UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS

FACULTAD DE INGENIERIA

**PROGRAMA ACADÉMICO DE INGENIERÍA DE REDES Y
COMUNICACIONES**

**Diseño de una Red de Seguridad Informática para la Protección del Sistema
Web de un Call Center ante Ataques Informáticos Aplicando la Norma ISO**

27033

TESIS

Para optar el título profesional de Ingeniero de Redes y Comunicaciones

AUTOR

Ochoa Palomino, Angel (0000-0002-5483-2203)

ASESOR

Seminario García, Hernán (0000-0001-6971-355X)

Lima, 03 de abril del 2019

DEDICATORIA

*Quiero dedicar este trabajo a
todas las personas que con
perseverancia han salido
adelante.*

RESUMEN

El presente trabajo de investigación presenta el Diseño de una Red de Seguridad Informática para la protección del Sistema Web del Call Center que ha estado bajo ataques informáticos con el objetivo de aumentar la disponibilidad del sistema.

Asimismo, se apunta a reducir las vulnerabilidades tecnológicas a las que está expuesta la empresa y, finalmente, a implementar una mejora sustancial en la red de datos del Call Center.

El principal instrumento utilizado para elaborar las medidas que permitan aumentar el nivel de seguridad de la empresa estudiada ha sido la norma ISO 27033 basada en recomendaciones, gestión de riesgos y que puede afianzarse con otras normas.

Cabe mencionar, que el modelo puede aplicarse a cualquier empresa sea o no del mismo ámbito comercial.

También, presentamos los costos de los elementos sugeridos para mejorar la situación del Call Center y una metodología desarrollada para determinar los tiempos con una precisión del 95.46% que servirán como guía en caso se quiera implementar el proyecto.

Palabras clave: ISO 27033; Seguridad Informática; Análisis de Brechas; PERT; Análisis de Riesgos; EDT.

Design of a Computer Security Network for the Protection of the Web System of a Call Center against Computer Attacks Applying ISO 27033

ABSTRACT

The present research work presents the design of a secure network based on Security Information concepts for the protection of a Web System of the Call Center that has been under computer attacks with the aim of increasing the availability of the system.

Likewise, it aims to reduce the technological vulnerabilities that the company is exposed and, finally, to implement a substantial improvement in the data network infrastructure Call Center.

The main instrument used to develop the measures to increase the level of safety of the company studied is the ISO 27033 standard based on recommendations, risk management and that can be established with other standards.

It is worth mentioning that the model can be applied to any company, whether it is in the same commercial area or not.

Also, we present the costs of the suggested elements to improve the situation of the Call Center and a methodology developed to determine the times with an accuracy of 95.46% that will serve as a guide in case you want to implement the project.

Keywords: ISO 27033; Informatic Security; Gap Analysis; PERT; Risk analysis; EDT.

TABLA DE CONTENIDOS

1	INTRODUCCIÓN:	1
1.1	MOTIVACIÓN DEL TEMA	1
1.2	ORGANIZACIÓN OBJETIVO	1
1.3	CAMPO DE ACCIÓN EN LA ORGANIZACIÓN OBJETIVO	2
1.3.1	Gestión de Logros	2
1.3.2	Gestión del Negocio	3
1.3.3	Gestión de TI	3
1.4	SITUACIÓN PROBLEMÁTICA	4
1.4.1	Primer Problema: Caída del sistema web	4
1.4.2	Segundo Problema: Lentitud en todos los terminales de los teleoperadores	6
1.4.3	Tercer Problema: El uso incorrecto de los usuarios de red y estaciones de trabajo	7
1.5	PROBLEMA POR RESOLVER	7
1.6	OBJETIVO GENERAL	7
1.7	OBJETIVOS ESPECÍFICOS	7
1.8	INDICADORES DE LOGRO DE OBJETIVOS	8
1.9	JUSTIFICACIÓN DEL PROYECTO	9
1.9.1	Valor Tecnológico	9
1.9.2	Valor Práctico	9
1.9.3	Valor Metodológico	9
1.9.4	Valor Productivo	10
1.10	ESTADO DEL ARTE	10
1.10.1	International Standarization Organization	10
1.10.2	Finalidades de las normas ISO	11
1.10.3	Ventajas	11
1.10.4	ISO/IEC serie 27000	11
1.10.5	Aplicación de las Principales normas en el Proyecto	13
2	MARCO TEÓRICO	13

