas	Abuso de derechos
			Ausencia de backup o respaldo de la información Extensiones .pst)	Robo o pérdida de documentación ingresada
			Falta de gestión de logs en servidor de correo para seguimiento o auditoria.	Abuso de derechos / Procesamiento ilegal de los datos
			Ausencia de documento donde se especifique que el personal que accede a la aplicación debe preservar la confidencialidad, integridad y de ser el caso la disponibilidad de la misma.	Abuso de derechos / Robo o pérdida de documentación ingresada

No	Nombre del Activo	Descripción	Vulnerabilidades	Amenazas
			Manejo inadecuado de software o herramientas brindadas por la organización.	Abuso de derechos / Robo de Información / Manipulación de la Información
			Ausencia de mecanismos de protección contra correo del tipo SPAM	Correos entrantes con contenidos maliciosos y/o SPAM
			Red cableada expuesta a acceso no autorizado.	Sniffer de Información / Perdidas de comunicación por manipulación
8	Internet / Servicios Dedicados	Servicio dedicado de Internet y Servicios dedicados de interconexión hacia las distintas Sedes	Fallas en tomas de alimentación eléctrica estabilizada (inestabilidad de alimentación eléctrica / no conectada en tomas de acceso a UPS).	Inoperatividad del Sistema
			Ausencia de responsable del bien.	Abuso de derechos / Robo o pérdida de información interna
			Falta de gestión de logs en consumo de recursos de Navegación en Internet para seguimiento o auditoria.	Abuso de derechos / Procesamiento ilegal de los datos / Saturación del circuito de Internet
			Falta de disponibilidad del servicio por parte del proveedor o ISP.	Perdida de actividad de labores
			Falta de Mantenimiento de equipamiento de acceso a Internet otorgado por el Proveedor o ISP	Inoperatividad del Sistema / Destrucción de equipo o propia aplicación
			Acceso a Data Center no definido mediante documentación y/o asignación de responsabilidades.	Abuso de derechos / Robo de Información
			Control de accesos de navegación a Internet no definidos mediante documentación o asignación de perfiles.	Abuso de derechos / Robo de Información
			Red perimetral de la organización carece de mecanismos de defensa ante ataques de día cero (Zero days), malware conocido o específicamente código malicioso	Acceso a destinos de alto riesgo de infección / Infección de Código malicioso: Virus, Spyware, Ransomware, entre otros en la red interna

No	Nombre del Activo	Descripción	Vulnerabilidades	Amenazas
			Ausencia de mecanismos de protección y concientización al usuario sobre ataques de Ingeniería Social y Phishing	Abuso de derechos / Robo de Información / Infección de Código malicioso: Virus, Spyware, Ransomware, entre otros en la red interna
			Red cableada expuesta a acceso no autorizado.	Sniffer de Información / Pérdidas de comunicación por manipulación
9	File Server (Servidor de Archivos)	Servidor de archivos que contiene los diversos directorios de las distintas áreas de la organización. Servicio de FTP dentro del propio servidor	Fallas en tomas de alimentación eléctrica estabilizada de servidor que aloja aplicación o software (inestabilidad de alimentación eléctrica / no conectada en tomas de acceso a UPS)	Inoperatividad del sistema o servicio / Destrucción de equipo / Falla en el suministro eléctrico
			Ausencia de controles contra modificación o alteración de contenido de carpeta.	Robo o pérdida de documentación ingresada
			Ausencia de hardware de backup.	Pérdida de Documentación ingresada
			Ausencia de responsable del bien.	Abuso de derechos / Robo o pérdida de documentación ingresada
			Ausencia de mantenimiento a servidor de archivos.	Inoperatividad del equipo y/o equipos / Destrucción de equipo
			Falta de gestión de logs en servidor de archivos para seguimiento o auditoria.	Abuso de derechos / Procesamiento ilegal de los datos
			Ausencia de backup o respaldo de la información interna.	Robo o pérdida de documentación ingresada
			Control de accesos no definidos mediante documentación o asignación de responsabilidades.	Abuso de derechos / Robo o pérdida de documentación ingresada

No	Nombre del Activo	Descripción	Vulnerabilidades	Amenazas
			Control de accesos a equipos, sistemas y aplicaciones mediante mecanismos técnicos	Acceso no autorizado al sistema / Acceso no autorizado al equipo / Fallas en el funcionamiento de equipo y/o equipos / Procesamiento ilegal de los datos
			Ausencia de documento donde se especifique que el personal que accede al servidor debe preservar la confidencialidad, integridad y de ser el caso la disponibilidad de la misma.	Abuso de derechos / Robo o pérdida de documentación ingresada / Acceso no autorizado al sistema / Acceso no autorizado al equipo
			Red cableada expuesta a acceso no autorizado.	Sniffer de Información / Perdidas de comunicación por manipulación
10	Infraestructura de Comunicaciones	Comprende equipamiento de infraestructura de comunicaciones, tales como: Router, modem, switches, servidores, aceleradores de ancho de banda, central telefónica, firewall, entre otros.	Fallas en tomas de alimentación eléctrica estabilizada de servidor que aloja aplicación o software (inestabilidad de alimentación eléctrica / no conectada en tomas de acceso a UPS)	Inoperatividad del Sistema / Destrucción de equipo / Falla en el suministro eléctrico
			Ausencia o falta de backup o respaldos de documentación interna de los equipos o de la información más relevante.	Robo o pérdida de documentación ingresada
			Ausencia de hardware de backup.	Robo o pérdida de documentación ingresada / Fallas en el funcionamiento de equipo y/o equipos / Inoperatividad del equipo y/o equipos / Robo de equipo
			Equipos que componen la Infraestructura de Comunicaciones que soportan los sistemas y servicios críticos no cuentan con equipos alternos en ubicaciones alternas que permitan la continuidad del negocio.	Falla masiva / Ataque de cualquier tipo que atente contra la continuidad del negocio / Desastre natural

No	Nombre del Activo	Descripción	Vulnerabilidades	Amenazas
			Ausencia de responsable del bien.	Abuso de derechos / Robo o pérdida de documentación ingresada
			Mala gestión de Contraseñas	Abuso de derechos / Ataque de diccionario
			Falta de Mantenimiento de equipamiento de Infraestructura	Inoperatividad del sistema o servicio / Inoperatividad del equipo y/o equipos / Fallas en el funcionamiento de equipo y/o equipos / Destrucción de equipo o propia aplicación
			Falta de gestión de logs en equipos de Infraestructura de comunicaciones para seguimiento o auditoria.	Abuso de derechos / Procesamiento ilegal de los datos
			Control de accesos no definidos mediante documentación o asignación de responsabilidades.	Abuso de derechos / Robo o pérdida de documentación ingresada
			Control de accesos a equipos, sistemas y aplicaciones mediante mecanismos técnicos	Acceso no autorizado al sistema / Fallas en el funcionamiento de equipo y/o equipos / Procesamiento ilegal de los datos
			Red cableada expuesta a acceso no autorizado.	Sniffer de Información / Perdidas de comunicación por manipulación
11	Personal	Personal que desarrolla las distintas actividades dentro y fuera de la organización.	Falta de inducción, capacitación y sensibilización sobre riesgos.	Incumplimiento de Normas establecidas respecto a Seguridad de la Información / Abuso de derecho / Ataques de Phishing / Ingeniería Social

No	Nombre del Activo	Descripción	Vulnerabilidades	Amenazas
			Renuncias y/o despidos del personal	Abuso de confidencialidad de datos / Apropiación indebida de activos
			Ausencia de documento donde se especifique que el personal que accede a la documentación de la organización debe preservar la confidencialidad, integridad y de ser el caos la disponibilidad de la misma.	Abuso de confidencialidad, integridad y disponibilidad de la información / Robo o pérdida de información ingresada / Procesamiento ilegal de los datos
			Manejo inadecuado de software o herramientas brindadas por la organización.	Abuso de derechos / Robo de Información / Manipulación de la Información
			Ausencia de orden en asignación de servicios a los distintos clientes de la empresa u organización.	No resolución de problemas tecnológicos / Negligencia en trabajos asignados / Clientes insatisfechos

ANEXO III: Matriz de Riesgos

RIESGOS			VULNERABILIDADES	Σ PROBABILIDAD DEL RIESGO	PROBABILIDAD DEL RIESGO	INTERPRETACIÓN DE LA PROBABILIDAD DEL RIESGO	NIVEL DE RIESGO (IMPACTO * PROBABILIDAD)	INTERPRETACIÓN DEL RIESGO	NIVEL DE ACEPTACIÓN DEL RIESGO
ACTIVO	INTEGRANTE	IMPACTO DEL ACTIVO	INTERPRETACIÓN DEL IMPACTO						
Sistema de Gestión de Tickets	A	5	MUY ALTO	63	4	ALTO	20	MUY ALTO	IMPORTANTE
	B	5	MUY ALTO	67	4	ALTO	20	MUY ALTO	IMPORTANTE
	C	5	MUY ALTO	67	4	ALTO	20	MUY ALTO	IMPORTANTE
	D	5	MUY ALTO	61	4	ALTO	20	MUY ALTO	IMPORTANTE
Contratos de Servicios, Instalación, entre otros	A	5	MUY ALTO	30	2	BAJO	10	ALTO	CONSIDERABLE
	B	5	MUY ALTO	31	2	BAJO	10	ALTO	CONSIDERABLE
	C	4	ALTO	32	2	BAJO	8	MEDIO	CONSIDERABLE
	D	5	MUY ALTO	35	2	BAJO	10	ALTO	CONSIDERABLE
Carpeta de Proyectos	A	5	MUY ALTO	42	3	MEDIO	15	ALTO	CONSIDERABLE
	B	5	MUY ALTO	41	3	MEDIO	15	ALTO	CONSIDERABLE
	C	5	MUY ALTO	41	3	MEDIO	15	ALTO	CONSIDERABLE
	D	5	MUY ALTO	45	3	MEDIO	15	ALTO	CONSIDERABLE

RIESGOS			VULNERABILIDADES	Z PROBABILIDAD DEL RIESGO	PROBABILIDAD DEL RIESGO	INTERPRETACIÓN DE LA PROBABILIDAD DEL RIESGO	NIVEL DE RIESGO (IMPACTO * PROBABILIDAD)	INTERPRETACIÓN DEL RIESGO	NIVEL DE ACEPTACIÓN DEL RIESGO
ACTIVO	INTEGRANTE	IMPACTO DEL ACTIVO	INTERPRETACIÓN DEL IMPACTO						
Carpeta de Licitaciones	A	5	MUY ALTO	42	3	MEDIO	15	ALTO	CONSIDERABLE
	B	5	MUY ALTO	42	3	MEDIO	15	ALTO	CONSIDERABLE
	C	5	MUY ALTO	42	3	MEDIO	15	ALTO	CONSIDERABLE
	D	5	MUY ALTO	45	3	MEDIO	15	ALTO	CONSIDERABLE
Carpetas de Áreas Administrativas y Contabilidad	A	5	MUY ALTO	41	3	MEDIO	15	ALTO	CONSIDERABLE
	B	5	MUY ALTO	41	3	MEDIO	15	ALTO	CONSIDERABLE
	C	5	MUY ALTO	42	3	MEDIO	15	ALTO	CONSIDERABLE
	D	5	MUY ALTO	45	3	MEDIO	15	ALTO	CONSIDERABLE
Equipos de Computo	A	4	ALTO	60	3	MEDIO	12	ALTO	CONSIDERABLE
	B	4	ALTO	60	3	MEDIO	12	ALTO	CONSIDERABLE
	C	5	MUY ALTO	68	4	ALTO	20	MUY ALTO	IMPORTANTE
	D	4	ALTO	59	3	MEDIO	12	ALTO	CONSIDERABLE
Correo Electrónico	A	5	MUY ALTO	60	3	MEDIO	15	ALTO	IMPORTANTE
	B	5	MUY ALTO	62	4	ALTO	20	MUY ALTO	IMPORTANTE
	C	5	MUY ALTO	61	4	ALTO	20	MUY ALTO	IMPORTANTE
	D	5	MUY ALTO	64	4	ALTO	20	MUY ALTO	IMPORTANTE

RIESGOS			VULNERABILIDADES	Σ PROBABILIDAD DEL RIESGO	PROBABILIDAD DEL RIESGO	INTERPRETACIÓN DE LA PROBABILIDAD DEL RIESGO	NIVEL DE RIESGO (IMPACTO * PROBABILIDAD)	INTERPRETACIÓN DEL RIESGO	NIVEL DE ACEPTACIÓN DEL RIESGO
ACTIVO	INTEGRANTE	IMPACTO DEL ACTIVO	INTERPRETACIÓN DEL IMPACTO						
Internet / Servicios dedicados	A	4	ALTO	32	2	BAJO	8	MEDIO	CONSIDERABLE
	B	4	ALTO	30	2	BAJO	8	MEDIO	CONSIDERABLE
	C	4	ALTO	31	2	BAJO	8	MEDIO	CONSIDERABLE
	D	4	ALTO	35	2	BAJO	8	MEDIO	CONSIDERABLE
File Server (Servidor de Archivos)	A	4	ALTO	45	3	MEDIO	12	ALTO	CONSIDERABLE
	B	5	MUY ALTO	45	3	MEDIO	15	ALTO	CONSIDERABLE
	C	5	MUY ALTO	45	3	MEDIO	15	ALTO	CONSIDERABLE
	D	5	MUY ALTO	48	3	MEDIO	15	ALTO	CONSIDERABLE
Infraestructura de Comunicaciones	A	5	MUY ALTO	40	2	BAJO	10	ALTO	CONSIDERABLE
	B	4	ALTO	40	2	BAJO	8	MEDIO	CONSIDERABLE
	C	5	MUY ALTO	39	2	BAJO	10	ALTO	CONSIDERABLE
	D	5	MUY ALTO	40	2	BAJO	10	ALTO	CONSIDERABLE
Personal	A	5	MUY ALTO	24	2	BAJO	10	ALTO	CONSIDERABLE
	B	5	MUY ALTO	22	2	BAJO	10	ALTO	CONSIDERABLE
	C	5	MUY ALTO	22	2	BAJO	10	ALTO	CONSIDERABLE
	D	5	MUY ALTO	23	2	BAJO	10	ALTO	CONSIDERABLE

ANEXO IV: Tratamiento del Riesgo

Ítem	Activo de Información	Interpretación del Riesgo	Nivel de Aceptación de Riesgos	Amenaza / Riesgo	Opción de Tratamiento del Riesgo	Dueño del Riesgo
1	Sistema de Gestión de Tickets	Muy Alto	Importante	Manipulación de Información	Reducción y Transferencia del Riesgo	Gerente Técnico
				Abuso de derechos		
				Procesamiento ilegal de los datos		
				Espionaje de contraseñas		
				Ataques de diccionario		
				Acceso no autorizado al sistema		
				Inoperatividad del sistema o servicio		
				Destrucción de la propia aplicación		
				Mal funcionamiento de software y/o aplicación		
				Robo o pérdida de información ingresada		
				Sniffer de Información		
				Pérdidas de comunicación por manipulación		
2	Contratos de Servicios, Instalación, entre otros	Alto	Considerable	Manipulación de Información	Reducción y Transferencia del Riesgo	Gerente Técnico
				Abuso de derechos		
				Robo o pérdida de documentación ingresada		
3	Carpeta de Proyectos	Alto	Considerable	Manipulación de Información	Reducción y Transferencia del Riesgo	Gerente Técnico
				Abuso de derechos		
				Robo o pérdida de Información ingresada		
				Sniffer de Información		
				Procesamiento ilegal de los datos		
				Pérdidas de comunicación por manipulación		
4	Carpeta de Licitaciones	Alto	Considerable	Manipulación de Información	Reducción y Transferencia del Riesgo	Gerente Técnico
				Abuso de derechos		

Ítem	Activo de Información	Interpretación del Riesgo	Nivel de Aceptación de Riesgos	Amenaza / Riesgo	Opción de Tratamiento del Riesgo	Dueño del Riesgo
				Robo o pérdida de información ingresada		
				Sniffer de Información		
				Procesamiento ilegal de los datos		
				Pérdidas de comunicación por manipulación		
5	Carpetas de Áreas Administrativas y Contabilidad	Alto	Considerable	Manipulación de Información	Reducción y Transferencia del Riesgo	Gerente Técnico
				Abuso de derechos		
				Robo o pérdida de Información ingresada		
				Sniffer de Información		
				Procesamiento ilegal de los datos		
				Pérdidas de comunicación por manipulación		
6	Equipos de cómputo	Alto	Considerable	Manipulación de Información	Reducción y Transferencia del Riesgo	Gerente Técnico
				Espionaje de Contraseñas		
				Ataques de diccionario		
				Acceso no autorizado al sistema		
				Acceso no autorizado al equipo		
				Abuso de derechos		
				Procesamiento ilegal de los datos		
				Manipulación de información		
				Robo o pérdida de información ingresada		
				Robo de equipo		
				Inoperatividad del equipo y/o equipos		
				Fallas en el funcionamiento de equipo y/o equipos		
				Sniffer de Información		
7	Correo Electrónico	Muy Alto	Importante	Manipulación de información	Reducción y Transferencia del Riesgo	Gerente Técnico
				Espionaje de contraseñas		

Ítem	Activo de Información	Interpretación del Riesgo	Nivel de Aceptación de Riesgos	Amenaza / Riesgo	Opción de Tratamiento del Riesgo	Dueño del Riesgo
				Ataques de diccionario		
				Acceso no autorizado al sistema		
				Inoperatividad del sistema o servicio		
				Robo o pérdida de información ingresada		
				Abuso de derechos		
				Procesamiento ilegal de los datos		
				Mal funcionamiento de software y/o aplicación		
				Destrucción de equipo o propia aplicación		
				Sniffer de información		
				Pérdidas de comunicación por manipulación		
				Correos entrantes con contenidos maliciosos y/o SPAM		
8	Internet / Servicios dedicados	Medio	Considerable	Inoperatividad del sistema o servicio	Reducción del Riesgo	Gerente Técnico
				Abuso de derechos		
				Procesamiento ilegal de los datos		
				Perdida de actividad de labores		
				Robo o pérdida de información interna		
				Sniffer de Información		
				Pérdidas de comunicación por manipulación		
				Saturación del circuito de Internet		
				Acceso a destinos de alto riesgo de infección		
				Infección de Código malicioso: Virus, Spyware, Ransomware, entre otros en la red interna		
9	File Server (Servidor de Archivos)	Alto	Considerable	Inoperatividad del sistema o servicio	Reducción y Transferencia del Riesgo	Gerente Técnico
				Destrucción del equipo		
				Acceso no autorizado al sistema		

Ítem	Activo de Información	Interpretación del Riesgo	Nivel de Aceptación de Riesgos	Amenaza / Riesgo	Opción de Tratamiento del Riesgo	Dueño del Riesgo
				Acceso no autorizado al equipo		
				Robo o pérdida de información ingresada		
				Abuso de derechos		
				Inoperatividad del equipo y/o equipos		
				Fallas en el funcionamiento de equipo y/o equipos		
				Procesamiento ilegal de los datos		
				Sniffer de información		
				Pérdidas de comunicación por manipulación		
				Falla en el suministro eléctrico		
10	Infraestructura de Comunicaciones	Alto	Considerable	Inoperatividad del sistema o servicio	Reducción y Transferencia del Riesgo	Gerente Técnico
				Destrucción del equipo		
				Robo de Información		
				Robo o pérdida de información ingresada		
				Abuso de derechos		
				Procesamiento ilegal de los datos		
				Espionaje de Contraseñas		
				Ataques de diccionario		
				Sniffer de Información		
				Robo de Equipo		
				Inoperatividad del equipo y/o equipos		
				Fallas en el funcionamiento de equipo y/o equipos		
				Acceso no autorizado al sistema		
				Pérdidas de comunicación por manipulación		
				Desastre natural		

Ítem	Activo de Información	Interpretación del Riesgo	Nivel de Aceptación de Riesgos	Amenaza / Riesgo	Opción de Tratamiento del Riesgo	Dueño del Riesgo
				Falla en el suministro eléctrico		
				Falla masiva		
				Ataque de cualquier tipo que atente contra la continuidad del negocio		
11	Personal	Alto	Considerable	Incumplimiento de normas establecidas respecto a Seguridad de la Información	Reducción del Riesgo	Gerente Técnico
				Abuso de derechos		
				Abuso de confidencialidad de datos		
				Abuso de confidencialidad, integridad y disponibilidad de la información		
				Robo de información		
				Manipulación de información		
				No resolución de problemas tecnológicos		
				Negligencia en trabajos asignados		
				Clientes insatisfechos		
				Robo o pérdida de información ingresada		
				Procesamiento ilegal de los datos		
				Apropiación indebida de activos		
				Ataques de Phishing		
				Ingeniería Social		

ANEXO V: Plan de Tratamiento de Riesgos

ITEM	ACTIVO	AMENAZAS / RIESGOS	OPCIONES DE TRATAMIENTO DEL RIESGO	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR	DUEÑO DEL RIESGO	RESPONSABLE DEL CONTROL	ESTADO DEL CONTROL
1	Sistema de Gestión de Tickets	Manipulación de información / Abusos de derechos / Procesamiento ilegal de los datos / Acceso no autorizado al sistema / Robo o Pérdida de Información ingresada / Sniffer de Información	Reducción del riesgo	A 5.1.1 CONJUNTO DE POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN / A 5.1.2 REVISIÓN DE LAS POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN / A 18.2.2 CUMPLIMIENTO DE LAS POLÍTICAS Y NORMAS DE SEGURIDAD	Norma ISO/IEC 27002:2013	Mantener implementados los lineamientos de la Política de Seguridad de la Información y las normas de seguridad dentro de la organización. Para lograr su cumplimiento la organización tendrá auditorias programadas y encuestas bimensuales como parte de la revisión del estatus del alcance de la misma. Asimismo, la Estructura Organizacional del Sistema de Gestión de Seguridad de la Información generará reportes sobre el estado de Seguridad de Información en la organización. En ello, se evaluará si existen incumplimientos y se determinará la causa del incumplimiento, se tomarán las acciones correctivas para garantizar la reducción de estos incumplimientos.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Manipulación de información / Abuso de derechos / Procesamiento ilegal de los datos / Acceso no autorizado al sistema / Robo o pérdida de información ingresada	Reducción del riesgo	A 6.2.2 TELETRABAJO	Norma ISO/IEC 27002:2013	Se debe implementar una política y unas medidas de seguridad de soporte para proteger la información a la que se tiene acceso, la cual es procesada o almacenada en los lugares en los que se realiza teletrabajo. Es decir, se debe establecer procedimientos para el acceso del Sistema de Gestión de Ticket desde fuera de la organización. Asimismo, se debe tener en cuenta la Política de Teletrabajo la cual indica los lineamientos de conexión por VPN y otras consideraciones en el acceso.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Manipulación de información / Abuso de derechos / Procesamiento ilegal de los datos / Acceso no autorizado al sistema / Robo o pérdida de información ingresada	Reducción del riesgo	A 8.2.3 MANIPULACIÓN / MANEJO DE ACTIVOS	Norma ISO/IEC 27002:2013	Se deben desarrollar e implementar procedimientos para el manejo del Sistema de Gestión de Tickets, de acuerdo con el esquema de clasificación de información adoptado por la organización: Confidencial, privada y pública	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado

ITEM	ACTIVO	AMENAZAS / RIESGOS	OPCIONES DE TRATAMIENTO DEL RIESGO	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR	DUEÑO DEL RIESGO	RESPONSABLE DEL CONTROL	ESTADO DEL CONTROL
		Manipulación de información / Abuso de derechos / Procesamiento ilegal de los datos / Acceso no autorizado al sistema / Robo o pérdida de información ingresada	Reducción del riesgo	A 9.1.1 POLÍTICA DE CONTROL DE ACCESOS / A 9.2.2 GESTIÓN DE LOS DERECHOS DE ACCESO ASIGNADOS A USUARIOS / A 9.2.3 GESTIÓN DE LOS DERECHOS DE ACCESOS CON PRIVILEGIOS ESPECIALES / A 9.2.4 GESTIÓN DE INFORMACIÓN CONFIDENCIAL DE AUTENTIFICACIÓN DE USUARIOS	Norma ISO/IEC 27002:2013	Mantener implementados los lineamientos de la política de control de acceso. Mantener controlados los accesos de los usuarios. Capacitar a los colaboradores de la empresa sobre la utilización de contraseña al Sistema de Gestión de Tickets. La Gerencia Técnica debe delegar la función de verificación continua de los privilegios y accesos que tiene cada colaborador en la empresa. Adicionalmente, registrar la fecha y horario de su ingreso y egreso.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Manipulación de información / Abuso de derechos / Procesamiento ilegal de los datos / Espionaje de contraseñas / Acceso no autorizado al sistema	Reducción del riesgo	A 9.3.1 USO DE INFORMACIÓN CONFIDENCIAL PARA LA AUTENTICACIÓN	Norma ISO/IEC 27002:2013	Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Manipulación de información / Abuso de derechos / Procesamiento ilegal de los datos / Espionaje de contraseñas / Acceso no autorizado al sistema	Reducción del riesgo	A 9.4.1 RESTRICCIÓN DEL ACCESO A LA INFORMACIÓN / 9.4.2 PROCEDIMIENTOS SEGUROS DE INICIO DE SESIÓN / A 9.4.3 GESTIÓN DE CONTRASEÑA DE USUARIO	Norma ISO/IEC 27002:2013	La Política de Control de Acceso a implementar respecto al acceso del Sistema de Gestión de Tickets se debe controlar mediante un proceso de ingreso seguro. Asimismo, los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Inoperatividad del sistema / Mal funcionamiento del software y/o aplicación	Reducción del riesgo	A 12.1.3 GESTIÓN DE CAPACIDAD	Norma ISO/IEC 27002:2013	Se debe revisar cotidianamente y en ciclos programados el consumo de recursos del servidor que contiene al Sistema de Gestión de Tickets. Se debe monitorear regularmente sus recursos, tales como: memoria, procesamiento y almacenamiento y realizar mejoras en los mismos recursos de ser necesario, incluso el cambio del equipo de acuerdo a un dimensionamiento previamente realizado.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado

ITEM	ACTIVO	AMENAZAS / RIESGOS	OPCIONES DE TRATAMIENTO DEL RIESGO	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR	DUEÑO DEL RIESGO	RESPONSABLE DEL CONTROL	ESTADO DEL CONTROL
		Manipulación de información / Abuso de derechos / Procesamiento ilegal de los datos	Reducción del riesgo	A 13.2.4 ACUERDOS DE CONFIDENCIALIDAD O DE NO DIVULGACIÓN (SECRETO)	Norma ISO/IEC 27002:2013	Se protege el manejo de la información contra divulgación no autorizada o uso inadecuado de información propia de la organización por medio de la firma de la cláusula de confidencialidad. Asimismo, la organización debe revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación, los cuales reflejen las necesidades de la organización en materia de Seguridad de la Información.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Inoperatividad del sistema / Robo o pérdida de información ingresada / Destrucción de la propia aplicación	Reducción del riesgo	A 12.3.1 COPIAS DE SEGURIDAD DE LA INFORMACIÓN	Norma ISO/IEC 27002:2013	La información de los servicios, proyectos, implementaciones, entre otros que se manejan dentro del Sistema de Gestión de Tickets debe contar con un respaldo, entendiendo que este un Sistema Integral que reúnen consolidados de cada área de la empresa. Es decir, los datos que almacena el servidor que aloja el sistema o aplicación deben estar salvaguardados y protegidos por un respaldo mensual, semanal, o un Schedule adecuado para la organización. Asimismo, debe almacenarse en sitios alternos a la organización.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Procesamiento ilegal de los datos / Robo de Información / Mal funcionamiento del software y/o aplicación / pérdidas de comunicación por manipulación	Reducción del riesgo	A 12.4.1 REGISTRO Y GESTIÓN DE EVENTOS DE ACTIVIDAD / A 16.1.2 NOTIFICACIÓN DE LOS DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN / A 16.1.3 NOTIFICACIÓN DE DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN	Norma ISO/IEC 27002:2013	Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario respecto al Sistema de Gestión de Tickets, tales como: Excepciones, fallas, eventos de seguridad de la información, historial del consumo de la aplicación, módulos utilizados, transacciones ejecutadas, entre otros. Asimismo, reportar cualquier incidente relacionado con la seguridad de la información del sistema referido y el propio consumo del recurso.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Inoperatividad del sistema / Robo o pérdida de información ingresada / Destrucción de la propia aplicación	Reducción del riesgo	A 18.1.3 PROTECCIÓN DE LOS REGISTROS DE LA ORGANIZACIÓN	Norma ISO/IEC 27002:2013	Los registros indexados al Sistema de Gestión de Tickets se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada. Lo comentado, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado

ITEM	ACTIVO	AMENAZAS / RIESGOS	OPCIONES DE TRATAMIENTO DEL RIESGO	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR	DUEÑO DEL RIESGO	RESPONSABLE DEL CONTROL	ESTADO DEL CONTROL
		Manipulación de información / Procesamiento ilegal de los datos / Robo o pérdida de información ingresada	Reducción del riesgo	A 18.1.4 PROTECCIÓN DE DATOS Y PRIVACIDAD DE LA INFORMACIÓN PERSONAL	Norma ISO/IEC 27002:2013	Se deben asegurar la privacidad y la protección de la información de datos personales de clientes de la organización. Lo comentado, como se exige en la Ley de Protección de Datos Personales, en cuanto a la clasificación de Banco de Datos.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Espionaje de contraseñas / Ataques de diccionario	Reducción del riesgo	TA 1. EJECUCIÓN DE PROCEDIMIENTOS PARA EL USO DE CONTRASEÑAS FUERTES / TA 2. LIMITAR EL NÚMERO DE ACCESO A CONTRASEÑAS INVALIDAS	Técnico Auxiliar	Ejecutar procedimientos técnicos para evitar el Espionaje de contraseñas, ataques de contraseñas o métodos de cracking. El procedimiento es indicado dentro de la Política de Control de Acceso, en el apartado "Gestión de Contraseñas de Usuario", propuesto en el presente proyecto.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Mal funcionamiento del software y/o aplicación	Reducción del riesgo	TA 3. IMPLEMENTACIÓN DE SOFTWARE DE MONITOREO DE ESTADO DE SALUD Y RENDIMIENTO DE LA APLICACIÓN	Técnico Auxiliar	La organización debe adquirir un software de monitoreo para la revisión de logs y recursos del sistema. Asimismo, este software permitirá evaluar el rendimiento de la aplicación mediante parámetros técnicos asociadas a su estructura.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Manipulación de información / Abuso de derechos / Procesamiento ilegal de los datos / Robo o pérdida de información ingresada	Reducción del riesgo	TA 4. IMPLEMENTACIÓN DE UN DATA LOSS PREVENTION (DLP)	Técnico Auxiliar	La organización debe contemplar la adopción de una solución de DLP (Data Loss Prevention) para la clasificación de Información y manejo adecuado de la misma dentro y fuera de la organización, ello en cumplimiento de las reglas o directrices indicadas por la misma.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Inoperatividad del Sistema / Destrucción de la propia aplicación	Transferencia del riesgo	TA 5. MIGRACIÓN DEL SISTEMA DE GESTIÓN DE TICKETS EN UN SERVICIO EN LA NUBE MEDIANTE IAAS	Técnico Auxiliar	La organización debe contemplar la aplicación y ejecución de uno de los modelos de Cloud Computing, es decir Infraestructura como Servicio (IaaS) y llevar el Servicio del Sistema de Gestión de Tickets a la nube, evitando gastos de capital y reduciendo los costos corrientes (energía, aire acondicionado, otros), por un pago mensual o anual según convenga.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado

ITEM	ACTIVO	AMENAZAS / RIESGOS	OPCIONES DE TRATAMIENTO DEL RIESGO	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR	DUEÑO DEL RIESGO	RESPONSABLE DEL CONTROL	ESTADO DEL CONTROL
2	Contratos de Servicios, Instalación, entre otros	Manipulación de información / Abuso de derechos / Robo o Pérdida de documentación ingresada	Reducción del riesgo	A 5.1.1 CONJUNTO DE POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN / A 5.1.2 REVISIÓN DE LAS POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN / A 18.2.2 CUMPLIMIENTO DE LAS POLÍTICAS Y NORMAS DE SEGURIDAD MANIPULACIÓN / MANEJO DE ACTIVOS /	Norma ISO/IEC 27002:2013	Mantener implementados los lineamientos de la Política de Seguridad de la Información y las normas de seguridad dentro de la organización. Para lograr su cumplimiento la organización tendrá auditorias programadas y encuestas bimensuales como parte de la revisión del estatus del alcance de la misma. Asimismo, la Estructura Organizacional del Sistema de Gestión de Seguridad de la Información generará reportes sobre el estado de Seguridad de Información en la organización. En ello, se evaluará si existen incumplimientos y se determinará la causa del incumplimiento, se tomarán las acciones correctivas para garantizar la reducción de estos incumplimientos.	Gerente Técnico / Gerente Comercial / Gerente de Administración y Finanzas	Oficial de Seguridad de la Información	No Implementado
		Manipulación de información / Robo o pérdida de documentación ingresada	Reducción del riesgo	A 8.2.1 DIRECTRICES DE LA CLASIFICACIÓN / A 8.2.2 ETIQUETADO MANIPULADO DE LA INFORMACIÓN / A 8.2.3 MANIPULACIÓN / MANEJO DE ACTIVO	Norma ISO/IEC 27002:2013	Etiquetar y dar adecuado manejo a la información confidencial de los Contratos de Servicios, Instalación, entre otros realizados por la organización.	Gerente Técnico / Gerente Comercial / Gerente de Administración y Finanzas	Oficial de Seguridad de la Información	No Implementado
		Manipulación de información / Robo o pérdida de documentación ingresada	Reducción del riesgo	A 9.1.1 POLÍTICA DE CONTROL DE ACCESOS / A 9.2.2 GESTIÓN DE LOS DERECHOS DE ACCESO ASIGNADOS A USUARIOS / A 9.2.3 GESTIÓN DE LOS DERECHOS DE ACCESOS CON PRIVILEGIOS ESPECIALES	Norma ISO/IEC 27002:2013	Mantener implementados los lineamientos de la política de control de acceso. Mantener controlados los accesos de los usuarios. Capacitar a los colaboradores de la empresa sobre la utilización de los Contratos de Servicios, Instalación, entre otros. La Gerencia Técnica debe delegar la función de verificación continua de los privilegios y accesos que tiene cada colaborador en la empresa. Adicionalmente, registrar la fecha y horario de su ingreso y egreso.	Gerente Técnico / Gerente Comercial / Gerente de Administración y Finanzas	Oficial de Seguridad de la Información	No Implementado
		Manipulación de información / Robo o pérdida de documentación ingresada	Reducción del riesgo	A 11.1.2 CONTROLES FISICOS DE ENTRADA / A 11.1.3 SEGURIDAD DE OFICINAS, DESPACHOS Y RECURSOS /	Norma ISO/IEC 27002:2013	Controlar y limitar el acceso de Contratos de Servicios, Instalación, entre otros y a las instalaciones de procesamiento de información, exclusivamente a las personas autorizadas. Es decir, el área donde se encuentra el activo deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.	Gerente Técnico / Gerente Comercial / Gerente de Administración y Finanzas	Oficial de Seguridad de la Información	No Implementado

ITEM	ACTIVO	AMENAZAS / RIESGOS	OPCIONES DE TRATAMIENTO DEL RIESGO	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR	DUEÑO DEL RIESGO	RESPONSABLE DEL CONTROL	ESTADO DEL CONTROL
		Manipulación de información / Robo o pérdida de documentación ingresada	Reducción del riesgo	A 13.2.1 POLÍTICAS Y PROCEDIMIENTOS DE INTERCAMBIO DE INFORMACIÓN / A 13.2.4 ACUERDOS DE CONFIDENCIALIDAD O DE NO DIVULGACIÓN (SECRETO)	Norma ISO/IEC 27002:2013	La organización debe contar con una política y procedimientos para el intercambio de información, ello para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones. Asimismo, se debe proteger el manejo de la información contra divulgación no autorizada o uso inadecuado por medio de la firma de una cláusula de confidencialidad. Por último, la organización debe realizar la clasificación de la información, como también su rotulado y protección.	Gerente Técnico / Gerente Comercial / Gerente de Administración y Finanzas	Oficial de Seguridad de la Información	No Implementado
		Manipulación de información / Robo o pérdida de documentación ingresada	Reducción del riesgo	A 12.3.1 COPIAS DE SEGURIDAD DE LA INFORMACIÓN	Norma ISO/IEC 27002:2013	Los contratos de Servicios, Instalación, entre otros, debe ser respaldado de manera física (copias físicas) o de manera lógica (escaneadas con valor legal).	Gerente Técnico / Gerente Comercial / Gerente de Administración y Finanzas	Oficial de Seguridad de la Información	No Implementado
		Manipulación de información / Abuso de derechos / Robo o pérdida de documentación ingresada	Reducción del riesgo	A 18.1.3 PROTECCIÓN DE LOS REGISTROS DE LA ORGANIZACIÓN	Norma ISO/IEC 27002:2013	Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	Gerente Técnico / Gerente Comercial / Gerente de Administración y Finanzas	Oficial de Seguridad de la Información	No Implementado
		Manipulación de información / Robo o pérdida de documentación ingresada	Transferencia del riesgo	TA 6. MIGRACIÓN DE COPIAS LEGALIZADAS A PROVEEDOR DE CUSTODIA DE ARCHIVOS	Técnico Auxiliar	La organización deberá tener en cuenta realizar copias físicas y digitales de contratos y/o archivos asociados a los Contratos de Servicios, Instalación, entre otros en custodia de un proveedor tercero, tal como: Hermes, Prosegur, entre otros que se encuentren disponibles en el mercado.	Gerente Técnico / Gerente Comercial / Gerente de Administración y Finanzas	Oficial de Seguridad de la Información	No Implementado
3	Carpeta de Proyectos	Manipulación de información / Abuso de derechos / Robo o pérdida de información ingresada / Procesamiento ilegal de los datos / Pérdidas de comunicación por manipulación / Sniffer de Información	Reducción del riesgo	A 5.1.1 CONJUNTO DE POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN / A 5.1.2 REVISIÓN DE LAS POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN / A 18.2.2 CUMPLIMIENTO DE LAS POLÍTICAS Y NORMAS DE SEGURIDAD	Norma ISO/IEC 27002:2013	Mantener implementados los lineamientos de la política de seguridad de la información de la organización. Para lograr el cumplimiento de todas las políticas y normas de seguridad de la información, la compañía se vale de los reportes generados por la Estructura Organizacional del Sistema de Gestión de Seguridad de la Información. De estos reportes, se evaluará si existen incumplimientos y se determinará la causa del incumplimiento, se tomarán las acciones	Gerencia de Operaciones / Gerencia Comercial	Oficial de Seguridad de la Información / Jefe de Servicios Post-Venta	No Implementado

ITEM	ACTIVO	AMENAZAS / RIESGOS	OPCIONES DE TRATAMIENTO DEL RIESGO	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR	DUEÑO DEL RIESGO	RESPONSABLE DEL CONTROL	ESTADO DEL CONTROL
						correctivas para garantizar la mitigación de estos incumplimientos, y se revisarán estas acciones.			
		Manipulación de información / Abuso de derechos / Robo o pérdida de información ingresada / Procesamiento ilegal de los datos / Pérdidas de comunicación por manipulación	Reducción del riesgo	A 8.2.1 DIRECTRICES DE LA CLASIFICACIÓN / A 8.2.3 MANIPULACIÓN / MANEJO DE ACTIVOS	Norma ISO/IEC 27002:2013	La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada. Asimismo, se deben desarrollar e implementar procedimientos para el manejo de la Carpeta de Proyectos, de acuerdo con el esquema de clasificación de información adoptado por la organización, tal sea: Confidencial, privada y pública.	Gerente Técnico	Oficial de Seguridad de la Información / Jefe de Servicios Post-Venta	No Implementado
		Manipulación de información / Abuso de derechos / Robo o pérdida de información ingresada / Procesamiento ilegal de los datos / Pérdidas de comunicación por manipulación	Reducción del riesgo	A 9.1.1 POLÍTICA DE CONTROL DE ACCESOS / A 9.2.1 GESTIÓN DE ALTAS / A 9.2.2 GESTIÓN DE LOS DERECHOS DE ACCESO ASIGNADOS A USUARIOS / A 9.2.3 GESTIÓN DE LOS DERECHOS DE ACCESOS CON PRIVILEGIOS ESPECIALES / A 9.2.5 REVISIÓN DE LOS DERECHOS DE ACCESO DE USUARIOS	Norma ISO/IEC 27002:2013	Mantener implementados los lineamientos de la política de control de acceso. Mantener controlados los accesos de los usuarios. Adicionalmente, se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso. Por otro lado, se debe capacitar a los colaboradores de la empresa sobre la utilización de la carpeta de proyectos. El conjunto que comprende la Estructura Organizacional del Sistema de Gestión de Seguridad de la Información debe realizar la verificación continua de los privilegios y accesos que tiene cada colaborador en la organización, respecto al contenido de la carpeta en mención. Adicionalmente, registrar la fecha y horario de su ingreso y egreso.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Manipulación de información / Abuso de derechos / Robo o pérdida de información ingresada / Procesamiento ilegal de los datos	Reducción del riesgo	A 9.2.6 RETIRADA DE LOS DERECHOS DE ACCESO	Norma ISO/IEC 27002:2013	Los derechos de acceso de todos los usuarios de la carpeta de proyectos se deben retirar al término de su empleo, contrato o acuerdo, los cuales se deben ajustar inmediatamente al término del vínculo laboral.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado

ITEM	ACTIVO	AMENAZAS / RIESGOS	OPCIONES DE TRATAMIENTO DEL RIESGO	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR	DUEÑO DEL RIESGO	RESPONSABLE DEL CONTROL	ESTADO DEL CONTROL
		Manipulación de información / Abuso de derechos / Robo o pérdida de información ingresada / Procesamiento ilegal de los datos / Pérdidas de comunicación por manipulación	Reducción del riesgo	A 9.4.1 RESTRICCIÓN DEL ACCESO A LA INFORMACIÓN	Norma ISO/IEC 27002:2013	La Política de Control de Acceso a implementar respecto al acceso del Sistema a la capeta de proyectos se debe controlar mediante un proceso de ingreso seguro.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Manipulación de información / Pérdidas de comunicación por manipulación	Reducción del riesgo	A 12.1.2 GESTIÓN DE CAMBIOS	Norma ISO/IEC 27002:2013	La organización debe contar con una política y/o procedimiento en donde se gestionen los cambios realizados en las carpetas que pertenecen al Servidor de Archivos y en general a todas las carpetas que contengan información de uso recurrente y confidencial para la misma. Asimismo, llevar un inventario de los cambios realizados y el personal asociado al mismo.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Inoperatividad del sistema / Robo o pérdida de información ingresada	Reducción del riesgo	A 12.3.1 COPIAS DE SEGURIDAD DE LA INFORMACIÓN	Norma ISO/IEC 27002:2013	Se debe realizar respaldos de la información contenida en el servidor que aloja la carpeta. Es decir, se deben hacer copias de respaldo de la información de la carpeta de proyectos y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Procesamiento ilegal de los datos / Robo o pérdida de Información ingresada / Mal funcionamiento del software y/o aplicación / pérdidas de comunicación por manipulación	Reducción del riesgo	A 12.4.2 PROTECCIÓN DE LOS REGISTROS DE INFORMACIÓN	Norma ISO/IEC 27002:2013	La información de registro de acceso y consumo del activo de información se deben proteger contra alteración y acceso no autorizado.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Manipulación de información / Robo o pérdida de información ingresada	Reducción del riesgo	A 13.2.1 POLÍTICAS Y PROCEDIMIENTOS DE INTERCAMBIO DE INFORMACIÓN / A 13.2.4 ACUERDOS DE CONFIDENCIALIDAD O DE NO DIVULGACIÓN (SECRETO)	Norma ISO/IEC 27002:2013	La organización debe contar con una política y procedimientos para el intercambio de información, ello para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones. Asimismo, se debe proteger el manejo de la información contra divulgación no autorizada o uso inadecuado por medio de la firma de una cláusula de confidencialidad.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado

ITEM	ACTIVO	AMENAZAS / RIESGOS	OPCIONES DE TRATAMIENTO DEL RIESGO	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR	DUEÑO DEL RIESGO	RESPONSABLE DEL CONTROL	ESTADO DEL CONTROL
		Procesamiento ilegal de los datos / Robo o pérdida de Información ingresada /	Reducción del riesgo	A 13.2.3 MENSAJERÍA ELECTRÓNICA	Norma ISO/IEC 27002:2013	La organización debe crear lineamientos para proteger adecuadamente la información incluida en la mensajería electrónica. Asimismo, impedir que mediante este medio se envíe información relacionada con la carpeta de proyectos.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Manipulación de la Información / Robo o pérdida de información ingresada	Reducción del riesgo	A 18.1.3 PROTECCIÓN DE LOS REGISTROS DE LA ORGANIZACIÓN / A 18.1.3 PROTECCIÓN DE LOS REGISTROS DE LA ORGANIZACIÓN / A 18.1.4 PROTECCIÓN DE DATOS Y PRIVACIDAD DE LA INFORMACIÓN PERSONAL	Norma ISO/IEC 27002:2013	Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio. Adicionalmente, se deben asegurar la privacidad y la protección de la información de datos personales de clientes de la organización. Lo comentado, como se exige en la Ley de Protección de Datos Personales, en cuanto a la clasificación de Banco de Datos.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Manipulación de la Información / Robo o pérdida de información ingresada / Abuso de derechos	Reducción del riesgo	TA 7. IMPLEMENTACIÓN DE SOFTWARE DE AUDITORIA DE USO DE DATOS DE CARPETA DE PROYECTOS	Técnico Auxiliar	La organización debe considerar la adopción de un software de auditoria de uso de los datos contenidos dentro de la carpeta de proyectos. Esto incluye: uso, acceso, horario de acceso, entre otros datos relevantes para la auditoria.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Manipulación de información / Abuso de derechos / Procesamiento ilegal de los datos / Robo o pérdida de información ingresada	Reducción del riesgo	TA 4. IMPLEMENTACIÓN DE UN DATA LOSS PREVENTION (DLP)	Técnico Auxiliar	La organización debe contemplar la adopción de una solución de DLP (Data Loss Prevention) para la clasificación de Información y manejo adecuado de la misma dentro y fuera de la organización, ello en cumplimiento de las reglas o directrices indicadas por la misma.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Inoperatividad del Sistema	Transferencia del riesgo	TA 8. MIGRACIÓN DE LA CARPETA DE PROYECTOS BAJO UN SERVICIO EN LA NUBE MEDIANTE IAAS	Técnico Auxiliar	La organización debe contemplar la aplicación y ejecución de uno de los modelos de Cloud Computing, es decir Infraestructura como Servicio (IaaS) y llevar el servidor FTP que contiene la Carpeta de Proyectos Servicio a la nube, evitando gastos de capital y reduciendo los costos corrientes (energía, aire acondicionado, otros), por un pago mensual o anual según convenga.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado

ITEM	ACTIVO	AMENAZAS / RIESGOS	OPCIONES DE TRATAMIENTO DEL RIESGO	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR	DUEÑO DEL RIESGO	RESPONSABLE DEL CONTROL	ESTADO DEL CONTROL
		Manipulación de la Información / Robo o pérdida de información ingresada / Abuso de Derechos	Transferencia del riesgo	TA 9. DESPLIEGUE DE UNA SOLUCIÓN DE REPOSITORIO EN LA NUBE DE ACCESO ESPECIFICO	Técnico Auxiliar	La organización debe contemplar una solución en donde pueda pasar los datos de la Carpeta de Proyectos a un repositorio en la nube y en ello categorizar su acceso mediante alternativas de acceso: confidencial, privada y pública de usuarios de la organización, para accesos dentro y fuera de la organización. Estas soluciones pueden ser tipo: Check Point Workspace u otras soluciones como CASB (Cloud Access Security Broker) para aplicaciones o recursos publicados propietarios.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
4	Carpeta de Licitaciones	Manipulación de información / Abuso de derechos / Robo o pérdida de información ingresada / Procesamiento ilegal de los datos / Pérdidas de comunicación por manipulación / Sniffer de Información	Reducción del riesgo	A 5.1.1 CONJUNTO DE POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN / A 5.1.2 REVISIÓN DE LAS POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN / A 18.2.2 CUMPLIMIENTO DE LAS POLÍTICAS Y NORMAS DE SEGURIDAD	Norma ISO/IEC 27002:2013	Mantener implementados los lineamientos de la política de seguridad de la información de la organización. Para lograr el cumplimiento de todas las políticas y normas de seguridad de la información, la compañía se vale de los reportes generados por la Estructura Organizacional del Sistema de Gestión de Seguridad de la Información. De estos reportes, se evaluará si existen incumplimientos y se determinará la causa del incumplimiento, se tomarán las acciones correctivas para garantizar la mitigación de estos incumplimientos, y se revisarán estas acciones.	Gerente Comercial / Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Manipulación de información / Abuso de derechos / Robo o pérdida de información ingresada / Procesamiento ilegal de los datos / pérdidas de comunicación por manipulación	Reducción del riesgo	A 8.2.1 DIRECTRICES DE LA CLASIFICACIÓN / A 8.2.3 MANIPULACIÓN / MANEJO DE ACTIVOS	Norma ISO/IEC 27002:2013	La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada. Asimismo, se deben desarrollar e implementar procedimientos para el manejo de la Carpeta de Proyectos, de acuerdo con el esquema de clasificación de información adoptado por la organización, tal sea: Confidencial, privada y pública.	Gerente Comercial / Gerente Técnico	Oficial de Seguridad de la Información	No Implementado

ITEM	ACTIVO	AMENAZAS / RIESGOS	OPCIONES DE TRATAMIENTO DEL RIESGO	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR	DUEÑO DEL RIESGO	RESPONSABLE DEL CONTROL	ESTADO DEL CONTROL
		Manipulación de información / Abuso de derechos / Robo o pérdida de información ingresada / Procesamiento ilegal de los datos / pérdidas de comunicación por manipulación	Reducción del riesgo	A 9.1.1 POLÍTICA DE CONTROL DE ACCESOS / A 9.2.1 GESTIÓN DE ALTAS / A 9.2.2 GESTIÓN DE LOS DERECHOS DE ACCESO ASIGNADOS A USUARIOS / A 9.2.3 GESTIÓN DE LOS DERECHOS DE ACCESOS CON PRIVILEGIOS ESPECIALES / A 9.2.5 REVISIÓN DE LOS DERECHOS DE ACCESO DE USUARIOS	Norma ISO/IEC 27002:2013	Mantener implementados los lineamientos de la política de control de acceso. Mantener controlados los accesos de los usuarios. Adicionalmente, se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso. Por otro lado, se debe capacitar a los colaboradores de la empresa sobre la utilización de la carpeta de proyectos. El conjunto que comprende la Estructura Organizacional del Sistema de Gestión de Seguridad de la Información debe realizar la verificación continua de los privilegios y accesos que tiene cada colaborador en la organización, respecto al contenido de la carpeta en mención. Adicionalmente, registrar la fecha y horario de su ingreso y egreso. Por último, los derechos de acceso de todos los usuarios de la carpeta de proyectos se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	Gerente Comercial / Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Manipulación de información / Abuso de derechos / Robo o pérdida de información ingresada / Procesamiento ilegal de los datos	Reducción del riesgo	A 9.2.6 RETIRADA DE LOS DERECHOS DE ACCESO	Norma ISO/IEC 27002:2013	Los derechos de acceso de todos los usuarios de la carpeta de licitaciones se deben retirar al término de su empleo, contrato o acuerdo, los cuales se deben ajustar inmediatamente al término del vínculo laboral.	Gerente Comercial / Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Manipulación de información / Abuso de derechos / Robo o pérdida de información ingresada / Procesamiento ilegal de los datos / Pérdidas de comunicación por manipulación	Reducción del riesgo	A 9.4.1 RESTRICCIÓN DEL ACCESO A LA INFORMACIÓN	Norma ISO/IEC 27002:2013	La Política de Control de Acceso a implementar respecto al acceso del Sistema a la carpeta de licitaciones se debe controlar mediante un proceso de ingreso seguro.	Gerente Comercial / Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Manipulación de información / Pérdidas de comunicación por manipulación	Reducción del riesgo	A 12.1.2 GESTIÓN DE CAMBIOS	Norma ISO/IEC 27002:2013	La organización debe contar con una política y/o procedimiento en donde se gestionen los cambios realizados en las carpetas que pertenecen al Servidor de Archivos y en general a todas las carpetas que contengan información de uso recurrente y confidencial para la misma. Asimismo, llevar un inventario de los cambios realizados y el personal	Gerente Comercial / Gerente Técnico	Oficial de Seguridad de la Información	No Implementado

ITEM	ACTIVO	AMENAZAS / RIESGOS	OPCIONES DE TRATAMIENTO DEL RIESGO	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR	DUEÑO DEL RIESGO	RESPONSABLE DEL CONTROL	ESTADO DEL CONTROL
						asociado al mismo.			
		Inoperatividad del sistema / Robo o pérdida de información ingresada	Reducción del riesgo	A 12.3.1 COPIAS DE SEGURIDAD DE LA INFORMACIÓN	Norma ISO/IEC 27002:2013	Se debe realizar respaldos de la información contenida en el servidor que aloja la carpeta. Es decir, se deben hacer copias de respaldo de la información de la carpeta de proyectos y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	Gerente Comercial / Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Procesamiento ilegal de los datos / Robo o pérdidas de información ingresada / Mal funcionamiento del software y/o aplicación / pérdidas de comunicación por manipulación	Reducción del riesgo	A 12.4.2 PROTECCIÓN DE LOS REGISTROS DE INFORMACIÓN	Norma ISO/IEC 27002:2013	La información de registro de acceso y consumo del activo de información se deben proteger contra alteración y acceso no autorizado.	Gerente Comercial / Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Manipulación de información / Robo o pérdida de información ingresada	Reducción del riesgo	A 13.2.1 POLÍTICAS Y PROCEDIMIENTOS DE INTERCAMBIO DE INFORMACIÓN / A 13.2.4 ACUERDOS DE CONFIDENCIALIDAD O DE NO DIVULGACIÓN (SECRETO)	Norma ISO/IEC 27002:2013	La organización debe contar con una política y procedimientos para el intercambio de información, ello para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones. Asimismo, se debe proteger el manejo de la información contra divulgación no autorizada o uso inadecuado por medio de la firma de una cláusula de confidencialidad.	Gerente Comercial / Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Procesamiento ilegal de los datos / Robo o pérdida de Información ingresada /	Reducción del riesgo	A 13.2.3 MENSAJERÍA ELECTRÓNICA	Norma ISO/IEC 27002:2013	La organización debe crear lineamientos para proteger adecuadamente la información incluida en la mensajería electrónica. Asimismo, impedir que mediante este medio se envíe información relacionada con la carpeta de licitaciones.	Gerente Comercial / Gerente Técnico	Oficial de Seguridad de la Información	No Implementado

ITEM	ACTIVO	AMENAZAS / RIESGOS	OPCIONES DE TRATAMIENTO DEL RIESGO	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR	DUEÑO DEL RIESGO	RESPONSABLE DEL CONTROL	ESTADO DEL CONTROL
		Manipulación de la Información / Robo o pérdida de información ingresada	Reducción del riesgo	A 18.1.3 PROTECCIÓN DE LOS REGISTROS DE LA ORGANIZACIÓN / A 18.1.3 PROTECCIÓN DE LOS REGISTROS DE LA ORGANIZACIÓN / A 18.1.4 PROTECCIÓN DE DATOS Y PRIVACIDAD DE LA INFORMACIÓN PERSONAL	Norma ISO/IEC 27002:2013	Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio. Adicionalmente, se deben asegurar la privacidad y la protección de la información de datos personales de clientes de la organización. Lo comentado, como se exige en la Ley de Protección de Datos Personales, en cuanto a la clasificación de Banco de Datos.	Gerente Comercial / Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Manipulación de la Información / Robo o pérdida de información ingresada / Abuso de derechos	Reducción del riesgo	TA 10. IMPLEMENTACIÓN DE SOFTWARE DE AUDITORIA DE USO DE DATOS DE CARPETA DE LICITACIONES	Técnico Auxiliar	La organización debe considerar la adopción de un software de auditoria de uso de los datos contenidos dentro de la carpeta de licitaciones. Esto incluye: uso, acceso, horario de acceso, entre otros datos relevantes para la auditoria.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Manipulación de información / Abuso de derechos / Procesamiento ilegal de los datos / Robo o pérdida de información ingresada	Reducción del riesgo	TA 4. IMPLEMENTACIÓN DE UN DATA LOSS PREVENTION (DLP)	Técnico Auxiliar	La organización debe contemplar la adopción de una solución de DLP (Data Loss Prevention) para la clasificación de Información y manejo adecuado de la misma dentro y fuera de la organización, ello en cumplimiento de las reglas o directrices indicadas por la misma.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Inoperatividad del Sistema	Transferencia del riesgo	TA 11. MIGRACIÓN DE LA CARPETA DE LICITACIONES BAJO UN SERVICIO EN LA NUBE MEDIANTE IAAS	Técnico Auxiliar	La organización debe contemplar la aplicación y ejecución de uno de los modelos de Cloud Computing, es decir Infraestructura como Servicio (IaaS) y llevar el servidor FTP que contiene la Carpeta de Licitaciones a la nube, evitando gastos de capital y reduciendo los costos corrientes (energía, aire acondicionado, otros), por un pago mensual o anual según convenga.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado

ITEM	ACTIVO	AMENAZAS / RIESGOS	OPCIONES DE TRATAMIENTO DEL RIESGO	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR	DUEÑO DEL RIESGO	RESPONSABLE DEL CONTROL	ESTADO DEL CONTROL
		Manipulación de la Información / Robo o pérdida de información ingresada / Abuso de Derechos	Transferencia del riesgo	TA 9. DESPLIEGUE DE UNA SOLUCIÓN DE REPOSITORIO EN LA NUBE DE ACCESO ESPECIFICO	Técnico Auxiliar	La organización debe contemplar una solución en donde pueda pasar los datos de la Carpeta de Licitaciones a un repositorio en la nube y en ello categorizar su acceso mediante alternativas de acceso: confidencial, privada y pública de usuarios de la organización, para accesos dentro y fuera de la organización. Estas soluciones pueden ser tipo: Check Point Workspace u otras soluciones como CASB (Cloud Access Security Broker) para aplicaciones o recursos publicados propietarios.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
5	Carpets de Áreas Administrativas y Contabilidad	Manipulación de información / Abuso de derechos / Robo o pérdida de información ingresada / Procesamiento ilegal de los datos / Pérdidas de comunicación por manipulación / Sniffer de Información	Reducción del riesgo	A 5.1.1 CONJUNTO DE POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN / A 5.1.2 REVISIÓN DE LAS POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN / A 18.2.2 CUMPLIMIENTO DE LAS POLÍTICAS Y NORMAS DE SEGURIDAD	Norma ISO/IEC 27002:2013	Mantener implementados los lineamientos de la política de seguridad de la información de la organización. Para lograr el cumplimiento de todas las políticas y normas de seguridad de la información, la compañía se vale de los reportes generados por la Estructura Organizacional del Sistema de Gestión de Seguridad de la Información. De estos reportes, se evaluará si existen incumplimientos y se determinará la causa del incumplimiento, se tomarán las acciones correctivas para garantizar la mitigación de estos incumplimientos, y se revisarán estas acciones.	Gerencia de Administración y Finanzas	Oficial de Seguridad de la Información	No Implementado
		Manipulación de información / Abuso de derechos / Robo o pérdida de información ingresada / Procesamiento ilegal de los datos / pérdidas de comunicación por manipulación	Reducción del riesgo	A 8.2.1 DIRECTRICES DE LA CLASIFICACIÓN / A 8.2.3 MANIPULACIÓN / MANEJO DE ACTIVOS	Norma ISO/IEC 27002:2013	La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada. Asimismo, se deben desarrollar e implementar procedimientos para el manejo de la Carpeta de Proyectos, de acuerdo con el esquema de clasificación de información adoptado por la organización, tal sea: Confidencial, privada y pública.	Gerencia de Administración y Finanzas	Oficial de Seguridad de la Información	No Implementado

ITEM	ACTIVO	AMENAZAS / RIESGOS	OPCIONES DE TRATAMIENTO DEL RIESGO	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR	DUEÑO DEL RIESGO	RESPONSABLE DEL CONTROL	ESTADO DEL CONTROL
		Manipulación de información / Abuso de derechos / Robo o pérdida de información ingresada / Procesamiento ilegal de los datos / pérdidas de comunicación por manipulación	Reducción del riesgo	A 9.1.1 POLÍTICA DE CONTROL DE ACCESOS / A 9.2.1 GESTIÓN DE ALTAS / A 9.2.2 GESTIÓN DE LOS DERECHOS DE ACCESO ASIGNADOS A USUARIOS / A 9.2.3 GESTIÓN DE LOS DERECHOS DE ACCESOS CON PRIVILEGIOS ESPECIALES / A 9.2.5 REVISIÓN DE LOS DERECHOS DE ACCESO DE USUARIOS	Norma ISO/IEC 27002:2013	Mantener implementados los lineamientos de la política de control de acceso. Mantener controlados los accesos de los usuarios. Adicionalmente, se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso. Por otro lado, se debe capacitar a los colaboradores de la empresa sobre la utilización de la carpeta de proyectos. El conjunto que comprende la Estructura Organizacional del Sistema de Gestión de Seguridad de la Información debe realizar la verificación continua de los privilegios y accesos que tiene cada colaborador en la organización, respecto al contenido de la carpeta en mención. Adicionalmente, registrar la fecha y horario de su ingreso y egreso. Por último, los derechos de acceso de todos los usuarios de la carpeta de proyectos se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	Gerencia de Administración y Finanzas	Oficial de Seguridad de la Información	No Implementado
		Manipulación de información / Abuso de derechos / Robo o pérdida de información ingresada / Procesamiento ilegal de los datos	Reducción del riesgo	A 9.2.6 RETIRADA DE LOS DERECHOS DE ACCESO	Norma ISO/IEC 27002:2013	Los derechos de acceso de todos los usuarios de la carpeta de Administrativas y Contabilidad se deben retirar al término de su empleo, contrato o acuerdo, los cuales se deben ajustar inmediatamente al término del vínculo laboral.	Gerente Comercial / Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Manipulación de información / Abuso de derechos / Robo o pérdida de información ingresada / Procesamiento ilegal de los datos / Pérdidas de comunicación por manipulación	Reducción del riesgo	A 9.4.1 RESTRICCIÓN DEL ACCESO A LA INFORMACIÓN	Norma ISO/IEC 27002:2013	La Política de Control de Acceso a implementar respecto al acceso del Sistema a la capeta de áreas administrativas y contabilidad se debe controlar mediante un proceso de ingreso seguro.	Gerencia de Administración y Finanzas	Oficial de Seguridad de la Información	No Implementado
		Manipulación de información / Pérdidas de comunicación por manipulación	Reducción del riesgo	A 12.1.2 GESTIÓN DE CAMBIOS	Norma ISO/IEC 27002:2013	La organización debe contar con una política y/o procedimiento en donde se gestionen los cambios realizados en las carpetas que pertenecen al Servidor de Archivos y en general a todas las carpetas que contengan información de uso recurrente y confidencial para la misma. Asimismo, llevar un inventario de los cambios realizados y el personal asociado al mismo.	Gerencia de Administración y Finanzas	Oficial de Seguridad de la Información	No Implementado

ITEM	ACTIVO	AMENAZAS / RIESGOS	OPCIONES DE TRATAMIENTO DEL RIESGO	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR	DUEÑO DEL RIESGO	RESPONSABLE DEL CONTROL	ESTADO DEL CONTROL
		Inoperatividad del sistema / Robo o pérdida de información ingresada	Reducción del riesgo	A 12.3.1 COPIÁS DE SEGURIDAD DE LA INFORMACIÓN	Norma ISO/IEC 27002:2013	Se debe realizar respaldos de la información contenida en el servidor que aloja la carpeta. Es decir, se deben hacer copias de respaldo de la información de la carpeta de proyectos y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	Gerencia de Administración y Finanzas	Oficial de Seguridad de la Información	No Implementado
		Procesamiento ilegal de los datos / Robo o pérdida de información ingresada / Mal funcionamiento del software y/o aplicación / pérdidas de comunicación por manipulación	Reducción del riesgo	A 12.4.2 PROTECCIÓN DE LOS REGISTROS DE INFORMACIÓN	Norma ISO/IEC 27002:2013	La información de registro de acceso y consumo del activo de información se deben proteger contra alteración y acceso no autorizado.	Gerencia de Administración y Finanzas	Oficial de Seguridad de la Información	No Implementado
		Manipulación de información / Robo o pérdida de información ingresada	Reducción del riesgo	A 13.2.1 POLÍTICAS Y PROCEDIMIENTOS DE INTERCAMBIO DE INFORMACIÓN / A 13.2.4 ACUERDOS DE CONFIDENCIALIDAD O DE NO DIVULGACIÓN (SECRETO)	Norma ISO/IEC 27002:2013	La organización debe contar con una política y procedimientos para el intercambio de información, ello para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones. Asimismo, se debe proteger el manejo de la información contra divulgación no autorizada o uso inadecuado por medio de la firma de una cláusula de confidencialidad.	Gerencia de Administración y Finanzas	Oficial de Seguridad de la Información	No Implementado
		Procesamiento ilegal de los datos / Robo o pérdida de Información ingresada	Reducción del riesgo	A 13.2.3 MENSAJERÍA ELECTRÓNICA	Norma ISO/IEC 27002:2013	La organización debe crear lineamientos para proteger adecuadamente la información incluida en la mensajería electrónica. Asimismo, impedir que mediante este medio se envíe información relacionada con la carpeta de áreas administrativas y contables.	Gerencia de Administración y Finanzas	Oficial de Seguridad de la Información	No Implementado
		Manipulación de la Información / Robo o pérdida de información ingresada	Reducción del riesgo	A 18.1.3 PROTECCIÓN DE LOS REGISTROS DE LA ORGANIZACIÓN / A 18.1.3 PROTECCIÓN DE LOS REGISTROS DE LA ORGANIZACIÓN / A 18.1.4 PROTECCIÓN DE DATOS Y PRIVACIDAD DE LA INFORMACIÓN PERSONAL	Norma ISO/IEC 27002:2013	Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio. Adicionalmente, se deben asegurar la privacidad y la protección de la información de datos personales de clientes de la organización. Lo comentado, como se exige en la Ley de Protección de Datos Personales, en cuanto a la clasificación de Banco de Datos.	Gerencia de Administración y Finanzas	Oficial de Seguridad de la Información	No Implementado

ITEM	ACTIVO	AMENAZAS / RIESGOS	OPCIONES DE TRATAMIENTO DEL RIESGO	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR	DUEÑO DEL RIESGO	RESPONSABLE DEL CONTROL	ESTADO DEL CONTROL
		Manipulación de la Información / Robo o pérdida de información ingresada / Abuso de derechos	Reducción del riesgo	TA 12. IMPLEMENTACIÓN DE SOFTWARE DE AUDITORIA DE USO DE DATOS DE CARPETAS DE ÁREAS ADMINISTRATIVAS Y CONTABILIDAD	Técnico Auxiliar	La organización debe considerar la adopción de un software de auditoria de uso de los datos contenidos dentro de la Carpetas de Áreas Administrativas y Contabilidad. Esto incluye: uso, acceso, horario de acceso, entre otros datos relevantes para la auditoria.	Gerencia de Administración y Finanzas	Oficial de Seguridad de la Información	No Implementado
		Manipulación de información / Abuso de derechos / Procesamiento ilegal de los datos / Robo o pérdida de información ingresada	Reducción del riesgo	TA 4. IMPLEMENTACIÓN DE UN DATA LOSS PREVENTION (DLP)	Técnico Auxiliar	La organización debe contemplar la adopción de una solución de DLP (Data Loss Prevention) para la clasificación de Información y manejo adecuado de la misma dentro y fuera de la organización, ello en cumplimiento de las reglas o directrices indicadas por la misma.	Gerencia de Administración y Finanzas	Oficial de Seguridad de la Información	No Implementado
		Inoperatividad del Sistema	Transferencia del riesgo	TA 13. MIGRACIÓN DE LA CARPETAS DE ÁREAS ADMINISTRATIVAS Y CONTABILIDAD BAJO UN SERVICIO EN LA NUBE MEDIANTE IAAS	Técnico Auxiliar	La organización debe contemplar la aplicación y ejecución de uno de los modelos de Cloud Computing, es decir Infraestructura como Servicio (IaaS) y llevar el servidor FTP que contiene la Carpetas de Áreas Administrativas y Contabilidad a la nube, evitando gastos de capital y reduciendo los costos corrientes (energía, aire acondicionado, otros), por un pago mensual o anual según convenga.	Gerencia de Administración y Finanzas	Oficial de Seguridad de la Información	No Implementado
		Manipulación de la Información / Robo o pérdida de información ingresada / Abuso de Derechos	Transferencia del riesgo	TA 9. DESPLIEGUE DE UNA SOLUCIÓN DE REPOSITORIO EN LA NUBE DE ACCESO ESPECIFICO	Técnico Auxiliar	La organización debe contemplar una solución en donde pueda pasar los datos de la Carpetas de Áreas Administrativas y Contabilidad a un repositorio en la nube y en ello categorizar su acceso mediante alternativas de acceso: confidencial, privada y pública de usuarios de la organización, para accesos dentro y fuera de la organización. Estas soluciones pueden ser tipo: Check Point Workspace u otras soluciones como CASB (Cloud Access Security Broker) para aplicaciones o recursos publicados propietarios.	Gerencia de Administración y Finanzas	Oficial de Seguridad de la Información	No Implementado

ITEM	ACTIVO	AMENAZAS / RIESGOS	OPCIONES DE TRATAMIENTO DEL RIESGO	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR	DUEÑO DEL RIESGO	RESPONSABLE DEL CONTROL	ESTADO DEL CONTROL
6	Equipos de cómputo	Manipulación de información / Acceso no autorizado al sistema / Abuso de derechos / Procesamiento ilegal de los datos / Robo o pérdida de información ingresada / Sniffer de Información	Reducción del riesgo	A 5.1.1 CONJUNTO DE POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN / A 5.1.2 REVISIÓN DE LAS POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN	Norma ISO/IEC 27002:2013	Mantener implementados los lineamientos de la política de seguridad de la información de la organización. Para lograr el cumplimiento de todas las políticas y normas de seguridad de la información, la compañía se vale de los reportes generados por la Estructura de Gestión de Seguridad de la Información. De estos reportes, se evaluará si existen incumplimientos y se determinará la causa del incumplimiento, se tomarán las acciones correctivas para garantizar la mitigación de estos incumplimientos, y se revisarán estas acciones.	Gerente Técnico / Gerente de Administración y Finanzas	Oficial de Seguridad de la Información	No Implementado
		Abuso de derechos / Robo de Equipo	Reducción del riesgo	A 8.1.1 INVENTARIO DE ACTIVOS / A 8.1.2 PROPIEDAD DE LOS ACTIVOS	Norma ISO/IEC 27002:2013	Realizar inventario de los equipos de cómputo con los que cuenta la organización. Asimismo, identificarlos como activos propiedad de la organización y revisarlo anualmente.	Gerente Técnico / Gerente de Administración y Finanzas	Oficial de Seguridad de la Información	No Implementado
		Abuso de derechos / Robo de Equipo	Reducción del riesgo	A 8.1.2 PROPIEDAD DE LOS ACTIVOS	Norma ISO/IEC 27002:2013	Los activos de información asociados a Infraestructura de Comunicaciones tienen su propietario estipulado, estos son responsabilidad de cada colaborador. Cada mismo debe darle adecuado uso, tanto al activo como a la información embebida.	Gerente Técnico / Gerente de Administración y Finanzas	Oficial de Seguridad de la Información	No Implementado
		Manipulación de información / Acceso no autorizado al sistema / Abuso de derechos / Procesamiento ilegal de los datos / Inoperatividad del equipo / Robo de Equipo	Reducción del riesgo	A 8.1.3 USO ACEPTABLE DE LOS ACTIVOS / A 8.1.4 DEVOLUCIÓN DE ACTIVOS	Norma ISO/IEC 27002:2013	Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información. Asimismo, se debe crear un procedimiento para documentar al termino del cargo o acuerdo deben la entre del equipo de cómputo a la organización.	Gerente Técnico / Gerente de Administración y Finanzas	Oficial de Seguridad de la Información	No Implementado
		Inoperatividad del equipo / Robo de Equipo /	Reducción del riesgo	A 8.3.3 SOPORTES FÍSICOS EN TRÁNSITO	Norma ISO/IEC 27002:2013	Los equipos de cómputo se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte a clientes por tareas asignadas a la organización o traslado de equipos al domicilio del trabajador.	Gerente Técnico / Gerente de Administración y Finanzas	Oficial de Seguridad de la Información	No Implementado

ITEM	ACTIVO	AMENAZAS / RIESGOS	OPCIONES DE TRATAMIENTO DEL RIESGO	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR	DUEÑO DEL RIESGO	RESPONSABLE DEL CONTROL	ESTADO DEL CONTROL
		Manipulación de información / Acceso no autorizado al sistema / Abuso de derechos / Robo o pérdida de información ingresada / Procesamiento ilegal de los datos / Manipulación de información	Reducción del riesgo	A 9.1.1 POLÍTICA DE CONTROL DE ACCESOS / A 9.1.2 CONTROL DE ACCESO A LAS REDES Y SERVICIOS ASOCIADOS / A 9.4.2 PROCEDIMIENTO SEGURO DE INICIO DE SESIÓN	Norma ISO/IEC 27002:2013	Mantener implementados los lineamientos de la Política de Control de Acceso. Asimismo, contar un procedimiento seguro para el inicio de sesión del equipo de cómputo. Asimismo, cada equipo se encuentra dentro de la red LAN de la organización deberá estar ingresado en el dominio de la misma (AD), identificado con un nombre de host en el dominio, con lo cual pueda con ello tener acceso a recursos internos.	Gerente Técnico / Gerente de Administración y Finanzas	Oficial de Seguridad de la Información	No Implementado
		Manipulación de información / Abuso de derechos / Robo o pérdida de documentación ingresada / Procesamiento ilegal de los datos	Reducción del riesgo	A 9.4.1 RESTRICCIÓN DE ACCESO A LA INFORMACIÓN	Norma ISO/IEC 27002:2013	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	Gerente Técnico / Gerente de Administración y Finanzas	Oficial de Seguridad de la Información	No Implementado
		Abuso de derechos / Manipulación de información / Espionaje de contraseñas	Reducción del riesgo	A 9.4.3 GESTIÓN DE CONTRASEÑAS DE USUARIOS	Norma ISO/IEC 27002:2013	El usuario que utiliza el equipo de cómputo debe utilizar contraseñas seguras y robustas para el acceso al activo e información.	Gerente Técnico / Gerente de Administración y Finanzas	Oficial de Seguridad de la Información	No Implementado
		Procesamiento ilegal de los datos / Sniffer de Información	Reducción del riesgo	A 11.2.3 SEGURIDAD DEL CABLEADO	Norma ISO/IEC 27002:2013	Mantener seguridad relativa al cableado que utiliza cada equipo de cómputo para inspeccionar que el cableado permanezca en adecuadas condiciones. Adicionalmente, inspeccionar que el cableado permanezca en adecuadas condiciones y sin puntos de acceso libres o tomas de accesos libres. La organización deberá contar con un sistema de cableado estructurado, efectuando las correspondientes revisiones periódicas que sean necesarias.	Gerente Técnico / Gerente de Administración y Finanzas	Oficial de Seguridad de la Información	No Implementado
		Inoperatividad del equipo y/o equipos / Fallas en el funcionamiento de equipo y/o equipos	Reducción del riesgo	A 11.2.4 MANTENIMIENTO DE LOS EQUIPOS	Norma ISO/IEC 27002:2013	Los equipos de cómputo deben estar sujetos a ciclos de mantenimiento lógico y físico en periodos adecuados para asegurar su disponibilidad e integridad continuo en el tiempo. Se debe realizar un programa de mantenimiento que se ejecute y posteriormente se realice su respectivo seguimiento.	Gerente Técnico / Gerente de Administración y Finanzas	Oficial de Seguridad de la Información	No Implementado

ITEM	ACTIVO	AMENAZAS / RIESGOS	OPCIONES DE TRATAMIENTO DEL RIESGO	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR	DUEÑO DEL RIESGO	RESPONSABLE DEL CONTROL	ESTADO DEL CONTROL
		Acceso no autorizado al sistema / Procesamiento ilegal de los datos / Manipulación de información / Inoperatividad del equipo / Robo de Equipo	Reducción del riesgo	A 11.2.5 A SALIDA DE ACTIVOS FUERA DE LAS DEPENDENCIAS DE LA EMPRESA / A 11.2.6 SEGURIDAD DE LOS EQUIPOS Y ACTIVOS FUERA DE LAS INSTALACIONES	Norma ISO/IEC 27002:2013	Los equipos de cómputo no se deben retirar de su sitio sin autorización previa. Asimismo, se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de ella.	Gerente Técnico / Gerente de Administración y Finanzas	Oficial de Seguridad de la Información	No Implementado
		Manipulación de información / Acceso no autorizado al sistema / Abuso de derechos / Procesamiento ilegal de los datos / Manipulación de información / Robo o pérdida de información ingresada	Reducción del riesgo	A 11.2.8 EQUIPO INFORMÁTICO DE USUARIO DESATENDIDO / A 11.2.9 POLÍTICA DE PUESTO DE TRABAJO DESPEJADO Y BLOQUEO DE PANTALLA	Norma ISO/IEC 27002:2013	Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada. Es decir, seguir los lineamientos de la política de escritorio y pantalla despejada para evitar que información confidencial, restringida o importante sea vista por personas ajenas a dicha información.	Gerente Técnico / Gerente de Administración y Finanzas	Oficial de Seguridad de la Información	No Implementado
		Abuso de derechos / Espionaje de contraseñas / Acceso no autorizado al sistema / Procesamiento ilegal de los datos / Manipulación de información / Robo o pérdida de información ingresada / Fallas en el funcionamiento de equipo y/o equipos	Reducción del riesgo	A.12.2.1 CONTROLES CONTRA EL CÓDIGO MALICIOSO	Norma ISO/IEC 27002:2013	Los equipos de cómputo deben contar con un Antivirus estándar como mínimo para la protección contra código malicioso, tales los virus comunes. Asimismo, la organización debe crear procedimientos en donde se especifiquen: Los usuarios no pueden instalar software no autorizado en los equipos sin autorización previa. Accionar en el buen uso del Internet, correo electrónico y medios de almacenamiento extraíbles.	Gerente Técnico / Gerente de Administración y Finanzas	Oficial de Seguridad de la Información	No Implementado
		Manipulación de información / Robo o pérdida de información ingresada / Inoperatividad del equipo y/o equipos / Robo de equipo	Reducción del riesgo	A 12.3.1 COPIAS DE SEGURIDAD DE LA INFORMACIÓN	Norma ISO/IEC 27002:2013	Se deben hacer respaldo de las carpetas específicas de cada área a las que se encuentra tachada cada equipo de cómputo, ello ante cualquier eventualidad, pérdida, modificación o destrucción de la información contenida en la misma. Asimismo, se deben crear horarios para que estos respaldos sean ejecutados en horarios que no afecten la operatividad del trabajador y los recursos del computador en horario laboral.	Gerente Técnico / Gerente de Administración y Finanzas	Oficial de Seguridad de la Información	No Implementado
		Manipulación de información / Abuso de derechos / Procesamiento ilegal de los datos / Robo o pérdida de información ingresada	Reducción del riesgo	A 12.4.1 REGISTRO Y GESTIÓN DE EVENTOS DE ACTIVIDAD	Norma ISO/IEC 27002:2013	Todos los equipos de cómputo deben ser ingresados al dominio para poder enviar logs sobre los accesos a recursos utilizados. Se debe tener en cuenta reportar todo incidente o cualquier evento de seguridad de la información que se presente en el equipo, con ello tomar la acción de prevención o	Gerente Técnico / Gerente de Administración y Finanzas	Oficial de Seguridad de la Información	No Implementado

ITEM	ACTIVO	AMENAZAS / RIESGOS	OPCIONES DE TRATAMIENTO DEL RIESGO	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR	DUEÑO DEL RIESGO	RESPONSABLE DEL CONTROL	ESTADO DEL CONTROL
						corrección necesaria.			
		Manipulación de información / Acceso no autorizado al sistema / Abuso de derechos / Procesamiento ilegal de los datos / Manipulación de información / Robo o pérdida de información ingresada / Robo de equipo / Fallas en el funcionamiento de equipo y/o equipos / Sniffer de Información	Reducción del riesgo	A 13.1.1 CONTROLES DE RED / A 13.1.2 MECANISMOS DE SEGURIDAD DE SEGURIDAD ASOCIADAS A SERVICIOS DE RED	Norma ISO/IEC 27002:2013	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones. Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	Gerente Técnico / Gerente de Administración y Finanzas	Oficial de Seguridad de la Información	No Implementado
		Espionaje de contraseñas / Ataques de diccionario / Acceso no autorizado al sistema / Abuso de derechos / Manipulación de información / Fallas en el funcionamiento de equipo y/o equipos / Sniffer de Información	Reducción del riesgo	A 16.1.2 NOTIFICACIÓN DE LOS DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN / A 16.1.3 NOTIFICACIÓN DE DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN	Norma ISO/IEC 27002:2013	Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible. Asimismo, reportar debilidades relativas a la seguridad del equipo de cómputo inmediatamente al Oficial de Seguridad de la Información o propiamente a las personas que integran la Estructura Organizacional del Sistema de Gestión de Seguridad de la Información.	Gerente Técnico / Gerente de Administración y Finanzas	Oficial de Seguridad de la Información	No Implementado
		Acceso no autorizado al sistema / Abuso de derechos / Procesamiento ilegal de los datos / Manipulación de información / Robo o pérdida de información ingresada / Sniffer de Información	Reducción del riesgo	A 16.1.5 RESPUESTA A LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	Norma ISO/IEC 27002:2013	La organización deberá contar con mecanismos de control de incidentes de Seguridad de la Información sobre la Infraestructura Tecnológica implementada y los propios equipos de cómputo asignados a los usuarios finales para la ejecución de sus labores diarias. Asimismo, se deberá monitorear regularmente las actividades del personal y el uso de los sistemas de información. Este monitoreo se lleva a cabo evaluando todos los incidentes de seguridad encontrados.	Gerente Técnico / Gerente de Administración y Finanzas	Oficial de Seguridad de la Información	No Implementado

ITEM	ACTIVO	AMENAZAS / RIESGOS	OPCIONES DE TRATAMIENTO DEL RIESGO	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR	DUEÑO DEL RIESGO	RESPONSABLE DEL CONTROL	ESTADO DEL CONTROL
		Espionaje de contraseñas / Ataques de diccionario	Reducción del riesgo	TA 1. EJECUCIÓN DE PROCEDIMIENTOS PARA EL USO DE CONTRASEÑAS FUERTES / TA 2. LIMITAR EL NÚMERO DE ACCESO A CONTRASEÑAS INVALIDAS	Técnico Auxiliar	Ejecutar procedimientos técnicos para evitar el Espionaje de contraseñas, ataques de contraseñas o métodos de cracking. El procedimiento es indicado dentro de la Política de Control de Acceso, en el apartado "Gestión de Contraseñas de Usuario", propuesto en el presente proyecto.	Gerente Técnico / Gerente de Administración y Finanzas	Oficial de Seguridad de la Información	No Implementado
		Manipulación de información / Abuso de derechos / Procesamiento ilegal de los datos / Robo o pérdida de información ingresada	Reducción del riesgo	TA 4. IMPLEMENTACIÓN DE UN DATA LOSS PREVENTION (DLP)	Técnico Auxiliar	La organización debe contemplar la adopción de una solución de DLP (Data Loss Prevention) para la clasificación de Información y manejo adecuado de la misma dentro y fuera de la organización, ello en cumplimiento de las reglas o directrices indicadas por la misma. El agente será instalado en el total de equipos de cómputo para la prevención de fuga de información como razón principal.	Gerente Técnico / Gerente de Administración y Finanzas	Oficial de Seguridad de la Información	No Implementado
		Acceso no autorizado al sistema / Abuso de derechos / Acceso no autorizado al equipo	Reducción del riesgo	TA 14. INGRESO LÓGICO DE CADA EQUIPO DE COMPUTO POR MEDIO DEL DIRECTORIO ACTIVO	Técnico Auxiliar	Cada equipo de cómputo deberá ser unido al dominio de la organización vía el soporte del Active Directory. Ello para contar con una administración de despliegue de política de seguridad, despliegue de paquetes de actualización, accesos a carpetas de archivos seleccionados y otras funcionalidades de manera centralizada.	Gerente Técnico / Gerente de Administración y Finanzas	Oficial de Seguridad de la Información	No Implementado
		Manipulación de información / Acceso no autorizado al sistema / Abuso de derechos / Procesamiento ilegal de los datos / Robo o pérdida de información ingresada	Reducción del riesgo	TA 15. IMPLEMENTACIÓN DE UNA SUITE O SOLUCIÓN DE ENDPOINT PARA PREVENIR ATAQUES DE FIRMAS COMUNES Y DE DÍA CERO	Técnico Auxiliar	La organización debe implementar una suite o solución de Endpoint para la protección y prevención contra ataques comunes y ataques de Dia Cero (Zero Days). Esta solución deberá contar con módulos de seguridad como: AV, Antibot, IPS, Antimalware (prevención y protección contra ataques de día cero) y otros Blades o módulos de seguridad embebidos.	Gerente Técnico / Gerente de Administración y Finanzas	Oficial de Seguridad de la Información	No Implementado

ITEM	ACTIVO	AMENAZAS / RIESGOS	OPCIONES DE TRATAMIENTO DEL RIESGO	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR	DUEÑO DEL RIESGO	RESPONSABLE DEL CONTROL	ESTADO DEL CONTROL
		Manipulación de Información / Procesamiento ilegal de los datos / Robo o pérdida de información ingresada / Inoperatividad del equipo y/o equipos	Reducción del riesgo	TA 16. IMPLEMENTACIÓN DE UNA SOLUCIÓN DE RESPALDO DE ENDPOINT O ESTACIONES DE TRABAJO Y/O SERVIDORES	Técnico Auxiliar	La organización debe considerar la implementación de una solución de respaldo de estaciones finales de trabajo o Endpoint y/o servidores, esto mediante un agente instalado en el computador, apuntando el respaldo a un Storage local o en nube: Soluciones como Barracuda Backup, Veeam Backup, Veritas, entre otras. Todas las PC's asociadas a la plana de Gerentes, Jefes y usuarios finales deben tener un respaldo del contenido del computador sin excepción, esto para fines de recuperación y auditoria.	Gerente Técnico / Gerente de Administración y Finanzas	Oficial de Seguridad de la Información	No Implementado
		Acceso no autorizado al Sistema / Inoperatividad del equipo y/o equipos / Fallas en el funcionamiento de equipo y/o equipos	Reducción del riesgo	TA 17. IMPLEMENTACIÓN DE UN SERVIDOR CENTRALIZADO PARA INSTALACIÓN DE PARCHES DE SEGURIDAD	Técnico Auxiliar	La organización debe implementar un servidor centralizado para la instalación de parches de seguridad, esto programado de manera automática o ejecutada de manera manual, lo cual aplique a todos los equipos de cómputo y la totalidad de servidores. Con ello, evitar o disminuir fallas de seguridad asociadas a versiones de Sistema Operativos, específicamente Windows (Servidor centralizado WSUS) debido a que es el Sistema Operativo utilizado en la organización.	Gerente Técnico / Gerente de Administración y Finanzas	Oficial de Seguridad de la Información	No Implementado
		Robo de equipo / Manipulación de Información / Sniffer de Información	Reducción del riesgo	TA 18. IMPLEMENTACIÓN DE UNA SOLUCIÓN DE ENDPOINT ENCRYPTION	Técnico Auxiliar	La organización debe contemplar implementar una solución de Endpoint Encryption (Encriptación de Endpoint o dispositivos finales) la cual ofrezca cifrado eficaz de disco completo y soportes extraíbles. Lo comentado mediante una administración centralizada para proteger la información confidencial y asegurar el cumplimiento normativo dentro de la organización.	Gerente Técnico / Gerente de Administración y Finanzas	Oficial de Seguridad de la Información	No Implementado
		Robo de equipo / Inoperatividad del equipo y/o equipos Fallas en el funcionamiento de equipo y/o equipos	Transferencia del riesgo	TA 19. ALQUILER DE EQUIPOS DE CÓMPUTO	Técnico Auxiliar	La organización debe evaluar el alquiler de equipos de cómputo para transferir los riesgos de pérdida del equipo (80% aproximado en laptop, 20% aproximado en PC de escritorio), inoperatividad o fallas en su funcionamiento. Asimismo, los acuerdos con la empresa que alquila los equipos deben cubrir cambio ante fallas, pérdidas (seguro o póliza que aplique), fallas en su funcionamiento, cambio de piezas o partes del computador, cambio por obsolescencia, entre otros acuerdos.	Gerente Técnico / Gerente de Administración y Finanzas	Oficial de Seguridad de la Información	No Implementado

ITEM	ACTIVO	AMENAZAS / RIESGOS	OPCIONES DE TRATAMIENTO DEL RIESGO	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR	DUEÑO DEL RIESGO	RESPONSABLE DEL CONTROL	ESTADO DEL CONTROL
7	Correo Electrónico	Manipulación de información / Acceso no autorizado al sistema / Robo o pérdida de información ingresada / Abuso de derechos / Procesamiento ilegal de los datos / Sniffer de Información	Reducción del riesgo	A 5.1.1 CONJUNTO DE POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN / A 5.1.2 REVISIÓN DE LAS POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN / A 18.2.2 CUMPLIMIENTO DE LAS POLÍTICAS Y NORMAS DE SEGURIDAD	Norma ISO/IEC 27002:2013	Mantener implementados los lineamientos de la Política de Seguridad de la Información y las normas de seguridad dentro de la organización. Para lograr su cumplimiento la organización tendrá auditorias programadas y encuestas bimensuales como parte de la revisión del estatus del alcance de la misma. Asimismo, la Estructura Organizacional del Sistema de Gestión de Seguridad de la Información generará reportes sobre el estado de Seguridad de Información en la organización. En ello, se evaluará si existen incumplimientos y se determinará la causa del incumplimiento, se tomarán las acciones correctivas para garantizar la reducción de estos incumplimientos.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Manipulación de información / Acceso no autorizado al sistema / Inoperatividad del sistema o servicio / Robo o pérdida de información ingresada / Abuso de derechos / Procesamiento ilegal de los datos	Reducción del riesgo	A 6.2.2 TELETRABAJO	Norma ISO/IEC 27002:2013	Se debe implementar una política y unas medidas de seguridad de soporte para proteger la información a la que se tiene acceso, la cual es procesada o almacenada en los lugares en los que se realiza teletrabajo. Es decir, se debe establecer procedimientos para el acceso al Correo Electrónico desde fuera de la organización, ya sea por vía OWA o cliente instalado en cada computador del usuario conectado. Asimismo, se debe tener en cuenta la Política de Teletrabajo la cual indica los lineamientos de conexión por VPN y otras consideraciones en el acceso.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Manipulación de información / Acceso no autorizado al sistema / / Robo o pérdida de información ingresada / Abuso de derechos / Procesamiento ilegal de los datos	Reducción del riesgo	A 9.1.1 POLÍTICA DE CONTROL DE ACCESOS / A 9.2.2 GESTIÓN DE LOS DERECHOS DE ACCESO ASIGNADOS A USUARIOS	Norma ISO/IEC 27002:2013	Mantener implementados los lineamientos de la política de control de acceso. Asimismo, se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para el acceso vía correo electrónico.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Manipulación de información / Espionaje de contraseñas / Acceso no autorizado al sistema / Abuso de derechos / Procesamiento ilegal de los datos	Reducción del riesgo	A 9.3.1 USO DE INFORMACIÓN CONFIDENCIAL PARA LA AUTENTICACIÓN	Norma ISO/IEC 27002:2013	Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado

ITEM	ACTIVO	AMENAZAS / RIESGOS	OPCIONES DE TRATAMIENTO DEL RIESGO	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR	DUEÑO DEL RIESGO	RESPONSABLE DEL CONTROL	ESTADO DEL CONTROL
		Manipulación de información / Espionaje de contraseñas / Acceso no autorizado al sistema / Robo o pérdida de información ingresada / Abuso de derechos / Procesamiento ilegal de los datos / Pérdidas de comunicación por manipulación	Reducción del riesgo	A 9.4.1 RESTRICCIÓN DEL ACCESO A LA INFORMACIÓN / 9.4.2 PROCEDIMIENTOS SEGUROS DE INICIO DE SESIÓN / A 9.4.3 GESTIÓN DE CONTRASEÑA DE USUARIO	Norma ISO/IEC 27002:2013	La Política de Control de Acceso a implementar debe controlar al acceso y uso del Correo Electrónico, ejecutándose de forma segura. Asimismo, los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Inoperatividad del sistema o servicio / Mal funcionamiento del software y/o aplicación	Reducción del riesgo	A 12.1.3 GESTIÓN DE CAPACIDAD	Norma ISO/IEC 27002:2013	Se debe revisar cotidianamente y en ciclos programados el consumo de recursos del servidor que al servicio de Correo Electrónico. Se debe monitorear regularmente sus recursos, tales como: memoria, procesamiento y almacenamiento y realizar mejoras en los mismos recursos de ser necesario, incluso el cambio del equipo de acuerdo a un dimensionamiento previamente realizado.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Manipulación de información / Robo o pérdida de información ingresada / Procesamiento ilegal de los datos	Reducción del riesgo	A 13.2.1 POLÍTICAS Y PROCEDIMIENTOS DE INTERCAMBIO DE INFORMACIÓN / A 13.2.4 ACUERDOS DE CONFIDENCIALIDAD O DE NO DIVULGACIÓN (SECRETO)	Norma ISO/IEC 27002:2013	La organización debe contar con una política y procedimientos para el intercambio de información, ello para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones. Asimismo, se debe proteger el manejo de la información contra divulgación no autorizada o uso inadecuado por medio de la firma de una cláusula de confidencialidad.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Robo o pérdida de información ingresada / Procesamiento ilegal de los datos	Reducción del riesgo	A 13.2.3 MENSAJERÍA ELECTRÓNICA	Norma ISO/IEC 27002:2013	La organización debe crear lineamientos para proteger adecuadamente la información incluida en la mensajería electrónica. Asimismo, impedir que mediante este medio se envíe información relacionada con información confidencial propia de la organización.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Manipulación de información / Robo o pérdida de información ingresada / Abuso de derechos / Procesamiento ilegal de los datos	Reducción del riesgo	A 13.2.4 ACUERDOS DE CONFIDENCIALIDAD O DE NO DIVULGACIÓN (SECRETO)	Norma ISO/IEC 27002:2013	Se protege el manejo de la información contra divulgación no autorizada o uso inadecuado de información propia de la organización por medio de la firma de la cláusula de confidencialidad. Asimismo, la organización debe revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación, los cuales	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado

ITEM	ACTIVO	AMENAZAS / RIESGOS	OPCIONES DE TRATAMIENTO DEL RIESGO	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR	DUEÑO DEL RIESGO	RESPONSABLE DEL CONTROL	ESTADO DEL CONTROL
						reflejen las necesidades de la organización en materia de Seguridad de la Información.			
		Manipulación de información / Inoperatividad del sistema / Robo o pérdida de información ingresada / Destrucción de equipo o propia aplicación / Mal funcionamiento del software y/o aplicación	Reducción del riesgo	A 12.3.1 COPIAS DE SEGURIDAD DE LA INFORMACIÓN	Norma ISO/IEC 27002:2013	La información asociada al correo electrónico debe contar con un respaldo, entendiendo que este un servicio crítico para la organización. Es decir, los datos asociados al correo electrónico alojados en el servidor deben estar salvaguardada y protegida por un respaldo mensual, semanal o un Schedule adecuado para la organización. Asimismo, debe almacenarse en sitios alternos a la misma.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Manipulación de información / Acceso no autorizado al sistema / Robo o pérdida de información ingresada / Abuso de derechos / Procesamiento ilegal de los datos / Mal funcionamiento del software y/o aplicación	Reducción del riesgo	A 12.4.1 REGISTRO Y GESTIÓN DE EVENTOS DE ACTIVIDAD / A 16.1.2 NOTIFICACIÓN DE LOS DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN / A 16.1.3 NOTIFICACIÓN DE DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN	Norma ISO/IEC 27002:2013	Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario respecto al Correo Electrónico, tales como: fallas, eventos de seguridad de la información, destinatarios de envíos, tamaños de adjunto, horarios, entre otros. Asimismo, reportar y notificar cualquier incidente relacionado con la seguridad de la información del sistema referido y el propio consumo del recurso.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Manipulación de información / Robo o pérdida de información ingresada / Procesamiento ilegal de los datos	Reducción del riesgo	A 18.1.4 PROTECCIÓN DE DATOS Y PRIVACIDAD DE LA INFORMACIÓN PERSONAL	Norma ISO/IEC 27002:2013	Se deben asegurar la privacidad y la protección de la información de datos personales de clientes de la organización, en el flujo de intercambio de información asociado en el servicio de Correo Electrónico. Este aseguramiento de la privacidad y protección de datos es tal como se exige en la Ley de Protección de Datos Personales, en cuanto a la clasificación de Banco de Datos.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado

ITEM	ACTIVO	AMENAZAS / RIESGOS	OPCIONES DE TRATAMIENTO DEL RIESGO	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR	DUEÑO DEL RIESGO	RESPONSABLE DEL CONTROL	ESTADO DEL CONTROL
		Espionaje de contraseñas / Ataques de diccionario	Reducción del riesgo	TA 1. EJECUCIÓN DE PROCEDIMIENTOS PARA EL USO DE CONTRASEÑAS FUERTES / TA 2. LIMITAR EL NÚMERO DE ACCESO A CONTRASEÑAS INVALIDAS	Técnico Auxiliar	Ejecutar procedimientos técnicos para evitar el Espionaje de contraseñas, ataques de contraseñas o métodos de cracking. El procedimiento es indicado dentro de la Política de Control de Acceso, en el apartado "Gestión de Contraseñas de Usuario", propuesto en el presente proyecto.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Mal funcionamiento del software y/o aplicación	Reducción del riesgo	TA 3. IMPLEMENTACIÓN DE SOFTWARE DE MONITOREO DE ESTADO DE SALUD Y RENDIMIENTO DE LA APLICACIÓN	Técnico Auxiliar	La organización debe adquirir un software de monitoreo para la revisión de logs y recursos del sistema. Asimismo, este software permitirá evaluar el rendimiento de la aplicación o servicio de correo mediante parámetros técnicos asociadas a su estructura.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Manipulación de información / Abuso de derechos / Procesamiento ilegal de los datos / Robo o pérdida de información ingresada	Reducción del riesgo	TA 4. IMPLEMENTACIÓN DE UN DATA LOSS PREVENTION (DLP)	Técnico Auxiliar	La organización debe contemplar la adopción de una solución de DLP (Data Loss Prevention) para la clasificación de Información y manejo adecuado de la misma dentro y fuera de la organización, ello en cumplimiento de las reglas o directrices indicadas por la misma.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Manipulación de la Información / Robo o pérdida de información ingresada / Abuso de derechos	Reducción del riesgo	TA 20. IMPLEMENTACIÓN DE SOFTWARE DE AUDITORIA DE USO DEL SERVICIO DE CORREO ELECTRÓNICO	Técnico Auxiliar	La organización debe considerar la adopción de un software de auditoria de uso o flujo de correos enviados y recibidos por los usuarios internos. Esto incluye: uso, acceso, envíos de correo, recepción de correos, horario de acceso, entre otros datos relevantes para la auditoria.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Correos entrantes con contenidos maliciosos y/o SPAM	Reducción del riesgo	TA 21. IMPLEMENTACIÓN DE UN SERVICIO O APPLIANCE DE ANTISPAM	Técnico Auxiliar	La organización debe considerar la adopción de un servicio o appliance dedicado para AntiSpam. Ello para el manejo de correos spam (basura o no deseados), así como también su uso para la protección contra código malicioso embebido dentro de los correos electrónicos, ya sea como adjunto, direccionamiento mediante un link de acceso, código malicioso incrustado dentro del cuerpo de correo, entre otras amenazas.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado

ITEM	ACTIVO	AMENAZAS / RIESGOS	OPCIONES DE TRATAMIENTO DEL RIESGO	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR	DUEÑO DEL RIESGO	RESPONSABLE DEL CONTROL	ESTADO DEL CONTROL
		Inoperatividad del Sistema / Destrucción de la propia aplicación	Transferencia del riesgo	TA 22. MIGRACIÓN DEL SERVICIO DE CORREO ELECTRÓNICO A LA NUBE MEDIANTE SAAS	Técnico Auxiliar	La organización debe contemplar la aplicación y ejecución de uno de los modelos de Cloud Computing, es decir el Software como Servicio (SaaS) y llevar el Servicio del Correo Electrónico a la nube, evitando gastos de capital y reduciendo los costos corrientes (energía, aire acondicionado, otros), por un pago mensual o anual según convenga.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
8	Internet	Abuso de derechos / Procesamiento ilegal de los datos / Robo de información interna / Sniffer de información	Reducción del riesgo	A 5.1.1 CONJUNTO DE POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN / A 5.1.2 REVISIÓN DE LAS POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN / A 18.2.2 CUMPLIMIENTO DE LAS POLÍTICAS Y NORMAS DE SEGURIDAD	Norma ISO/IEC 27002:2013	Mantener implementados los lineamientos de la política de seguridad de la información de la organización. Para lograr el cumplimiento de todas las políticas y normas de seguridad de la información, la compañía se vale de los reportes generados por la Estructura de Gestión de Seguridad de la Información. De estos reportes, se evaluará si existen incumplimientos y se determinará la causa del incumplimiento, se tomarán las acciones correctivas para garantizar la mitigación de estos incumplimientos, y se revisarán estas acciones.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Abuso de derechos / Procesamiento ilegal de los datos / Robo de información interna	Reducción del riesgo	A 9.1.1 POLÍTICA DE CONTROL DE ACCESOS	Norma ISO/IEC 27002:2013	La organización debe implementar procedimientos que estén dentro de la Política de Control de Acceso, en donde haga referencia al uso del recurso de Internet por parte de los colaboradores dentro de la organización. Ello se estipulará dentro del apartado "Control de Acceso a Red" mencionada en dicha Política. Adicionalmente, la organización debe continuamente supervisar que se ejecute los lineamientos indicados dentro de la Política.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Abuso de derechos / Procesamiento ilegal de los datos / Robo de información interna / Sniffer de Información	Reducción del riesgo	A 9.1.2 CONTROL DE ACCESO A LAS REDES Y SERVICIOS ASOCIADOS	Norma ISO/IEC 27002:2013	La organización dentro de su Política de Uso Aceptable de los Sistema de Información, Internet y Correo Electrónico, especifica el acceso de los usuarios a Internet para los que hayan sido previamente autorizados. Asimismo, la organización especifica lineamientos a cumplir dentro de la Política de Control de Acceso.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado

ITEM	ACTIVO	AMENAZAS / RIESGOS	OPCIONES DE TRATAMIENTO DEL RIESGO	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR	DUEÑO DEL RIESGO	RESPONSABLE DEL CONTROL	ESTADO DEL CONTROL
		Abuso de derechos	Reducción del riesgo	A 12.1.1 DOCUMENTACIÓN DE PROCEDIMIENTOS DE OPERACIÓN	Norma ISO/IEC 27002:2013	Los procedimientos de operación deben ser documentados por la organización y ponerlos a disposición de todos los usuarios dentro de la misma. Asimismo, el acceso a Internet será utilizado con propósitos autorizados, tomando en cuenta los procedimientos de operación o uso del acceso a Internet.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Inoperatividad del sistema o servicio / Pérdida de actividad de labores	Reducción del riesgo	A 12.1.3 GESTIÓN DE CAPACIDAD	Norma ISO/IEC 27002:2013	Se debe revisar cotidianamente y en ciclos programados el consumo de recursos del Router que brinda el servicio de Internet. Se debe monitorear regularmente sus recursos, tales como: memoria, procesamiento y almacenamiento y realizar mejoras en los mismos recursos de ser necesario, incluso el cambio del equipo de acuerdo a un dimensionamiento previamente realizado.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Abuso de derechos / Procesamiento ilegal de los datos / Pérdida de actividad de labores / Inoperatividad del sistema o servicio / Robo de información interna	Reducción del riesgo	A.12.2.1 CONTROLES CONTRA EL CÓDIGO MALICIOSO	Norma ISO/IEC 27002:2013	Fortalecer la protección en uso del Internet mediante herramientas de seguridad como Firewall, Antivirus, AntiSpam y Antimalware.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Inoperatividad del sistema o servicio / Abuso de derechos / Procesamiento ilegal de los datos / Robo de información interna	Reducción del riesgo	A 12.4.1 REGISTRO Y GESTIÓN DE EVENTOS DE ACTIVIDAD / A 16.1.2 NOTIFICACIÓN DE LOS DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN / A 16.1.3 NOTIFICACIÓN DE DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN	Norma ISO/IEC 27002:2013	Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario respecto al uso de acceso a Internet, tales como: fallas, eventos de seguridad de la información, historial de navegación, sitios más concurridos, usuarios top, entre otros. Asimismo, reportar y notificar cualquier incidente relacionado con la seguridad de la información del acceso a Internet y el propio consumo del recurso.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Inoperatividad del sistema o servicio / Pérdida de actividad de labores	Reducción del riesgo	A 17.2.1 DISPONIBILIDAD DE INSTALACIONES DE PROCESAMIENTO DE INFORMACIÓN	Norma ISO/IEC 27002:2013	El servicio de acceso a Internet se debe implementar con redundancia suficiente para cumplir los requisitos de disponibilidad. Este apartado debe estar incluido dentro del Plan ante Desastre (DRP) diseñado y posteriormente implementado por la propia organización.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado

ITEM	ACTIVO	AMENAZAS / RIESGOS	OPCIONES DE TRATAMIENTO DEL RIESGO	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR	DUEÑO DEL RIESGO	RESPONSABLE DEL CONTROL	ESTADO DEL CONTROL
		Saturación del circuito de Internet / Acceso a destinos de alto riesgo de infección	Reducción del riesgo	TA 23. IMPLEMENTACIÓN DE SOFTWARE DE MONITOREO DEL CONSUMO DE INTERNET	Técnico Auxiliar	La organización debe adquirir un software de monitoreo para la revisión y análisis del consumo de Internet. Con ello, revisar en base a los reportes, quienes son los destinos más concurridos y su categorización de seguridad. Con ello, ajustar los accesos y disminuir el riesgo de infección o ataques de día cero provenientes de destinos previamente identificados como malignos.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Saturación del circuito de Internet / Acceso a destinos de alto riesgo de infección	Reducción del riesgo	TA 24. IMPLEMENTACIÓN DE SOFTWARE DE MONITOREO DEL CONSUMO DE INTERNET	Técnico Auxiliar	La organización debe adquirir un software de monitoreo para la revisión y análisis del consumo de Internet. Con ello, revisar en base a los reportes, quienes son los destinos más concurridos y su categorización de seguridad. Con ello, ajustar los accesos y disminuir el riesgo de infección o ataques de día cero provenientes de destinos previamente identificados como malignos.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Acceso a destinos de alto riesgo de infección / Infección de Código malicioso: Virus, Spyware, Ransomware, entre otros en la red interna	Reducción del riesgo	TA 25. IMPLEMENTACIÓN DE UNA SUITE O SOLUCIÓN PERIMETRAL PARA PREVENIR ATAQUES DE DÍA CERO	Técnico Auxiliar	La organización debe implementar una suite o solución de perimetral para la protección y prevención contra ataques de Dia Cero (Zero Days). Esta solución deberá contar con módulos de seguridad de antimalware, ya sea en un despliegue de appliance físico o un análisis ejecutado en la nube del fabricante.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
9	Servidor de archivos (File Server)	Robo o pérdida de información ingresada / Abuso de derechos / Procesamiento ilegal de los datos / Sniffer de Información	Reducción del riesgo	A 5.1.1 CONJUNTO DE POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN / A 5.1.2 REVISIÓN DE LAS POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN / A 18.2.2 CUMPLIMIENTO DE LAS POLÍTICAS Y NORMAS DE SEGURIDAD	Norma ISO/IEC 27002:2013	Mantener implementados los lineamientos de la política de seguridad de la información de la organización. Para lograr el cumplimiento de todas las políticas y normas de seguridad de la información, la compañía se vale de los reportes generados por la Estructura de Gestión de Seguridad de la Información. De estos reportes, se evaluará si existen incumplimientos y se determinará la causa del incumplimiento, se tomarán las acciones correctivas para garantizar la mitigación de estos incumplimientos, y se revisarán estas acciones.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado

ITEM	ACTIVO	AMENAZAS / RIESGOS	OPCIONES DE TRATAMIENTO DEL RIESGO	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR	DUEÑO DEL RIESGO	RESPONSABLE DEL CONTROL	ESTADO DEL CONTROL
		Inoperatividad del sistema o servicio / Robo o pérdida de información ingresada / Abuso de derechos / Procesamiento ilegal de los datos	Reducción del riesgo	A 6.2.2 TELETRABAJO	Norma ISO/IEC 27002:2013	Se debe implementar una política y unas medidas de seguridad de soporte para proteger la información a la que se tiene acceso, la cual es procesada o almacenada en los lugares en los que se realiza teletrabajo. Es decir, se debe establecer procedimientos para el acceso a las carpetas de datos o información que integran al Servidor de Archivos desde fuera de la organización. Asimismo, se debe tener en cuenta la Política de Teletrabajo la cual indica los lineamientos de conexión por VPN y otras consideraciones en el acceso.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Robo o pérdida de información ingresada / Abuso de derechos / Procesamiento ilegal de los datos	Reducción del riesgo	A 9.1.1 POLÍTICA DE CONTROL DE ACCESOS	Norma ISO/IEC 27002:2013	La organización debe implementar procedimientos que estén dentro de la Política de Control de Acceso, en donde se logre establecer procedimientos que regulen el acceso al Servidor de Archivos. Asimismo, salvaguardar la confidencialidad e integridad del procesamiento de los datos inmersos en el servidor. Adicionalmente, la organización debe continuamente supervisar que se ejecute los lineamientos indicados dentro de la Política.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Robo o pérdida de información ingresada / Abuso de derechos / Procesamiento ilegal de los datos	Reducción del riesgo	A 9.2.1 GESTIÓN DE ALTAS / A 9.2.2 GESTIÓN DE LOS DERECHOS DE ACCESO ASIGNADOS A USUARIOS / A 9.2.3 GESTIÓN DE LOS DERECHOS DE ACCESOS CON PRIVILEGIOS ESPECIALES / A 9.2.4 GESTIÓN DE INFORMACIÓN CONFIDENCIAL DE AUTENTIFICACIÓN DE USUARIOS / A 9.2.5 REVISIÓN DE LOS DERECHOS DE ACCESO DE USUARIOS	Norma ISO/IEC 27002:2013	Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso. El conjunto que comprende la Estructura Organizacional del Sistema de Gestión de Seguridad de la Información debe realizar la verificación continua de los privilegios y accesos que tiene cada colaborador en la organización, respecto al contenido del servidor de archivos. Adicionalmente, registrar la fecha y horario de su ingreso y egreso. Por último, los derechos de acceso de todos los usuarios de la carpeta de proyectos se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado

ITEM	ACTIVO	AMENAZAS / RIESGOS	OPCIONES DE TRATAMIENTO DEL RIESGO	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR	DUEÑO DEL RIESGO	RESPONSABLE DEL CONTROL	ESTADO DEL CONTROL
		Manipulación de información / Abuso de derechos / Robo o pérdida de información ingresada / Procesamiento ilegal de los datos	Reducción del riesgo	A 9.2.6 RETIRADA DE LOS DERECHOS DE ACCESO	Norma ISO/IEC 27002:2013	Los derechos de acceso de todos los usuarios de las carpetas de datos embebidos en el Servidor de Archivos se deben retirar al término de su empleo, contrato o acuerdo, los cuales se deben ajustar inmediatamente al término del vínculo laboral.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Abuso de derechos / Procesamiento ilegal de los datos	Reducción del riesgo	A 9.3.1 USO DE INFORMACIÓN CONFIDENCIAL PARA LA AUTENTICACIÓN	Norma ISO/IEC 27002:2013	Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Robo o pérdida de información ingresada / Abuso de derechos / Procesamiento ilegal de los datos / Pérdidas de comunicación por manipulación	Reducción del riesgo	A 9.4.1 RESTRICCIÓN DE ACCESO A LA INFORMACIÓN	Norma ISO/IEC 27002:2013	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Inoperatividad del sistema o servicio / Destrucción del equipo / Abuso de derechos / Inoperatividad del equipo y/o equipos / Sniffer de Información	Reducción del riesgo	A 11.2.1 EMPLAZAMIENTO / UBICACIÓN Y PROTECCION DE LOS EQUIPOS	Norma ISO/IEC 27002:2013	El servidor de archivos debe de estar ubicado y protegido para reducir los riesgos de amenazas y peligros del entorno, y las propias posibilidades de acceso no autorizado.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Inoperatividad del sistema / Destrucción del equipo / Inoperatividad del equipo y/o equipos / Falla en el suministro eléctrico	Reducción del riesgo	A 11.2.2 INSTALACIONES DE SUMINISTROS	Norma ISO/IEC 27002:2013	El Servidor de Archivos se debe proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro eléctrico. Se recomienda la adquisición de un UPS.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Inoperatividad del sistema o servicio/ Inoperatividad del equipo y/o equipos / Procesamiento ilegal de los datos / Sniffer de Información / Pérdidas de comunicación por manipulación	Reducción del riesgo	A 11.2.3 SEGURIDAD DEL CABLEADO	Norma ISO/IEC 27002:2013	Mantener seguridad relativa al cableado que utiliza la conexión del servidor de archivos. Adicionalmente, inspeccionar que el cableado permanezca en adecuadas condiciones. Adicionalmente, inspeccionar que el cableado permanezca en adecuadas condiciones y sin puntos de acceso libres o tomas de accesos libres. La organización deberá contar con un sistema de cableado estructurado, efectuando las correspondientes revisiones periódicas que sean necesarias.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado

ITEM	ACTIVO	AMENAZAS / RIESGOS	OPCIONES DE TRATAMIENTO DEL RIESGO	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR	DUEÑO DEL RIESGO	RESPONSABLE DEL CONTROL	ESTADO DEL CONTROL
		Inoperatividad del equipo y/o equipos / Fallas en el funcionamiento de equipo y/o equipos	Reducción del riesgo	A 11.2.4 MANTENIMIENTO DE LOS EQUIPOS	Norma ISO/IEC 27002:2013	Someter al servidor de archivos (File Server) a tareas de mantenimiento preventivo lógico y físico. Ello de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor. Inicialmente se realiza un programa de mantenimiento que se va ejecutando y posteriormente se realiza su respectivo seguimiento.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Pérdidas de comunicación por manipulación	Reducción del riesgo	A 12.1.2 GESTIÓN DE CAMBIOS	Norma ISO/IEC 27002:2013	La organización debe contar con una política y/o procedimiento en donde se gestionen los cambios realizados en las carpetas que pertenecen al Servidor de Archivos y en general a todas las carpetas que contengan información de uso recurrente y confidencial para la misma. Asimismo, llevar un inventario de los cambios realizados y el personal asociado al mismo.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Inoperatividad del sistema o servicio / Destrucción del equipo / Inoperatividad del equipo y/o equipos	Reducción del riesgo	A 12.1.3 GESTIÓN DE CAPACIDAD	Norma ISO/IEC 27002:2013	Se debe revisar cotidianamente y en ciclos programados el consumo de recursos del servidor de archivos que contiene las carpetas de Proyectos, Licitaciones, Áreas Administrativas y Contables, y otra clase de información embebida en ella. Se debe monitorear regularmente sus recursos, tales como: memoria, procesamiento y almacenamiento y realizar mejoras en los mismos recursos de ser necesario, incluso el cambio del equipo de acuerdo a un dimensionamiento previamente realizado.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Abuso de derechos / Robo o pérdida de información ingresada / Procesamiento ilegal de los datos / Fallas en el funcionamiento de equipo y/o equipos	Reducción del riesgo	A.12.2.1 CONTROLES CONTRA EL CÓDIGO MALICIOSO	Norma ISO/IEC 27002:2013	Los equipos de cómputo deben contar con un Antivirus estándar como mínimo para la protección contra código malicioso, tales los virus comunes. Asimismo, la organización debe crear procedimientos en donde se especifiquen: Los usuarios no pueden instalar software no autorizado en los equipos sin autorización previa. Accionar en el buen uso del Internet, correo electrónico y medios de almacenamiento extraíbles.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado

ITEM	ACTIVO	AMENAZAS / RIESGOS	OPCIONES DE TRATAMIENTO DEL RIESGO	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR	DUEÑO DEL RIESGO	RESPONSABLE DEL CONTROL	ESTADO DEL CONTROL
		Inoperatividad del sistema o servicio / Destrucción del equipo / Robo o pérdida de información ingresada / Inoperatividad del equipo y/o equipos	Reducción del riesgo	A 12.3.1 COPIAS DE SEGURIDAD DE LA INFORMACIÓN	Norma ISO/IEC 27002:2013	Se debe realizar respaldos de la información contenida en el servidor de archivos. Adicionalmente, el servidor de archivos debe estar salvaguardada y protegida por un respaldo mensual, semanal u otro que la organización crea conveniente. Asimismo, dichos backup deben almacenarse en sitios alternos a la organización.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Inoperatividad del sistema o servicio / Robo o pérdida de información ingresada / Abuso de derechos / Inoperatividad del equipo y/o equipos / Procesamiento ilegal de los datos	Reducción del riesgo	A 12.4.1 REGISTRO Y GESTIÓN DE EVENTOS DE ACTIVIDAD / A 16.1.2 NOTIFICACIÓN DE LOS DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN / A 16.1.3 NOTIFICACIÓN DE DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN	Norma ISO/IEC 27002:2013	Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario respecto al servidor de archivos, tales como: fallas, eventos de seguridad de la información, historial de acceso a carpetas, consumo de datos, usuarios top, entre otros. Asimismo, reportar y notificar cualquier incidente relacionado con la seguridad de la información del sistema referido y el propio consumo del recurso.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Inoperatividad del sistema / Robo o pérdida de información ingresada / Abuso de derechos / Procesamiento ilegal de los datos / Sniffer de Información	Reducción del riesgo	A 13.1.1 CONTROLES DE RED / A 13.1.2 MECANISMOS DE SEGURIDAD DE SEGURIDAD ASOCIADAS A SERVICIOS DE RED	Norma ISO/IEC 27002:2013	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones. Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Robo o pérdida de información ingresada / Abuso de derechos / Procesamiento ilegal de los datos / Sniffer de Información / Pérdidas de comunicación por manipulación	Reducción del riesgo	A 16.1.5 RESPUESTA A LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	Norma ISO/IEC 27002:2013	La organización deberá contar con mecanismos de control de incidentes de Seguridad de la Información sobre la Infraestructura Tecnológica implementada y los propios equipos de cómputo asignados a los usuarios finales para la ejecución de sus labores diarias. Asimismo, se deberá monitorear regularmente las actividades del personal y el uso de los sistemas de información. Este monitoreo se lleva a cabo evaluando todos los incidentes de seguridad encontrados.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado

ITEM	ACTIVO	AMENAZAS / RIESGOS	OPCIONES DE TRATAMIENTO DEL RIESGO	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR	DUEÑO DEL RIESGO	RESPONSABLE DEL CONTROL	ESTADO DEL CONTROL
		Inoperatividad del sistema o servicio / Destrucción del equipo / Inoperatividad del equipo y/o equipos	Reducción del riesgo	A 17.2.1 DISPONIBILIDAD DE INSTALACIONES DE PROCESAMIENTO DE INFORMACIÓN	Norma ISO/IEC 27002:2013	El servicio que brinda y el propio Servidor de Archivos debe contar con una redundancia suficiente para cumplir los requisitos de disponibilidad, esto debido al contenido de información crítica para la organización embebida en el mismo. Este apartado debe estar incluido dentro del Plan de Recuperación ante Desastre (DRP) diseñado y posteriormente implementado por la propia organización.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Inoperatividad del sistema o servicio / Robo o pérdida de información ingresada / Abuso de derechos / Inoperatividad del equipo y/o equipos / Procesamiento ilegal de los datos	Reducción del riesgo	A 18.1.3 PROTECCIÓN DE LOS REGISTROS DE LA ORGANIZACIÓN	Norma ISO/IEC 27002:2013	Los registros de acceso al Servidor de Archivos se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Robo o pérdida de información ingresada / Procesamiento ilegal de los datos	Reducción del riesgo	A 18.1.4 PROTECCIÓN DE DATOS Y PRIVACIDAD DE LA INFORMACIÓN PERSONAL	Norma ISO/IEC 27002:2013	Se deben asegurar la privacidad y la protección de la información de datos personales de clientes de la organización, en el flujo de intercambio de información asociado a las carpetas de datos embebidas en el Servidor de Archivos. Este aseguramiento de la privacidad y protección de datos es tal como se exige en la Ley de Protección de Datos Personales, en cuanto a la clasificación de Banco de Datos.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Espionaje de contraseñas / Ataques de diccionario	Reducción del riesgo	TA 1. EJECUCIÓN DE PROCEDIMIENTOS PARA EL USO DE CONTRASEÑAS FUERTES / TA 2. LIMITAR EL NÚMERO DE ACCESO A CONTRASEÑAS INVALIDAS	Técnico Auxiliar	Ejecutar procedimientos técnicos para evitar el Espionaje de contraseñas, ataques de contraseñas o métodos de cracking. El procedimiento es indicado dentro de la Política de Control de Acceso, en el apartado "Gestión de Contraseñas de Usuario", propuesto en el presente proyecto.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado

ITEM	ACTIVO	AMENAZAS / RIESGOS	OPCIONES DE TRATAMIENTO DEL RIESGO	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR	DUEÑO DEL RIESGO	RESPONSABLE DEL CONTROL	ESTADO DEL CONTROL
		Abuso de derechos / Procesamiento ilegal de los datos / Robo o pérdida de información ingresada	Reducción del riesgo	TA 4. IMPLEMENTACIÓN DE UN DATA LOSS PREVENTION (DLP)	Técnico Auxiliar	La organización debe contemplar la adopción de una solución de DLP (Data Loss Prevention) para la clasificación de Información y manejo adecuado de la misma dentro y fuera de la organización, ello en cumplimiento de las reglas o directrices indicadas por la misma. Las carpetas embebidas dentro del servidor deben ser ingresadas a la solución para la aplicación de las políticas de Seguridad y evitar fugas de información.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Acceso no autorizado al sistema / Acceso no autorizado al equipo / Abuso de derechos / Procesamiento ilegal de los datos / Robo o pérdida de información ingresada	Reducción del riesgo	TA 15. IMPLEMENTACIÓN DE UNA SUITE O SOLUCIÓN DE ENDPOINT PARA PREVENIR ATAQUES DE FIRMAS COMUNES Y DE DÍA CERO	Técnico Auxiliar	La organización debe implementar una suite o solución de Endpoint para la protección y prevención contra ataques comunes y ataques de Dia Cero (Zero Days). Esta solución deberá contar con módulos de seguridad como: AV, Antibot, IPS, Antimalware (prevención y protección contra ataques de día cero) y otros Blades o módulos de seguridad embebidos.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Procesamiento ilegal de los datos / Robo o pérdida de información ingresada / Inoperatividad del equipo y/o equipos / Destrucción del equipo	Reducción del riesgo	TA 16. IMPLEMENTACIÓN DE UNA SOLUCIÓN DE RESPALDO DE ENDPOINT O ESTACIONES DE TRABAJO Y/O SERVIDORES	Técnico Auxiliar	La organización debe considerar la implementación de una solución de respaldo de estaciones finales de trabajo o Endpoint y servidores, esto mediante un agente instalado en el computador, apuntando el respaldo a un Storage local o en nube: Soluciones como Barracuda Backup, Veeam Backup, Veritas, entre otras. Todas las PC's asociadas a la plana de Gerentes, Jefes y usuarios finales deben tener un respaldo del contenido del computador sin excepción, esto para fines de recuperación y auditoria.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Acceso no autorizado al Sistema / Inoperatividad del equipo y/o equipos / Fallas en el funcionamiento de equipo y/o equipos	Reducción del riesgo	TA 17. IMPLEMENTACIÓN DE UN SERVIDOR CENTRALIZADO PARA INSTALACIÓN DE PARCHES DE SEGURIDAD	Técnico Auxiliar	La organización debe implementar un servidor centralizado para la instalación de parches de seguridad, esto programado de manera automática o ejecutada de manera manual, lo cual aplique a todos los equipos de cómputo y la totalidad de servidores. Con ello, evitar o disminuir fallas de seguridad asociadas a versiones de Sistema Operativos, específicamente Windows (Servidor centralizado WSUS) debido a que es el Sistema Operativo utilizado en la organización.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado

ITEM	ACTIVO	AMENAZAS / RIESGOS	OPCIONES DE TRATAMIENTO DEL RIESGO	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR	DUEÑO DEL RIESGO	RESPONSABLE DEL CONTROL	ESTADO DEL CONTROL
		Robo o pérdida de información ingresada / Abuso de derechos	Reducción del riesgo	TA 26. IMPLEMENTACIÓN DE SOFTWARE DE AUDITORIA DE USO DEL CONTENIDOS DE LOS EQUIPOS DE INFRAESTRUCTURA DE COMUNICACIONES	Técnico Auxiliar	La organización debe considerar la adopción de un software de auditoria de uso de los datos contenidos dentro de los equipos que componen la Infraestructura de Comunicaciones (Incluye servidores). Esto incluye: uso, acceso, horario de acceso, entre otros datos relevantes para la auditoria.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Acceso no autorizado al sistema / Abuso de derechos / Acceso no autorizado al equipo / Acceso no autorizado al sistema	Reducción del riesgo	TA 27. INGRESO LÓGICO DEL SERVIDOR DE ARCHIVOS POR MEDIO DEL DIRECTORIO ACTIVO	Técnico Auxiliar	El servidor de archivos deberá ser unido al dominio de la organización vía el soporte del Active Directory. Ello para contar con una administración de despliegue de política de seguridad, despliegue de paquetes de actualización, accesos a carpetas de archivos seleccionados y otras funcionalidades de manera centralizada.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Inoperatividad del Sistema / Destrucción del equipo	Transferencia del riesgo	TA 28. MIGRACIÓN DEL SERVICIO DE FTP BAJO UN SERVICIO EN LA NUBE MEDIANTE IAAS	Técnico Auxiliar	La organización debe contemplar la aplicación y ejecución de uno de los modelos de Cloud Computing, es decir Infraestructura como Servicio (IaaS) y llevar el servidor FTP que contiene las distintas carpetas de datos con información de la organización a la nube, evitando gastos de capital y reduciendo los costos corrientes (energía, aire acondicionado, otros), por un pago mensual o anual según convenga.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
10	Infraestructura de Comunicaciones	Robo o pérdida de información ingresada / Abuso de derechos / Procesamiento ilegal de los datos / Sniffer de Información	Reducción del riesgo	A 5.1.1 CONJUNTO DE POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN / A 5.1.2 REVISIÓN DE LAS POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN		Mantener implementados los lineamientos de la política de seguridad de la información de la organización. Para lograr el cumplimiento de todas las políticas y normas de seguridad de la información, la compañía se vale de los reportes generados por la Estructura de Gestión de Seguridad de la Información. De estos reportes, se evaluará si existen incumplimientos y se determinará la causa del incumplimiento, se tomarán las acciones correctivas para garantizar la mitigación de estos incumplimientos, y se revisarán estas acciones.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado

ITEM	ACTIVO	AMENAZAS / RIESGOS	OPCIONES DE TRATAMIENTO DEL RIESGO	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR	DUEÑO DEL RIESGO	RESPONSABLE DEL CONTROL	ESTADO DEL CONTROL
		Robo de Equipo / Destrucción de equipo / Abuso de derechos	Reducción del riesgo	A 8.1.1 INVENTARIO DE ACTIVOS	Norma ISO/IEC 27002:2013	Realizar inventario de los equipos de Infraestructura con los que cuenta la organización; identificarlos como activos propiedad de la organización y revisarlo anualmente.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Abuso de derechos / Robo de Equipo	Reducción del riesgo	A 8.1.2 PROPIEDAD DE LOS ACTIVOS	Norma ISO/IEC 27002:2013	Los activos de información asociados a Infraestructura de Comunicaciones tienen su propietario estipulado, estos son responsabilidad de cada colaborador. Cada mismo debe darle adecuado uso, tanto al activo como a la información embebida.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Acceso no autorizado al sistema / Abuso de derechos / Procesamiento ilegal de los datos / Inoperatividad del equipo y/o equipos / Robo de equipo / Pérdidas de comunicación por manipulación	Reducción del riesgo	A 8.1.3 USO ACEPTABLE DE LOS ACTIVOS	Norma ISO/IEC 27002:2013	Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información. Asimismo, se debe crear un procedimiento para documentar al termino del cargo	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Robo o pérdida de información ingresada / Pérdida de información ingresada / Abuso de derechos / Procesamiento ilegal de los datos	Reducción del riesgo	A 9.1.1 POLÍTICA DE CONTROL DE ACCESOS	Norma ISO/IEC 27002:2013	La organización debe implementar procedimientos que estén dentro de la Política de Control de Acceso, en donde se logre establecer procedimientos que regulen el acceso a los equipos y recursos que componen a la Infraestructura de Comunicaciones. Asimismo, salvaguardar la confidencialidad e integridad del procesamiento de los datos inmersos en el servidor. Adicionalmente, la organización debe continuamente supervisar que se ejecute los lineamientos indicados dentro de la Política.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado

ITEM	ACTIVO	AMENAZAS / RIESGOS	OPCIONES DE TRATAMIENTO DEL RIESGO	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR	DUEÑO DEL RIESGO	RESPONSABLE DEL CONTROL	ESTADO DEL CONTROL
		Robo o pérdida de información ingresada / Abuso de derechos / Procesamiento ilegal de los datos / Sniffer de Información / Pérdidas de comunicación por manipulación	Reducción del riesgo	A 9.1.2 CONTROL DE ACCESO A LAS REDES Y SERVICIOS ASOCIADOS	Norma ISO/IEC 27002:2013	La organización dentro de su Política de Uso Aceptable de los Sistema de Información, Internet y Correo Electrónico, especifica el acceso de los usuarios a los servicios que integran la Infraestructura de Comunicaciones para los que hayan sido previamente autorizados. Asimismo, la organización especifica lineamientos a cumplir dentro de la Política de Control de Acceso.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Robo o pérdida de información ingresada / Pérdida de información ingresada / Abuso de derechos / Procesamiento ilegal de los datos / Pérdidas de comunicación por manipulación	Reducción del riesgo	A 9.4.1 RESTRICCIÓN DE ACCESO A LA INFORMACIÓN	Norma ISO/IEC 27002:2013	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Abuso de derechos	Reducción del riesgo	A 9.4.3 GESTIÓN DE CONTRASEÑAS DE USUARIOS	Norma ISO/IEC 27002:2013	El usuario que utiliza equipos que pertenezcan a la Infraestructura de Comunicaciones debe utilizar contraseñas seguras y robustas para el acceso al activo e información.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Inoperatividad del sistema / Destrucción del equipo / Abuso de derechos / Inoperatividad del equipo y/o equipos / Fallas en el funcionamiento de equipo y/o equipos / Acceso no autorizado al sistema	Reducción del riesgo	A 11.1.1 PERIMETRO DE SEGURIDAD FÍSICA / A 11.1.2 CONTROLES FÍSICOS DE ENTRADA	Norma ISO/IEC 27002:2013	El área de acceso a los equipos que componen la Infraestructura de Comunicaciones deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Inoperatividad del sistema / Destrucción del equipo / Abuso de derechos / Sniffer de Información / Robo de Equipo / Inoperatividad del equipo y/o equipos / Fallas en el funcionamiento de equipo y/o equipos	Reducción del riesgo	A 11.2.1 EMPLAZAMIENTO / UBICACIÓN Y PROTECCION DE LOS EQUIPOS	Norma ISO/IEC 27002:2013	Los equipos que componen la Infraestructura de Comunicaciones deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las propias posibilidades de acceso no autorizado.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado

ITEM	ACTIVO	AMENAZAS / RIESGOS	OPCIONES DE TRATAMIENTO DEL RIESGO	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR	DUEÑO DEL RIESGO	RESPONSABLE DEL CONTROL	ESTADO DEL CONTROL
		Inoperatividad del sistema o servicio / Destrucción de equipo / Inoperatividad del equipo y/o equipos / Falla en el suministro eléctrico	Reducción del riesgo	A 11.2.2 INSTALACIONES DE SUMINISTROS	Norma ISO/IEC 27002:2013	Los equipos que componen la Infraestructura de Comunicaciones: Especialmente el Servidor que contiene el Sistema de Gestión de Tickets, Servidor de Archivos, Servidor de Correo e Internet se debe proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro eléctrico. Se recomienda la adquisición de un UPS.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Inoperatividad del sistema o servicio / Procesamiento ilegal de los datos / Sniffer de Información / Pérdidas de comunicación por manipulación	Reducción del riesgo	A 11.2.3 SEGURIDAD DEL CABLEADO	Norma ISO/IEC 27002:2013	Mantener seguridad relativa al cableado que utiliza cada equipo de la Infraestructura de Comunicaciones para inspeccionar que el cableado permanezca en adecuadas condiciones. Adicionalmente, inspeccionar que el cableado permanezca en adecuadas condiciones y sin puntos de acceso libres o tomas de accesos libres. La organización deberá contar con un sistema de cableado estructurado, efectuando las correspondientes revisiones periódicas que sean necesarias.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Inoperatividad del equipo y/o equipos / Fallas en el funcionamiento de equipo y/o equipos	Reducción del riesgo	A 11.2.4 MANTENIMIENTO DE LOS EQUIPOS	Norma ISO/IEC 27002:2013	Los equipos asociados a la Infraestructura de Comunicaciones (Servidor que aloja el Sistema de Gestión de Tickets, Servidor de Correo, entre otros) deben mantenerse correctamente para asegurar su disponibilidad e integridad continuas. Se debe coordinar un plan de mantenimiento lógico y físico sobre los equipos de Infraestructura de Comunicaciones.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Inoperatividad del sistema / Destrucción del equipo / Inoperatividad del equipo y/o equipos / Fallas en el funcionamiento de equipo y/o equipos	Reducción del riesgo	A 12.1.3 GESTIÓN DE CAPACIDAD	Norma ISO/IEC 27002:2013	Se debe revisar cotidianamente y en ciclos programados el consumo de recursos de los equipos que componen la Infraestructura de Comunicaciones. Se debe monitorear regularmente sus recursos, tales como: memoria, procesamiento y almacenamiento y realizar mejoras en los mismos recursos de ser necesario, incluso el cambio del equipo de acuerdo a un dimensionamiento previamente realizado.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado

ITEM	ACTIVO	AMENAZAS / RIESGOS	OPCIONES DE TRATAMIENTO DEL RIESGO	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR	DUEÑO DEL RIESGO	RESPONSABLE DEL CONTROL	ESTADO DEL CONTROL
		Abuso de derechos / Inoperatividad del sistema o servicio / Robo o pérdida de información ingresada / Procesamiento ilegal de los datos / Inoperatividad del equipo y/o equipos / Fallas en el funcionamiento del equipo / Acceso no autorizado al sistema	Reducción del riesgo	A.12.2.1 CONTROLES CONTRA EL CÓDIGO MALICIOSO	Norma ISO/IEC 27002:2013	Los equipos que componen la Infraestructura de Comunicaciones (esencialmente servidores) deben contar con un Antivirus estándar como mínimo para la protección contra código malicioso, tales los virus comunes. Asimismo, la organización debe crear procedimientos en donde se especifiquen: Los usuarios no pueden instalar software no autorizado en los equipos sin autorización previa. Accionar en el buen uso del Internet, correo electrónico y medios de almacenamiento extraíbles.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Inoperatividad del sistema o servicio / Destrucción del equipo / Robo o pérdida de información ingresada / Robo de Equipo / Inoperatividad del equipo y/o equipos / Fallas en el funcionamiento del equipo / Falla en el suministro eléctrico	Reducción del riesgo	A 12.3.1 COPIAS DE SEGURIDAD DE LA INFORMACIÓN	Norma ISO/IEC 27002:2013	Se deben hacer copias de respaldo de la información y configuración que cuentan los equipos que integran la Infraestructura de Comunicaciones y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas. Ello con el fin de proteger la información dentro del activo contra la pérdida de datos.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Inoperatividad del sistema / Robo o pérdida de información ingresada / Abuso de derechos / Procesamiento ilegal de los datos / Inoperatividad del equipo y/o equipos / Fallas en el funcionamiento de equipo y/o equipos	Reducción del riesgo	A12.4.1 REGISTRO Y GESTIÓN DE EVENTOS DE ACTIVIDAD	Norma ISO/IEC 27002:2013	Reportar todo incidente físico, lógico o cualquier evento de seguridad de la información que se presente en los equipos de Infraestructura de Comunicaciones y su propio registro de accesos a los mismos.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Inoperatividad del sistema / Robo o pérdida de información ingresada / Abuso de derechos / Procesamiento ilegal de los datos / Sniffer de Información / Fallas en el funcionamiento de equipo y/o equipos	Reducción del riesgo	A 13.1.1 CONTROLES DE RED / A 13.1.2 MECANISMOS DE SEGURIDAD DE SEGURIDAD ASOCIADAS A SERVICIOS DE RED	Norma ISO/IEC 27002:2013	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones. Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado

ITEM	ACTIVO	AMENAZAS / RIESGOS	OPCIONES DE TRATAMIENTO DEL RIESGO	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR	DUEÑO DEL RIESGO	RESPONSABLE DEL CONTROL	ESTADO DEL CONTROL
		Inoperatividad del sistema / Destrucción del equipo / Abuso de derechos / Procesamiento ilegal de los datos / Sniffer de Información / Inoperatividad del equipo y/o equipos / Fallas en el funcionamiento de equipo y/o equipos / Pérdidas de comunicación por manipulación	Reducción del riesgo	A 15.1.3 CADENA DE SUMINISTRO EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES	Norma ISO/IEC 27002:2013	Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con los equipos que componen la Infraestructura de Comunicaciones. Asimismo, llegar a acuerdos para brindar los recursos necesarios en caso de falla o interrupción en la continuidad del servicio asociada a ellas.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Robo o pérdida de información ingresada / Abuso de derechos / Procesamiento ilegal de los datos / Sniffer de Información / Fallas en el funcionamiento de equipo y/o equipos / pérdidas de comunicación por manipulación	Reducción del riesgo	A 16.1.2 NOTIFICACIÓN DE LOS DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN / A 16.1.3 NOTIFICACIÓN DE DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN	Norma ISO/IEC 27002:2013	Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible. Asimismo, reportar debilidades relativas a la seguridad del equipo de cómputo inmediatamente al Oficial de Seguridad de la Información o propiamente a las personas que integran la Estructura Organizacional del Sistema de Gestión de Seguridad de la Información.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Inoperatividad del sistema o servicio / Destrucción del equipo / Robo o pérdida de información ingresada / Abuso de derechos / Procesamiento ilegal de los datos / Sniffer de Información / Fallas en el funcionamiento de equipo y/o equipos / Pérdidas de comunicación por manipulación	Reducción del riesgo	A 16.1.5 RESPUESTA A LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	Norma ISO/IEC 27002:2013	La organización deberá contar con mecanismos de control de incidentes de Seguridad de la Información sobre la Infraestructura Tecnológica implementada y los propios equipos de cómputo asignados a los usuarios finales para la ejecución de sus labores diarias. Asimismo, se deberá monitorear regularmente las actividades del personal y el uso de los sistemas de información. Este monitoreo se lleva a cabo evaluando todos los incidentes de seguridad encontrados.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Inoperatividad del sistema / Destrucción del equipo Inoperatividad del equipo y/o equipos / Desastre Natural / Falla masiva / Ataque de cualquier tipo que atente contra la continuidad del negocio	Reducción del riesgo	A 17.1.1 PLANIFICACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN / A 17.1.2 IMPLANTACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	Norma ISO/IEC 27002:2013	La Alta Dirección junto con los integrantes de la Estructura Organizacional del Sistema de Gestión de Seguridad de la Información debe plantear planes de continuidad del negocio o DRP (ración ante Desastre) que serán de utilidad para resguardar toda la información manejada en la organización.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado

ITEM	ACTIVO	AMENAZAS / RIESGOS	OPCIONES DE TRATAMIENTO DEL RIESGO	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR	DUEÑO DEL RIESGO	RESPONSABLE DEL CONTROL	ESTADO DEL CONTROL
		Inoperatividad del sistema o servicio / Destrucción del equipo / Inoperatividad del equipo y/o equipos / Desastre Natural / Falla masiva / Ataque de cualquier tipo que atente contra la continuidad del negocio	Reducción del riesgo	A 17.2.1 DISPONIBILIDAD DE INSTALACIONES DE PROCESAMIENTO DE INFORMACIÓN	Norma ISO/IEC 27002:2013	La organización debe diseñar y posteriormente implementar un Plan de Recuperación ante Desastre (DRP) ante la ejecución de cualquier un evento que imposibilita la continuación de las funciones normales de operación de la organización. Con ello, la organización tomará las precauciones necesarias para que los efectos de un desastre se reduzcan al mínimo y la organización sea capaz de mantener o reanudar rápidamente funciones de misión crítica, específicamente los equipos y servicios críticos que se manejan en la Infraestructura de Comunicaciones.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Robo de Información / Robo o pérdida de información ingresada / Abuso de derechos / Procesamiento ilegal de los datos / Fallas en el funcionamiento de equipo y/o equipos	Reducción del riesgo	A 18.2.2 CUMPLIMIENTO DE LAS POLÍTICAS Y NORMAS DE SEGURIDAD	Norma ISO/IEC 27002:2013	Tener conocimiento y seguir los lineamientos de las políticas y normas de seguridad de la organización. Para lograr el cumplimiento de todas las políticas y normas de seguridad de la información, la organización se vale de los reportes generados por la Estructura de Gestión de Seguridad de la Información. De estos reportes, se evaluará si existen incumplimientos y se determinará la causa del incumplimiento, se tomarán las acciones correctivas para garantizar la mitigación de estos incumplimientos y se revisarán estas acciones.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Espionaje de contraseñas / Ataques de diccionario	Reducción del riesgo	TA 1. EJECUCIÓN DE PROCEDIMIENTOS PARA EL USO DE CONTRASEÑAS FUERTES / TA 2. LIMITAR EL NÚMERO DE ACCESO A CONTRASEÑAS INVALIDAS	Técnico Auxiliar	Ejecutar procedimientos técnicos para evitar el Espionaje de contraseñas, ataques de contraseñas o métodos de cracking. El procedimiento es indicado dentro de la Política de Control de Acceso, en el apartado "Gestión de Contraseñas de Usuario", propuesto en el presente proyecto.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado

ITEM	ACTIVO	AMENAZAS / RIESGOS	OPCIONES DE TRATAMIENTO DEL RIESGO	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR	DUEÑO DEL RIESGO	RESPONSABLE DEL CONTROL	ESTADO DEL CONTROL
		Abuso de derechos / Procesamiento ilegal de los datos / Robo o pérdida de información ingresada	Reducción del riesgo	TA 4. IMPLEMENTACIÓN DE UN DATA LOSS PREVENTION (DLP)	Técnico Auxiliar	La organización debe contemplar la adopción de una solución de DLP (Data Loss Prevention) para la clasificación de Información y manejo adecuado de la misma dentro y fuera de la organización, ello en cumplimiento de las reglas o directrices indicadas por la misma. La información confidencial contenida en los distintos servidores con los que cuenta la organización debe ser ingresada a la solución para la aplicación de las políticas de Seguridad y evitar fugas de información.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Acceso no autorizado al equipo / Abuso de derechos / Procesamiento ilegal de los datos / Robo o pérdida de información ingresada	Reducción del riesgo	TA 15. IMPLEMENTACIÓN DE UNA SUITE O SOLUCIÓN DE ENDPOINT PARA PREVENIR ATAQUES DE FIRMAS COMUNES Y DE DÍA CERO	Técnico Auxiliar	La organización debe implementar una suite o solución de Endpoint para la protección y prevención contra ataques comunes y ataques de Dia Cero (Zero Days). Esta solución deberá contar con módulos de seguridad como: AV, Antibot, IPS, Antimalware (prevención y protección contra ataques de día cero) y otros Blades o módulos de seguridad embebidos.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Procesamiento ilegal de los datos / Robo o pérdida de información ingresada / Inoperatividad del equipo y/o equipos / Destrucción del equipo	Reducción del riesgo	TA 16. IMPLEMENTACIÓN DE UNA SOLUCIÓN DE RESPALDO DE ENDPOINT O ESTACIONES DE TRABAJO Y/O SERVIDORES	Técnico Auxiliar	La organización debe considerar la implementación de una solución de respaldo de estaciones finales de trabajo o Endpoint y servidores, esto mediante un agente instalado en el computador, apuntando el respaldo a un Storage local o en nube: Soluciones como Barracuda Backup, Veeam Backup, Veritas, entre otras. Todas las PC's asociadas a la plana de Gerentes, Jefes y usuarios finales deben tener un respaldo del contenido del computador sin excepción, esto para fines de recuperación y auditoria.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado

ITEM	ACTIVO	AMENAZAS / RIESGOS	OPCIONES DE TRATAMIENTO DEL RIESGO	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR	DUEÑO DEL RIESGO	RESPONSABLE DEL CONTROL	ESTADO DEL CONTROL
		Acceso no autorizado al Sistema / Inoperatividad del equipo y/o equipos / Fallas en el funcionamiento de equipo y/o equipos	Reducción del riesgo	TA 17. IMPLEMENTACIÓN DE UN SERVIDOR CENTRALIZADO PARA INSTALACIÓN DE PARCHES DE SEGURIDAD	Técnico Auxiliar	La organización debe implementar un servidor centralizado para la instalación de parches de seguridad, esto programado de manera automática o ejecutada de manera manual, lo cual aplique a todos los equipos de cómputo y la totalidad de servidores. Con ello, evitar o disminuir fallas de seguridad asociadas a versiones de Sistema Operativos, específicamente Windows (Servidor centralizado WSUS) debido a que es el Sistema Operativo utilizado en la organización.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Robo o pérdida de información ingresada / Abuso de derechos	Reducción del riesgo	TA 26. IMPLEMENTACIÓN DE SOFTWARE DE AUDITORIA DE USO DEL CONTENIDOS DE LOS EQUIPOS DE INFRAESTRUCTURA DE COMUNICACIONES	Técnico Auxiliar	La organización debe considerar la adopción de un software de auditoria de uso de los datos contenidos dentro de los equipos que componen la Infraestructura de Comunicaciones (Incluye servidores). Esto incluye: uso, acceso, horario de acceso, entre otros datos relevantes para la auditoria.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Acceso no autorizado al sistema / Abuso de derechos / Acceso no autorizado al equipo / Acceso no autorizado al sistema	Reducción del riesgo	TA 29. INGRESO LÓGICO DEL SERVIDOR DE ARCHIVOS POR MEDIO DEL DIRECTORIO ACTIVO	Técnico Auxiliar	Los servidores que componen la Infraestructura de Comunicaciones deberán ser unidos al dominio de la organización vía el soporte del Active Directory. Ello para contar con una administración de despliegue de política de seguridad, despliegue de paquetes de actualización, accesos a carpetas de archivos seleccionados y otras funcionalidades de manera	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado
		Falla masiva / Ataque de cualquier tipo que atente contra la continuidad del negocio / Desastre natural	Transferencia del riesgo	TA 30. EVALUACIÓN E IMPLEMENTACIÓN DE UN DATA CENTER ALTERNO	Técnico Auxiliar	La organización debe evaluar un Site Alterno o Data Center Alterno en el cual se pueda sostener la operación de los servicios más críticos que dan continuidad al negocio, esto ante alguna eventualidad de para de continuidad de labores, desastre natural, ataque cibernético o cualquier ataque que atente contra la continuidad del negocio.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado

ITEM	ACTIVO	AMENAZAS / RIESGOS	OPCIONES DE TRATAMIENTO DEL RIESGO	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR	DUEÑO DEL RIESGO	RESPONSABLE DEL CONTROL	ESTADO DEL CONTROL
11	Personal	Incumplimiento de Normas establecidas respecto a Seguridad de la Información / Abuso de derechos / Abuso de confidencialidad de datos / Abuso de confidencialidad, integridad y disponibilidad de la información / Robo de información	Reducción del riesgo	A 5.1.1 CONJUNTO DE POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN / A 5.1.2 REVISIÓN DE LAS POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN	Norma ISO/IEC 27002:2013	Mantener implementados los lineamientos de la política de seguridad de la información de la organización. Para lograr el cumplimiento de todas las políticas y normas de seguridad de la información, la compañía se vale de los reportes generados por la Estructura de Gestión de Seguridad de la Información. De estos reportes, se evaluará si existen incumplimientos y se determinará la causa del incumplimiento, se tomarán las acciones correctivas para garantizar la mitigación de estos incumplimientos, y se revisarán estas acciones.	Gerente Administrativo y Financiero	Oficial de Seguridad de la Información	No Implementado
		Incumplimiento de Normas establecidas respecto a Seguridad de la Información / Abuso de derechos / Abuso de confidencialidad de datos / Abuso de confidencialidad, integridad y disponibilidad de la información	Reducción del riesgo	A 6.1.1 ASIGNACIÓN DE RESPONSABILIDADES PARA LA SEGURIDAD DE LA INFORMACIÓN / A 6.1.2 SEGREGACIÓN DE TAREAS	Norma ISO/IEC 27002:2013	Dentro de la Estructura de Organizacional del Sistema de Gestión de Seguridad de la Información se deben asignada las responsabilidades de seguridad de la información a los cargos correspondientes.	Gerente Administrativo y Financiero	Oficial de Seguridad de la Información	No Implementado
		Incumplimiento de Normas establecidas respecto a Seguridad de la Información / Abuso de derechos / Abuso de confidencialidad, integridad y disponibilidad de la información / Robo de información / Negligencia en trabajos asignados / Clientes insatisfechos	Reducción del riesgo	A 7.1.1 INVESTIGACIÓN DE ANTECEDENTES / SELECCIÓN / A 7.1.2 TÉRMINOS Y CONDICIONES DE CONTRATACIÓN	Norma ISO/IEC 27002:2013	La Alta Dirección define los términos y condiciones laborales y asegura que se definan los perfiles de los colaboradores de la compañía.	Gerente Administrativo y Financiero	Oficial de Seguridad de la Información	No Implementado
		Incumplimiento de Normas establecidas respecto a Seguridad de la Información / Abuso de derechos / Abuso de confidencialidad, integridad y disponibilidad de la información / Robo de información / Manipulación de información	Reducción del riesgo	A 7.2.2 CONCIETIZACIÓN, EDUCACIÓN Y CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN.	Norma ISO/IEC 27002:2013	Prevenir el uso inadecuado de los servicios de procesamiento de la información mediante capacitaciones constantes dirigidas al personal operativo divulgadas por Gerentes y Jefes de área.	Gerente Administrativo y Financiero	Oficial de Seguridad de la Información	No Implementado

ITEM	ACTIVO	AMENAZAS / RIESGOS	OPCIONES DE TRATAMIENTO DEL RIESGO	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR	DUEÑO DEL RIESGO	RESPONSABLE DEL CONTROL	ESTADO DEL CONTROL
		Incumplimiento de Normas establecidas respecto a Seguridad de la Información / Abuso de derechos / Abuso de confidencialidad, integridad y disponibilidad de la información / Robo de información / Manipulación de información / Negligencia en trabajos asignados	Reducción del riesgo	A.7.2.3 PROCESO DISCIPLINARIO	Norma ISO/IEC 27002:2013	Todo personal, colaborador de la organización, que incumpla las normas de seguridad establecidas será sometido a una amonestación verbal, si el incidente es recurrente se generará una suspensión y un despido de acuerdo a la gravedad del incidente.	Gerente Administrativo y Financiero	Oficial de Seguridad de la Información	No Implementado
		Abuso de derechos / Abuso de confidencialidad, integridad y disponibilidad de la información / Robo de información / Manipulación de información	Reducción del riesgo	A 7.3.1 CESE O CAMBIO DE PUESTO DE TRABAJO	Norma ISO/IEC 27002:2013	Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o proveedor y se deben hacer cumplir en su totalidad. Ello en beneficio del correcto resguardo de la información propia de la organización.	Gerente Administrativo y Financiero	Oficial de Seguridad de la Información	No Implementado
		Abuso de derechos / Abuso de confidencialidad de datos / Abuso de confidencialidad, integridad y disponibilidad de la información / Robo de información / Manipulación de información	Reducción del riesgo	A 8.1.3 USO ACEPTABLE DE LOS ACTIVOS	Norma ISO/IEC 27002:2013	Todo personal de la organización debe hacer buen uso de los activos que le sean proporcionados, teniendo en cuenta el uso adecuado del correo electrónico y del internet, el uso adecuado de dispositivos móviles, mantener el escritorio despejado, hacer buen uso de las contraseñas, mantener la disponibilidad, integridad y confidencialidad de la información, uso adecuado de los equipos de cómputo y activos asignados para las labores.	Gerente Administrativo y Financiero	Oficial de Seguridad de la Información	No Implementado
		Abuso de derechos / Abuso de confidencialidad, integridad y disponibilidad de la información / Robo de información / Apropiación indebida de activos	Reducción del riesgo	A 8.1.4 DEVOLUCIÓN DE LOS ACTIVOS	Norma ISO/IEC 27002:2013	Al término del empleo, contrato o acuerdo, todos los empleados y/o personal de la organización deben devolver todos los activos propios de la organización que se encuentren a su cargo.	Gerente Administrativo y Financiero	Oficial de Seguridad de la Información	No Implementado

ITEM	ACTIVO	AMENAZAS / RIESGOS	OPCIONES DE TRATAMIENTO DEL RIESGO	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR	DUEÑO DEL RIESGO	RESPONSABLE DEL CONTROL	ESTADO DEL CONTROL
		Abuso de derechos / Abuso de confidencialidad de datos / Abuso de confidencialidad, integridad y disponibilidad de la información / Robo de información	Reducción del riesgo	A 9.1.1 POLÍTICA DE CONTROL DE ACCESOS	Norma ISO/IEC 27002:2013	Capacitar al personal sobre la utilización de contraseña en el equipo, mantener el equipo protegido cuando se encuentre inactivo, hacer buen uso del internet, correo electrónico y en general de los recursos de la organización. Asimismo, supervisar a los visitantes a áreas protegidas y registrar la fecha y horario de su ingreso y egreso mediante una bitácora de acceso. Lo comentado, y otros recursos adicionales, deberán estar registrado dentro de la Política de Control de Acceso elaborada por la organización.	Gerente Administrativo y Financiero	Oficial de Seguridad de la Información	No Implementado
		Abuso de derechos / Abuso de confidencialidad, integridad y disponibilidad de la información	Reducción del riesgo	A 9.3.1 USO DE INFORMACIÓN CONFIDENCIAL PARA LA AUTENTICACIÓN	Norma ISO/IEC 27002:2013	Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	Gerente Administrativo y Financiero	Oficial de Seguridad de la Información	No Implementado
		Incumplimiento de Normas establecidas respecto a Seguridad de la Información / Abuso de derechos / Abuso de confidencialidad de datos / Abuso de confidencialidad, integridad y disponibilidad de la información / Robo de información / Robo o pérdida de información ingresada Manipulación de información / Procesamiento ilegal de los datos	Reducción del riesgo	A 13.2.1 POLÍTICAS Y PROCEDIMIENTOS DE INTERCAMBIO DE INFORMACIÓN / A 13.2.2 ACUERDOS SOBRE INTERCAMBIO DE INFORMACIÓN	Norma ISO/IEC 27002:2013	El personal colaborador de la organización deberá ejecutar los lineamientos indicados en la Política y Procedimientos de Intercambio de Información. Ello con la finalidad de proteger la información propia de la organización contra su divulgación no autorizada o uso inadecuado.	Gerente Administrativo y Financiero	Oficial de Seguridad de la Información	No Implementado
		Robo o pérdida de información ingresada / Procesamiento ilegal de los datos	Reducción del riesgo	A 13.2.3 MENSAJERÍA ELECTRÓNICA	Norma ISO/IEC 27002:2013	El personal de la organización deberá ejecutar los lineamientos para proteger adecuadamente la información incluida dentro de la mensajería electrónica, tal lo indicado en la Política de Uso Aceptable de los Sistema de Información, Intranet y Correo Electrónico.	Gerente Técnico	Oficial de Seguridad de la Información	No Implementado

ITEM	ACTIVO	AMENAZAS / RIESGOS	OPCIONES DE TRATAMIENTO DEL RIESGO	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR	DUEÑO DEL RIESGO	RESPONSABLE DEL CONTROL	ESTADO DEL CONTROL
		Incumplimiento de Normas establecidas respecto a Seguridad de la Información / Abuso de derechos / Abuso de confidencialidad de datos / Abuso de confidencialidad, integridad y disponibilidad de la información / Robo de información / Manipulación de información	Reducción del riesgo	A 13.2.4 ACUERDOS DE CONFIDENCIALIDAD O DE NO DIVULGACIÓN (SECRETO)	Norma ISO/IEC 27002:2013	Con el fin de proteger la información de la organización, respecto a toda la información propia de la organización, la cual es manejada dentro y fuera de la misma, el personal deberá firmar acuerdos de confidencialidad o no divulgación. Asimismo, los componentes de la Estructura Organizacional del Sistema de Seguridad de la Información deberán asegurar que los riesgos de seguridad de la información sean identificados, incluyendo los riesgos de las partes externas. Los colaboradores de la empresa firman una cláusula de confidencialidad al inicio del contrato laboral.	Gerente Administrativo y Financiero	Oficial de Seguridad de la Información	No Implementado
		Ataques de Phishing	Reducción del riesgo	TA 31. ADOPCIÓN DE SISTEMA DE SIMULACIÓN DE EJECUCIÓN DE PHISING	Técnico Auxiliar	La organización debe adoptar un sistema de preparación contra Phising para evaluar a los empleados respecto a la que acciones tomar ante esta clase de ataques cibernéticos. Para ello, es necesario para establecer una línea base que permita implementar un programa eficaz de preparación contra el Phishing. Tomar como referencia el "Phishing Readiness Services" del fabricante Symantec.	Gerente Administrativo y Financiero	Oficial de Seguridad de la Información	No Implementado
		Ingeniería Social	Reducción del riesgo	TA 32. PROGRAMAS DE INFORMACIÓN SOBRE TÉCNICAS DE ATAQUES DE INGENIERÍA SOCIAL	Técnico Auxiliar	La organización debe plantear programas de capacitación al personal de la empresa en donde se explique y detalle las técnicas de ataques de Ingeniería Social utilizadas por los delincuentes informáticos.	Gerente Administrativo y Financiero	Oficial de Seguridad de la Información	No Implementado

ANEXO VI: Declaración de Aplicabilidad - SOA

CLÁUSULA	OBJETIVOS DE CONTROL	CONTROLES	APLICABILIDAD	JUSTIFICACIÓN
A.5 POLITICAS DE SEGURIDAD	A 5.1 DIRECTRICES DE LA DIRECCIÓN EN SEGURIDAD DE LA INFORMACIÓN	A 5.1.1 CONJUNTO DE POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN	SI	Se ha identificado los riesgos de información en la organización. Por ello, es necesario establecer una política de seguridad de la información para informar y concientizar a todos los colaboradores y partes interesadas sobre los riesgos a los que se encuentran expuestos. Asimismo, informar e indicar los controles implementados para evitar la materialización de estos riesgos.
		A 5.1.2 REVISIÓN DE LAS POLITICAS PARA LA SEGURIDAD DE LA INFORMACIÓN	SI	La Política de seguridad de la información deberá definir claramente responsables de su desarrollo e implementación. Asimismo, la Política de Seguridad de la información deberá ser constantemente revisada para asegurar su idoneidad y cumplimiento con respecto a los riesgos de información. Está política debe ser comunicada a todas las partes interesadas y colaboradores de la organización en general.
A.6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	A 6.1 ORGANIZACIÓN INTERNA	A 6.1.1 ASIGNACIÓN DE RESPONSABILIDADES PARA LA SEGURIDAD DE LA INFORMACIÓN	SI	La organización mediante su Política de Seguridad de la Información debe establecer el compromiso y asignación de responsabilidades para su cumplimiento en materia de seguridad de la información. Asimismo, velar por mantener protegida su información mediante la revisión del sistema de gestión de seguridad de la información (SGSI), la firma de los acuerdos de confidencialidad, manteniendo contacto con las autoridades y con grupos de interés especiales. La revisión independiente de seguridad de la información es crucial para el establecimiento de controles en vías del mejoramiento de la organización interna de seguridad de la información.
		A 6.1.2 SEGREGACIÓN DE TAREAS	SI	

CLÁUSULA	OBJETIVOS DE CONTROL	CONTROLES	APLICABILIDAD	JUSTIFICACIÓN
		A 6.1.3 CONTACTO CON LAS AUTORIDADES	NO	No contemplado para la organización
		A 6.1.4 CONTACTO CON GRUPOS DE INTERÉS ESPECIAL	NO	No contemplado para la organización
		A 6.1.5 SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS.	NO	No contemplado para la organización
	A 6.2 DISPOSITIVOS PARA MOVILIDAD Y TELETRABAJO	A 6.2.1 POLÍTICA DE USO DE DISPOSITIVOS PARA MOVILIDAD	NO	No contemplado para la organización
		A 6.2.2 TELETRABAJO	SI	La organización asiste a las tareas de los colaboradores de la misma mediante el Teletrabajo y la propia atención de atenciones de servicios. Esta práctica debe estar regulada para un correcto y seguro acceso de los recursos brindados por la organización.
A.7 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	A 7.1 ANTES DE LA CONTRATACIÓN	A 7.1.1 INVESTIGACIÓN DE ANTECEDENTES / SELECCIÓN	SI	La organización buscará los medios de información necesarios para revisar el perfil profesional y antecedentes del personal que se requiera, esto para cualquier área de la organización. Por lo comentado, es importante implementar controles basándose en los reglamentos, la ética y las leyes pertinentes, que aseguren un proceso de verificación de antecedentes, asignación de roles y responsabilidades, términos de contratación y condiciones laborales previo acceso a la información propia de la organización.
		A 7.1.2 TÉRMINOS Y CONDICIONES DE CONTRATACIÓN	SI	

CLÁUSULA	OBJETIVOS DE CONTROL	CONTROLES	APLICABILIDAD	JUSTIFICACIÓN
	A 7.2 DURANTE LA CONTRATACIÓN	A 7.2.1 RESPONSABILIDADES DE LA DIRECCIÓN / RESPONSABILIDADES DE GESTIÓN	NO	No contemplado para la organización
		A 7.2.2 CONCIENTIZACIÓN, EDUCACIÓN Y CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN.	SI	El personal de la organización en el desarrollo de las actividades para las cuales fueron contratados interactúa permanentemente con la información, ya sea interna o externa. Por ello, es necesario establecer controles para asegurar que son conscientes de los riesgos. Asimismo, definir las responsabilidades y deberes con respecto a seguridad de la información. Por otro lado, es necesario capacitar y concientizar al personal permanentemente en temas de seguridad de la información según sea pertinente para sus funciones laborales.
		A.7.2.3 PROCESO DISCIPLINARIO	SI	La organización debe establecer un proceso disciplinario que permita a la organización saber cómo actuar en caso de que los colaboradores / trabajadores cometan alguna violación de la seguridad. Sin embargo, para evitar al máximo que se presente incidentes la organización, mediante los mecanismos que crea conveniente, exigirá a los colaboradores el cumplimiento de las políticas y procedimientos establecidos.

CLÁUSULA	OBJETIVOS DE CONTROL	CONTROLES	APLICABILIDAD	JUSTIFICACIÓN
	A 7.3 CESE O CAMBIO DE PUESTO DE TRABAJO	A7.3.1 CESE O CAMBIO DE PUESTO DE TRABAJO	SI	La organización establece la duración del vínculo laboral con el trabajador de la misma, la cual comprende un inicio y fin. Por ello, es necesario establecer controles que permitan asegurar la devolución de los activos de la organización y el retiro o cambio de los derechos de acceso cuando se presentan renunciaciones, terminaciones o cambios de la contratación del personal que conforman los diferentes proyectos o áreas transversales de la organización.
A.8 GESTION DE ACTIVOS	A 8.1 RESPONSABILIDAD SOBRE LOS ACTIVOS	A 8.1.1 INVENTARIO DE ACTIVOS	SI	La organización dentro del proceso de implementación y mantenimiento del SGSI debe realizar un inventario de todos los activos de información asociado al proceso en estudio. Por ello, es importante identificar los propietarios de estos activos, realizar un inventario de los más importantes y garantizar el uso adecuado de los mismos a través de reglas documentadas e implementadas.
		A 8.1.2 PROPIEDAD DE LOS ACTIVOS	SI	
		A 8.1.3 USO ACEPTABLE DE LOS ACTIVOS	SI	
		A 8.1.4 DEVOLUCIÓN DE LOS ACTIVOS	SI	Los activos de la organización deberán ser devueltos por los colaboradores al finalizar el vínculo laboral. La organización deberá asegurar la devolución de los activos cuando se presentan renunciaciones, terminaciones o cambios de la contratación del personal que conforman la planilla de la misma.
	A 8.2 CLASIFICACIÓN DE LA INFORMACIÓN	A 8.2.1 DIRECTRICES DE LA CLASIFICACIÓN	SI	La organización cuenta información de diferentes tipos importancia y protección. Por lo comentado, se deben implementar controles y procedimientos que permitan dar a la información de la organización el nivel adecuado de protección y manejo con base en la clasificación de información que se utilice, tomando en cuenta su valor, los requisitos legales,
		A 8.2.2 ETIQUETADO Y MANIPULADO DE LA INFORMACIÓN	SI	

CLÁUSULA	OBJETIVOS DE CONTROL	CONTROLES	APLICABILIDAD	JUSTIFICACIÓN
	A 8.3 MANEJO DE LOS SOPORTES DE ALMACENAMIENTO	A 8.2.3 MANIPULACIÓN / MANEJO DE ACTIVOS	SI	confidencialidad y la importancia para la misma.
		A 8.3.1. GESTIÓN DE MEDIOS / SOPORTES EXTRAIBLES	NO	No contemplado para la organización
		A 8.3.2 DISPOSICIÓN DE LOS MEDIOS / ELIMINACIÓN DE SOPORTES	NO	No contemplado para la organización
		A 8.3.3 SOPORTES FISICOS EN TRÁNSITO / TRANSFERENCIA DE MEDIOS FÍSICOS	SI	Para el desarrollo de las actividades de consultoría, auditoría, atención de servicios a clientes en general y el propio traslado de equipos de cómputo de los colaboradores la organización debe establecer controles para asegurar que se eviten eventos no deseados como divulgación, modificación, retiro o destrucción o robo del activo o la propia información embebida en el mismo.
A.9 CONTROL DE ACCESOS	A 9.1 REQUISITOS DEL NEGOCIO PARA CONTROL DE ACCESO	A 9.1.1 POLÍTICA DE CONTROL DE ACCESOS	SI	La organización debe establecer una Política de Control de Acceso que controle el acceso y seguridad de los recursos brindados por la organización, los cuales hacen consumo los colaboradores de la misma. Asimismo, los colaboradores deben consumir estos recursos de manera consciente y adecuada, accediendo solo a la información a las cuales tienen privilegios o permisos.

CLÁUSULA	OBJETIVOS DE CONTROL	CONTROLES	APLICABILIDAD	JUSTIFICACIÓN
	A 9.2 GESTIÓN DE ACCESO DE USUARIOS	A 9.1.2 CONTROL DE ACCESO A LAS REDES Y SERVICIOS ASOCIADOS	SI	La organización para su operación cuenta con una red que soporta las actividades de los diferentes usuarios. Asimismo, es crucial tener un control centralizado de los derechos para navegación a los distintos sitios de la Internet, mediante la creación de políticas de navegación. Por lo tanto, es necesario establecer controles de seguridad para asegurar que los usuarios solo tienen acceso a los servicios para los cuales están autorizados.
		A 9.2.1 GESTIÓN DE ALTAS / BAJAS EN EL REGISTRO DE USUARIOS	SI	Es muy importante gestionar de forma adecuada el acceso de los usuarios de acuerdo al área o proyecto en el cual se encuentra involucrados, o específicamente a la información a la cual deba hacer uso para el cumplimiento de sus funciones. Por ello, es importante establecer controles que aseguren el acceso de usuarios autorizados, así como evitar el acceso de usuarios no autorizados a información fuera de su área, proyecto o a la cual no deba tener acceso.
		A 9.2.2 GESTIÓN DE LOS DERECHOS DE ACCESO ASIGNADOS A USUARIOS	SI	
		A 9.2.3 GESTIÓN DE LOS DERECHOS DE ACCESOS CON PRIVILEGIOS ESPECIALES	SI	
		A 9.2.4 GESTIÓN DE INFORMACIÓN CONFIDENCIAL DE AUTENTIFICACIÓN DE USUARIOS	SI	
		A 9.2.5 REVISIÓN DE LOS DERECHOS DE ACCESO DE LOS USUARIOS	SI	

CLÁUSULA	OBJETIVOS DE CONTROL	CONTROLES	APLICABILIDAD	JUSTIFICACIÓN
	A 9.3 RESPONSABILIDADES DEL USUARIO	A 9.2.6 RETIRADA O ADAPTACIÓN DE LOS DERECHOS DE ACCESO	SI	
		A 9.3.1 USO DE INFORMACIÓN CONFIDENCIAL PARA LA AUTENTICACIÓN	SI	La organización debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.
	A 9.4 CONTROL DE ACCESO A SISTEMAS Y APLICACIONES	A 9.4.1 RESTRICCIÓN DEL ACCESO A LA INFORMACIÓN	SI	El personal de la institución maneja un usuario único e intransferible para acceder a los servicios de red y los propios recursos de información de la organización. El control de vigencia de contraseñas y todo lo relacionado al control de acceso se encuentra estipulado en la Política de Control de Acceso de la organización.
		A 9.4.2 PROCEDIMIENTOS SEGUROS DE INICIO DE SESIÓN	SI	
		A 9.4.3 GESTIÓN DE CONTRASEÑAS DE USUARIOS	SI	
		A 9.4.4 USO DE HERRAMIENTAS / PROGRAMAS DE ADMINISTRACIÓN DE SISTEMAS	NO	No contemplado para la organización
		A 9.4.5 CONTROL DE ACCESO AL CÓDIGO FUENTE DE LOS PROGRAMAS	NO	No contemplado para la organización
A.10 CIFRADO / CRIPTOGRAFIA	A 10.1 CONTROLES CRIPTOGRAFICOS	A 10.1.1 POLÍTICA DE USO DE CONTROLES CRIPTOGRÁFICOS	NO	No contemplado para la organización

CLÁUSULA	OBJETIVOS DE CONTROL	CONTROLES	APLICABILIDAD	JUSTIFICACIÓN
		A 10.1.2 GESTIÓN DE CLAVES	NO	No contemplado para la organización
A. 11 SEGURIDAD FÍSICA Y AMBIENTAL	A 11.1 ÁREAS SEGURAS	A 11.1.1 PERÍMETRO DE SEGURIDAD FÍSICA	SI	La organización para el desarrollo de sus actividades cuenta con una infraestructura física donde se encuentran los activos de información. Por ello, es importante establecer los controles de seguridad para evitar el acceso físico no autorizado, el daño a la infraestructura y los propios activos de información.
		A 11.1.2 CONTROLES FÍSICOS DE ENTRADA	SI	
		A 11.1.3 SEGURIDAD DE OFICINAS, DESPACHOS Y RECURSOS	SI	
		A 11.1.4 PROTECCIÓN CONTRA LAS AMENAZAS EXTERNAS Y AMBIENTALES	NO	No contemplado para la organización
		A 11.1.5 EL TRABAJO EN ÁREAS SEGURAS	NO	No contemplado para la organización
		A 11.1.6 ÁREAS DE ACCESO PÚBLICO, CARGA Y DESCARGA	NO	No contemplado para la organización
	A 11.2 SEGURIDAD DE LOS EQUIPOS	A 11.2.1 EMPLAZAMIENTO / UBICACIÓN Y PROTECCION DE LOS EQUIPOS	SI	Para el desarrollo de las actividades propias del negocio de la organización la misma utiliza equipos tales como: Servidores, computadores de escritorio, portátiles, equipos que soportan la Infraestructura de Comunicaciones, entre otros medios o dispositivos electrónicos. En estos equipos se procesa la información de la organización por tal razón es necesario establecer controles que permitan evitar la ocurrencia de eventos como pérdida, daño, robo o interrupción de los equipos tanto dentro como fuera de la misma.
		A 11.2.2 INSTALACIONES DE SUMINSITRO	SI	
		A 11.2.3 SEGURIDAD DEL CABLEADO	SI	
		A 11.2.4 MANTENIMIENTO DE LOS	SI	

CLÁUSULA	OBJETIVOS DE CONTROL	CONTROLES	APLICABILIDAD	JUSTIFICACIÓN
		EQUIPOS		
		A 11.2.5 SALIDA DE ACTIVOS FUERA DE LAS DEPENDENCIAS DE LA EMPRESA	SI	
		A 11.2.6 SEGURIDAD DE LOS EQUIPOS Y ACTIVOS FUERA DE LAS INSTALACIONES	SI	
		A 11.2.7 REUTILIZACIÓN O RETIRADA SEGURA DE DISPOSITIVOS DE ALMACENAMIENTO	NO	No contemplado para la organización
		A 11.2.8 EQUIPO INFORMÁTICO DE USUARIO DESATENDIDO	SI	El personal de la organización es responsable de los activos de información que se encuentran a su cargo, así como de la protección de los mismos en cuanto a confidencialidad, integridad y disponibilidad. Por ello, se han definido responsabilidades claras en la Política de Control de Acceso y en la Política de Puesto de Trabajo despejado y Bloqueo de Pantalla, ello para evitar el acceso de usuarios no autorizados y el robo de información.
		A 11.2.9 POLÍTICA DE PUESTO DE TRABAJO DESPEJADO Y BLOQUEO DE PANTALLA	SI	
A.12 SEGURIDAD DE LAS OPERACIONES	A 12.1 RESPONSABILIDADES Y PROCEDIMIENTOS DE OPERACIÓN	A 12.1.1 DOCUMENTACIÓN DE PROCEDIMIENTOS DE OPERACIÓN	SI	La organización para el desarrollo de sus actividades de negocio utiliza herramientas ofimáticas y tecnológicas, con las cuales interactúan permanentemente el personal a través de los equipos asignados. Por ello, es necesario establecer controles de seguridad

CLÁUSULA	OBJETIVOS DE CONTROL	CONTROLES	APLICABILIDAD	JUSTIFICACIÓN
		A 12.1.2 GESTIÓN DE CAMBIOS	SI	que garanticen que todos los cambios se controlan, se revisan y se someten a pruebas para no comprometer la seguridad del sistema ni el entorno operativo. Asimismo, evitar así una posible o inminente fuga de información.
		A 12.1.3 GESTIÓN DE CAPACIDAD	SI	
		A 12.1.4 SEPARACION DE ENTORNOS DE DESARROLLO, PRUEBA Y PRODUCCIÓN	NO	No contemplado para la organización
	A 12.2 PROTECCION CONTRA CÓDIGO MALICIOSO	A.12.2.1 CONTROLES CONTRA EL CÓDIGO MALICIOSO	SI	Para el desarrollo de las actividades de la organización se utilizan servicios como Internet, medios extraíbles, los cuales pueden afectar el correcto funcionamiento de activos de información como equipos, software entre otros. Por lo comentado, es importante establecer controles de seguridad que permitan la detección y prevención de la acción de códigos maliciosos. Asimismo, procedimientos de concientización de los usuarios.
	A 12.3 COPIAS DE SEGURIDAD	A 12.3.1 COPIAS DE SEGURIDAD DE LA INFORMACIÓN	SI	La información de la organización se encuentra ubicada en los equipos asignados a los colaboradores, como también en el servidor de archivos. Por ello, es importante establecer controles de seguridad que respalden la ejecución de procedimientos de backup y recuperación que permitan restaurar en el menor tiempo posible la información ante la materialización de un riesgo. Con ello se logrará la continuidad del negocio, no creando perjuicios a la operatividad de la organización.