2.1	IPS	13
2.1.1	Funciones del IPS	13
2.1.2	Estrategias.....	14
2.2	IDS.....	14
2.2.1	Tipos de IDS	14
2.2.2	Comparación con el Firewall.....	14
2.2.3	Mecanismos de Detección de Ataque.....	15
2.2.4	Diferencias entre el IPS e IDS	15
2.3	HERRAMIENTAS WEB DE ANÁLISIS	16
2.3.1	Virus Total.....	16
2.3.2	Mxtoolbox	17
2.4	ISO/IEC 27033:2009	17
2.4.1	Descripción General	19
2.4.2	Procesos.....	20
2.4.3	Anexo A de la norma ISO 27033	27
3	DEFINICIÓN DEL PROBLEMA	32
3.1	ENTORNO DE DESPLIEGUE	32
3.1.1	Situación Actual de la Red	32
3.2	METODOLOGÍA	36
3.2.1	Parametrización	37
3.2.2	Inventario de Activos.....	37
3.2.3	Análisis de Riesgos.....	45
3.2.4	Evaluación de Riesgos.....	64
3.2.5	Tratamiento de Riesgos	69
3.3	DESARROLLO DE ANÁLISIS DE BRECHAS (GRAP ANALYST)	73
3.4	NIVEL DE CUMPLIMIENTO DE LA NORMA ISO 27033	88
3.5	EDT Y REGISTRO DE INTERESADOS.....	90
3.5.1	Registro de Interesados.....	91
3.5.2	Matriz de Poder	92
3.5.3	Nivel de Compromiso de Interesados.....	93
3.6	HITOS PRINCIPALES DEL PROYECTO	94
3.7	RECOPIACIÓN Y PRIORIZACIÓN DE REQUERIMIENTOS.....	94

3.8	PRINCIPALES CONSIDERACIONES PARA LA IMPLEMENTACIÓN DE LA RED DE SEGURIDAD INFORMÁTICA	94
3.9	DESCRIPCIÓN DE LOS ENTREGABLES DEL PROYECTO	95
3.10	PROCEDIMIENTO PARA LA ELABORACIÓN DEL EDT	95
3.11	PROCEDIMIENTO PARA ELABORAR UN DICCIONARIO DE LA EDT	96
3.12	PROCEDIMIENTO DE VALIDACIÓN DEL ALCANCE	96
3.13	EDT DEL PROYECTO	98
3.14	PLAN DE IMPLEMENTACIÓN DEL PROYECTO	99
3.14.1	Planificación	99
3.14.2	Organización.....	102
3.15	CONTROL DEL DISEÑO DE RED	105
3.15.1	Formulario de Control de Actividades	106
3.16	FORMULARIO DE CONTROL DE SUBSISTEMAS.....	107
3.17	ÍNDICES DE EVALUACIÓN.	108
3.17.1	Índice de actividades programadas ejecutadas	108
3.17.2	Índice de duración de actividades.....	108
3.17.3	Índice de actividades programadas retrasadas.....	109
4	DISEÑO DE LA RED INFORMÁTICA.....	110
4.1	IMPLEMENTACIÓN DE LA GESTIÓN UNIFICADA DE AMENAZAS: UTM.....	110
4.2	ZONA DESMILITARIZADA: DMZ.....	110
4.2.1	Beneficios de la Implementación una DMZ.....	110
4.3	USO DE DIFERENTES IP PÚBLICAS	111
4.4	RECOMENDACIONES A APLICAR PARA LA LA RED PROPUESTA	112
4.4.1	Perímetro Lógico	112
4.4.2	Red Interna	112
4.4.3	Servidores	112
4.4.4	Aplicación.....	112
4.4.5	Políticas de seguridad para Servidores y Estaciones de Trabajo.....	112
4.4.6	Protección contra descargas eléctricas.	113
4.4.7	Políticas de Cuentas de Usuario	113
4.4.8	Políticas de clave de acceso a los programas administrativos.....	114
4.5	COSTOS DE LA SOLUCIÓN PLANTEADA	114