CLÁUSULA	OBJETIVOS DE CONTROL	CONTROLES	APLICABILIDAD	JUSTIFICACIÓN
	A 12.4 REGISTRO Y SEGUIMIENTO	A12.4.1 REGISTRO Y GESTIÓN DE EVENTOS DE ACTIVIDAD	SI	La institución para el desarrollo de sus actividades cuenta con colaboradores / trabajadores que tienen acceso a los diferentes activos de información para la ejecución de sus actividades. Por ello, es importante establecer controles de seguridad que permitan la detección oportuna de actividades de procesamiento de información no autorizadas y herramientas para investigaciones futuras de incidentes de seguridad de la información.
		A12.4.2 PROTECCIÓN DE LOS REGISTROS DE INFORMACIÓN	SI	
		A12.4.3 REGISTROS DE ACTIVIDAD DEL ADMINISTRADOR Y OPERADOR DEL SISTEMA	NO	No contemplado para la organización
		A12.4.4 SINCRONIZACIÓN DE RELOJES	NO	No contemplado para la organización
	A 12.5 CONTROL DE SOFTWARE OPERACIONAL	A 12.5.1 INSTALACIÓN DEL SOFTWARE EN SISTEMAS EN PRODUCCIÓN	NO	No contemplado para la organización
	A 12.6 GESTION DE LA VULNERABILIDAD TÉCNICA	A 12.6.1 GESTIÓN DE LAS VULNERABILIDADES TÉCNICAS	NO	No contemplado para la organización
		A 12.6.2 RESTRICCIONES EN LA INSTALACIÓN DE SOFTWARE	NO	No contemplado para la organización
	A 12.7 CONSIDERACIONES DE LAS AUDITORIAS DE LOS SISTEMAS DE INFORMACIÓN	A 12.7.1 CONTROLES DE AUDITORIAS DE LOS SISTEMAS DE INFORMACIÓN	NO	No contemplado para la organización

CLÁUSULA	OBJETIVOS DE CONTROL	CONTROLES	APLICABILIDAD	JUSTIFICACIÓN
A. 13 SEGURIDAD EN LAS TELECOMUNICACIONES	A 13.1 GESTIÓN DE LA SEGURIDAD EN LAS REDES	A 13.1.1 CONTROLES DE RED	SI	La organización para el desarrollo de sus actividades de negocio cuenta con una red sobre la que se desarrollan todas las aplicaciones ejecutadas por los usuarios. En base a ello, es importante establecer controles de seguridad para asegurar la información en la red, protegerla de amenazas y garantizar la infraestructura de comunicaciones.
		A 13.1.2 MECANISMOS DE SEGURIDAD ASOCIADOS A SERVICIOS EN RED	SI	
		A 13.1.3 SEGREGACIÓN DE REDES	NO	No contemplado para la organización
	A 13.2 INTERCAMBIO / TRANSFERENCIA DE INFORMACIÓN CON PARTES EXTERNAS	A 13.2.1 POLÍTICAS Y PROCEDIMIENTOS DE INTERCAMBIO DE INFORMACIÓN	SI	Dentro del desarrollo normal de las actividades de la organización se presentan actividades de intercambio de información con clientes, colaboradores, entre otros como parte del desarrollo de los proyectos. Por ello, es importante establecer controles de seguridad para asegurar que se cumplen las políticas y procedimientos de la empresa para el intercambio de información y para garantizar que no se presente un uso inadecuado o corrupción cuando la información sale fuera de las instalaciones de la organización.
		A 13.2.2 ACUERDOS SOBRE INTERCAMBIO DE INFORMACIÓN	SI	
		A 13.2.3 MENSAJERIA ELECTRÓNICA	SI	

CLÁUSULA	OBJETIVOS DE CONTROL	CONTROLES	APLICABILIDAD	JUSTIFICACIÓN
		A 13.2.4 ACUERDOS DE CONFIDENCIALIDAD O DE NO DIVULGACIÓN (SECRETO)	SI	La organización mediante su política de seguridad de la información establece su compromiso, organización y asignación de responsabilidades para su cumplimiento. Asimismo, de igual forma vela por mantener protegido sus activos de información mediante la revisión del sistema de gestión de seguridad de la información, la firma de los acuerdos de confidencialidad, manteniendo contacto con las autoridades, con grupos de interés especiales y la revisión independiente de seguridad de la información.
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	A 14.1 REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN	A 14.1.1 ÁNÁLISIS Y ESPECIFICACIÓN DE LOS REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN	NO	No contemplado para la organización
		A 14.1.2 SEGURIDAD DE LAS COMUNICACIONES EN SERVICIOS ACCESIBLES POR REDES PÚBLICAS	NO	No contemplado para la organización
		A 14.1.3 PROTECCIÓN DE LAS TRANSACCIONES POR REDES TELEMÁTICAS	NO	No contemplado para la organización
	A 14.2 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y	A 14.2.1 POLÍTICA DE DESARROLLO SEGURO DE SOFTWARE	NO	No contemplado para la organización

CLÁUSULA	OBJETIVOS DE CONTROL	CONTROLES	APLICABILIDAD	JUSTIFICACIÓN
	SOPORTE	A 14.2.2 PROCEDIMIENTO DE CONTROL DE CAMBIOS EN LOS SISTEMAS	NO	No contemplado para la organización
		A 14.2.3 REVISIÓN TÉCNICAS DE LAS APLICACIONES TRAS EFECTUAR CAMBIOS EN EL SISTEMA OPERATIVO	NO	No contemplado para la organización
		A 14.2.4 RESTRICCIONES A LOS CAMBIOS EN LOS PAQUETES DE SOFTWARE	NO	No contemplado para la organización
		A 14.2.5 USO DE PRINCIPIOS DE INGENIERÍA EN PROTECCIÓN DE SISTEMAS	NO	No contemplado para la organización
		A 14.2.6 SEGURIDAD EN ENTORNOS DE DESARROLLO	NO	No contemplado para la organización
		A 14.2.7 EXTERNALIZACIÓN DEL DESARROLLO DE SOFTWARE	NO	No contemplado para la organización
		A 14.2.8 PRUEBAS DE FUNCIONALIDAD DURANTE EL DESARROLLO DE LOS SISTEMAS	NO	No contemplado para la organización
		A 14.2.9 PRUEBAS DE ACEPTACIÓN DE SISTEMAS	NO	No contemplado para la organización

CLÁUSULA	OBJETIVOS DE CONTROL	CONTROLES	APLICABILIDAD	JUSTIFICACIÓN
	A 14.3 DATOS DE PRUEBA	A14.3.1 PROTECCIÓN DE LOS DATOS UTILIZADOS EN PRUEBAS	NO	No contemplado para la organización
A.15 RELACIONES CON LOS PROVEEDORES / SUMINISTRADORES	A. 15.1 SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES / SUMINISTRADORES	A 15.1.1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA PROVEEDORES / SUMINISTRADORES	NO	No contemplado para la organización
		A 15.1.2 TRATAMIENTO DEL RIESGO DENTRO DE LOS ACUERDOS CON PROVEEDORES / SUMINISTRADORES	NO	No contemplado para la organización
		A 15.1.3 CADENA DE SUMINISTRO EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES	SI	La organización requiere para la ejecución de sus proyectos "Llave en mano" alianzas con terceros y proveedores alternos. Para ello, la organización debe exigir el cumplimiento de las buenas prácticas y cumplimiento de las políticas de la organización para su desarrollo. Cabe indicar que el proveedor de algún servicio brindado a la institución debe cumplir cabalmente los niveles de servicio indicados en el SLA.
	A. 15.12 GESTIÓN DE LA PRESTACIÓN DEL SERVICIO POR PROVEEDORES / SUMINISTRADORES	A 15.2.1 SUPERVISIÓN Y REVISIÓN DE LOS SERVICIOS PRESTADOS POR TERCEROS (PROVEEDORES / SUMINISTRADORES)	NO	No contemplado para la organización

CLÁUSULA	OBJETIVOS DE CONTROL	CONTROLES	APLICABILIDAD	JUSTIFICACIÓN
		A 15.2.2 GESTIÓN DE CAMBIOS EN LOS SERVICIOS PRESTADOS POR TERCEROS (PROVEEDORES / SUMINISTRADORES)	NO	No contemplado para la organización
A.16 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION	A 16.1 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y MEJORAS	A 16.1.1 RESPONSABILIDADES Y PROCEDIMIENTOS	NO	No contemplado para la organización
		A 16.1.2 NOTIFICACIÓN DE LOS DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN	SI	La organización cuenta con 11 activos de información a los que se les ha realizado su respectivo análisis, evaluación y tratamiento de los riesgos. Aquellos pueden ser objeto de incidentes de seguridad de la información, por lo cual es importante establecer controles que aseguren que los eventos y debilidades de seguridad de la información son comunicados oportunamente a través de los canales de gestión apropiados al área de seguridad de la información para su respectiva gestión tan pronto como sea posible.
		A 16.1.3 NOTIFICACIÓN DE DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN	SI	
		A 16.1.4 VALORACIÓN DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN Y TOMA DE DECISIONES	NO	No contemplado para la organización
		A 16.1.5 RESPUESTA A LOS INCIDENTES DE SEGUIRIDAD DE LA INFORMACIÓN	SI	La organización debe contemplar la adopción de sistemas de respuesta a incidentes sobre los activos de información, así llevar un resguardo y control sobre los mismos.

CLÁUSULA	OBJETIVOS DE CONTROL	CONTROLES	APLICABILIDAD	JUSTIFICACIÓN
		A 16.1.6 APRENDIZAJE DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	NO	No contemplado para la organización
		A 16.1.7 RECOPIACIÓN DE EVIDENCIAS	NO	No contemplado para la organización
A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO	A 17.1 CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN	A 17.1.1 PLANIFICACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	SI	La organización debe contemplar proponer y adoptar un Plan de Recuperación antes Desastre (PRD o DRP) y evaluar los sistemas y recursos más críticos en la organización, para evaluar su despliegue en un Site Alternativo, Data Center Alternativo o mediante un servicio de Cloud Computing (IaaS, SaaS, PaaS u otro que sea necesario).
		A 17.1.2 IMPLANTACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	SI	
		A 17.1.3 VERIFICACIÓN, REVISIÓN Y EVALUACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	NO	No contemplado para la organización

CLÁUSULA	OBJETIVOS DE CONTROL	CONTROLES	APLICABILIDAD	JUSTIFICACIÓN
	A 17.2 REDUNDANCIAS	A 17.2.1 DISPONIBILIDAD DE INSTALACIONES DE PROCESAMIENTO DE INFORMACIÓN	SI	La organización debe evaluar servicios críticos, los cuales se deban implementar con redundancia suficiente para cumplir los requisitos de disponibilidad. Este apartado debe estar incluido dentro del Plan de Recuperación de Desastre (DRP) propuesto y adoptado posteriormente por la propia organización.
A. 18 CUMPLIMIENTO	A 18.1 CUMPLIMIENTO DE LOS REQUISITOS LEGALES Y CONTRACTUALES	A 18.1.1 IDENTIFICACIÓN DE LA LEGISLACIÓN APLICABLE Y DE LOS REQUISITOS CONTRACTUALES.	NO	No contemplado para la organización
		A 18.1.2 DERECHOS DE PROPIEDAD INTELECTUAL (DPI)	NO	No contemplado para la organización
		A 18.1.3 PROTECCIÓN DE LOS REGISTROS DE LA ORGANIZACIÓN	SI	Los registros de uso, manipulación, extracción, verificación y toda acción que sea reflejada en el uso de la información embebida en los activos de información valorizados se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada. Lo comentado, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.

CLÁUSULA	OBJETIVOS DE CONTROL	CONTROLES	APLICABILIDAD	JUSTIFICACIÓN
		A 18.1.4 PROTECCIÓN DE DATOS Y PRIVACIDAD DE LA INFORMACIÓN PERSONAL	SI	Se deben asegurar la privacidad y la protección de la información de datos personales de clientes de la organización, en el flujo de intercambio de información del propio activo de información asociado. Este aseguramiento de la privacidad y protección de datos es tal como se exige en la Ley de Protección de Datos Personales, en cuanto a la clasificación de Banco de Datos.
		A 18.1.5 REGULACIÓN DE LOS CONTROLES CRIPTOGRÁFICOS	NO	No contemplado para la organización
	A 18.2 REVISIONES DE LA SEGURIDAD DE LA INFORMACIÓN	A 18.2.1 REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN	NO	No contemplado para la organización
		A 18.2.2 CUMPLIMIENTO DE LAS POLÍTICAS Y NORMAS DE SEGURIDAD	SI	El personal colaborador de la organización interactúa permanentemente con los activos de información, Para ello, se han diseñado políticas y controles en materia de seguridad de la información, que establezcan controles de seguridad que garanticen que todo el personal de la misma conoce y aplica las políticas de seguridad de la información y los respectivos controles.
		A 18.2.3 COMPROBACIÓN DEL CUMPLIMIENTO	NO	No contemplado para la organización

ANEXO VII: Controles Técnicos Auxiliares

ITEM	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR
TA 1	TA 1. EJECUCIÓN DE PROCEDIMIENTOS PARA EL USO DE CONTRASEÑAS FUERTES	Técnico Auxiliar	Ejecutar procedimientos técnicos para evitar el Espionaje de contraseñas, ataques de contraseñas o métodos de cracking. El procedimiento es indicado dentro de la Política de Control de Acceso, en el apartado "Gestión de Contraseñas de Usuario", propuesto en el presente proyecto.
TA 2	TA 2. LIMITAR EL NÚMERO DE ACCESO A CONTRASEÑAS INVALIDAS	Técnico Auxiliar	Ejecutar procedimientos técnicos para evitar el Espionaje de contraseñas, ataques de contraseñas o métodos de cracking. El procedimiento es indicado dentro de la Política de Control de Acceso, en el apartado "Gestión de Contraseñas de Usuario", propuesto en el presente proyecto.
TA 3	TA 3. IMPLEMENTACIÓN DE SOFTWARE DE MONITOREO DE ESTADO DE SALUD Y RENDIMIENTO DE LA APLICACIÓN	Técnico Auxiliar	La organización debe adquirir un software de monitoreo para la revisión de logs y recursos del sistema. Asimismo, este software permitirá evaluar el rendimiento de la aplicación mediante parámetros técnicos asociadas a su estructura.
TA 4	TA 4. IMPLEMENTACIÓN DE UN DATA LOSS PREVENTION (DLP)	Técnico Auxiliar	La organización debe contemplar la adopción de una solución de DLP (Data Loss Prevention) para la clasificación de Información y manejo adecuado de la misma dentro y fuera de la organización, ello en cumplimiento de las reglas o directrices indicadas por la misma.

ITEM	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR
TA 5	TA 5. MIGRACIÓN DEL SISTEMA DE GESTIÓN DE TICKETS EN UN SERVICIO EN LA NUBE MEDIANTE IAAS	Técnico Auxiliar	La organización debe contemplar la aplicación y ejecución de uno de los modelos de Cloud Computing, es decir Infraestructura como Servicio (IaaS) y llevar el Servicio del Sistema de Gestión de Tickets a la nube, evitando gastos de capital y reduciendo los costos corrientes (energía, aire acondicionado, otros), por un pago mensual o anual según convenga.
TA 6	TA 6. MIGRACIÓN DE COPIAS LEGALIZADAS A PROVEEDOR DE CUSTODÍA DE ARCHIVOS	Técnico Auxiliar	La organización deberá tener en cuenta realizar copias físicas y digitales de contratos y/o archivos asociados a los Contratos de Servicios, Instalación, entre otros en custodia de un proveedor tercero, tal como: Hermes, Prosegur, entre otros que se encuentren disponibles en el mercado.
TA 7	TA 7. IMPLEMENTACIÓN DE SOFTWARE DE AUDITORIA DE USO DE DATOS DE CARPETA DE PROYECTOS	Técnico Auxiliar	La organización debe considerar la adopción de un software de auditoria de uso de los datos contenidos dentro de la carpeta de proyectos. Esto incluye: uso, acceso, horario de acceso, entre otros datos relevantes para la auditoria.
TA 8	TA 8. MIGRACIÓN DE LA CARPETA DE PROYECTOS BAJO UN SERVICIO EN LA NUBE MEDIANTE IAAS	Técnico Auxiliar	La organización debe contemplar la aplicación y ejecución de uno de los modelos de Cloud Computing, es decir Infraestructura como Servicio (IaaS) y llevar el servidor FTP que contiene la Carpeta de Proyectos Servicio a la nube, evitando gastos de capital y reduciendo los costos corrientes (energía, aire acondicionado, otros), por un pago mensual o anual según convenga.

ITEM	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR
TA 9	TA 9. DESPLIEGUE DE UNA SOLUCIÓN DE REPOSITORIO EN LA NUBE DE ACCESO ESPECIFICO	Técnico Auxiliar	La organización debe contemplar una solución en donde pueda pasar los datos de la Carpeta de Proyectos a un repositorio en la nube y en ello categorizar su acceso mediante alternativas de acceso: confidencial, privada y pública de usuarios de la organización, para accesos dentro y fuera de la organización. Estas soluciones pueden ser tipo: Check Point Workspace u otras soluciones como CASB (Cloud Access Security Broker) para aplicaciones o recursos publicados propietarios.
TA 10	TA 10. IMPLEMENTACIÓN DE SOFTWARE DE AUDITORIA DE USO DE DATOS DE CARPETA DE LICITACIONES	Técnico Auxiliar	La organización debe considerar la adopción de un software de auditoria de uso de los datos contenidos dentro de la carpeta de licitaciones. Esto incluye: uso, acceso, horario de acceso, entre otros datos relevantes para la auditoria.
TA 11	TA 11. MIGRACIÓN DE LA CARPETA DE LICITACIONES BAJO UN SERVICIO EN LA NUBE MEDIANTE IAAS	Técnico Auxiliar	La organización debe contemplar la aplicación y ejecución de uno de los modelos de Cloud Computing, es decir Infraestructura como Servicio (IaaS) y llevar el servidor FTP que contiene la Carpeta de Licitaciones a la nube, evitando gastos de capital y reduciendo los costos corrientes (energía, aire acondicionado, otros), por un pago mensual o anual según convenga.
TA 12	TA 12. IMPLEMENTACIÓN DE SOFTWARE DE AUDITORIA DE USO DE DATOS DE CARPETAS DE ÁREAS ADMINISTRATIVAS Y CONTABILIDAD	Técnico Auxiliar	La organización debe considerar la adopción de un software de auditoria de uso de los datos contenidos dentro de la Carpetas de Áreas Administrativas y Contabilidad. Esto incluye: uso, acceso, horario de acceso, entre otros datos relevantes para la auditoria.

ITEM	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR
TA 13	TA 13. MIGRACIÓN DE LA CARPETAS DE ÁREAS ADMINISTRATIVAS Y CONTABILIDAD BAJO UN SERVICIO EN LA NUBE MEDIANTE IAAS	Técnico Auxiliar	La organización debe contemplar la aplicación y ejecución de uno de los modelos de Cloud Computing, es decir Infraestructura como Servicio (IaaS) y llevar el servidor FTP que contiene la Carpetas de Áreas Administrativas y Contabilidad a la nube, evitando gastos de capital y reduciendo los costos corrientes (energía, aire acondicionado, otros), por un pago mensual o anual según convenga.
TA 14	TA 14. INGRESO LÓGICO DE CADA EQUIPO DE COMPUTO POR MEDIO DEL DIRECTORIO ACTIVO	Técnico Auxiliar	Cada equipo de cómputo deberá ser unido al dominio de la organización vía el soporte del Active Directory. Ello para contar con una administración de despliegue de política de seguridad, despliegue de paquetes de actualización, accesos a carpetas de archivos seleccionados y otras funcionalidades de manera centralizada.
TA 15	TA 15. IMPLEMENTACIÓN DE UNA SUITE O SOLUCIÓN DE ENDPOINT PARA PREVENIR ATAQUES DE FIRMAS COMUNES Y DE DÍA CERO	Técnico Auxiliar	La organización debe implementar una suite o solución de Endpoint para la protección y prevención contra ataques comunes y ataques de Día Cero (Zero Days). Esta solución deberá contar con módulos de seguridad como: AV, Antibot, IPS, Antimalware (prevención y protección contra ataques de día cero) y otros Blades o módulos de seguridad embebidos.

ITEM	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR
TA 16	TA 16. IMPLEMENTACIÓN DE UNA SOLUCIÓN DE RESPALDO DE ENPOINT O ESTACIONES DE TRABAJO Y/O SERVIDORES	Técnico Auxiliar	La organización debe considerar la implementación de una solución de respaldo de estaciones finales de trabajo o Endpoint, esto mediante un agente instalado en el computador, apuntando el respaldo a un Storage local o en nube: Soluciones como Barracuda Backup, Veeam Backup, Veritas, entre otras. Todas las PC's asociadas a la plana de Gerentes, Jefes y usuarios finales deben tener un respaldo del contenido del computador sin excepción, esto para fines de recuperación y auditoria.
TA 17	TA 17. IMPLEMENTACIÓN DE UN SERVIDOR CENTRALIZADO PARA INSTALACIÓN DE PARCHES DE SEGURIDAD	Técnico Auxiliar	La organización debe implementar un servidor centralizado para la instalación de parches de seguridad, esto programado de manera automática o ejecutada de manera manual. Con ello, evitar o disminuir fallas de seguridad asociadas a versiones de Sistema Operativos, específicamente Windows (Servidor centralizado WSUS) debido a que es el Sistema Operativo utilizado en la organización.
TA 18	TA 18. IMPLEMENTACIÓN DE UNA SOLUCIÓN DE ENDPOINT ENCRYPTION	Técnico Auxiliar	La organización debe contemplar implementar una solución de Endpoint Encryption (Encriptación de Endpoint o dispositivos finales) la cual ofrezca cifrado eficaz de disco completo y soportes extraíbles. Lo comentado mediante una administración centralizada para proteger la información confidencial y asegurar el cumplimiento normativo dentro de la organización.

ITEM	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR
TA 19	TA 19. ALQUILER DE EQUIPOS DE CÓMPUTO	Técnico Auxiliar	La organización debe evaluar el alquiler de equipos de cómputo para transferir el riesgo de pérdida del equipo (80% aproximado en laptop, 20% aproximado en PC de escritorio), inoperatividad o fallas en su funcionamiento. Asimismo, los acuerdos con la empresa que alquila los equipos deben cubrir cambio ante fallas, pérdidas (seguro o póliza que aplique), fallas en su funcionamiento, cambio de piezas o partes del computador, cambio por obsolescencia, entre otros acuerdos.
TA 20	TA 20. IMPLEMENTACIÓN DE SOFTWARE DE AUDITORIA DE USO DEL SERVICIO DE CORREO ELECTRÓNICO	Técnico Auxiliar	La organización debe considerar la adopción de un software de auditoria de uso o flujo de correos enviados y recibidos por los usuarios internos. Esto incluye: uso, acceso, envíos de correo, recepción de correos, horario de acceso, entre otros datos relevantes para la auditoria.
TA 21	TA 21. IMPLEMENTACIÓN DE UN SERVICIO O APPLIANCE DE ANTISPAM	Técnico Auxiliar	La organización debe considerar la adopción de un servicio o appliance dedicado para AntiSpam. Ello para el manejo de correos spam (basura o no deseados), así como también su uso para la protección contra código malicioso embebido dentro de los correos electrónicos, ya sea como adjunto, direccionamiento mediante un link de acceso, código malicioso incrustado dentro del cuerpo de correo, entre otras amenazas.
TA 22	TA 22. MIGRACIÓN DEL SERVICIO DE CORREO ELECTRÓNICO A LA NUBE MEDIANTE SAAS	Técnico Auxiliar	La organización debe contemplar la aplicación y ejecución de uno de los modelos de Cloud Computing, es decir el Software como Servicio (SaaS) y llevar el Servicio del Correo Electrónico a la nube, evitando gastos de capital y reduciendo los costos corrientes (energía, aire acondicionado, otros), por un pago mensual o anual según convenga.
TA 23	TA 23. IMPLEMENTACIÓN DE SOFTWARE DE MONITOREO DEL CONSUMO DE INTERNET	Técnico Auxiliar	La organización debe adquirir un software de monitoreo para la revisión y análisis del consumo de Internet. Con ello, revisar en base a los reportes, quienes son los destinos más concurridos y su categorización de seguridad. Con ello, ajustar los accesos y disminuir el riesgo de infección o ataques de día cero provenientes de destinos previamente identificados como malignos.

ITEM	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR
TA 24	TA 24. IMPLEMENTACIÓN DE SOFTWARE DE MONITOREO DEL CONSUMO DE INTERNET	Técnico Auxiliar	La organización debe adquirir un software de monitoreo para la revisión y análisis del consumo de Internet. Con ello, revisar en base a los reportes, quienes son los destinos más concurridos y su categorización de seguridad. Con ello, ajustar los accesos y disminuir el riesgo de infección o ataques de día cero provenientes de destinos previamente identificados como malignos.
TA 25	TA 25. IMPLEMENTACIÓN DE UNA SUITE O SOLUCIÓN PERIMETRAL PARA PREVENIR ATAQUES DE DÍA CERO	Técnico Auxiliar	La organización debe implementar una suite o solución de perimetral para la protección y prevención contra ataques de Día Cero (Zero Days). Esta solución deberá contar con módulos de seguridad de antimalware, ya sea en un despliegue de appliance físico o un análisis ejecutado en la nube del fabricante.
TA 26	TA 26. IMPLEMENTACIÓN DE SOFTWARE DE AUDITORIA DE USO DEL CONTENIDOS DE LOS EQUIPOS DE INFRAESTRUCTURA DE COMUNICACIONES	Técnico Auxiliar	La organización debe considerar la adopción de un software de auditoria de uso de los datos contenidos dentro de los equipos que componen la Infraestructura de Comunicaciones (Incluye servidores). Esto incluye: uso, acceso, horario de acceso, entre otros datos relevantes para la auditoria.
TA 27	TA 27. INGRESO LÓGICO DEL SERVIDOR DE ARCHIVOS POR MEDIO DEL DIRECTORIO ACTIVO	Técnico Auxiliar	El servidor de archivos deberá ser unido al dominio de la organización vía el soporte del Active Directory. Ello para contar con una administración de despliegue de política de seguridad, despliegue de paquetes de actualización, accesos a carpetas de archivos seleccionados y otras funcionalidades de manera centralizada.
TA 28	TA 28. MIGRACIÓN DEL SERVICIO DE FTP BAJO UN SERVICIO EN LA NUBE MEDIANTE IAAS	Técnico Auxiliar	La organización debe contemplar la aplicación y ejecución de uno de los modelos de Cloud Computing, es decir Infraestructura como Servicio (IaaS) y llevar el servidor FTP que contiene las distintas carpetas de datos con información de la organización a la nube, evitando gastos de capital y reduciendo los costos corrientes (energía, aire acondicionado, otros), por un pago mensual o anual según convenga.

ITEM	CONTROL	TIPO DE CONTROL	DESCRIPCIÓN / ACCIONES A TOMAR
TA 29	TA 29. INGRESO LÓGICO DEL SERVIDOR DE ARCHIVOS POR MEDIO DEL DIRECTORIO ACTIVO	Técnico Auxiliar	Los servidores que componen la Infraestructura de Comunicaciones deberán ser unidos al dominio de la organización vía el soporte del Active Directory. Ello para contar con una administración de despliegue de política de seguridad, despliegue de paquetes de actualización, accesos a carpetas de archivos seleccionados y otras funcionalidades de manera
TA 30	TA 30. EVALUACIÓN E IMPLEMENTACIÓN DE UN DATA CENTER ALTERNO	Técnico Auxiliar	La organización debe evaluar un Site Alterno o Data Center Alterno en el cual se pueda sostener la operación de los servicios más críticos que dan continuidad al negocio, esto ante alguna eventualidad de para de continuidad de labores, desastre natural, ataque cibernético o cualquier ataque que atente contra la continuidad del negocio.
TA 31	TA 31. ADOPCIÓN DE SISTEMA DE SIMULACIÓN DE EJECUCIÓN DE PHISING	Técnico Auxiliar	La organización debe adoptar un sistema de preparación contra Phising para evaluar a los empleados respecto a la que acciones tomar ante estas clases de ataques cibernéticos. Para ello, es necesario para establecer una línea base que permita implementar un programa eficaz de preparación contra el Phishing. Tomar como referencia el "Phishing Readiness Services" del fabricante Symantec.
TA 32	TA 32. PROGRAMAS DE INFORMACIÓN SOBRE TÉCNICAS DE ATAQUES DE INGENIERÍA SOCIAL	Técnico Auxiliar	La organización debe plantear programas de capacitación al personal de la empresa en donde se explique y detalle las técnicas de ataques de Ingeniería Social utilizadas por los delincuentes informáticos.

ANEXO VIII: Ejecución de Pruebas de Escritorio para Objetivo Especifico I

IDENTIFICACIÓN DEL ACTIVO		PRUEBAS DE ESCRITORIO	VALORACIÓN DEL ACTIVO						
No	Nombre del Activo	Integrantes	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	¿ IMPACTO	IMPACTO	INTERPRETACIÓN IMPACTO	IMPACTO RESULTANTE
1	Sistema de Gestión de Tickets	A	5	5	5	15	5	MUY ALTO	MUY ALTO
		B	5	5	5	15	5	MUY ALTO	
		C	5	5	5	15	5	MUY ALTO	
		D	5	5	5	15	5	MUY ALTO	
2	Contratos de Servicios, Instalación, entre otros	A	5	5	5	15	5	MUY ALTO	MUY ALTO
		B	5	5	5	15	5	MUY ALTO	
		C	4	4	4	12	4	ALTO	
		D	5	5	5	15	5	MUY ALTO	
3	Carpetas de proyectos	A	5	5	5	15	5	MUY ALTO	MUY ALTO
		B	5	5	5	15	5	MUY ALTO	
		C	5	5	5	15	5	MUY ALTO	
		D	4	5	5	14	5	MUY ALTO	
4	Carpeta de Licitaciones	A	5	5	5	15	5	MUY ALTO	MUY ALTO
		B	5	5	5	15	5	MUY ALTO	
		C	5	5	5	15	5	MUY ALTO	
		D	4	5	5	14	5	MUY ALTO	
5	Carpetas de Áreas Administrativas y Contabilidad	A	5	5	5	15	5	MUY ALTO	MUY ALTO
		B	5	5	5	15	5	MUY ALTO	
		C	5	5	5	15	5	MUY ALTO	
		D	5	5	5	15	5	MUY ALTO	
6	Equipos de Computo	A	4	4	4	12	4	ALTO	ALTO
		B	3	4	5	12	4	ALTO	
		C	5	5	3	13	5	MUY ALTO	
		D	4	4	3	11	4	ALTO	
7	Correo Electrónico	A	5	5	5	15	5	MUY ALTO	MUY ALTO
		B	5	5	5	15	5	MUY ALTO	
		C	5	5	5	15	5	MUY ALTO	
		D	5	4	4	13	5	MUY ALTO	
8	Internet / Servicios Dedicados	A	3	3	5	11	4	ALTO	ALTO
		B	4	4	4	12	4	ALTO	
		C	4	4	4	12	4	ALTO	
		D	4	4	3	11	4	ALTO	
9	Sistema de Gestión de movilidad	A	5	5	5	15	5	MUY ALTO	MEDIO
		B	1	1	4	6	2	BAJO	
		C	3	3	3	9	3	MEDIO	
		D	2	3	2	7	3	MEDIO	
10	File Server (Servidor de Archivos)	A	4	4	4	12	4	ALTO	MUY ALTO
		B	4	4	4	12	4	MUY ALTO	
		C	5	5	5	15	5	MUY ALTO	
		D	5	4	5	14	5	MUY ALTO	

IDENTIFICACIÓN DEL ACTIVO		PRUEBAS DE ESCRITORIO	VALORACIÓN DEL ACTIVO						
11	Infraestructura de Comunicaciones	A	5	4	4	13	5	MUY ALTO	MUY ALTO
		B	4	4	4	12	4	ALTO	
		C	5	5	5	15	5	MUY ALTO	
		D	5	4	4	13	5	MUY ALTO	
12	Personal	A	5	5	5	15	5	MUY ALTO	MUY ALTO
		B	5	5	5	15	5	MUY ALTO	
		C	5	5	5	15	5	MUY ALTO	
		D	5	4	4	13	5	MUY ALTO	
13	Imagen de la Organización	A	4	4	4	12	4	ALTO	MEDIO
		B	4	4	4	12	4	ALTO	
		C	2	2	2	6	2	BAJO	
		D	3	3	3	9	3	MEDIO	

ANEXO IX: Ejecución de Pruebas de Escritorio para Objetivo Específico II

RIESGOS			VULNERABILIDADES	AMENAZAS DETECTADAS							
				Falta de cierre de inicio de sesión en cada logueo realizado.	No existe definición de roles de usuarios. Es decir, el mismo usuario además de crear boletas de atención, puede observar módulos contables no autorizados, entre otros.	Servicios innecesarios para los usuarios que acceden al sistema.	Contraseñas de acceso definidas son de un nivel de protección o durabilidad muy baja.	Fallas en tomas de alimentación eléctrica estabilizada de servidor que aloja aplicación o software (inestabilidad de alimentación eléctrica / no conectada en tomas de acceso a UPS)	Aplicación no cuenta con un sistema de respaldo en otro servidor dedicado teniendo en cuenta la criticidad del mismo.	Ausencia de Mantenimiento de servidor que aloja aplicación o software de Gestión de Tickets.	Ausencia de Mantenimiento de servidor que aloja aplicación o software de Correo Electrónico
ACTIVO	INTEGRANTE	IMPACTO DEL ACTIVO	INTERPRETACIÓN DEL IMPACTO	PROBABILIDAD: PROBABILIDAD QUE UNA AMENAZA APROVECHE UNA VULNERABILIDAD PARA CAUSAR UN DAÑO EN EL ACTIVO DE INFORMACIÓN							
Sistema de Gestión de Tickets	A	5	MUY ALTO	5	4	5	4	4	4	4	
	B	5	MUY ALTO	5	4	5	4	5	3	5	
	C	5	MUY ALTO	5	5	4	4	3	5	4	
	D	5	MUY ALTO	5	5	4	4	5	3	3	
Contratos de Servicios, Instalación, entre otros	A	5	MUY ALTO								
	B	5	MUY ALTO								
	C	4	ALTO								
	D	5	MUY ALTO								
Carpeta de Proyectos	A	5	MUY ALTO								
	B	5	MUY ALTO								
	C	5	MUY ALTO								
	D	5	MUY ALTO								
Carpeta de Licitaciones	A	5	MUY ALTO								
	B	5	MUY ALTO								
	C	5	MUY ALTO								
	D	5	MUY ALTO								
Carpetas de Áreas Administrativas y Contabilidad	A	5	MUY ALTO								
	B	5	MUY ALTO								
	C	5	MUY ALTO								
	D	5	MUY ALTO								

RIESGOS			VULNERABILIDADES	AMENAZAS DETECTADAS							
				Falta de cierre de inicio de sesión en cada logueo realizado.	No existe definición de roles de usuarios. Es decir, el mismo usuario además de crear boletas de atención, puede observar módulos contables no autorizados, entre otros.	Servicios innecesarios para los usuarios que acceden al sistema.	Contraseñas de acceso definidas son de un nivel de protección o durabilidad muy baja.	Fallas en tomas de alimentación eléctrica estabilizada de servidor que aloja aplicación o software (inestabilidad de alimentación eléctrica / no conectada en tomas de acceso a UPS)	Aplicación no cuenta con un sistema de respaldo en otro servidor dedicado teniendo en cuenta la criticidad del mismo.	Ausencia de Mantenimiento de servidor que aloja aplicación o software de Gestión de Tickets.	Ausencia de Mantenimiento de servidor que aloja aplicación o software de Correo Electrónico
Equipos de Computo	A	4	ALTO	4			4				
	B	4	ALTO	4			4				
	C	5	MUY ALTO	4			5				
	D	4	ALTO	5			4				
Correo Electrónico	A	5	MUY ALTO	5			5	5	3		4
	B	5	MUY ALTO	4			4	5	5		4
	C	5	MUY ALTO	5			4	5	5		4
	D	5	MUY ALTO	5			5	5	4		3
Internet / Servicios dedicados	A	4	ALTO					4			
	B	4	ALTO					4			
	C	4	ALTO					4			
	D	4	ALTO					5			
File Server (Servidor de Archivos)	A	4	ALTO					4			
	B	5	MUY ALTO					4			
	C	5	MUY ALTO					4			
	D	5	MUY ALTO					5			
Infraestructura de Comunicaciones	A	5	MUY ALTO					4			
	B	4	ALTO					5			
	C	5	MUY ALTO					5			
	D	5	MUY ALTO					5			
Personal	A	5	MUY ALTO								
	B	5	MUY ALTO								
	C	5	MUY ALTO								
	D	5	MUY ALTO								

RIESGOS			VULNERABILIDADES	AMENAZAS DETECTADAS							
				Falta de logs de la aplicación o software para posteriores auditorias.	Transmisión de contraseñas de acceso por teléfono o vía correo.	Ausencia de Responsable de acceso y/o modificación de aplicativo	Falta de actualizaciones en servidor donde se aloja la aplicación y de la propia aplicación.	Acceso a información se encuentra en un armario de total acceso a usuarios no autorizados, no existen candado ni llaves para su acceso.	Ausencia de Responsable de acceso a documentación física	No existe definición de procedimientos para el movimiento o traslado del activo dentro y fuera de la oficina.	Falta de mecanismos de backup para la documentación Física
				PROBABILIDAD: PROBABILIDAD QUE UNA AMENAZA APROVECHE UNA VULNERABILIDAD PARA CAUSAR UN DAÑO EN EL ACTIVO DE INFORMACIÓN							
ACTIVO	INTEGRANTE	IMPACTO DEL ACTIVO	INTERPRETACIÓN DEL IMPACTO								
Sistema de Gestión de Tickets	A	5	MUY ALTO	4	1	4	2				
	B	5	MUY ALTO	4	2	5	4				
	C	5	MUY ALTO	4	3	5	4				
	D	5	MUY ALTO	3	2	4	3				
Contratos de Servicios, Instalación, entre otros	A	5	MUY ALTO					4	4	4	5
	B	5	MUY ALTO					5	5	5	4
	C	4	ALTO					5	4	5	5
	D	5	MUY ALTO					5	5	5	5
Carpeta de Proyectos	A	5	MUY ALTO								
	B	5	MUY ALTO								
	C	5	MUY ALTO								
	D	5	MUY ALTO								

RIESGOS			VULNERABILIDADES	AMENAZAS DETECTADAS							
				Falta de logs de la aplicación o software para posteriores auditorias.	Transmisión de contraseñas de acceso por teléfono o vía correo.	Ausencia de Responsable de acceso y/o modificación de aplicativo	Falta de actualizaciones en servidor donde se aloja la aplicación y de la propia aplicación.	Acceso a información se encuentra en un armario de total acceso a usuarios no autorizados, no existen candado ni llaves para su acceso.	Ausencia de Responsable de acceso a documentación física	No existe definición de procedimientos para el movimiento o traslado del activo dentro y fuera de la oficina.	Falta de mecanismos de backup para la documentación Física
Carpeta de Licitaciones	A	5	MUY ALTO								
	B	5	MUY ALTO								
	C	5	MUY ALTO								
	D	5	MUY ALTO								
Carpetas de Áreas Administrativas y Contabilidad	A	5	MUY ALTO								
	B	5	MUY ALTO								
	C	5	MUY ALTO								
	D	5	MUY ALTO								
Equipos de Computo	A	4	ALTO		4					5	
	B	4	ALTO		5					4	
	C	5	MUY ALTO		4					4	
	D	4	ALTO		4					4	
Correo Electrónico	A	5	MUY ALTO		4		5				
	B	5	MUY ALTO		5		4				
	C	5	MUY ALTO		4		4				
	D	5	MUY ALTO		5		4				

RIESGOS			VULNERABILIDADES	AMENAZAS DETECTADAS							
				Falta de logs de la aplicación o software para posteriores auditorias.	Transmisión de contraseñas de acceso por teléfono o vía correo.	Ausencia de Responsable de acceso y/o modificación de aplicativo	Falta de actualizaciones en servidor donde se aloja la aplicación y de la propia aplicación.	Acceso a información se encuentra en un armario de total acceso a usuarios no autorizados, no existen candado ni llaves para su acceso.	Ausencia de Responsable de acceso a documentación física	No existe definición de procedimientos para el movimiento o traslado del activo dentro y fuera de la oficina.	Falta de mecanismos de backup para la documentación Física
Internet / Servicios dedicados	A	4	ALTO								
	B	4	ALTO								
	C	4	ALTO								
	D	4	ALTO								
File Server (Servidor de Archivos)	A	4	ALTO								
	B	5	MUY ALTO								
	C	5	MUY ALTO								
	D	5	MUY ALTO								
Infraestructura de Comunicaciones	A	5	MUY ALTO								
	B	4	ALTO								
	C	5	MUY ALTO								
	D	5	MUY ALTO								
Personal	A	5	MUY ALTO								
	B	5	MUY ALTO								
	C	5	MUY ALTO								
	D	5	MUY ALTO								

RIESGOS			VULNERABILIDADES	AMENAZAS DETECTADAS							
				No existen controles para su acceso a nivel de acceso y seguridad de carpetas a pesar de comunicado difundido	Ausencia de Responsable de acceso a carpeta.	Ausencia de backup o respaldo de documentación de carpeta.	Uso inadecuado de contenido de la carpeta	Ausencia de controles contra modificación o alteración de contenido de carpeta.	Algunos equipos no se encuentran ingresadas en el dominio, no cumpliendo los estándares de seguridad aplicados por la organización.	No existe controles de desinstalación de programas/aplicaciones auditable instaladas por la organización	Ausencia o falta de backup o respaldos de documentación interna de los equipos o de la información más relevante.
ACTIVO	INTEGRANTE	IMPACTO DEL ACTIVO	INTERPRETACIÓN DEL IMPACTO	PROBABILIDAD: PROBABILIDAD QUE UNA AMENAZA APROVECHE UNA VULNERABILIDAD PARA CAUSAR UN DAÑO EN EL ACTIVO DE INFORMACIÓN							
Sistema de Gestión de Tickets	A	5	MUY ALTO								
	B	5	MUY ALTO								
	C	5	MUY ALTO								
	D	5	MUY ALTO								
Contratos de Servicios, Instalación, entre otros	A	5	MUY ALTO								
	B	5	MUY ALTO								
	C	4	ALTO								
	D	5	MUY ALTO								
Carpeta de Proyectos	A	5	MUY ALTO	5	5	4	4	5			
	B	5	MUY ALTO	5	5	4	5	5			
	C	5	MUY ALTO	5	4	4	5	5			
	D	5	MUY ALTO	5	5	5	5	5			

RIESGOS			VULNERABILIDADES	AMENAZAS DETECTADAS							
				No existen controles para su acceso a nivel de acceso y seguridad de carpetas a pesar de comunicado difundido	Ausencia de Responsable de acceso a carpeta.	Ausencia de backup o respaldo de documentación de carpeta.	Uso inadecuado de contenido de la carpeta	Ausencia de controles contra modificación o alteración de contenido de carpeta.	Algunos equipos no se encuentran ingresadas en el dominio, no cumpliendo los estándares de seguridad aplicados por la organización.	No existe controles de desinstalación de programas/aplicaciones auditables instaladas por la organización	Ausencia o falta de backup o respaldos de documentación interna de los equipos o de la información más relevante.
Carpeta de Licitaciones	A	5	MUY ALTO	5	4	5	4	5			
	B	5	MUY ALTO	5	4	5	4	5			
	C	5	MUY ALTO	5	4	4	5	4			
	D	5	MUY ALTO	5	5	5	5	5			
Carpetas de Áreas Administrativas y Contabilidad	A	5	MUY ALTO	4	5	4	5	5			
	B	5	MUY ALTO	5	4	5	5	5			
	C	5	MUY ALTO	4	4	5	4	5			
	D	5	MUY ALTO	5	5	5	5	5			
Equipos de Computo	A	4	ALTO						4	4	4
	B	4	ALTO						4	4	4
	C	5	MUY ALTO						5	4	5
	D	4	ALTO						5	4	4
Correo Electrónico	A	5	MUY ALTO								
	B	5	MUY ALTO								
	C	5	MUY ALTO								
	D	5	MUY ALTO								

RIESGOS			VULNERABILIDADES	AMENAZAS DETECTADAS							
				No existen controles para su acceso a nivel de acceso y seguridad de carpetas a pesar de comunicado difundido	Ausencia de Responsable de acceso a carpeta.	Ausencia de backup o respaldo de documentación de carpeta.	Uso inadecuado de contenido de la carpeta	Ausencia de controles contra modificación o alteración de contenido de carpeta.	Algunos equipos no se encuentran ingresadas en el dominio, no cumpliendo los estándares de seguridad aplicados por la organización.	No existe controles de desinstalación de programas/aplicaciones auditables instaladas por la organización	Ausencia o falta de backup o respaldos de documentación interna de los equipos o de la información más relevante.
Internet / Servicios dedicados	A	4	ALTO								
	B	4	ALTO								
	C	4	ALTO								
	D	4	ALTO								
File Server (Servidor de Archivos)	A	4	ALTO					4			
	B	5	MUY ALTO					5			
	C	5	MUY ALTO					4			
	D	5	MUY ALTO					5			
Infraestructura de Comunicaciones	A	5	MUY ALTO								5
	B	4	ALTO								4
	C	5	MUY ALTO								4
	D	5	MUY ALTO								4
Personal	A	5	MUY ALTO								
	B	5	MUY ALTO								
	C	5	MUY ALTO								
	D	5	MUY ALTO								

RIESGOS			VULNERABILIDADES	AMENAZAS DETECTADAS							
				Falta de mecanismos de autenticación de usuarios sobre los equipos de cómputo asignados.	Ausencia de protección física para el retiro de equipos a clientes.	Ausencia de hardware de backup	Ausencia de responsable del bien	Ausencia de controles de retiro de equipos para labores a realizar en los distintos clientes	Ausencia de políticas y/o procedimientos para envío de correos (tamaño, destinatario, adjunto, etc).	Mala gestión de Contraseñas	Ausencia de backup o respaldo de la información Extensiones .pst)
				PROBABILIDAD: PROBABILIDAD QUE UNA AMENAZA APROVECHE UNA VULNERABILIDAD PARA CAUSAR UN DAÑO EN EL ACTIVO DE INFORMACIÓN							
ACTIVO	INTEGRANTE	IMPACTO DEL ACTIVO	INTERPRETACIÓN DEL IMPACTO								
Sistema de Gestión de Tickets	A	5	MUY ALTO				5			3	
	B	5	MUY ALTO				4			4	
	C	5	MUY ALTO				4			5	
	D	5	MUY ALTO				4			4	
Contratos de Servicios, Instalación, entre otros	A	5	MUY ALTO				4				
	B	5	MUY ALTO				3				
	C	4	ALTO				4				
	D	5	MUY ALTO				5				
Carpeta de Proyectos	A	5	MUY ALTO				4				
	B	5	MUY ALTO				4				
	C	5	MUY ALTO				4				
	D	5	MUY ALTO				5				

RIESGOS			VULNERABILIDADES	AMENAZAS DETECTADAS							
				Falta de mecanismos de autenticación de usuarios sobre los equipos de cómputo asignados.	Ausencia de protección física para el retiro de equipos a clientes.	Ausencia de hardware de backup	Ausencia de responsable del bien	Ausencia de controles de retiro de equipos para labores a realizar en los distintos clientes	Ausencia de políticas y/o procedimientos para envío de correos (tamaño, destinatario, adjunto, etc).	Mala gestión de Contraseñas	Ausencia de backup o respaldo de la información Extensiones .pst)
Carpeta de Licitaciones	A	5	MUY ALTO				4				
	B	5	MUY ALTO				5				
	C	5	MUY ALTO				5				
	D	5	MUY ALTO				5				
Carpetas de Áreas Administrativas y Contabilidad	A	5	MUY ALTO				4				
	B	5	MUY ALTO				4				
	C	5	MUY ALTO				5				
	D	5	MUY ALTO				5				
Equipos de Computo	A	4	ALTO	4	4		4	4		3	
	B	4	ALTO	4	4		4	3		4	
	C	5	MUY ALTO	5	5		5	4		5	
	D	4	ALTO	4	4		4	3		4	
Correo Electrónico	A	5	MUY ALTO				5		4	4	4
	B	5	MUY ALTO				4		5	5	5
	C	5	MUY ALTO				4		4	4	5
	D	5	MUY ALTO				5		5	5	5

RIESGOS			VULNERABILIDADES	AMENAZAS DETECTADAS							
				Falta de mecanismos de autenticación de usuarios sobre los equipos de cómputo asignados.	Ausencia de protección física para el retiro de equipos a clientes.	Ausencia de hardware de backup	Ausencia de responsable del bien	Ausencia de controles de retiro de equipos para labores a realizar en los distintos clientes	Ausencia de políticas y/o procedimientos para envío de correos (tamaño, destinatario, adjunto, etc).	Mala gestión de Contraseñas	Ausencia de backup o respaldo de la información Extensiones .pst)
Internet / Servicios dedicados	A	4	ALTO				5				
	B	4	ALTO				4				
	C	4	ALTO				4				
	D	4	ALTO				5				
File Server (Servidor de Archivos)	A	4	ALTO			4	5				
	B	5	MUY ALTO			5	4				
	C	5	MUY ALTO			5	5				
	D	5	MUY ALTO			5	4				
Infraestructura de Comunicaciones	A	5	MUY ALTO			5	5			5	
	B	4	ALTO			4	5			4	
	C	5	MUY ALTO			5	5			4	
	D	5	MUY ALTO			5	4			4	
Personal	A	5	MUY ALTO								
	B	5	MUY ALTO								
	C	5	MUY ALTO								
	D	5	MUY ALTO								

RIESGOS			VULNERABILIDADES	AMENAZAS DETECTADAS							
				Falta de gestión de logs en servidor de correo para seguimiento o auditoria.	Falta de gestión de logs en consumo de recursos de Navegación en Internet para seguimiento o auditoria.	Falta de disponibilidad del servicio por parte del proveedor o ISP.	Falta de Mantenimiento de equipamiento de Infraestructura	Falta de Mantenimiento de equipamiento de acceso a Internet otorgado por el Proveedor o ISP	Acceso a Data Center no definido mediante documentación y/o asignación de responsabilidades.	Ausencia de mantenimiento a servidor de archivos	Falta de gestión de logs en equipos de Infraestructura de comunicaciones para seguimiento o auditoria.
ACTIVO	INTEGRANTE	IMPACTO DEL ACTIVO	INTERPRETACIÓN DEL IMPACTO	PROBABILIDAD: PROBABILIDAD QUE UNA AMENAZA APROVECHE UNA VULNERABILIDAD PARA CAUSAR UN DAÑO EN EL ACTIVO DE INFORMACIÓN							
Sistema de Gestión de Tickets	A	5	MUY ALTO								
	B	5	MUY ALTO								
	C	5	MUY ALTO								
	D	5	MUY ALTO								
Contratos de Servicios, Instalación, entre otros	A	5	MUY ALTO								
	B	5	MUY ALTO								
	C	4	ALTO								
	D	5	MUY ALTO								
Carpeta de Proyectos	A	5	MUY ALTO								
	B	5	MUY ALTO								
	C	5	MUY ALTO								
	D	5	MUY ALTO								

RIESGOS			VULNERABILIDADES	AMENAZAS DETECTADAS							
				Falta de gestión de logs en servidor de correo para seguimiento o auditoria.	Falta de gestión de logs en consumo de recursos de Navegación en Internet para seguimiento o auditoria.	Falta de disponibilidad del servicio por parte del proveedor o ISP.	Falta de Mantenimiento de equipamiento de Infraestructura	Falta de Mantenimiento de equipamiento de acceso a Internet otorgado por el Proveedor o ISP	Acceso a Data Center no definido mediante documentación y/o asignación de responsabilidades.	Ausencia de mantenimiento a servidor de archivos	Falta de gestión de logs en equipos de Infraestructura de comunicaciones para seguimiento o auditoria.
Carpeta de Licitaciones	A	5	MUY ALTO								
	B	5	MUY ALTO								
	C	5	MUY ALTO								
	D	5	MUY ALTO								
Carpetas de Áreas Administrativas y Contabilidad	A	5	MUY ALTO								
	B	5	MUY ALTO								
	C	5	MUY ALTO								
	D	5	MUY ALTO								
Equipos de Computo	A	4	ALTO								
	B	4	ALTO								
	C	5	MUY ALTO								
	D	4	ALTO								
Correo Electrónico	A	5	MUY ALTO	4							
	B	5	MUY ALTO	5							
	C	5	MUY ALTO	4							
	D	5	MUY ALTO	5							

RIESGOS			VULNERABILIDADES	AMENAZAS DETECTADAS							
				Falta de gestión de logs en servidor de correo para seguimiento o auditoria.	Falta de gestión de logs en consumo de recursos de Navegación en Internet para seguimiento o auditoria.	Falta de disponibilidad del servicio por parte del proveedor o ISP.	Falta de Mantenimiento de equipamiento de Infraestructura	Falta de Mantenimiento de equipamiento de acceso a Internet otorgado por el Proveedor o ISP	Acceso a Data Center no definido mediante documentación y/o asignación de responsabilidades.	Ausencia de mantenimiento a servidor de archivos	Falta de gestión de logs en equipos de Infraestructura de comunicaciones para seguimiento o auditoria.
Internet / Servicios dedicados	A	4	ALTO		4	4		5	5		
	B	4	ALTO		5	4		5	4		
	C	4	ALTO		4	5		5	5		
	D	4	ALTO		5	5		5	5		
File Server (Servidor de Archivos)	A	4	ALTO							5	
	B	5	MUY ALTO							4	
	C	5	MUY ALTO							4	
	D	5	MUY ALTO							4	
Infraestructura de Comunicaciones	A	5	MUY ALTO				5				4
	B	4	ALTO				5				4
	C	5	MUY ALTO				4				4
	D	5	MUY ALTO				4				4
Personal	A	5	MUY ALTO								
	B	5	MUY ALTO								
	C	5	MUY ALTO								
	D	5	MUY ALTO								

RIESGOS			VULNERABILIDADES	AMENAZAS DETECTADAS							
				Falta de gestión de logs en servidor de archivos para seguimiento o auditoria (recursos del equipo)	Falta de gestión de logs de accesos y contenido de recursos de datos alojados en carpetas de File Server (Servidor de Archivos)	Ausencia de backup o respaldo de la información interna.	Control de accesos no definidos mediante documentación o asignación de responsabilidades.	Control de accesos de navegación a Internet no definidos mediante documentación o asignación de perfiles.	Falta de inducción, capacitación y sensibilización sobre riesgos.	Renuncias y/o despidos del personal	Ausencia de documento donde se especifique que el personal que accede a la documentación de la organización debe preservar la confidencialidad, integridad y de ser el caso la disponibilidad de la misma.
ACTIVO	INTEGRANTE	IMPACTO DEL ACTIVO	INTERPRETACIÓN DEL IMPACTO	PROBABILIDAD: PROBABILIDAD QUE UNA AMENAZA APROVECHE UNA VULNERABILIDAD PARA CAUSAR UN DAÑO EN EL ACTIVO DE INFORMACIÓN							
Sistema de Gestión de Tickets	A	5	MUY ALTO				5				
	B	5	MUY ALTO				4				
	C	5	MUY ALTO				3				
	D	5	MUY ALTO				4				
Contratos de Servicios, Instalación, entre otros	A	5	MUY ALTO				4				5
	B	5	MUY ALTO				5				4
	C	4	ALTO				5				4
	D	5	MUY ALTO				5				5
Carpeta de Proyectos	A	5	MUY ALTO		5		5				5
	B	5	MUY ALTO		4		4				5
	C	5	MUY ALTO		5		4				5
	D	5	MUY ALTO		5		5				5

RIESGOS			VULNERABILIDADES	AMENAZAS DETECTADAS							
				Falta de gestión de logs en servidor de archivos para seguimiento o auditoria (recursos del equipo)	Falta de gestión de logs de accesos y contenido de recursos de datos alojados en carpetas de File Server (Servidor de Archivos)	Ausencia de backup o respaldo de la información interna.	Control de accesos no definidos mediante documentación o asignación de responsabilidades.	Control de accesos de navegación a Internet no definidos mediante documentación o asignación de perfiles.	Falta de inducción, capacitación y sensibilización sobre riesgos.	Renuncias y/o despidos del personal	Ausencia de documento donde se especifique que el personal que accede a la documentación de la organización debe preservar la confidencialidad, integridad y de ser el caso la disponibilidad de la misma.
Carpeta de Licitaciones	A	5	MUY ALTO		5		5				5
	B	5	MUY ALTO		5		5				4
	C	5	MUY ALTO		5		5				5
	D	5	MUY ALTO		5		5				5
Carpetas de Áreas Administrativas y Contabilidad	A	5	MUY ALTO		5		4				5
	B	5	MUY ALTO		5		4				4
	C	5	MUY ALTO		5		5				5
	D	5	MUY ALTO		5		5				5
Equipos de Computo	A	4	ALTO			4	4				
	B	4	ALTO			3	4				
	C	5	MUY ALTO			4	4				
	D	4	ALTO			3	3				
Correo Electrónico	A	5	MUY ALTO								
	B	5	MUY ALTO								
	C	5	MUY ALTO								
	D	5	MUY ALTO								

RIESGOS			VULNERABILIDADES	AMENAZAS DETECTADAS							
				Falta de gestión de logs en servidor de archivos para seguimiento o auditoria (recursos del equipo)	Falta de gestión de logs de accesos y contenido de recursos de datos alojados en carpetas de File Server (Servidor de Archivos)	Ausencia de backup o respaldo de la información interna.	Control de accesos no definidos mediante documentación o asignación de responsabilidades.	Control de accesos de navegación a Internet no definidos mediante documentación o asignación de perfiles.	Falta de inducción, capacitación y sensibilización sobre riesgos.	Renuncias y/o despidos del personal	Ausencia de documento donde se especifique que el personal que accede a la documentación de la organización debe preservar la confidencialidad, integridad y de ser el caso la disponibilidad de la misma.
Internet / Servicios dedicados	A	4	ALTO					5			
	B	4	ALTO					4			
	C	4	ALTO					4			
	D	4	ALTO					5			
File Server (Servidor de Archivos)	A	4	ALTO	4		4	5				
	B	5	MUY ALTO	5		4	5				
	C	5	MUY ALTO	5		4	5				
	D	5	MUY ALTO	5		5	5				
Infraestructura de Comunicaciones	A	5	MUY ALTO				4				
	B	4	ALTO				4				
	C	5	MUY ALTO				5				
	D	5	MUY ALTO				5				
Personal	A	5	MUY ALTO						4	5	
	B	5	MUY ALTO						4	4	
	C	5	MUY ALTO						4	5	
	D	5	MUY ALTO						5	4	

RIESGOS			VULNERABILIDADES	AMENAZAS DETECTADAS					
				Ausencia de documento donde se especifique que el personal que accede a la documentación de la organización debe preservar la confidencialidad, integridad y de ser el caso la disponibilidad de la misma.	Ausencia de documento donde se especifique que el personal que accede a la aplicación debe preservar la confidencialidad, integridad y de ser el caso la disponibilidad de la misma.	Ausencia de documento donde se especifique que el personal que accede al servidor debe preservar la confidencialidad, integridad y de ser el caso la disponibilidad de la misma.	Manejo inadecuado de software o herramientas brindadas por la organización.	Ausencia de orden en asignación de servicios a los distintos clientes de la empresa u organización.	Red cableada expuesta a acceso no autorizado.
				PROBABILIDAD: PROBABILIDAD QUE UNA AMENAZA APROVECHE UNA VULNERABILIDAD PARA CAUSAR UN DAÑO EN EL ACTIVO DE INFORMACIÓN					
ACTIVO	INTEGRANTE	IMPACTO DEL ACTIVO	INTERPRETACIÓN DEL IMPACTO						
Sistema de Gestión de Tickets	A	5	MUY ALTO		5		4		
	B	5	MUY ALTO		4		5		
	C	5	MUY ALTO		4		5		
	D	5	MUY ALTO		5		3		
Contratos de Servicios, Instalación, entre otros	A	5	MUY ALTO	5					
	B	5	MUY ALTO	4					
	C	4	ALTO	4					
	D	5	MUY ALTO	5					
Carpeta de Proyectos	A	5	MUY ALTO	5					
	B	5	MUY ALTO	5					
	C	5	MUY ALTO	5					
	D	5	MUY ALTO	5					

RIESGOS			VULNERABILIDADES	AMENAZAS DETECTADAS					
				Ausencia de documento donde se especifique que el personal que accede a la documentación de la organización debe preservar la confidencialidad, integridad y de ser el caso la disponibilidad de la misma.	Ausencia de documento donde se especifique que el personal que accede a la aplicación debe preservar la confidencialidad, integridad y de ser el caso la disponibilidad de la misma.	Ausencia de documento donde se especifique que el personal que accede al servidor debe preservar la confidencialidad, integridad y de ser el caso la disponibilidad de la misma.	Manejo inadecuado de software o herramientas brindadas por la organización.	Ausencia de orden en asignación de servicios a los distintos clientes de la empresa u organización.	Red cableada expuesta a acceso no autorizado.
Carpeta de Licitaciones	A	5	MUY ALTO	5					
	B	5	MUY ALTO	4					
	C	5	MUY ALTO	5					
	D	5	MUY ALTO	5					
Carpetas de Áreas Administrativas y Contabilidad	A	5	MUY ALTO	5					
	B	5	MUY ALTO	4					
	C	5	MUY ALTO	5					
	D	5	MUY ALTO	5					
Equipos de Computo	A	4	ALTO						4
	B	4	ALTO						5
	C	5	MUY ALTO						5
	D	4	ALTO						4
Correo Electrónico	A	5	MUY ALTO		4		4		
	B	5	MUY ALTO		4		3		
	C	5	MUY ALTO		5		4		
	D	5	MUY ALTO		5		3		

RIESGOS			VULNERABILIDADES	AMENAZAS DETECTADAS					
				Ausencia de documento donde se especifique que el personal que accede a la documentación de la organización debe preservar la confidencialidad, integridad y de ser el caso la disponibilidad de la misma.	Ausencia de documento donde se especifique que el personal que accede a la aplicación debe preservar la confidencialidad, integridad y de ser el caso la disponibilidad de la misma.	Ausencia de documento donde se especifique que el personal que accede al servidor debe preservar la confidencialidad, integridad y de ser el caso la disponibilidad de la misma.	Manejo inadecuado de software o herramientas brindadas por la organización.	Ausencia de orden en asignación de servicios a los distintos clientes de la empresa u organización.	Red cableada expuesta a acceso no autorizado.
Internet / Servicios dedicados	A	4	ALTO						
	B	4	ALTO						
	C	4	ALTO						
	D	4	ALTO						
File Server (Servidor de Archivos)	A	4	ALTO			5			5
	B	5	MUY ALTO			5			4
	C	5	MUY ALTO			4			5
	D	5	MUY ALTO			5			5
Infraestructura de Comunicaciones	A	5	MUY ALTO						3
	B	4	ALTO						5
	C	5	MUY ALTO						3
	D	5	MUY ALTO						5
Personal	A	5	MUY ALTO			5	5	5	
	B	5	MUY ALTO			5	4	5	
	C	5	MUY ALTO			5	4	4	
	D	5	MUY ALTO			5	4	5	

RIESGOS			VULNERABILIDADES	Σ PROBABILIDAD DEL RIESGO	PROBABILIDAD DEL RIESGO	INTERPRETACIÓN DE LA PROBABILIDAD DEL RIESGO	NIVEL DE RIESGO (IMPACTO * PROBABILIDAD)	INTERPRETACIÓN DEL RIESGO	INTERPRETACIÓN DEL RIESGO RESULTANTE	NIVEL DE ACEPTACIÓN DEL RIESGO	NIVEL DE ACEPTACIÓN DEL RIESGO RESULTANTE	TIENE CONTROLES
ACTIVO	INTEGRANTE	IMPACTO DEL ACTIVO	INTERPRETACIÓN DEL IMPACTO									
Sistema de Gestión de Tickets	A	5	MUY ALTO	63	4	ALTO	20	MUY ALTO	MUY ALTO	IMPORTANTE	IMPORTANTE	NO
	B	5	MUY ALTO	67	4	ALTO	20	MUY ALTO		IMPORTANTE		NO
	C	5	MUY ALTO	67	4	ALTO	20	MUY ALTO		IMPORTANTE		NO
	D	5	MUY ALTO	61	4	ALTO	20	MUY ALTO		IMPORTANTE		NO
Contratos de Servicios, Instalación, entre otros	A	5	MUY ALTO	30	2	BAJO	10	ALTO	ALTO	CONSIDERABLE	CONSIDERABLE	NO
	B	5	MUY ALTO	31	2	BAJO	10	ALTO		CONSIDERABLE		NO
	C	4	ALTO	32	2	BAJO	8	MEDIO		CONSIDERABLE		NO
	D	5	MUY ALTO	35	2	BAJO	10	ALTO		CONSIDERABLE		NO
Carpeta de Proyectos	A	5	MUY ALTO	42	3	MEDIO	15	ALTO	ALTO	CONSIDERABLE	CONSIDERABLE	NO
	B	5	MUY ALTO	41	3	MEDIO	15	ALTO		CONSIDERABLE		NO
	C	5	MUY ALTO	41	3	MEDIO	15	ALTO		CONSIDERABLE		NO
	D	5	MUY ALTO	45	3	MEDIO	15	ALTO		CONSIDERABLE		NO

RIESGOS			VULNERABILIDADES	Σ PROBABILIDAD DEL RIESGO	PROBABILIDAD DEL RIESGO	INTERPRETACIÓN DE LA PROBABILIDAD DEL RIESGO	NIVEL DE RIESGO (IMPACTO * PROBABILIDAD)	INTERPRETACIÓN DEL RIESGO	INTERPRETACIÓN DEL RIESGO RESULTANTE	NIVEL DE ACEPTACIÓN DEL RIESGO	NIVEL DE ACEPTACIÓN DEL RIESGO RESULTANTE	TIENE CONTROLES
ACTIVO	INTEGRANTE	IMPACTO DEL ACTIVO	INTERPRETACIÓN DEL IMPACTO									
Carpeta de Licitaciones	A	5	MUY ALTO	42	3	MEDIO	15	ALTO	ALTO	CONSIDERABLE	CONSIDERABLE	NO
	B	5	MUY ALTO	42	3	MEDIO	15	ALTO		CONSIDERABLE		NO
	C	5	MUY ALTO	42	3	MEDIO	15	ALTO		CONSIDERABLE		NO
	D	5	MUY ALTO	45	3	MEDIO	15	ALTO		CONSIDERABLE		NO
Carpetas de Áreas Administrativas y Contabilidad	A	5	MUY ALTO	41	3	MEDIO	15	ALTO	ALTO	CONSIDERABLE	CONSIDERABLE	NO
	B	5	MUY ALTO	41	3	MEDIO	15	ALTO		CONSIDERABLE		NO
	C	5	MUY ALTO	42	3	MEDIO	15	ALTO		CONSIDERABLE		NO
	D	5	MUY ALTO	45	3	MEDIO	15	ALTO		CONSIDERABLE		NO
Equipos de Computo	A	4	ALTO	60	3	MEDIO	12	ALTO	ALTO	CONSIDERABLE	CONSIDERABLE	NO
	B	4	ALTO	60	3	MEDIO	12	ALTO		CONSIDERABLE		NO
	C	5	MUY ALTO	68	4	ALTO	20	MUY ALTO		IMPORTANTE		NO
	D	4	ALTO	59	3	MEDIO	12	ALTO		CONSIDERABLE		NO
Correo Electrónico	A	5	MUY ALTO	60	3	MEDIO	15	ALTO	MUY ALTO	IMPORTANTE	IMPORTANTE	NO
	B	5	MUY ALTO	62	4	ALTO	20	MUY ALTO		IMPORTANTE		NO
	C	5	MUY ALTO	61	4	ALTO	20	MUY ALTO		IMPORTANTE		NO
	D	5	MUY ALTO	64	4	ALTO	20	MUY ALTO		IMPORTANTE		NO

RIESGOS			VULNERABILIDADES	Σ PROBABILIDAD DEL RIESGO	PROBABILIDAD DEL RIESGO	INTERPRETACIÓN DE LA PROBABILIDAD DEL RIESGO	NIVEL DE RIESGO (IMPACTO * PROBABILIDAD)	INTERPRETACIÓN DEL RIESGO	INTERPRETACIÓN DEL RIESGO RESULTANTE	NIVEL DE ACEPTACIÓN DEL RIESGO	NIVEL DE ACEPTACIÓN DEL RIESGO RESULTANTE	TIENE CONTROLES
ACTIVO	INTEGRANTE	IMPACTO DEL ACTIVO	INTERPRETACIÓN DEL IMPACTO									
Internet / Servicios dedicados	A	4	ALTO	32	2	BAJO	8	MEDIO	MEDIO	CONSIDERABLE	CONSIDERABLE	NO
	B	4	ALTO	30	2	BAJO	8	MEDIO		CONSIDERABLE		NO
	C	4	ALTO	31	2	BAJO	8	MEDIO		CONSIDERABLE		NO
	D	4	ALTO	35	2	BAJO	8	MEDIO		CONSIDERABLE		NO
File Server (Servidor de Archivos)	A	4	ALTO	45	3	MEDIO	12	ALTO	ALTO	CONSIDERABLE	CONSIDERABLE	NO
	B	5	MUY ALTO	45	3	MEDIO	15	ALTO		CONSIDERABLE		NO
	C	5	MUY ALTO	45	3	MEDIO	15	ALTO		CONSIDERABLE		NO
	D	5	MUY ALTO	48	3	MEDIO	15	ALTO		CONSIDERABLE		NO
Infraestructura de Comunicaciones	A	5	MUY ALTO	40	2	BAJO	10	ALTO	ALTO	CONSIDERABLE	CONSIDERABLE	NO
	B	4	ALTO	40	2	BAJO	8	MEDIO		CONSIDERABLE		NO
	C	5	MUY ALTO	39	2	BAJO	10	ALTO		CONSIDERABLE		NO
	D	5	MUY ALTO	40	2	BAJO	10	ALTO		CONSIDERABLE		NO
Personal	A	5	MUY ALTO	24	2	BAJO	10	ALTO	ALTO	CONSIDERABLE	CONSIDERABLE	NO
	B	5	MUY ALTO	22	2	BAJO	10	ALTO		CONSIDERABLE		NO
	C	5	MUY ALTO	22	2	BAJO	10	ALTO		CONSIDERABLE		NO
	D	5	MUY ALTO	23	2	BAJO	10	ALTO		CONSIDERABLE		NO

ANEXO X: Roles, Responsabilidades y autoridades organizacionales especificados en la norma ISO/IEC 27001:2013

5. LIDERAZGO

5.1 Liderazgo y compromiso

La alta dirección debe demostrar liderazgo y compromiso respecto del sistema de gestión de seguridad de la información:

- a) asegurando que la política de seguridad de la información y los objetivos de seguridad de la información son establecidos y compatibles con la dirección estratégica de la organización;
- b) asegurando la integración de los requisitos del sistema de gestión de seguridad de la información en los procesos de la organización;
- c) asegurando que los recursos necesarios para el sistema de gestión de seguridad de la información estén disponibles;
- d) comunicando la importancia de una efectiva gestión de seguridad de la información y en conformidad con los requisitos del sistema de gestión de seguridad de la información;
- e) asegurando que el sistema de gestión de seguridad de la información logre su(s) resultado(s) previsto(s);
- f) dirigiendo y apoyando a las personas para que contribuyan con la efectividad del sistema de gestión de seguridad de la información;
- g) promoviendo la mejora continua; y

© ISO/IEC 2013 - © INDECOPI 2014 - Todos los derechos son reservados

- h) apoyando a otros roles relevantes de gestión para demostrar su liderazgo tal como se aplica a sus áreas de responsabilidad.

5.2 Política

La alta dirección debe establecer una política de seguridad de la información que:

- a) es apropiada al propósito de la organización;
- b) incluye objetivos de seguridad de la información (véase 6.2) o proporciona el marco de referencia para fijar los objetivos de seguridad de la información;
- c) incluye un compromiso de satisfacer requisitos aplicables relacionados a la seguridad de la información; e
- d) incluye un compromiso de mejora continua del sistema de gestión de seguridad de la información.

La política de seguridad de la información debe:

- e) estar disponible como información documentada;
- f) estar comunicada dentro de la organización; y
- g) estar disponible a las partes interesadas, según sea apropiado.

5.3 Roles, responsabilidades y autoridades organizacionales

La alta dirección debe asegurar que las responsabilidades y la autoridad para los roles relevantes a la seguridad de la información estén asignadas y comunicadas.

La alta dirección debe asignar la responsabilidad y la autoridad para:

- a) asegurar que el sistema de gestión de seguridad de la información esté conforme a los requisitos de esta Norma Técnica Peruana; y

© ISO/IEC 2013 • © INDECOPI 2014 • Todos los derechos son reservados

- b) reportar sobre el desempeño del sistema de gestión de seguridad de la información a la alta dirección.

NOTA: La alta dirección también puede asignar responsabilidades y la autoridad para reportar desempeño del sistema de gestión de seguridad de la información dentro de la organización.

ANEXO XI: Resolución Ministerial N° 004-2016-PCM

575410

NORMAS LEGALES

Jueves 14 de enero de 2016 / El Peruano

ANEXO 2

RELACIÓN DE REPRESENTANTES DEL GOBIERNO NACIONAL
ANTE COMISIÓN INTERGUBERNAMENTAL DEL SECTOR
AGRICULTURA Y RIEGO, CONFORMADA EN EL MARCO DEL
DECRETO SUPREMO N° 047-2009-PCM

	CARGO	DEPENDENCIA / INSTITUCIÓN	CARGO
1	Viceministro (a) de Política Agrarias	Despacho Viceministerial	Presidente Comisión Intergubernamental
2	Director (a) de la Oficina General de Planeamiento	Oficina General de Planeamiento y Presupuesto	Miembro
3	Profesional		Miembro Alterno
4	Profesional	Oficina General de Asesoría Jurídica	Miembro
5	Profesional	Oficina General de Administración	Miembro
6	Profesional	Oficina General de Gestión de Recursos Humanos	Miembro
7	Director (a) General de Articulación Intergubernamental	Dirección General de Articulación Intergubernamental	Miembro
8	Director (a) de Gestión Descentralizada		Miembro
9	Director de Seguimiento y Evaluación de Políticas (a)	Dirección General de Seguimiento y Evaluación de Políticas	Miembro
10	Director (a) de Estadística Agraria		Miembro Alterno
11	Director (a) General de Políticas Agrarias	Dirección General de Políticas Agrarias	Miembro
12	Director (a) de Políticas y Normatividad Agraria		Miembro
13	Profesional	Dirección General de Negocios Agrarios	Miembro
14	Profesional		Miembro Alterno
15	Profesional	Dirección General de Asuntos Ambientales Agrarios	Miembro
		Dirección General de	

Aprueban el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática

RESOLUCIÓN MINISTERIAL N° 004-2016-PCM

Lima, 8 de enero de 2016

CONSIDERANDO:

Que, mediante Resolución Ministerial N° 246-2007-PCM se aprobó el uso de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2ª. Edición", en todas las entidades del Sistema Nacional de Informática;

Que, mediante Resolución Ministerial N° 197-2011-PCM, se estableció el plazo para que determinadas entidades de la Administración Pública implementen el Plan de Seguridad de la Información dispuesto en la Norma Técnica Peruana antes señalada; posteriormente, mediante Resolución Ministerial N° 129-2012-PCM se estableció un nuevo cronograma y la incorporación del rol del oficial de seguridad para el proceso de implementación de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2008";

Que, la Norma Técnica Peruana "NTP ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Requisitos", aprobada mediante Resolución N° 42-2008/INDECOPI-CNB, por la Comisión de Normalización y de Fiscalización de Barreras Comerciales No Arancelarias del Instituto Nacional de Defensa de la Competencia y de Protección de la Propiedad Intelectual (INDECOPI) ha sido reemplazada por la nueva versión de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Requisitos. 2ª Edición" aprobada por Resolución N° 129-2014/DNB-INDECOPI;

16	Profesional	Infraestructura Agraria y Riego	Miembro
17	Profesional	Servicio Nacional Forestal y de Fauna Silvestre	Miembro
18	Profesional	Programa de Desarrollo Productivo Agrario Rural - AGRODECOR	Miembro
19	Profesional	Programa de Desarrollo Productivo Agrario Rural - AGRODECOR	Miembro
20	Profesional	Programa de Desarrollo Productivo Agrario Rural - AGRODECOR	Miembro
21	Jefe (a) del Programa	Programa de Compensaciones para la Competitividad - AGROIDEAS	Miembro
22	Jefe (a) de la Unidad de Planificación, Seguimiento y Evaluación	Programa de Compensaciones para la Competitividad - AGROIDEAS	Miembro
23	Director (a) de Gestión del Riego	Programa Sub Sectorial de Irrigaciones (PSI)	Miembro
24	Profesional	Programa Sub Sectorial de Irrigaciones (PSI)	Miembro
25	Director (a) de la Unidad de Estudios y Cooperación de la Oficina de Planificación y Desarrollo Institucional	Servicio Nacional de Sanidad Agraria (SENASA)	Miembro
26	Profesional	Servicio Nacional de Sanidad Agraria (SENASA)	Miembro
27	Director (a) General de la Oficina de Planeamiento y Presupuesto	Instituto Nacional de Innovación Agraria (INIA)	Miembro
28	Profesional	Instituto Nacional de Innovación Agraria (INIA)	Miembro
29	Director (a) de Conservación y Planeamiento de Recursos Hídricos	Autoridad Nacional del Agua (ANA)	Miembro

1332846-1

Que, de acuerdo a lo establecido en el numeral 4.8 del artículo 4 y el artículo 49 del Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado por el Decreto Supremo N° 063-2007-PCM, la Presidencia del Consejo de Ministros actúa como ente rector del Sistema Nacional de Informática a través de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), siendo ésta la encargada de implementar la Política Nacional de Gobierno Electrónico e Informática;

Que, el "Plan de Desarrollo de la Sociedad de la Información en el Perú - La Agenda Digital Peruana 2.0" aprobado mediante Decreto Supremo N° 066-2011-PCM, establece en su Objetivo N° 7, la necesidad de promover una Administración Pública de calidad orientada a la población, determinando como parte de su Estrategia N° 4, la implementación de mecanismos para mejorar la seguridad de la información, la necesidad de contar con una Estrategia Nacional de Ciberseguridad con el objetivo de minimizar los riesgos en caso de sufrir algún tipo de incidente en los recursos informáticos del Estado, así como, la disuasión del crimen cibernético, que se producen mediante el uso de redes teleinformáticas, entre otros;

Que, la actual Política Nacional de Gobierno Electrónico 2013 – 2017, aprobada mediante el Decreto Supremo N° 081-2013-PCM, prevé determinados Lineamientos Estratégicos para el Gobierno Electrónico en el Perú, entre otros, el relacionado con la Seguridad de la Información, el mismo que busca velar por la integridad, seguridad y disponibilidad de los datos debiendo establecerse lineamientos de seguridad de la información a fin de mitigar el riesgo de exposición de información sensible del ciudadano, correspondiendo que en uso de las funciones atribuidas al ente rector del Sistema

Nacional de Informática, para el caso ONGEI-PCM, a cargo de implementar dicha Política Nacional, articular la implementación efectiva del acotado lineamiento por parte de los distintos entes del sector público;

Que, estando a lo indicado en los considerandos precedentes la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) de la Presidencia del Consejo de Ministros a través del Memorando N° 152-2015-PCM/ONGEI, recomienda la aplicación y uso de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Requisitos. 2ª Edición", en todas las entidades del Sistema Nacional de Informática, con la finalidad de coadyuvar con la infraestructura de Gobierno Electrónico, por considerar a la seguridad de la información, como un componente crucial para dicho objetivo;

De conformidad con lo dispuesto en la Ley N° 29158, Ley Orgánica del Poder Ejecutivo; la Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado; y, el Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros aprobado mediante Decreto Supremo N° 063-2007-PCM y sus modificatorias;

SE RESUELVE:

Artículo 1.- De la aprobación

Apruébese el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición", en todas las entidades integrantes del Sistema Nacional de Informática.

Artículo 2.- Publicación

La Norma Técnica Peruana NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición" será publicada en el Portal de la Presidencia del Consejo de Ministros (www.pcm.gob.pe) y en el Portal de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) (www.ongei.gob.pe) el mismo día de la publicación de la presente resolución en el Diario Oficial El Peruano.

- El/la responsable de planificación o quien haga sus veces;

- El/la responsable del área de informática o quien haga sus veces;

- El/la responsable de área legal o quien haga sus veces y

- El/la oficial de seguridad de la información.

Las funciones del Comité de Gestión de Seguridad de la Información, serán establecidas por cada entidad de acuerdo a la norma que se aprueba mediante el Artículo 1º de la presente Resolución Ministerial.

Artículo 6.- De la responsabilidad de la implementación

La responsabilidad de la implementación de la presente norma será del titular de cada entidad.

Artículo 7.- Déjese sin efecto

Deróguese la Resolución Ministerial N° 129-2012-PCM.

Regístrese, comuníquese y publíquese.

PEDRO CATERIANO BELLIDO
Presidente del Consejo de Ministros

1333015-1

AGRICULTURA Y RIEGO

Delegan facultades a diversos funcionarios del Ministerio durante el Ejercicio 2016

RESOLUCIÓN MINISTERIAL
N° 0006-2016-MINAGRI

Lima, 12 de enero de 2016

CONSIDERANDO:

Que, mediante la Ley N° 29158, Ley Orgánica del

<p>Artículo 3.- De la implementación Las entidades integrantes del Sistema Nacional de Informática, tendrán un plazo máximo de dos (2) años para la implementación y/o adecuación de la presente norma.</p> <p>Dichas entidades públicas tendrán un plazo de 60 días contados a partir de la fecha de publicación de la presente norma, para la presentación del cronograma de implementación y/o adecuación del sistema de gestión de la Seguridad de la Información, que deberá ser presentado a la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) de la Presidencia del Consejo de Ministros.</p> <p>La ONGEI brindará asistencia técnica a las entidades que lo requieran. Las entidades públicas que a la fecha cuenten con la certificación ISO 27001, están exoneradas del presente proceso de implementación.</p> <p>Artículo 4.- De la certificación de la norma Las entidades que requieran certificarse de acuerdo a lo establecido en la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2 Edición"; podrán realizar dicha certificación de forma opcional y con recursos propios de cada entidad.</p> <p>Artículo 5.- Del Comité de Gestión de Seguridad de la Información Cada entidad designará un Comité de Gestión de Seguridad de la Información, conformado por:</p> <ul style="list-style-type: none"> - El/la titular de la entidad; - El/la responsable de administración o quien haga sus veces; 	<p>Poder Ejecutivo, se definen las funciones generales y la estructura orgánica de los Ministerios, precisando en el último párrafo de su artículo 25, que los Ministros de Estado pueden delegar, en los funcionarios de su cartera ministerial, las facultades y atribuciones que no sean privativas a su función, siempre que la normatividad lo autorice;</p> <p>Que, de acuerdo a lo dispuesto en el último párrafo del artículo 9 del Decreto Legislativo N° 997, Decreto Legislativo que aprueba la Ley de Organización y Funciones del Ministerio de Agricultura, modificado por la Ley N° 30048, en adelante la LOF del MINAGRI, el Ministro puede delegar las facultades y atribuciones que no sean privativas a su función;</p> <p>Que, el tercer párrafo del literal c) del artículo 8 de la Ley N° 30225, Ley de Contrataciones del Estado, señala que el Titular de la Entidad podrá delegar, mediante resolución, la autoridad que dicha Ley le otorga, salvo los casos expresamente previstos en el referido literal;</p> <p>Que, según el numeral 7.1 del artículo 7 del Texto Único Ordenado de la Ley N° 28411, Ley General del Sistema Nacional de Presupuesto, aprobado mediante Decreto Supremo N° 304-2012-EF, el Titular de una Entidad es la más alta Autoridad Ejecutiva y puede delegar sus funciones en materia presupuestal cuando lo establezca expresamente, entre otras, la citada Ley General;</p> <p>Que, asimismo, el numeral 40.2 del artículo 40 del referido Texto Único Ordenado de la Ley N° 28411, establece que las modificaciones presupuestarias en el nivel Funcional Programático son aprobadas mediante Resolución del Titular, a propuesta de la Oficina de Presupuesto o de la que haga sus veces en la Entidad, y que el Titular puede delegar dicha facultad de aprobación, a través de disposición expresa, la misma que debe ser publicada en el Diario Oficial El Peruano;</p>
--	--

ANEXO XII: Taller de Implementación de la norma ISO/IEC 27001

Fase I Organización

Desarrollar las actividades principales para la dirección e inicio de la implantación del SGSI.

- Obtener el apoyo institucional
- Determinar el alcance del Sistema de Gestión de Seguridad de la Información
- Determinar la declaración de Política de Seguridad de la Información y objetivos
- Determinar criterios para la evaluación y aceptación de riesgos

Organización de la Seguridad

ANEXO XIII: Estructura Organizacional del SGSI-Curso UPC

Organización del SGSI

SGSI - 06 Definición de las políticas, Organización, Alcance..flv

Seguridad de la Información

5

Estructura Organizacional de Seguridad

- Uno de los factores claves para diseñar e implementar un SGSI es el compromiso y participación y de la Alta Dirección con respecto a la gestión de la Seguridad de la Información.
- Este compromiso se debe materializar en el establecimiento de una **Política de Seguridad de la Información**, la cual deberá ser el punto de partida para establecer el SGSI.
- Es necesario también establecer los **roles y responsabilidades del personal** en materia de Seguridad de la Información.
- Para ello será necesario conformar un **Comité de Gestión de Seguridad de la Información**, un **Comité Operativo o Grupo Interdisciplinario**, así como, el rol del **Oficial de Seguridad de la Información**.

```
graph TD; AD[Alta Dirección] --> UTI[Unidad de Tecnología de la Información]; UTI --> OA[Oficina de Administración]; UTI --> OAJ[Oficina de Asesoría Jurídica]; UTI --> OPP[Oficina de Planeamiento Presupuesto];
```

Seguridad de la Información

6

Estructura Organizacional del SGSI

Comité de Gestión de Seguridad de la Información
(CGSI)

Gerencia General, Gerentes de línea

Grupo Interdisciplinario de Seguridad de la Información
(GSI)

- Jefes de Área, Supervisores

Oficial de Seguridad de la Información

Propietarios, Custodios, Usuarios

ANEXO XIV: Inclusiones en la norma ISO/IEC 27001

respecto a su norma antecesora

ISO 27001 2013: Los riesgos y las oportunidades

26 julio, 2016 ISO 27001:2013

ISO 27001 2013

El tema sobre el que queremos hablar hoy es la **visión que ofrece la norma ISO 27001 2013** sobre el análisis de riesgos. Un tema que se desarrollaba en la norma ISO 27001 2007 pero que ha sufrido algunos cambios muy relevantes.