4.6	EFFECTIVIDAD DE LA SOLUCIÓN	116
4.7	NIVEL WAN.....	116
4.7.1	Caso de Ataque de SPAM:	118
4.8	NIVEL END POINT.....	122
4.8.1	Caso de Navegación Insegura	125
4.8.2	Caso de UPDATE del Sistema Operativo en las Estaciones de Trabajo.....	132
5	PRUEBAS, RESULTADOS Y VALIDACIÓN	138
5.1	PRUEBAS Y RESULTADOS DEL INDICADOR 1: MATRIZ DE VALORIZACIÓN DE ACTIVOS DE INFORMACIÓN.	139
5.2	PRUEBAS Y RESULTADOS DEL INDICADOR 2: RIESGOS QUE SOBREPASAN EL NIVEL DE TOLERANCIA	142
5.3	PRUEBAS Y RESULTADOS DEL INDICADOR 3: NÚMERO DE CONTROLES RECOMENDADOS POR LA NORMATIVA ISO 27033 CUMPLIDOS	144
5.4	PRUEBAS Y RESULTADOS DEL INDICADOR 4: CÁLCULOS DE TIEMPO EN PROYECTOS DE SEGURIDAD DE LA INFORMACIÓN.....	148
6	COMETARIOS	153
7	CONCLUSIONES DE LOS OBJETIVOS ESPECÍFICOS DESARROLLADOS 154	
8	RECOMENDACIONES	155
9	REFERENCIAS	156
10	ANEXOS	158

ÍNDICE DE TABLAS

Tabla 1. <i>Comparativa entre los Objetivos Específicos, Indicadores y Métricas</i>	8
Tabla 2. <i>Dominios de la norma ISO 27033</i>	18
Tabla 3. <i>Procesos de la norma ISO 27033</i>	20
Tabla 4. <i>Anexos del Estándar 27033</i>	27
Tabla 5. <i>Anexo A.1 del Estándar 27033</i>	28
Tabla 6. <i>Anexo A.2 del Estándar 27033</i>	29
Tabla 7. <i>Anexo A.6 del Estándar 27033</i>	29
Tabla 8. <i>Anexo A.10 del Estándar 27033</i>	30
Tabla 9. <i>Anexo A.13 del Estándar 27033</i>	31
Tabla 10. <i>Estadísticas de Fallos</i>	35
Tabla 11. <i>Metodología de la Gestión de Riesgos</i>	36
Tabla 12. <i>Símbolos de los Activo de la Información</i>	37
Tabla 13. <i>Clasificación de los Activos de Información según la Ubicación</i>	38
Tabla 14. <i>Clasificación de los Activos de Información según su Pertenencia</i>	39
Tabla 15. <i>Activos de la Información identificados en el Call Center 1</i>	40
Tabla 16. <i>Activos de la Información identificados en el Call Center 2</i>	41
Tabla 17. <i>Valor del Activo de Información</i>	43
Tabla 18. <i>Valor de Tasación de los Activo de Información</i>	44
Tabla 19. <i>Amenazas a los enlaces de Comunicaciones 1</i>	46
Tabla 20. <i>Amenazas a los enlaces de Comunicaciones 2</i>	46
Tabla 21. <i>Amenazas a los enlaces de Comunicaciones 3</i>	47
Tabla 22. <i>Amenazas a los enlaces de Comunicaciones 4</i>	47
Tabla 23. <i>Amenazas a los enlaces de Comunicaciones 5</i>	48
Tabla 24. <i>Amenazas a los enlaces de Comunicaciones 6</i>	48
Tabla 25. <i>Amenazas a los dispositivos del Call Center 1</i>	49
Tabla 26. <i>Amenazas a los dispositivos del Call Center 2</i>	49
Tabla 27. <i>Amenazas a la Información del Call Center 1</i>	50
Tabla 28. <i>Amenazas a la Información del Call Center 2</i>	50
Tabla 29. <i>Amenazas a la Información del Call Center 3</i>	51
Tabla 30. <i>Amenazas a la Información del Call Center 4</i>	51