- **Oportunidades y apreciación de riesgos:** la empresa no sólo debe centrarse en los riesgos encontrados, sino que el análisis de riesgos debe ser la base para cumplir con el objetivo de mejora continua y, en el caso de detectar anomalías en la operaciones se deberán corregir e **implantar acciones para evitar posibles amenazas** en el proceso. Además, esto puede ser de utilidad a la hora de revisar los sistemas o procesos en los cuales se pueden encontrar oportunidades de mejora, independientemente de si los riesgos identificados pueden implicar un fallo del servicio de la calidad de la prestación del mismo.
- **Enfoque a procesos:** la apreciación de los riesgos debe ser sistematizada y orientada a los procesos, es decir, es necesario integrarlo en el día a día de la empresa. Esto no supone que las apreciaciones de riesgos se deban hacer a diario, pero sí se deben tener en cuenta los aspectos, reportando a los responsables de seguridad, para que en sus revisiones periódicas pongan dichas incidencias sobre la mesa. El objetivo que se persigue es la mejora continua de los procesos.
- **Dueños de los riesgos:** en la apreciación de riesgos y su posterior evaluación se deben determinar todos los responsables que se van a encargar de dirigir y controlar las acciones de mejora para que **exista una trazabilidad y no se detecten riesgos** que luego no vayan a ser tratados, controlados y evaluados. De ahí la figura del responsable del riesgo.
- **Criterios de aceptación de riesgos:** este aspecto ya se incluye en la norma ISO 27001 2007 y la ISO 27001 2013 se encarga de reforzarlo, obligando a la alta dirección a establecer ciertos criterios **para el tratamiento de riesgos**, por lo que aquellos riesgos que superen el umbral objetivo marcado, deberán ser tratados o gestionados.
- **Tratamiento de riesgos:** se puede tomar como referencia el Anexo A de la norma ISO 27001 2013 que incluye un listado de controles que sirve para orientarse en las posibles **acciones a efectuar para disminuir los riesgos**. Estas acciones pueden formar parte de un plan mucho más complejo, llamado Plan de Tratamiento de Riesgos el cual debe contener todas las acciones planificadas, con sus dueños y responsables en los que se intenta, mediante salvaguardar técnicas, reducir el impacto de las amenazas sobre los activos de información.
- **Declaración de aplicabilidad:** la declaración de aplicabilidad es otro de los aspectos que ganan en importancia y relevancia. **Incorpora todos los controles implantados** y, por lo tanto, es un aspecto que no debe ser pasado por alto, ya que proporciona una guía para la apreciación, la gestión de riesgos y las oportunidades.

ANEXO XV: Resolución Ministerial N° 166-2017-PCM

6

NORMAS LEGALES

Miércoles 21 de junio de 2017 / El Peruano

IVIA) y el componente 3 (esquemas competitivos de Asignación Integral y de Asignación Independiente para Propuestas de I+D y de I+D+i en Áreas Prioritarias y Áreas Generales de Conocimiento).

- Aquellas funciones que se encuentren en el Acuerdo de Préstamo N° 8682-PE y otras establecidas en la normativa de la materia.

Artículo 4.- Secretaría Técnica

La Secretaría Técnica del grupo de trabajo recae en el Director Ejecutivo del Fondo Nacional de Desarrollo Científico y de Innovación Tecnológica – FONDECYT.

Artículo 5.- Instalación y periodo de vigencia

En el plazo no mayor de tres (3) días hábiles contado desde el día hábil siguiente de la publicación de la presente Resolución, el grupo de trabajo debe proceder a su instalación, y ejerce sus funciones hasta la fecha de cierre del Proyecto.

Artículo 6.- De la aprobación del Reglamento Interno

El grupo de trabajo aprueba su Reglamento Interno en un plazo no mayor a quince (15) días hábiles, contados a partir del día hábil siguiente de su instalación.

Artículo 7.- Gastos

Los integrantes del grupo de trabajo ejercen el cargo ad honorem. Los gastos que demande la participación de los integrantes del grupo de trabajo, en cumplimiento a sus funciones, son cubiertos con cargo a los presupuestos institucionales de las entidades e instituciones a los que representan, no irrogando gastos adicionales al Tesoro Público.

Artículo 8.- Publicación

Dispóngase la publicación de la presente Resolución Ministerial en el Diario Oficial El Peruano, asimismo en el Portal Institucional de la Presidencia del Consejo de Ministros (www.pcm.gob.pe); del Consejo Nacional de Ciencia, Tecnología e Innovación Tecnológica – CONCYTEC, (www.concytec.gob.pe); y del Fondo Nacional de Desarrollo Científico y de Innovación Tecnológica – FONDECYT (www.cienciaactiva.gob.pe).

Regístrese, comuníquese y publíquese.

FERNANDO ZAVALA LOMBARDI
Presidente del Consejo de Ministros

1535494-1

Modifican el artículo 5 de la R.M. N° 004-2016-PCM referente al Comité de Gestión de Seguridad de la Información

RESOLUCIÓN MINISTERIAL N° 166-2017-PCM

Lima, 20 de junio de 2017

CONSIDERANDO:

Que, mediante Resolución Ministerial N° 004-2016-PCM se aprobó el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 - Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición", en todas las entidades integrantes del Sistema Nacional de Informática;

Que, el Comité de Gestión de Seguridad de la Información debe contar con el liderazgo y compromiso necesario para la implementación de la citada Norma Técnica Peruana, por lo que resulta relevante precisar sus funciones tomando como referencia lo establecido en el numeral 5.1 de la NTP-ISO/IEC 27001:2014 - Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición;

Que, se requiere priorizar la implementación del Sistema de Gestión de Seguridad de la Información en las entidades públicas, sobre todo en sus procesos misionales y de soporte que resulten críticos y relevantes para su operatividad, siendo necesario contar para ello con el rol del Oficial de Seguridad de la Información, como responsable de coordinar la implementación de dicho Sistema, ello con la finalidad de coadyuvar al desarrollo del Gobierno Electrónico y la Digitalización del Estado;

Que, de acuerdo a lo establecido en los artículos 47 y 51 del Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado mediante Decreto Supremo N° 022-2017-PCM, la Presidencia del Consejo de Ministros actúa como ente rector del Sistema Nacional de Informática a través de la Secretaría de Gobierno Digital (SEGDI), siendo ésta la encargada de formular y proponer normas y estándares para el desarrollo e implementación de la Seguridad de la Información, así como de supervisar su cumplimiento, resulta pertinente modificar el artículo 5 de la Resolución Ministerial N° 004-2016-PCM a fin de que el Comité de Gestión de Seguridad de la Información se encuentre conformado por los funcionarios y/o directivos competentes para la ejecución de sus funciones;

De conformidad con lo dispuesto en la Ley N° 29158, Ley Orgánica del Poder Ejecutivo, y el Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros aprobado mediante Decreto Supremo N° 022-2017-PCM;

SE RESUELVE:

Artículo 1.- Modificación del artículo 5 de la Resolución Ministerial N° 004-2016-PCM.

Modifíquese el artículo 5 de la Resolución Ministerial N° 004-2016-PCM, en los términos siguientes:

"Artículo 5.- Del Comité de Gestión de Seguridad de la Información

Cada entidad designará un Comité de Gestión de Seguridad de la Información, conformado como mínimo por:

- El/la titular de la entidad o su representante.
- El/la responsable de administración o quien haga sus veces;
- El/la responsable de planificación o quien haga sus veces;
- El/la responsable del área de informática o quien haga sus veces;
- El/la responsable de área legal o quien haga sus veces y
- El/la oficial de seguridad de la información."

Artículo 2.- Incorporación del artículo 5-A a la Resolución Ministerial N° 004-2016-PCM.

Incorpórese el artículo 5-A a la Resolución Ministerial N° 004-2016-PCM, conforme al siguiente texto:

"Artículo 5-A.- De las Funciones del Comité de Gestión de Seguridad de la Información

El Comité de Gestión de Seguridad de la Información debe cumplir, como mínimo, las siguientes funciones:

- a) Proponer la política y objetivos de seguridad de la información alineados con el Plan Estratégico Institucional, con la Política Nacional de Gobierno Electrónico y regulación en el ámbito de seguridad de la información;
- b) Promover y gestionar la implementación del Sistema de Gestión de Seguridad de la Información;
- c) Promover la gestión de seguridad de la información en los procesos y cultura organizacional;
- d) Gestionar la asignación del personal y recursos necesarios para la implementación del Sistema de Gestión de Seguridad de la Información;
- e) Difundir la importancia de una efectiva gestión de seguridad de la información a las partes interesadas, en conformidad con los requisitos del Sistema de Gestión de Seguridad de la Información;
- f) Evaluar el desempeño del Sistema de Gestión de Seguridad de la Información;

g) Otras funciones que se le asigne en el ámbito de su competencia y aquellas concordantes con la materia."

Artículo 3.- Priorización del Alcance del Sistema de Gestión de Seguridad de la Información

Las entidades comprendidas en el artículo 1 de la Resolución Ministerial N° 004-2016-PCM deben asegurar la implementación del Sistema de Gestión de Seguridad de la Información en su institución, priorizando en el alcance los procesos misionales y aquellos que sean relevantes para su operatividad.

Artículo 4.- Del Oficial de Seguridad de la Información

El Titular de entidad, dentro del plazo de diez (10) días hábiles, contados a partir de la publicación de la presente resolución, debe designar a un Oficial de Seguridad de la Información, quien será responsable de coordinar la implementación del Sistema de Gestión de Seguridad de la Información en la entidad.

Dicha designación debe ser puesta en conocimiento a la Secretaría de Gobierno Digital para las coordinaciones y acciones correspondientes.

Regístrese, comuníquese y publíquese.

FERNANDO ZAVALA LOMBARDI
Presidente del Consejo de Ministros

1535494-2

Que, mediante Resolución Suprema N° 004-2016-MINAM, se conforma el Grupo de Trabajo de la Comisión Multisectorial Ambiental, que depende del Ministerio del Ambiente, cuyo objeto es revisar y evaluar las recomendaciones del Estudio del Desempeño Ambiental del Perú CEPAL/OCDE, así como elaborar un plan de acción para su implementación;

Que, mediante el Acta N° 05-GTCMA/2016, el Grupo de Trabajo de la Comisión Multisectorial Ambiental aprobó la versión validada del Plan de Acción para implementar las Recomendaciones de la Evaluación de Desempeño Ambiental del Perú;

Que, la Comisión Multisectorial Ambiental tiene entre sus funciones coordinar y concertar políticas en materia ambiental, de acuerdo a lo dispuesto en el artículo 27 del Reglamento de la Ley N° 28245, Ley Marco del Sistema Nacional de Gestión Ambiental, aprobado por Decreto Supremo N° 008-2005-PCM, y en el artículo 15 del Reglamento de Organización y Funciones del Ministerio del Ambiente, aprobado por Decreto Supremo N° 007-2008-MINAM;

Que, resulta necesario que el Ministerio del Ambiente efectúe las acciones de seguimiento y monitoreo a la ejecución del precitado Plan, en el marco de la Comisión Multisectorial Ambiental, en la medida que las acciones estratégicas de dicho Plan de Acción se vinculan a las competencias de distintas entidades del Estado;

De conformidad con el numeral 8) del artículo 118 de la Constitución Política del Perú; el numeral 3 del artículo 11 de la Ley N° 29158, Ley Orgánica del Poder Ejecutivo;

ANEXO XVI : Encuesta sobre el desempeño de la Estructura Organizacional del Sistema de Gestión de Seguridad de la Información

Dirigido a personal Administrativo, Operativo y Consultivo de la Organización.

Objetivos:

- Conocer si el personal que integra la organización conocen la existencia de la Estructura Organizacional del Sistema de Gestión de Seguridad de la Información
- Conocer si el personal que integra la organización conocen las labores y funciones de la Estructura Organizacional del Sistema de Gestión de Seguridad de la Información
- Conocer como personal de la organización percibe el desempeño de las labores y funciones de la Estructura Organizacional del Sistema de Gestión de Seguridad de la Información
- Evaluar el desempeño de las labores y funciones de la Estructura Organizacional del Sistema de Gestión de Seguridad de la Información

Instrucciones:

Para desarrollar este cuestionario, cada colaborador de la organización debe leer cada pregunta y escoger una de las alternativas propuestas con una “X” dentro de los paréntesis o llenar dentro de las líneas punteadas según sea su criterio.

1. Sexo:
Masculino () Femenino ()
2. Cargo del Informante:
3. A qué departamento de la organización pertenece:
.....
4. ¿Le han indicado o comentado alguna vez que existe una Estructura Organizacional del Sistema de Gestión de Seguridad de la Información?:
SI () NO ()
Si su respuesta es **SI**; ¿Sabe cómo está compuesta?

SI () NO ()

Suponiendo que conoce que existe una Estructura organizacional del Sistema de Gestión de Seguridad de la Información. Responda las siguientes preguntas:

5. ¿Conoce cuáles son las labores y funciones que desempeña el Comité de Gestión de Seguridad de la Información (CGSI)?

SI () NO ()

Si su respuesta es **SI**; ¿Cree que las cumple a cabalidad?

SI () NO ()

¿Sabe cuáles son sus miembros?

SI () NO ()

Si su respuesta es **SI**; Indique por favor quien o quienes la componen:

.....

6. ¿Conoce cuáles son las labores y funciones que desempeña el Grupo Interdisciplinario de Seguridad de la Información (GISI)?

SI () NO ()

Si su respuesta es **SI**; ¿Cree que las cumple a cabalidad?

SI () NO ()

¿Sabe cuáles son sus miembros?

SI () NO ()

Si su respuesta es **SI**; Indique por favor quien o quienes la componen:

.....

SI () NO ()

7. ¿Conoce cuáles son las labores y funciones que desempeña el Oficial de Seguridad de la Información (OSI)?

SI () NO ()

Si su respuesta es **SI**; ¿Cree que las cumple a cabalidad?

SI () NO ()

¿Sabe cuáles son sus miembros?

SI () NO ()

Si su respuesta es **SI**; Indique por favor quien o quienes la componen:

.....

SI () NO ()

8. ¿Conoce cuáles son las labores y funciones que desempeña los Propietarios de Activos de la Información?

SI () NO ()

Si su respuesta es **SI**; ¿Cree que las cumple a cabalidad?

SI () NO ()

¿Sabe cuáles son sus miembros?

SI () NO ()

Si su respuesta es **SI**; Indique por favor quien o quienes la componen:

.....

SI () NO ()

9. ¿Conoce cuáles son las labores y funciones que desempeña los Custodios de Activos de la Información?

SI () NO ()

Si su respuesta es **SI**; ¿Cree que las cumple a cabalidad?

SI () NO ()

¿Sabe cuáles son sus miembros?

SI () NO ()

Si su respuesta es **SI**; Indique por favor quien o quienes la componen:

.....

SI () NO ()

10. ¿Conoce cuáles son las labores y funciones que desempeña los Usuarios de Activos de Información?

SI () NO ()

Si su respuesta es **SI**; ¿Cree que las cumple a cabalidad?

SI () NO ()

¿Sabe cuáles son sus miembros?

SI () NO ()

¿Sabe que Ud. es uno de sus miembros?

SI () NO ()

Indique por favor quien o quienes la componen:

.....

SI () NO ()

11. ¿Considera Usted que existe un ciclo de mejora continua en los procesos obtenidos para la mejora en la salvaguarda de los activos de la información y en si todo lo referido a Seguridad de la información, esto liderado por la Estructura Organizacional de la Seguridad de la Información?

SI () NO () No lo sé () No opina ()

12. ¿De qué forma considera Usted que cada componente de la Estructura Organizacional de la Seguridad de la Información realiza el seguimiento de actividades relacionadas a Seguridad de la Información?

.....
.....

13. ¿Ha recibido Usted algún acercamiento de algún componente de la Estructura Organizacional de la Seguridad de la Información?

Si su respuesta es **SI**; ¿Cree que ha sido provechoso para el mejor desempeño de la Seguridad de la Información y la salvaguarda de activos?

SI () NO ()

14. ¿Considera Usted que existe influencia directa de la Alta Dirección en la toma de decisiones de cada componente de la Estructura Organizacional de la Seguridad de la Información, es decir no son componentes autónomos?

A veces () Casi siempre () Siempre () Nunca ()

15. ¿Qué falencias cree Usted que cuenta la estructura organizacional de Sistema de Gestión de Seguridad de la Información consultada? ¿Qué recomendaría Usted para mejorar la organización de la Seguridad de la Información?

.....
.....

ANEXO A: Manual del Sistema de Gestión de Seguridad de la Información

1. Introducción

Como preservar la Seguridad de los activos de información es un problema actual que sufren la gran parte de organizaciones en el mundo. Es difícil crear conciencia sobre cultural organizaciones en Seguridad de la Información y crear lineamientos que preserven una correcta gestión sobre la información. En base a ello, la organización ha creído conveniente la adopción de un Sistema de Gestión de Seguridad de la Información (SGSI) que permita gestionar de manera adecuada la Seguridad de sus activos de información. Asimismo, lograr garantizar que los riesgos de la seguridad sobre los propios activos de información sean conocidos, asumidos, gestionados y minimizados por la misma.

En base a lo comentado, este manual permite detallar que procedimientos ejecuta la organización para alinear el proceso de negocio del área de Servicio Post-Venta con los objetivos de seguridad de la información que la componen, buscando agregar valor a sus accionistas, clientes y colaboradores, los cuales han depositado en la misma la confianza en el manejo de su Infraestructura Tecnológica.

2. Objetivo

El objetivo del presente Manual del Sistema de Gestión de Seguridad de la Información es mostrar las directivas, acciones, lineamientos y políticas a seguir para la posterior implementación de un Sistema de Gestión de Seguridad de la Información. Lo comentado, con el objetivo principal de minimizar las vulnerabilidades y amenazas de seguridad de la información presentes sobre los activos de información de la organización.

3. Alcance del Manual de Seguridad de la Información

El alcance del presente manual, el cual se basa en los lineamientos solicitados por la norma ISO/IEC 27001:2013 y tiene como alcance los procesos embebidos en el área de Servicio Post-Venta de la organización. Asimismo, el contenido del presente manual como información e instructivo aplica a todo el personal o colaboradores de la organización.

4. Sistema de Gestión de Seguridad de la Información

4.1. Visión General

La organización al tener en cuenta la gran dependencia sobre sus Sistemas de Información y la información que maneja, propia y de clientes, ha decidido adoptar un Sistema de Gestión de Seguridad de la Información soportada por los lineamientos de la norma ISO/IEC 27001 en su versión 2013. Ello como una decisión estratégica y diferenciadora de negocio, la cual es influenciada por las necesidades, objetivos, requisitos de seguridad y los procesos de la organización, específicamente el área de Servicios Post-Venta de la misma. En base a lo comentado, se presentan a continuación los lineamientos estratégicos por los cuales se rige la organización, los cuales apoyan al Sistema de Gestión de Seguridad de la Información.

4.2. Alcance

Cumplir con los pilares de la Seguridad de la Información, preservando la Confidencialidad, integridad y disponibilidad de los activos de información y la propia información que se maneja en el área de Servicios Post-Venta.

4.3. Política de Seguridad de la Información

La Política de Seguridad de la Información se encuentra desarrollada en el Anexo B, incluida al presente proyecto. Asimismo, la Política de Seguridad de la Información tiene como finalidad dictar en cumplimiento de las disposiciones legales vigentes y como ejecutar el proceso de gestión adecuado para la Seguridad de la Información dentro de la organización, específicamente a los activos de información y propia información del área de Servicios Post-Venta que aplica.

Por otro lado, el alcance de difusión, conocimiento y cumplimiento de la Política de Seguridad de la Información aplica a todo el personal o colaboradores de la organización.

4.4. Compromiso de la Dirección

El compromiso de la Alta Dirección en la organización es vital para el éxito del Sistema de Gestión de Seguridad de la Información. Por ello, la Alta Dirección cuenta con un alto compromiso con la Seguridad de la Información y adopta las fases que la componen: Planear, Hacer, Monitorear y Actuar sobre las mejoras teniendo un ciclo continuo de mejora. Tener en cuenta que la finalidad del proyecto en estudio es

realizar el Diseño de un SGSI, dejando el lineamiento para su posterior implementación. En base a ello, la dirección cuenta con los siguientes compromisos:

- Tener conocimiento y consideración de los controles que integran el anexo A de la norma ISO/IEC 27001:2013, es decir la ISO/IEC 27002.
- Comunicar los requerimientos de la norma ISO/IEC 27001:2013 a los Gerentes o Jefes de área y ellos a los demás colaboradores de la organización a su cargo.
- Realizar capacitaciones sobre concientización de Seguridad de la Información al personal de la organización.
- Asignar los recursos necesarios para que la organización oriente su esfuerzo a minimizar la ocurrencia e impacto de los eventos de riesgo de seguridad sobre los activos de información que comprenden el área de Servicios Post-Venta de la empresa. Es decir, asignar los recursos necesarios para cumplir con los controles que apliquen del Anexo A de la norma ISO/IEC 27001:2013.
- Si bien es cierto la Alta Dirección no integra el Comité de Gestión de Seguridad de la Información (CGSI), la Alta Dirección delegará sobre este CGSI la responsabilidad de establecer las políticas y directrices a seguir en el Sistema de Gestión de Seguridad de la Información, supervisando en todo momento su desempeño, tomando las acciones que la Alta dirección crea necesario para alienarlo a sus objetivos trazados en materia de Seguridad de la Información.
- Asignar la responsabilidad al Dueño del Riesgo realizar el seguimiento de las medidas adoptadas por la organización en la labor de reducción del riesgo sobre los activos de información. Asimismo, con el seguimiento y pruebas realizadas el Propietario del Riesgos deberá evaluar la efectividad de los controles ejecutados aplicables indicados en la Declaración de Aplicabilidad (SOA).
- Asignar al Oficial de Seguridad de la Información el cual tendrá la función de proponer metodologías, procedimientos, estatutos, herramientas, planes, programas y procesos para la seguridad de la información dentro de la organización. Asimismo, dar apoyo al Dueño del Riesgo en la evaluación de controles ejecutados aplicables indicados en la Declaración de Aplicabilidad (SOA).

4.5. Planificación del SGSI

Si bien es cierto que el presente proyecto establece el Diseño de un Sistema de Gestión de Seguridad de la Información para la organización, existen cuatro (04)

etapas para su puesta en marcha y revisión posterior a su implementación. Estas etapas son:

- Planificación del Sistema de Gestión de Seguridad de la Información
- Implementación del Sistema de Gestión de Seguridad de la Información
- Evaluación del Sistema de Gestión de Seguridad de la Información mediante auditorías internas y externas
- Mejora continua del Sistema de Gestión de Seguridad de la Información mediante la retroalimentación de la etapa previa de la evaluación de la misma

Cabe indicar que el presente proyecto tiene como alcance la Planificación del Sistema de Gestión de Seguridad de la Información, dejando a un segundo nivel la posterior implementación del mismo.

5. Valoración del riesgo por parte de la Organización

5.1. Metodología para la Evaluación de Riesgos

La organización aplica una metodología propia para la evaluación de riesgos de Seguridad de la Información, tomando unas síntesis de metodología adoptadas en el mercado como Magerit, Mehari, entre otras. Esta metodología tiene en consideración las siguientes fases:

- Identificación de Activos de Información
- Valoración de Activos de Información
- Análisis Identificación de Vulnerabilidades y Amenazas sobre los activos de Información
- Análisis y Evaluación de Riesgos sobre los Activos de Información
- Matriz de Riesgos sobre los Activos de Información
- Opciones de Tratamiento de Riesgos sobre los activos de Información

5.2. Criterios para la Evaluación de Riesgos

La organización toma en cuenta las siguientes consideraciones para la evaluación de los riesgos sobre los activos de información:

- La identificación de los riesgos se hará en base al juicio de expertos, es decir el personal que esta involucrado en el proceso donde interviene cada activo de información valorizado.

- Personal calificado en Seguridad de la Información, lo cual de una visión global de los riesgos inminentes sobre los activos de información.
- Documentación y buenas prácticas usadas en el mercado sobre los riesgos de información sobre activos de información. Ello creara conciencia en cuanto a los riesgos que puedan estar sujetos los activos de información y qué medidas adoptar en primera instancia.

Por otro lado, la valoración del riesgo sobre el activo de información se muestra a continuación:

Valores de Riesgo				
Escala		Valor	Nivel de aceptación del riesgo	
Muy Bajo	1-2	1	Insignificante	Riesgo aceptable para la empresa u organización
Bajo	3-6	2	Insignificante	Riesgo aceptable para la empresa u organización
Medio	7-9	3	Considerable	Riesgo inaceptable para la empresa u organización, se necesita la ejecución de un control de seguridad
Alto	10-16	4	Considerable	Riesgo inaceptable para la empresa u organización, se necesita la ejecución de un control de seguridad
Muy Alto	17-25	5	Importante	Riesgo inaceptable para la empresa u organización, se necesita la ejecución de un control de seguridad

En base al cuadro mostrado la organización tomara la decisión de alguna opción de tratamiento de riesgos solo para los que apliquen como “Considerable” e “Importante”.

5.3. Opciones de Tratamiento de Riesgos

Las opciones de tratamiento de riesgos adoptada por la organización se comenta a continuación:

- **Reducción del Riesgo:** Cuando la organización reduce los niveles de riesgo a niveles aceptables para la misma, aplicando controles de seguridad que sean acordes a los objetivos de negocio previamente identificados.
- **Aceptación del Riesgo:** Cuando la organización no encuentra controles para mitigar el riesgo efectivo y la misma optan por la aceptación del riesgo previa documentación, en donde se indique los criterios utilizados para tal efecto.

- **Transferencia del Riesgo:** Cuando para la organización es complicado reducir o controlar el riesgo a un nivel aceptable.
- **Eliminación del Riesgo:** Implica la eliminación de un activo, proceso o área de negocio que es fuente del riesgo para un activo o grupo de activos.

5.4. Plan de Tratamiento de Riesgos

Las opciones de tratamiento de riesgos adoptada por la organización se comenta a continuación:

Acto seguido de haber efectuado el Análisis de Riesgos sobre los activos de información el Comité de Gestión de Seguridad de la Información (CGSI), el Oficial de Seguridad de la Información y el área involucrada sobre el riesgo del activo de información deberán reunirse y efectuar un plan de tratamiento de riesgos para los riesgos considerados como “Considerables” o “Importantes”, tal como se mostró en la tabla anterior. Asimismo, el Plan de Tratamiento de Riesgo tendrá el siguiente formato:

Ítem	Activo de Información	Interpretación del Riesgo	Nivel de Aceptación de Riesgos	Amenaza / Riesgo	Opción de Tratamiento del Riesgo	Dueño del Riesgo
------	-----------------------	---------------------------	--------------------------------	------------------	----------------------------------	------------------

6. Declaración de Aplicabilidad

La Declaración de Aplicabilidad o SOA (Statement of Applicability) brinda un resumen de las decisiones que la organización cree conveniente adoptar en cuanto al tratamiento de los riesgos de seguridad sobre los activos de información. Asimismo, en la propia Declaración de Aplicabilidad se justifica la aplicabilidad o no aplicabilidad del control de seguridad en la organización. La declaración de Aplicabilidad del Sistema de Gestión de Seguridad de la Información de la organización se encuentra dentro del presente proyecto.

7. Requisitos de Documentación

La organización dentro de su Estructura del Sistema de Gestión de Seguridad de la Información delega como responsabilidad al Comité de Gestión de Seguridad de la Información (GISI) y al propio Oficial de Seguridad de la Información los lineamientos de gestión documental, definidos bajo las siguientes acciones de gestión necesarias:

- Revisar, aprobar y actualizar, de ser necesario, los documentos que integran el Sistema de Gestión de Seguridad de la Información. Estas acciones deben tomarse en cuenta antes de su publicación las veces que apliquen.
- Asegurar la fácil comprensión, identificación y comprensión de objetivos que persigue los documentos de Seguridad de la Información.
- Asegurar la disponibilidad y distribución de los documentos que confirman la Gestión de Seguridad de la Información, en base a los privilegios de acceso del personal solicitante.
- Tener un control adecuado y eficaz de documentos obsoletos que integran el Sistema de Gestión de Seguridad de la Información. Asimismo, dar de baja los documentos obsoletos y/o actualizarlos según sea necesario.

8. Políticas del Sistema de Gestión de Seguridad de la Información

Las Políticas que componen en Sistema de Gestión de Seguridad de la Información son de obligatorio cumplimiento para todo el personal y colaboradores de la organización. Estas políticas tienen el propósito de establecer las acciones necesarias para la protección de la información de los activos de información que componen el área de Servicios Post-Venta de la organización. Las Políticas que las integran son la siguiente:

- Política de Seguridad de la Información – Especificada en el Anexo B
- Política de Control de Acceso - Especificada en el Anexo C
- Política de Uso Aceptable de los Sistema de Información, Internet y Correo Electrónico - Especificada en el Anexo D
- Política de Puesto de Trabajo despejado y Bloqueo de Pantalla - Especificada en el Anexo E
- Política de Teletrabajo - Especificada en el Anexo F
- Política de Gestión de Incidentes de Seguridad de la Información - Especificada en el Anexo G
- Política y Procedimientos de Intercambio de Información - Especificada en el Anexo H

9. Seguimiento y revisión del SGSI

Aunque el presente proyecto tiene como finalidad realizar el Diseño de un Sistema de Gestión de Seguridad de la Información, la organización tendrá en cuenta auditorías

internas y externas después de implementado el SGSI. Ello con la finalidad de evaluar su desempeño y cumplimiento de lo establecido en el mismo.

10. Mantener la Seguridad de la Información en Niveles Óptimos

Para lo comentado, es necesario evaluar constantemente el desempeño y efectividad del Sistema de Gestión de Seguridad de la Información (SGSI). Asimismo, debe evaluar el sistema de gestión va acorde a los niveles de exigencia de la Organización, al igual que persiga los objetivos organizacionales previamente trazados. Para ello, debe tomar en cuenta el desarrollo del contenido de la norma ISO/IEC 27001:2013, como también el Código de Buenas Practicas, llamado también la Norma ISO/IEC 27002:2013.

11. Incumplimiento

El incumplimiento de lo indicado en el presente Manual de Seguridad de la Información tendrá como resultado la aplicación de diversas sanciones, conforme a la magnitud y característica del aspecto no cumplido. Asimismo, un empleado que se descubra que ha violado algún ítem incluido en este manual estará sujeto a medidas disciplinarias que pueden incluir el despido o alguna otra acción que la organización crea conveniente.

12. Historial de Revisiones

Fecha de Cambio	Responsable	Resumen de Cambios

13. Documentos y Registros Asociados

Nombre de Documento	Ubicación de Almacenamiento	Propietario	Control de Protección	Programación de Retención
Indicados en el Anexo	File Server	Organización	Restringido	4 años

14. Gestión de Documentos

Este documento es válido desde 12/Diciembre/2017. Este documento se revisa periódicamente y por lo menos una vez al año para garantizar que se cumplen los siguientes criterios establecidos:

- Conformidad con los requisitos de la norma ISO 27001:2013
- Requisitos legislativos definidos por la ley que corresponda

ANEXO B : Política de Seguridad de la Información

1. Introducción

La información es un recurso que, como el resto de los activos, tiene valor importante para la organización. Por ello, consiguiente debe ser debidamente protegida, garantizando la continuidad de los sistemas de información, minimizando los riesgos de daño y contribuyendo de esta manera, al cumplimiento de los objetivos de negocio previamente trazados por la organización.

Para que estos principios de la Política de Seguridad de la Información sean efectivos, es transcendental la implementación de una Política de Seguridad de la Información que forme parte de la cultura organizacional de la Organización. Lo comentado implica un compromiso de todos los trabajadores de la Organización, para contribuir a la difusión, consolidación y cumplimiento de su contenido.

Como consecuencia de lo expuesto, la Organización ha creído conveniente la adopción de políticas para seguridad de la Información que contribuyan al correcto resguardo de los activos de información seleccionados. Asimismo, ha utilizado como guía de buenas prácticas, la adopción de controles especificados en la ISO/IEC 27002:2013, para la aplicabilidad de controles necesarios, después de definir y realizar el análisis de riesgos a los que se encuentran asociados los activos de información seleccionados.

2. Términos y Definiciones Operativas

Con el objeto de precisar el alcance de los principales conceptos utilizados en el presente documento, se comentan las definiciones de los términos más utilizados, esto para una mayor comprensión y entendimiento.

2.1. Seguridad de la Información

Definida como la preservación de los pilares de los siguientes pilares:

- **Confidencialidad:** Garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- **Integridad:** Salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

- Disponibilidad: Garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requiera.
- Adicionalmente, deberán considerarse los conceptos de:
- Autenticidad: Tiene como principal meta asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
- Auditabilidad: Define que todos los eventos de un sistema deben poder ser registrados para su control posterior.
- Protección a la duplicación: Consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
- No repudio: Evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
- Legalidad: Cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organización.
- Confiabilidad de la Información: La información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las funciones.

2.2. Información

Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

2.3. Sistema de Gestión de Seguridad de la Información

Sistema de Gestión de una Organización, con base en un enfoque de riesgos, que tiene como función establecer, implementar, operar y supervisar la seguridad de la información, en un ciclo de mejora continua.

3. Políticas de Seguridad de la Información

3.1. Objetivos

- Proteger los recursos de información de Organización, resguardando de manera correcta los activos de información, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de los pilares de la Seguridad de la Información: confidencialidad, integridad, disponibilidad para la totalidad de activos de la información seleccionados. Asimismo, se pretende conservar la legalidad y confiabilidad de la información.
- Asegurar la implementación de las medidas de seguridad comprendidas en esta Política. En consecuencia, es obligación de los miembros de la Estructura Organizacional de Gestión de Seguridad de la Información velar por el cumplimiento de los controles seleccionados e implantados. Asimismo, otras medidas de seguridad de la información que se encuentren especificadas en el presente documento.
- Mantener la Política de Seguridad de la Organización actualizada para asegurar su vigencia y nivel de eficacia.

3.2. Alcance

Esta Política se aplica en todo el ámbito de la organización, a sus recursos y a la totalidad de los procesos, ya sean internos o externos vinculados a la organización a través de contratos o acuerdos con terceros. En base a ello, el nivel de aplicabilidad de la política es:

- Los sistemas que pertenecen o están bajo control de la organización.
- Información almacenada o en uso dentro de cada activo de información perteneciente a la organización
- Información de la organización en tránsito a través de medios de redes de voz o datos
- Control de Información en la organización y los propios recursos de acceso a la información
- Todas las personas involucradas en el acceso o el uso de sistemas de información de la organización, lo cual incluye: personal, contratistas y cualquier otra parte que haga uso de los recursos de la organización.
- La aplicación de esta política se aplica a lo largo del ciclo de vida de la información desde la adquisición / creación, utilización, almacenamiento y/o eliminación.

3.3. Declaración de Política

La política de seguridad de la información se basa en los principios enunciados en la Norma Internacional para la seguridad de la información - ISO/IEC 27001:2013. La organización está comprometida con el desarrollo y mantenimiento de un sistema de gestión de seguridad de información basado en el estándar internacional y ha desarrollado esta Política de seguridad de la Información buscando:

- Proporcionar orientación y apoyo para la seguridad de los activos de información identificados en conformidad con los requisitos de la organización, regulaciones y requisitos legales.
- Definir responsabilidades a los empleados, socios/partner, contratistas y cualquier otra persona u organización que tenga acceso a recursos de la organización.
- Conocer el estado de la administración con la intención de apoyar los objetivos y principios de la seguridad en concordancia con la estrategia de negocio y objetivos.
- Proporcionar un marco en el que la confidencialidad, integridad y disponibilidad de recursos de la organización puede ser mantenida.
- Optimizar la gestión de los riesgos mediante la prevención y minimización del impacto de los incidentes de seguridad sobre los activos.
- Asegurar que todas las infracciones de la seguridad sobre los activos de información son reportadas, investigadas y tomar las medidas adecuadas cuando sea necesario.
- Asegurar que las políticas y procedimientos de seguridad apoyan la seguridad y protección de la información de la organización se revisan periódicamente para garantizar la continuidad de las buenas prácticas y la protección frente a nuevas amenazas.
- Garantizar que los requerimientos de la seguridad de la información TI se comunican periódicamente a todas las áreas pertinentes.

4. Cumplimento

La organización cumplirá con toda la legislación peruana relacionada al procesamiento y almacenamiento de información, para la cual tomará en consideración:

- La ley de Protección de Datos Personales, Reglamento de Ley N° 29733
- Disposiciones de legislación en base a requerimientos de clientes.

- Requerimientos de cumplimiento de leyes establecidas de manera contractual, cuando sean referidas en la relación comercial.

La organización también cumplirá con cualquiera de los requisitos contractuales, normas y principios necesarios para mantener las funciones de negocios de la organización, incluyendo:

- Protección de los derechos de propiedad intelectual.
- Protección de registros propios de la organización
- Verificación de cumplimiento y procedimientos de auditoría que sean necesarios
- Prevención del uso indebido de instalaciones y toma de acciones necesarias para su remediación
- Los códigos de conexión a redes y servicios de terceros.
- Se tiene un listado de normatividad que se revisa para mantener al día los requerimientos relacionados a la empresa

4.1. Reporte de Incidencia

Los usuarios serán continuamente alentados a informar de cualquier infracción a la Política de Seguridad de la Información vía una pestaña exclusiva dentro del Sistema de Gestión de Tickets. Las infracciones pueden involucrar no sólo a los equipos de tecnología de la información, sino también los datos que se manejan de forma incorrecta, perdidos , con abuso o cualquier otro incidente que pueda provocar un problema de seguridad y que puedan infringir las políticas asociadas de la organización. Este ítem embebido en el Sistema de Gestión de Tickets para el control de incidentes de seguridad, dará un procedimiento de gestión de incidencias como herramienta para realizar el proceso de acciones correctivas y mejora.

4.2. Gestión de Incidencia

Durante la presentación de una infracción, los detalles del incidente se introducirán mediante el reporte por la persona que reporte la incidencia mediante el Sistema de Gestión de Tickets. Una vez que el reporte ha sido introducido en el sistema, se realizara seguimiento en concordancia con el procedimiento de gestión de incidentes de seguridad. El Oficial de Seguridad de la Información (OSI) realizará la gestión para que en conjunto de las partes involucradas se tomen las medidas correctivas apropiadas, esto en conjunto con los líderes de área, para su posterior análisis y solución de los incidentes de seguridad.

5. Organización de la Seguridad

La organización de la Seguridad está basada en una Estructura Organizacional del Sistema de Gestión de Seguridad de la Información (SGSI), las cuales persigue los siguientes objetivos:

- Administrar la seguridad de la información dentro de la Organización y establecer un marco gerencial para iniciar y controlar su implementación.
- Definir la distribución de funciones y responsabilidades en materia de Seguridad de la Información.
- Fomentar la consulta y cooperación con las Organizaciones que sean necesarias para la obtención de asesoría en materia de seguridad de la información.
- Garantizar la aplicación de medidas de seguridad y controles adecuados para el control interno y externo a los distintos activos de la información.

5.1. Estructura

Asimismo, como se comentó la organización de la Seguridad está basada en una Estructura Organizacional del Sistema de Gestión de Seguridad de la Información (SGSI), las cuales se detalla a continuación:

5.1.1. Comité de Gestión de Seguridad de la Información (CGSI)

Dentro de la empresa u organismo es el ente máximo que tendrá las principales funciones:

- Procederá a revisar y proponer la máxima autoridad para la ejecución de la Política de Gestión de Seguridad de la Información y la delegación de funciones en materia de Seguridad de la Información, alineados a los objetivos de negocio.
- Ser gestor responsable de todo lo relacionado a la implementación del SGSI, verificación de su continuidad y evaluación de su desempeño.
- Ser ente líder en la difusión de la importancia del SGSI dentro de la organización.
- Asignar roles y responsabilidades en materia de seguridad de información a cada área, esto según los procesos organizacionales en estudio.

- Promover la difusión y apoyo de la seguridad de la información dentro de la organización, creando un ambiente seguro y compacto que genere bienestar e identificación con las políticas y procedimientos establecidos.

Para el caso específico de la organización, los integrantes del Comité de Gestión de Seguridad de la Información (CGSI) serán: El Gerente General, Gerente Técnico, Gerente Comercial, Gerente Administrativo y Financiero, y Gerente de Recursos Humanos.

5.1.2. Grupo Interdisciplinario de Seguridad de la Información (GISI)

Dentro de la empresa u organismo aseguran que las actividades de Seguridad de la Información sean ejecutadas en conformidad con la Política de Gestión de Seguridad de la Información, aprobando metodologías y procesos que permitan al personal de la organización a expresar sus dudas e inquietudes en materia de Seguridad de la información, generando confianza y concientización en los estatutos y procedimientos indicados en la Política de SGSI.

Para el caso específico de la organización, los integrantes del Grupo Interdisciplinario de Seguridad de la Información (GISI) serán los Jefes que integran la Gerencia Técnica: Jefes de Proyectos, Jefe de Servicios Post-Venta y Desarrollo.

5.1.3. Oficial de Seguridad de la Información (OSI)

Dentro de la empresa u organismo, el Oficial de la Información propone metodologías, procedimientos, estatutos, herramientas, planes, programas y procesos para la seguridad de la información, y en si para el cumplimiento de controles que rigen para el cumplimiento de la misma. En adición a lo comentado, administrar los incidentes y vulnerabilidades de los distintos activos de información para identificar los controles a implementar, elaborando y actualizando el plan de Seguridad de la Información.

Adicionalmente, tiene como responsabilidad el monitoreo constante de incidentes relativos a la seguridad de la información, estableciendo parámetros de mejora en base a análisis previamente realizados.

Para el caso específico de la organización, para la elección del Oficial de la Seguridad de la Información, se tomaron rigurosas pruebas en referencia al conocimiento, experiencia en diseño e implementación de la norma ISO /IEC

27001:2013. El oficial de Seguridad de la Información será el Jefe de Servicios Post-Venta de la organización.

5.1.4. Dueño del Riesgo

La norma ISO/IEC 27001 en su versión 2013 establece la figura de Dueño del Riesgo la persona(s) responsable (s) de gestionar los riesgos asociados a los activos de información valorizados. Es decir, gestionar de manera correcta las actividades y recursos necesarios para evitar la materialización de amenazas sobre las vulnerabilidades existentes en los activos de información. El rol no implica necesariamente que sea la persona que finalmente ejecuta los controles, sino alguien que se responsabiliza de que realmente los controles aplicables sobre los activos de información se están llevando a cabo acorde a lo establecido.

Adicionalmente, del dueño del riesgo debe monitorear cambios significativos en los riesgos que afectan los activos de información previamente identificados, esto frente a las amenazas más relevantes que afecten o puedan afectar los activos de información seleccionados.

El Dueño del Riesgo será el Gerente Técnico de la organización.

5.1.5. Propietarios de Activos de la Información

Son los responsables de clasificar los activos de información con el grado de sensibilidad y criticidad necesario. Añadido a lo comentado, deberán documentar y mantener actualizadas la clasificación de activos de información realizada y definir qué usuarios tiene o no acceso a los distintos activos de información que tiene bajo su custodia. Para el caso específico de la organización, para la elección de los Propietarios de Activos de la Información serán tomados en cuenta los Gerentes que representen cada área que disponga los múltiples activos de información que hayan sido seleccionados. Por nombrar un ejemplo, los contratos de Mantenimiento de Servicios Post-Venta de los distintos clientes con los que cuenta la organización, será propiedad del Gerente de Operaciones.

5.1.6. Custodio de los Activos de Información

Administran y resguardan los activos de información, monitoreando el cumplimiento de controles de seguridad en los activos que se encuentren bajo su administración. En pocas palabras es el nexo entre el Propietario de la

Información y el usuario de los activos de información. Para el caso específico de la organización, los custodios de los activos de información serán los Jefes del Área Técnica: Jefe de Proyectos, Jefe de Post-Venta y Jefe de Desarrollo

5.1.7. Usuarios de Activos de Información

Son los usuarios finales que hacen uso del activo de información para la ejecución de sus deberes. Para el caso específico de la organización, los usuarios de los activos de Información son todas las personas que tengan a su cargo cualquier activo (bien, proceso, servicio, entre otro) que sea asignado bajo un documento formal y explicito, en mutuo acuerdo entre ambas partes.

6. Prevención de Riesgos y Aplicación de Controles

Los responsables de la información deben identificar, evaluar y tratar de manera correcta y eficaz los riesgos de seguridad de la información. Para ello, deben valerse de la metodología de riesgos utilizada, cumpliendo con todos sus estatutos y tomando en cuenta los niveles de valoración de Riesgos y los controles que sean necesarios para contrarrestar la materialización de amenazas sobre los activos de información.

7. Mantener la Seguridad de la Información en Niveles Óptimos

Para lo comentado, es necesario evaluar constantemente el desempeño y efectividad del Sistema de Gestión de Seguridad de la Información (SGSI). Asimismo, la organización deberá evaluar que el sistema de gestión vaya acorde a los niveles de exigencia de la misma y persiga los objetivos organizacionales previamente trazados. Para ello, debe tomar en cuenta el desarrollo del contenido del Anexo A de la norma ISO/IEC 27001:2013, conocido también como el Código de Buenas Practicas o Norma ISO/IEC 27002:2013.

8. Incumplimiento

Las infracciones de esta Política de Seguridad de la Información dada por su incumplimiento tendrá como resultado la aplicación de diversas sanciones, conforme a la magnitud y característica del aspecto no cumplido.

Asimismo, las infracciones de esta política y/o incidentes de seguridad son definidos como eventos que tienen como resultado, pérdidas o daños en activos para la organización, o en su defecto eventos que violan procedimientos y políticas de seguridad para la misma. Un empleado que se descubra que ha violado esta política

será sujeto a medidas disciplinarias, las cuales pueden incluir el despido o alguna acción que la organización crea conveniente.

9. Documentos y Registros Asociados

Nombre de Documento	Ubicación de Almacenamiento	Propietario	Control de Protección	Programación de Retención
Indicados en el Anexo	File Server	Organización	Restringido	4 años

10. Historial de Revisiones

Fecha de Cambio	Responsable	Resumen de Cambios

11. Gestión de Documentos

Este documento es válido desde 03/Diciembre/2017. Este documento se revisa periódicamente y por lo menos una vez al año para garantizar que se cumplen los siguientes criterios establecidos:

- Conformidad con los requisitos de la norma ISO 27001:2013
- Requisitos legislativos definidos por la ley que corresponda

ANEXO C: Política de Control de Acceso

1. Resumen

El presente documento establece las políticas y normas para garantizar un adecuado uso y control de acceso a los sistemas de información de la organización y los propios activos de información.

2. Propósito

El presente documento tiene como propósito definir y detallar el uso adecuado de los Sistemas de Información para impedir el acceso no autorizado a los sistemas de información e implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización (designación de privilegios de accesos a carpetas compartidas críticas).

Por otro lado, tiene como finalidad concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos, y garantizar la seguridad de la información en todos sus ámbitos.

3. Alcance

Esta política se aplica al control de acceso de a los Sistemas de Información y repositorios de información crítica y/o sensible de la organización. Todos los empleados, contratistas, consultores, temporales y otros trabajadores de la organización y sus subsidiarias son responsables de ejercer un buen juicio con respecto al uso apropiado de los recursos mencionados, ello de acuerdo con las políticas y normas de la organización, y leyes y regulaciones locales e impuestas por la organización.

4. Política

La política de control de acceso permite establecer medidas de control de acceso a nivel de red, sistema operativo, sistemas de información y los propios servicios de la organización. Los controles de acceso deben ser conocidos por todos empleados de la organización y limitar el acceso hacia los activos de información de acuerdo a lo establecido por el perfil de cargo.

Adicionalmente, e deben implementar procedimientos para la asignación de privilegios de acceso a los sistemas de información, bases de datos y servicios, estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

4.1. Normas generales aplicables para el Control de Acceso

4.1.1. Norma N°1: Requerimientos para el Control de Acceso

Los controles de acceso deberán contemplar:

- Requerimientos de seguridad de cada uno de los Sistemas de Información y las propias aplicaciones para el consumo de recursos internos de la misma.
- Definir los perfiles o privilegios de acceso de los usuarios a los Sistemas de Información, Carpetas compartidas y las propias aplicaciones de acuerdo a su perfil de cargo impuesto por la organización.
- Accesos para interacción de equipos de Infraestructura de Comunicaciones.

4.1.2. Norma N°2: Administración de Accesos de Usuarios

La organización establece procedimientos para controlar la asignación de derechos de acceso a los sistemas de información, servicios de información y los propios activos de información.

4.1.3. Norma N°3: Creación de Usuarios

- La organización mantendrá los registros de acceso donde cada uno de los responsables de los procesos involucrados haya autorizado el consumo de sus recursos. Esto incluye a personal propio de la empresa o personal externos. Tener en cuenta que la organización tendrá cuidado en otorgar accesos a los recursos internos, diferenciando su consumo de la manera que la organización lo crea conveniente, esto preservando la confidencialidad, integridad y disponibilidad de la información.

- Los datos de acceso a los sistemas de información deberán estar compuestos por un ID o nombre de usuario y contraseña que será único para usuario.
- Cuando se retire o cambie de contrato cualquier empleado de la organización se deberá aplicar la eliminación o cambios de privilegios en los sistemas de información a los que el usuario estaba autorizado.
- El oficial de Seguridad de la Información y el propio Comité de Gestión de Seguridad de la Información (CGSI) deberá realizar revisiones de privilegios de acceso a los diferentes sistemas de información por parte de los servicios otorgados por la organización, manteniendo los registros de las revisiones y hallazgos de su consumo.

4.1.4. Norma N°4: Gestión de Contraseñas de Usuario

La organización tendrá una gestión de contraseña, la cual deberá cumplir con las siguientes especificaciones:

- Las contraseñas de acceso deberán cumplir con un mínimo de 8 caracteres y la combinación de números, letras mayúsculas y minúsculas, en lo posible utilizar caracteres especiales.
- El acceso de todos los recursos internos y públicos de la organización deberán cambiar su contraseña de acceso a los diferentes sistemas de información con una frecuencia mínima de 3 meses
- Para el caso anterior, se exceptuará aquellos accesos que contengan información confidencial en cuyo caso el cambio deberá ser mensual.
- Los sistemas de información deberán bloquear permanentemente al usuario luego de 5 intentos fallidos de autenticación a excepción de aquellos que contengan información confidencial o sensible en cuyo caso después de 3 intentos fallidos de autenticación se realizará el bloqueo.

4.1.5. Norma N°5: Uso de Contraseñas

Los usuarios que consumen recursos de la organización deberán cumplir las siguientes normas:

- Mantener los datos de acceso en total secreto. La divulgación de los datos de acceso cae bajo responsabilidad del usuario, con las faltas y penalidades que la organización disponga.
- Las contraseñas no deberán estar basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo nombres, números de teléfono, fecha de nacimiento, entre otro.
- Las contraseñas deberán ser fáciles de recordar por el usuario y difíciles de adivinar.
- Se deberá notificar cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad.

4.1.6. Norma N°6: Equipos desatendidos en áreas de Usuarios

Los usuarios en el uso de las computadoras deberán tener en cuenta las siguientes normas para garantizar que los equipos desatendidos sean protegidos adecuadamente:

- Los equipos instalados en áreas de usuarios, por ejemplo estaciones de trabajo, en el Datacenter como servidores de archivos u otros, requieren una protección específica contra accesos no autorizados cuando se encuentren desatendidos.
- Las computadoras u ordenadores asignados a cada colaborador tendrán candados especiales para cada dispositivo. En ello, solo las personas autorizadas a bien tendrán las llaves para algún traslado del activo, o en caso específico de laptops para el traslado a clientes o reuniones dentro o fuera de la organización.
- Más detalles sobre tratamiento de equipos desatendidos deberá revisar la Política de Puesto de Trabajo desatendido y Bloqueo de Pantalla.

4.1.7. Norma N°7: Control de Acceso a Red

- La organización deberá asegurar el bloqueo al acceso de páginas de contenido para adultos, redes sociales, hacking, descargas (FTP), mensajería instantánea y cualquier página que represente riesgo potencial para la organización.

- El bloqueo referido se realizará mediante el uso de reglas de filtrados de contenido configuradas en el Firewall.
- El acceso a las carpetas de contenido crítico y sensible, tales como: Carpeta de Proyectos, Carpeta de Licitaciones y Carpetas de áreas Administrativas y contabilidad serán accedidas únicamente a personal autorizado, esto mediante la configuración de permisos sobre a carpeta. Asimismo, el acceso contendrá permisos diferenciados de lectura o escritura, previa diferenciación del uso adecuado, constatado y autorizado por las autoridades pertinentes de la Organización: Jefe de área inmediato y el Comité de Gestión de Seguridad de la Información (CGSI).
- Las excepciones de acceso, serán aprobados por el Jefe de área inmediato, según la necesidad del cargo y verificación previa de que las paginas solicitadas no contengan código malicioso con el visto bueno del oficial de seguridad de la información.

4.1.8. Norma N°8: Autenticación de Usuarios para Conexiones Externas

La autenticación de usuarios remotos deberá ser aprobada por el Jefe inmediato del usuario que solicita el permiso. Tener en cuenta que existe una Política de Teletrabajo el cual contiene las normas y requisitos asociadas para la conexión externa segura.

4.1.9. Norma N°9: Control de Conexión a Redes

La organización deberá con sectorización de redes: Distintas áreas de usuarios, Servidores, DMZ (Servidores de uso Público) y otras que se estime conveniente. Con ello, garantizar la confidencialidad de los datos que se transmitan entre redes, esto fortalecida por reglas de firewall, esto si aplica el caso.

4.1.10. Norma N°10: Seguridad en los Servicios de Red

- La organización deberá mantener instalados y habilitados sólo aquellos servicios y puertos que sean utilizados por los sistemas de información y el propio software de la misma.

- Controlar el acceso lógico a los servicios, tanto a su uso como a su administración mediante bloqueo de puertos en el firewall de la entidad o la creación de listas de acceso mediante el Switch de Core.

4.1.11. Norma N°11: Control de Identificación y Autenticación de Usuarios

- Todos los usuarios (incluido el personal de soporte técnico, como los operadores, administradores de red, programadores de sistemas y administradores de bases de datos) tendrán un identificador único (ID de Usuario) solamente para su uso personal exclusivo, de manera que las actividades tengan trazabilidad.
- Este identificador único (ID de usuario) será estructurado por la organización mediante un procedimiento propio, el cual no se incluye su descripción en el presente documento.
- La información de la estructuración del Identificador Único (ID de usuario) será proporcionado por el área de Soporte Técnico.

4.1.12. Norma N°12: Sistema de Administración de Contraseñas

La organización deberá mantener un Sistema de administración de contraseñas el cual deberá:

- Obligar el uso del Identificador Único (ID de Usuario) y contraseñas individuales para determinar responsabilidades.
- Permitir a los usuarios seleccionar y cambiar sus propias contraseñas luego de cumplido el plazo mínimo de mantenimiento de las mismas o cuando consideren que la misma ha sido comprometida.
- Deberá incluir un procedimiento de confirmación para contemplar los errores de ingreso. Los eventos de contraseñas mal ingresadas serán registradas en el sistema.
- Obligar a los usuarios a cambiar las contraseñas provisionales o que han sido asignadas por el administrador del sistema de información (contraseñas por defecto).
- No permitir mostrar las contraseñas en texto claro cuando son ingresadas.
- Almacenar las contraseñas en forma cifrada.

4.1.13. Norma N°13: Sesiones Inactivas

- Si el usuario debe abandonar la estación de trabajo momentáneamente, activará protectores de pantalla con contraseñas, con el fin de evitar que personas ajenas puedan ver su trabajo o continuar con la sesión de usuario habilitada.
- Si los sistemas de información detectan inactividad por un periodo igual o superior a cinco minutos, deben automáticamente aplicar, “timeout” es decir, finalizar la sesión de usuario.

4.1.14. Norma N°14: Registro de Conexión a Sistemas de Información

Los accesos a recursos internos, ya sean Sistema de Información o las propias carpetas embebidas en servidores específicos, lo cual llevan embebido información crítica y confidencial tendrán en todo momento registros de acceso, mediante el envío de login de acceso al Sistema de Control de Eventos o registros.

4.1.15. Norma N°14: Accesos a Infraestructura de Comunicaciones

El acceso a equipos que componen la Infraestructura de Comunicaciones tendrá las siguientes consideraciones:

- Todos los Accesos de configuración al equipo serán mediante la validación del Identificador Único (ID de Usuario) en el equipo TACACS (Terminal Access Controller Access Control System), esto previa autorización.
- Todo el registro de actividad se verá en logs de eventos del Servidor, para la posterior auditoria de ser el caso.
- Cuando haya la necesidad de ingresar a interactuar físicamente con el servidor, será acompañado de un personal de Soporte Técnico (de ser un proveedor) o un personal propio de la empresa autorizado.
- El personal que acceda a los recursos de manera física tendrá que llenar un formulario de ingreso, en donde detalle: Nombre Completo, Documento de Identidad, motivo, hora de ingreso, hora de salida y empresa (de ser externo).
- La organización tendrá en consideración implementar un Sistema Biométrico para el acceso físico a las instalaciones del Datacenter.

5. Cumplimiento de Política

5.1. Medición del Cumplimiento

La Organización y en especial el Oficial de Seguridad de la Información (OSI) verificará el cumplimiento de esta política a través de varios métodos, que incluyen: Visitas periódicas, monitoreo de video, informes de herramientas comerciales, auditorías internas y externas e inspección, entre otros, lo cual proporcionarán comentarios al propietario de la política y al negocio correspondiente gerente de la unidad.

5.2. Excepciones

Cualquier excepción a la política debe ser aprobada por el Gerente de área respectivo y el Grupo Interdisciplinario de Seguridad de la Información (GISI)

5.3. Incumplimiento

Un empleado que se descubra que ha violado esta política será sujeto a medidas disciplinarias, las cuales pueden incluir el despido o alguna acción que la organización crea conveniente.

6. Documentos y Registros Asociados

Nombre de Documento	Ubicación de Almacenamiento	Propietario	Control de Protección	Programación de Retención
Política de Intercambio de Información	File Server	Organización	Restringido	4 años

7. Historial de Revisiones

Fecha de Cambio	Responsable	Resumen de Cambios

8. Gestión de Documentos

Este documento es válido desde 12/Diciembre/2017. Este documento se revisará periódicamente por lo menos una vez al año para garantizar que se cumplen los siguientes criterios establecidos con los requisitos de la norma ISO 27001:2013 y requisitos legislativos definidos por la ley que corresponda.

ANEXO D: Política de Uso Aceptable de los Sistemas de Información, Internet y Correo Electrónico

1. Resumen

La intención de la organización en publicar una Política de uso aceptable de los Sistemas de Información, Internet y Correo Electrónico no es imponer restricciones que sean contrarias a la cultura de apertura, confianza e integridad establecida por la organización. En base a ello, la organización se compromete a proteger a los empleados, socios y la empresa de las acciones ilegales o perjudiciales de las personas, con o sin conocimiento propio de la misma. Asimismo, los sistemas información (servidores FTP con carpetas críticas detectados), Internet y Correo Electrónico, que son propiedad de la organización, se utilizarán con fines comerciales al servicio de los intereses de la misma y de sus clientes.

2. Propósito

El presente documento tiene como propósito definir y detallar el uso adecuado de los Sistemas de Información, Internet y Correo electrónico en la organización, ello con el fin de proteger al usuario y a la propia organización de situaciones que pongan en peligro los sistemas y la información contenida en estos. Esta política es de obligado cumplimiento para el personal de la organización y todos los que accedan a estos recursos, sin diferenciación alguna. Es decir, todo el personal interno o externo que haga el consumo de estos activos de información será de obligado cumplimiento de la misma.

3. Alcance

Esta política se aplica al uso de los Sistemas de Información, Internet y Correo electrónico en la organización. Todos los empleados, contratistas, consultores, temporales y otros trabajadores de la organización y sus subsidiarias son responsables de ejercer un buen juicio con respecto al uso apropiado de los sistemas de información, Internet y Correo electrónico, respectivamente, ello de acuerdo con las políticas y normas de la organización, y leyes y regulaciones locales e impuestas por la organización.

4. Política

La política de uso aceptable pretende facilitar y agilizar los procesos y mejorar la calidad en la prestación de servicios a los usuarios. La mejora de los procesos en los Sistemas de Información supone regular el uso apropiado de sus componentes y equipos, así como implantación de aquellas medidas necesarias para garantizar la confidencialidad de la información. Para conseguir estos objetivos resulta necesario establecer políticas que garanticen el uso efectivo y seguro de los Sistemas de Información y las herramientas asociadas a estos. Este documento tiene como objetivo fijar las normas fundamentales que deben regir el comportamiento de los empleados para garantizar el uso adecuado de estos recursos. Estas normas serán revisadas, actualizadas y publicadas periódicamente y es responsabilidad de los usuarios estar actualizados en el contenido de las mismas.

4.1. Normas generales aplicables al uso de los Sistemas de Información

4.1.1. Norma N°1

- Los sistemas de información de la organización, incluyendo el Sistema de Gestión de programas / aplicaciones (Sistema de Gestión de Tickets) y archivos electrónicos (Carpetas de Proyectos, Licitaciones y de áreas Administrativas y Contabilidad) sólo pueden utilizarse para fines relacionados con el desempeño de las tareas que los usuarios de la organización tengan encomendadas. Esta misma consideración se aplica a la información almacenada en su ordenador o la emitida o comunicada a través de los Sistemas de Información de la misma.

4.1.2. Norma N°2

- Los Sistemas de Información y las herramientas asociadas, como el correo electrónico y la conexión a Internet, sólo podrán ser utilizados por personal debidamente autorizado.
- Será responsabilidad de cada área definir las tareas que conllevan el acceso a tales herramientas y el uso de tales recursos deberá circunscribirse al ámbito profesional con el propósito de agilizar los trabajos de la organización.

- No se autoriza su uso con fines personales. Asimismo, la información desarrollada, transmitida o almacenada en los Sistemas de Información de la organización pertenece a la propia organización.
- Son de aplicación todas las disposiciones legales aplicables a los documentos privados, los cuales se encuentra dentro de las carpetas asociadas, identificadas como activos de Información, tales son: Carpetas de Proyectos, Carpeta de Licitaciones y Carpetas de áreas Administrativas y Contabilidad. Tener en cuenta que la divulgación de tal información sin autorización está estrictamente prohibida.
- La alteración, destrucción o distribución fraudulenta o malintencionada de cualquier documento en formato electrónico propiedad de la organización puede perjudicar su desempeño y constituir una infracción grave. En base a ello, se adoptarán las medidas disciplinarias previstas por parte de la organización, reservándose la entidad el derecho a interponer cuantas acciones legales sean necesarias

4.1.3. Norma N°3

- No está permitido la modificación de ficheros dentro de la: Carpeta de Proyectos, Carpeta de Licitaciones, Carpetas de áreas Administrativas y Contabilidad u otra que sea colectora de información sensible manejada por la organización, esto sin previa autorización del Gerente y/o Jefe del área respectiva donde se desempeña el usuario y el propio Grupo Interdisciplinario de Seguridad de la Información (GISI). Lo comentado, con objetivo de adoptar las medidas necesarias para asegurar la legalidad y seguridad del tratamiento de la información.

4.1.4. Norma N°4

- Los usuarios de los sistemas de información deben respetar los derechos de propiedad intelectual de los autores de las obras, programas, aplicaciones, archivos u otros, manejadas o accedidas a través de dicho sistema.

4.1.5. Norma N°5

- El cliente del Sistema de Gestión de Ticket y los programas o recursos utilizados en la organización deben ser autorizados en su uso por las distintas áreas donde se desempeña cada trabajador.
- El cliente del Sistema de Gestión de Ticket sólo podrán ser instalados por personal autorizado a tales efectos. Asimismo, los programas y aplicaciones distribuidos por la organización no podrán reproducirse sin autorización o ser utilizados para fines ajenos a las funciones y tareas encomendadas por la misma.

4.1.6. Norma N°6

- La organización será responsable de establecer las normas mediante las cuales se asignan las cuentas de acceso, incluyendo las medidas de seguridad aplicables tales como: claves secretas, contraseñas, controles de acceso a los servidores y sistemas para auditar su uso, la integridad y la seguridad de los datos y comunicaciones que se envían.

4.1.7. Norma N°7

- Los usuarios de los sistemas deberán cumplir con todas las normas de uso y las relativas a la seguridad de la información emitidas por la organización.

4.1.8. Norma N°8

- Cada usuario será individualmente responsable por el manejo adecuado de las claves de acceso o contraseñas asignadas.

4.1.9. Norma N°9

- La correspondiente asignación de claves de acceso no impedirá que el uso de los Sistemas de Información sea auditado por el personal autorizado por la organización, ya sea interno externo. Ello con el propósito de garantizar el uso apropiado de los recursos.

4.1.10. Norma N°10

- El acceso a información o a una cuenta ajena sin autorización, obtenido mediante la modificación de privilegios de acceso o la interceptación de

información en cualquier otra manera está prohibida y estará sujeto a las medidas disciplinarias pertinentes.

4.1.11. Norma N°11

- El custodio de la Información, rol asignado dentro de la Estructura Organizacional del Sistema de Gestión de Seguridad de la Información, será el responsable de custodiar la información contenida en los Sistemas de Información.
- El Comité de Gestión de Seguridad de la Información (CGSI) dará las directrices necesarias para evitar accesos no autorizados para protegerla y definir las políticas necesarias para garantizar su integridad.

4.1.12. Norma N°12

- Las normas aquí establecidas deben interpretarse como complementarias a las normas legales comúnmente aplicables, ello en materia de leyes aplicables en el ámbito nacional. Asimismo, la violación de estas normas puede conllevar la revocación de cualquier privilegio de uso de los Sistemas de Información y será notificada al responsable del área al que pertenece el activo de información, el Oficial de Seguridad de la Información y el Comité de Gestión de Seguridad de la Información (CGSI).

4.1.13. Norma N°13

- Las violaciones a lo estipulado en las normas que integran la presente Política de Uso Aceptable deberán ser informadas al área de Recursos Humanos para la inclusión de la falta dentro de la hoja de vida del trabajador y para conocimiento propio, las cuales traerá consigo las acciones disciplinarias que sean correspondientes.

4.1.14. Norma N°14

- Los usuarios de la organización utilizarán el Sistema de Gestión de Tickets para comunicar las incidencias informáticas y realizar las solicitudes correspondientes al personal de Seguridad de Información a cargo.

4.2. Normas aplicables al uso de Internet y del correo electrónico

4.2.1. Norma N°1

- Los sistemas de comunicación y acceso a Internet de la organización deberán ser utilizados exclusivamente como una herramienta de trabajo conforme a las normas que rigen el comportamiento del personal de misma y no para actividades personales.

4.2.2. Norma N°2

- Las operaciones realizadas a través de Internet pueden generar responsabilidad por parte de la organización. En base a ello, la organización se reserva el derecho a intervenir y auditar los accesos realizados por los usuarios a la red y a Internet y el contenido de lo accedido.

4.2.3. Norma N°3

- La organización establecerá la asignación de las cuentas de correo electrónico, las medidas de seguridad aplicables, las claves de acceso y las contraseñas, los controles de acceso al servidor y el método de auditoría del sistema y las comunicaciones enviadas.

4.2.4. Norma N°4

- El sistema de correo electrónico y el propio dominio es propiedad de la organización. En base a ello, la misma puede intervenir, auditar e investigar el uso adecuado del mismo.
- Las cuentas están sujetas a auditorías y revisiones sin previo aviso. Esta auditoria será ejecutada por personal autorizado de la organización, encargado de la Seguridad de los Sistemas de Información. Los usuarios internos se rigen a los requisitos estipulados por la organización.

4.2.5. Norma N°5

- La organización establecerá normativas en relación al envío por correo electrónico de documentos que contengan información

confidencial o sensible de la organización o de los que tratan de asuntos internos que no deben ser divulgados.

- De ser necesario enviar tal información, la misma deberá ser cifrada. En el caso de sospechar que se ha producido una interceptación o divulgación de tal información, se deberá informar de inmediato al Oficial de Seguridad de la Información para tomar las acciones correspondientes.

4.2.6. Norma N°6

- La organización tiene expresamente prohibido ver o descargar de cualquier red o medio de almacenamiento, material relacionado con pornografía y/o asociados a sitios maliciosos.
- Toda comunicación electrónica que resulte amenazante, discriminatoria (basada en raza, credo, color de piel, edad, sexo, condiciones físicas o mentales, orientación sexual, etc), difamatoria u ofensiva está expresamente prohibida.
- La alteración o destrucción de comunicaciones electrónicas con la intención de causar daño a la organización o a una persona vinculada a la misma está estrictamente prohibida.

4.2.7. Norma N°7

- Los usuarios de la organización que accedan al Correo Electrónico mediante el acceso OWA, es decir vía Internet mediante un acceso Web, deben tener en cuenta que su ingreso será mediante un doble factor de autenticación.
- Este doble factor de autenticación se encuentra integrado al Directorio Activo (AD) y enviara un mensaje de texto (SMS) al celular del usuario. Tener en cuenta que el celular mencionado es un equipo telefónico proporcionado por la propia organización al usuario final.
- Los accesos vía OWA son limitados a una lista de usuarios que la organización disponga. Esta lista ira creciendo a medida que los accesos vía OWA sean necesarios para cada usuario, el cual debe

ser previamente sustentado y aprobado por su Jefe inmediato y el Comité de Gestión de Seguridad de la Información (CGSI).

5. Cumplimiento De Política

5.1. Medición del Cumplimiento

La Organización y en especial el Oficial de Seguridad de la Información (OSI) verificará el cumplimiento de esta política a través de varios métodos, que incluyen: Visitas periódicas, monitoreo de video, informes de herramientas comerciales, auditorías internas y externas e inspección, entre otros, lo cual proporcionarán comentarios al propietario de la política y al negocio correspondiente gerente de la unidad.

5.2. Excepciones

Cualquier excepción a la política debe ser aprobada por el Gerente de área respectivo y el Grupo Interdisciplinario de Seguridad de la Información (GISI)

5.3. Incumplimiento

Un empleado que se descubra que ha violado esta política será sujeto a medidas disciplinarias, las cuales pueden incluir el despido o alguna acción que la organización crea conveniente.

6. Documentos y Registros Asociados

Nombre de Documento	Ubicación de Almacenamiento	Propietario	Control de Protección	Programación de Retención
Política de Intercambio de Información	File Server	Organización	Restringido	4 años

7. Historial de Revisiones

Fecha de Cambio	Responsable	Resumen de Cambios

8. Gestión de Documentos

Este documento es válido desde 12/Diciembre/2017. Este documento se revisará periódicamente por lo menos una vez al año para garantizar que se cumplen los siguientes criterios establecidos con los requisitos de la norma ISO 27001:2013 y requisitos legislativos definidos por la ley que corresponda.

ANEXO E: Política de Puesto de Trabajo despejado y Bloqueo de Pantalla

1. Resumen

El presente documento establece las políticas y normas para garantizar un adecuado uso del puesto de trabajo despejado y bloqueo de pantalla de la computadora u ordenador cuando no esté en uso.

2. Propósito

El presente documento tiene como propósito definir y detallar los lineamientos necesarios para mejorar la protección de la información almacenada en los puestos de trabajo y en el computador. Lo comentado, mediante el establecimiento de mecanismos automáticos de bloqueo para las computadoras cuando no estén en uso por parte del colaborador de la organización.

3. Alcance

Esta política se aplica a todos los puestos de trabajo y computadoras u ordenadores asignados a cada colaborador de la organización. Es responsabilidad de cada uno de los mencionados ejercer un buen juicio con respecto al uso apropiado de los recursos mencionados. Lo comentado, de acuerdo con las políticas y normas de la organización y regulaciones locales que apliquen.

4. Política

La Política de Puesto de trabajo desatendido y Bloqueo de Pantalla se adopta para concientizar a cada colaborador de la organización en materia de Seguridad de la Información respecto a contar con lineamientos respecto al puesto de trabajo limpio, libre de documentación, medios de almacenamiento removibles u otros accesorios como medios de información. Adicionalmente, establece una política de pantalla limpia en las instalaciones de procesamiento de información, tales son las computadoras o puesto de trabajo asignados a cada colaborador.

4.1. Normas general aplicable para Puestos de Trabajo Desatendido y Bloqueo de Pantalla

4.1.1. Norma N°1: Puesto de Trabajo Desatendido y Bloqueo de Pantalla

Los usuarios en el uso de las computadoras u ordenadores deberán tener en cuenta las siguientes consideraciones para garantizar que los equipos desatendidos sean protegidos adecuadamente:

- Los equipos instalados en áreas de usuarios, por ejemplo estaciones de trabajo, en el Datacenter como servidores de archivos u otros, requieren una protección específica contra accesos no autorizados cuando se encuentren desatendidos.
- Se deberán bloquear el equipo de cómputo tras abandonar el puesto de trabajo y/o al culminar las labores.
- Se deberá configurar un bloqueo automático de la sesión en cada estación de trabajo, servidor o equipo de Infraestructura de Comunicaciones tras una inactividad superior a 5 minutos.
- Se tendrá en consideración un fondo de pantalla único para todos los usuarios.
- Apagar los equipos de cómputo al finalizar la jornada laboral (Aplicable solo a computadoras o estaciones de trabajo de usuarios finales).

4.1.2. Norma N°2: Puestos de Trabajo Limpios

Se deberán tomar en cuenta las siguientes consideraciones:

- Mantener el puesto de trabajo libre de documentos, papeles, revistas, entre otros. Es decir, limpia y despejada de documentación que pueda ser observada por personal ajeno a la misma.
- Está prohibido dejar papeles, sticker pegados en la pantalla o en lugares de fácil acceso en la cual se encuentre información de inicio de sesión o contraseñas de acceso a los sistemas de información, la cual por ser observada o manipulada por terceras personas.
- Mantener la documentación con información sensible o confidencial bajo buen recaudo.

5. Cumplimiento de Política

5.1. Medición del Cumplimiento

La Organización y en especial el Oficial de Seguridad de la Información (OSI) verificará el cumplimiento de esta política a través de varios métodos, que incluyen: Visitas periódicas, monitoreo de video, informes de herramientas comerciales, auditorías internas y externas e inspección, entre otros, lo cual proporcionarán comentarios al propietario de la política y al negocio correspondiente gerente de la unidad.

5.2. Excepciones

Cualquier excepción a la política debe ser aprobada por el Gerente de área respectivo y el Grupo Interdisciplinario de Seguridad de la Información (GISI)

5.3. Incumplimiento

Un empleado que se descubra que ha violado esta política será sujeto a medidas disciplinarias, las cuales pueden incluir el despido o alguna acción que la organización crea conveniente.

6. Documentos y Registros Asociados

Nombre de Documento	Ubicación de Almacenamiento	Propietario	Control de Protección	Programación de Retención
Política de Intercambio de Información	File Server	Organización	Restringido	4 años

7. Historial de Revisiones

Fecha de Cambio	Responsable	Resumen de Cambios

8. Gestión de Documentos

Este documento es válido desde 12/Diciembre/2017. Este documento se revisará periódicamente por lo menos una vez al año para garantizar que se cumplen los siguientes criterios establecidos con los requisitos de la norma ISO 27001:2013 y requisitos legislativos definidos por la ley que corresponda.

ANEXO F: Política de Teletrabajo

1. Resumen

El acceso remoto a la organización es esencial para mantener la productividad de los recursos internos de la misma. En base a ello, teniendo en cuenta que en muchos casos el acceso remoto se origina desde redes comprometidas o desde un nivel de seguridad menor a la red interna organizativa, se debe tener en cuenta la presente Política de Seguridad de Teletrabajo para reducir los riesgos externos asociados de la mejor manera posible.

2. Propósito

El propósito de esta política es definir reglas y requisitos para conectarse a la red de la organización desde cualquier red externa. Estas reglas y requisitos están diseñados para reducir la exposición potencial a la organización de los daños que pueden resultar del uso no autorizado de los recursos de la misma. Los daños incluyen la pérdida de datos confidenciales o sensibles de la organización, propiedad intelectual, daños a la imagen pública, daños a los sistemas críticos de la organización, y multas u otras responsabilidades financieras incurridas como resultado de esas pérdidas.

3. Alcance

Esta política se aplica a todos los empleados con una computadora o estación de trabajo propiedad de la organización utilizada para conectarse a consumir recursos locales de la misma. No está incluido dentro de la conexión remota cualquier otro dispositivos que no se una computadora o estación de trabajo que no haya sido registrada previamente en los accesos. Asimismo, esta política se aplica a las conexiones de acceso remoto que se utilizan para trabajar de manera remota, incluida lectura, escritura o el envío de correo electrónico y la visualización de los recursos internos. Esta política cubre todas y cada una de las implementaciones técnicas de acceso remoto utilizadas para conectarse a la organización.

4. Política

Es responsabilidad de los empleados de la organización con privilegios de acceso remoto a la red corporativa garantizar que su conexión de acceso remoto reciba la misma consideración que la conexión en el sitio del usuario de la organización.

Las normas asociadas son las siguientes:

4.1. Normas de uso para el caso de Teletrabajo

4.1.1. Norma N°1

El acceso remoto seguro debe controlarse estrictamente con configuraciones con algoritmos de cifrado (es decir, redes privadas virtuales (VPN)) y autenticación fuertes. Para ello, existe un procedimiento de configuración de conexión en Fase 1 y Fase 2 cliente VPN a instalarse en las computadoras o estación de trabajo. De ser necesario el detalle de esta configuración puede consultarse al personal del área de Soporte Técnico de la organización.

4.1.2. Norma N°2

El uso de acceso remoto para uso de recursos externos debe ser aprobado previamente por el Gerente de área que pertenece el usuario (Gerente Técnico, Gerencia Administrativa y Financiera y Gerencia Comercial), esto previamente revisado por el Grupo Interdisciplinario de Seguridad de la Información (GISI).

4.1.3. Norma N°3

El acceso a estas computadoras o estaciones de trabajo se realizará previamente mediante la inclusión y autorización de la Mac-Address del dispositivo. En ello, la lista completa de acceso para estos dispositivos serán agregados a la regla de Firewall, permitiendo su ingreso a recursos internos previamente autorizados según sus áreas de acceso.

4.1.4. Norma N°4

Al utilizar un equipo de la organización para conectarse de forma remota a la red corporativa, los usuarios autorizados se asegurarán de que el host remoto no esté conectado a ninguna otra red al mismo tiempo, a excepción de las redes personales redes que están bajo su completo control o bajo el control completo del usuario.

4.1.5. Norma N°5

Todos los hosts que están conectados a las redes internas de la organización a través de tecnologías de acceso remoto deben usar el software antivirus más actualizado implementado en la organización.

4.1.6. Norma N°6

Al conectarse y consumir recursos internos de la organización, el usuario se compromete a navegar a redes seguras de acceso externo, es decir la Internet. Ello, teniendo en cuenta que al acceder vía cliente VPN a la organización, las políticas de navegación son las mismas a las que si estuviera dentro de ellas. Tener en cuenta que registro de navegación de usuarios será enviado a una consola de logs, los cuales podrán ser revisados posteriormente cuando se genere el historial de navegación del usuario, esto de ser necesario.

5. Cumplimiento de Política

5.1. Medición del Cumplimiento

La Organización y en especial el Oficial de Seguridad de la Información (OSI) verificará el cumplimiento de esta política a través de varios métodos, que incluyen: Visitas periódicas, monitoreo de video, informes de herramientas comerciales, auditorías internas y externas e inspección, entre otros, lo cual proporcionarán comentarios al propietario de la política y al negocio correspondiente gerente de la unidad.

5.2. Excepciones

Cualquier excepción a la política debe ser aprobada por el Gerente de área respectivo y el Grupo Interdisciplinario de Seguridad de la Información (GISI)

5.3. Incumplimiento

Un empleado que se descubra que ha violado esta política será sujeto a medidas disciplinarias, las cuales pueden incluir el despido o alguna acción que la organización crea conveniente.

6. Documentos y Registros Asociados

Nombre de Documento	Ubicación de Almacenamiento	Propietario	Control de Protección	Programación de Retención
Política de Intercambio de Información	File Server	Organización	Restringido	4 años

7. Historial de Revisiones

Fecha de Cambio	Responsable	Resumen de Cambios

8. Gestión de Documentos

Este documento es válido desde 12/Diciembre/2017. Este documento se revisará periódicamente por lo menos una vez al año para garantizar que se cumplen los siguientes criterios establecidos con los requisitos de la norma ISO 27001:2013 y requisitos legislativos definidos por la ley que corresponda.

ANEXO G : Política de Gestión de Incidentes de Seguridad de la Información

1. Resumen

La Política de Gestión de Incidente crea lineamientos en el correcto manejo y administración de los incidentes de Seguridad sobre los Activos de Información. Asimismo, constituye un documento altamente útil, calificado y de constante revisión para el personal o colaboradores de la empresa para la toma de acciones necesarias sobre incidentes de Seguridad.

2. Propósito

La Política busca establecer lineamientos generales para la gestión de incidentes de seguridad de la información. Ello con la finalidad de prevenir y limitar el impacto de la materialización de alguna amenaza sobre los activos de información.

3. Alcance

Esta política se aplica a todo el personal o colaboradores de la organización los cuales tenga autorizado el acceso al consumo de recursos de los Sistemas de Información o el manejo o interacción con los propios activos de información propiedad de la organización.

4. Política

Es responsabilidad del personal o colaboradores de la organización conocer la política y el alcance de la misma. Asimismo, tener en consideración el registro de incidencias dentro del Sistema de Gestión d Tickets de la Organización. En base a ello, las normas que incluyen la Política de Gestión de Incidentes de Seguridad son:

4.1. Normas para la Gestión de Incidentes de Seguridad de la Información

4.1.1. Norma N°1: Sistema de Gestión de Incidentes

- La Organización cuenta con un Sistema de Gestión de Incidentes de Seguridad de la Información, el cual se encuentra embebido en un ítem del Sistema de Gestión de Tickets. Dentro de ello, se llevará una bitácora de

todos los incidentes de seguridad y un inventario del historial del mismo, el cual contendrá: Persona que alertó sobre el incidente, descripción del incidente, activo de información comprometido, acción preliminar ejecutada, entre otros atributos necesarios para la correcta gestión y acción inmediata sobre el incidente.

4.1.2. Norma N°2: Obligación de la Organización

- La Organización adoptará medidas de seguridad eficientes para asegurar la protección de sus activos de información críticos.
- La Organización analizará los eventos de Seguridad asociados a los activos de información, con el fin de revisar, evidenciar y/o determinar que se trata de un incidente de seguridad de la información.
- La Organización tendrá en consideración ejecutar procedimientos de respuesta a incidentes para la reducción o contención del riesgo de seguridad sobre el activo de información.
- La Organización constantemente investigará los incidentes de seguridad de la información que apliquen y no apliquen sobre los activos de información y los documentará para crear información necesaria al personal o colaboradores de la organización. Ello, permitirá para prevenir nuevas ocurrencias de incidentes sobre los activos.
- La Organización tendrá en consideración actividades Post-incidente para minimizar las consecuencias de la materialización de una amenaza sobre el activo de información. Asimismo, todo este procedimiento deberá ser documentado.

4.1.3. Norma N°3: Obligación del personal o colaborador de la Organización

- Es responsabilidad del personal o colaboradores de la organización reportar cualquier evento o incidente relacionado con incidentes sobre los activos de información de la misma, ello con la mayor prontitud posible.

5. Cumplimiento de Política

5.1 Medición del Cumplimiento

La Organización y en especial el Oficial de Seguridad de la Información (OSI) y el Propietario del Riesgo de cada activo de información seleccionado verificarán el cumplimiento de esta política a través de varios métodos posibles, tales como pruebas simuladas de amenazas sobre los activos de información u otros métodos que la organización crea conveniente.

5.2 Excepciones

Cualquier excepción a la política debe ser aprobada por el Gerente de área respectivo y el Grupo Interdisciplinario de Seguridad de la Información (GISI)

5.3 Incumplimiento

Un empleado que se descubra que ha violado esta política será sujeto a medidas disciplinarias, las cuales pueden incluir el despido o alguna acción que la organización crea conveniente.

6. Documentos y Registros Asociados

Nombre de Documento	Ubicación de Almacenamiento	Propietario	Control de Protección	Programación de Retención
Política de Gestión de Incidentes de Seguridad de la Información	File Server	Organización	Restringido	4 años

7. Historial de Revisiones

Fecha de Cambio	Responsable	Resumen de Cambios

8. Gestión de Documentos

Este documento es válido desde 12/Diciembre/2017. Este documento se revisará periódicamente por lo menos una vez al año para garantizar que se cumplen los siguientes criterios establecidos con los requisitos de la norma ISO 27001:2013 y requisitos legislativos definidos por la ley que corresponda.

ANEXO H : Política y Procedimientos de intercambio de información

1. Resumen

La intención de la Política es concientizar a los colaboradores de la organización criterios de Seguridad en el intercambio de Información que puede darse dentro de la misma o fuera de ella, preservando los principios de confidencialidad, disponibilidad e integridad sobre la misma.

2. Propósito

El presente documento tiene como propósito definir y detallar los lineamientos, políticas, procedimientos de transferencia de información que permitan mitigar el riesgo de fuga o pérdida de información restringida, confidencial o sensible propiedad de la organización.

3. Alcance

Esta política se aplica al uso del intercambio la información embebida dentro de los activos de información de la organización. Todos los empleados o colaboradores, contratistas, consultores, temporales y otros trabajadores de la organización son responsables un correcto uso y tratamiento de la misma, ello de acuerdo con las políticas, leyes y regulaciones locales e impuestas por la organización.

4. Política

La Política y Procedimientos de Intercambio de Información pretende establecer procedimientos y controles de intercambio por medio de la utilización de todo tipo de servicios de comunicación. Es decir, crear lineamientos y consideraciones en el intercambio de información de la organización dentro de ella, entre organizaciones o terceras partes. Asimismo, el intercambio de información debe estar controlado y se deben cumplir todas las legislaciones y normas que correspondan, lo cual conlleve a mantener una adecuada protección de la información de la misma.

4.1. Normas generales aplicables a la Transferencia de Información

4.1.1. Norma N°1: Intercambio de Información en medios físicos o lógicos

Es imprescindible que durante el transporte físico o lógico de la información de la organización, el cual circula en medios informáticos esté protegida contra acceso no autorizado, uso no adecuado o posible corrupción de la misma. Para ello, se debe tomar en cuenta las siguientes consideraciones:

- Utilizar en todo momento medio de transportes confiables en el intercambio o traslado de información en equipos físicos.
- Los equipos físicos donde se almacena la información a trasladar deben estar lo suficientemente protegidos contra daño físico que pueda ocurrir durante su transporte. Es mandatorio que el activo de información físico sea embalado y protegido correctamente con el material de protección necesario.
- En el caso de medios extraíbles o los propios discos duros que sean trasladados por los colaboradores o personal de la organización serán previamente encriptados por un Sistema de Cifrado de Disco mediante tecnología PGP (Pretty Good Privacy - Privacidad Bastante Buena). Solo el colaborador y el administrador del Sistema tendrán las llaves privadas para el descifrado correspondiente.
- Los colaboradores o empleados de la organización no deben revelar ninguna información confidencial o sensible propia de la organización o de clientes de la misma. Esto incluye medios telefónicos, vía correo, medios extraíbles o cualquier canal de audio específico.
- La información confidencial que sea asociada a información de clientes y que estos la soliciten, será entregada en un formato impreso y enviada a la oficina del cliente correspondiente. Adicionalmente, la organización contará con un repositorio de acceso restringido con información de cada cliente, el cual será revisada por el mismo mediante un acceso previo de doble factor de autenticación: Usuario/Clave y mensaje de Texto con un ID aleatorio al teléfono del cliente previamente registrado.
- Los colaboradores o personal de la organización no deberán dejar mensajes con información sensible o confidencial en buzones de voz o contestadores automáticas que puedan reproducirse por personas no autorizadas.

4.1.2. Norma N°2: Responsabilidad del Personal de la Organización

El uso inadecuado en la transferencia de información que cause fuga de información confidencial o restringida de la organización o de los propios clientes serán sujeto a:

- Sanciones que podrán llegar hasta la terminación del contrato de trabajo.
- La organización quedará libre de perjuicio de las acciones legales a las que incurra, según las leyes aplicables vigentes.

5. Cumplimiento de Política

5.1. Medición del Cumplimiento

La Organización y en especial el Oficial de Seguridad de la Información (OSI) verificará el cumplimiento de esta política a través de varios métodos, que incluyen: Visitas periódicas, monitoreo de video, informes de herramientas comerciales, auditorías internas y externas e inspección, entre otros, lo cual proporcionarán comentarios al propietario de la política y al negocio correspondiente gerente de la unidad.

5.2. Excepciones

Cualquier excepción a la política debe ser aprobada por el Gerente de área respectivo y el Grupo Interdisciplinario de Seguridad de la Información (GISI)

5.3. Incumplimiento

Un empleado que se descubra que ha violado esta política será sujeto a medidas disciplinarias, las cuales pueden incluir el despido o alguna acción que la organización crea conveniente.

6. Documentos y Registros Asociados

Nombre de Documento	Ubicación de Almacenamiento	Propietario	Control de Protección	Programación de Retención
Política de Intercambio de Información	File Server	Organización	Restringido	4 años

7. Historial de Revisiones

Fecha de Cambio	Responsable	Resumen de Cambios

8. Gestión de Documentos

Este documento es válido desde 12/Diciembre/2017. Este documento se revisará periódicamente por lo menos una vez al año para garantizar que se cumplen los siguientes criterios establecidos con los requisitos de la norma ISO 27001:2013 y requisitos legislativos definidos por la ley que corresponda.