Tabla 31. Amenazas provenientes del Personal del Call Center 1	52
Tabla 32. Amenazas provenientes del Personal del Call Center 2	52
Tabla 33. Amenazas provenientes del Personal del Call Center 3	53
Tabla 34. Amenazas provenientes del Personal del Call Center 4	53
Tabla 35. Amenazas al Data Center del Call Center 1	54
Tabla 36. Amenazas al Data Center del Call Center 2	54
Tabla 37. Amenazas al Data Center del Call Center 3	55
Tabla 38. Amenazas al Data Center del Call Center 4	55
Tabla 39. Amenazas al Data Center del Call Center 5	56
Tabla 40. Amenazas al Data Center del Call Center 6	56
Tabla 41. Amenazas al Data Center del Call Center 7	57
Tabla 42. Amenazas al Data Center del Call Center 8	57
Tabla 43. Vulnerabilidades del Data Center del Call Center	58
Tabla 44. Vulnerabilidades del Hardware del Call Center.....	59
Tabla 45. Vulnerabilidades en la Información del Call Center	60
Tabla 46. Vulnerabilidades en los enlaces de Comunicaciones del Call Center	60
Tabla 47. Vulnerabilidades del Personal del Call Center.....	61
Tabla 48. Riesgos en todos los activos de la Información del Call Center	62
Tabla 49. Riesgos en todos los activos de la Información del Call Center (Continuación)	63
Tabla 50. Impacto de los Riesgos en todos los activos de la Información del Call Center	64
Tabla 51. Probabilidad de Ocurrencia del Riesgo en la red Call Center.....	65
Tabla 52. Tasación de la Exposición del Riesgo en la red Call Center	66
Tabla 53. Principales Riesgos detectados	68
Tabla 54. Tasación del Riesgo en la red Call Center.....	69
Tabla 55. Tratamiento de Riesgos según los controles propuestos.....	70
Tabla 56. Tratamiento de Riesgos según los controles propuestos.....	71
Tabla 57. Tratamiento de Riesgos según los controles propuestos.....	72
Tabla 58. Cláusulas que se usarán en el Diseño de la Red Informática.....	73
Tabla 59. Nivel de cumplimiento de las recomendaciones dadas por la norma ISO 27033 en % 1	75
Tabla 60. Nivel de cumplimiento de las recomendaciones dadas por la norma ISO 27033 en % 2	77

Tabla 61. Nivel de cumplimiento de las recomendaciones dadas por la norma ISO 27033 en % 3	78
Tabla 62. Nivel de cumplimiento de las recomendaciones dadas por la norma ISO 27033 en % 4	80
Tabla 63. Nivel de cumplimiento de las recomendaciones dadas por la norma ISO 27033 en % 5	81
Tabla 64. Nivel de cumplimiento de las recomendaciones dadas por la norma ISO 27033 en % 6	82
Tabla 65. Nivel de cumplimiento de las recomendaciones dadas por la norma ISO 27033 en % 7	84
Tabla 66. Nivel de cumplimiento de las recomendaciones dadas por la norma ISO 27033 en % 8	85
Tabla 67. Nivel de cumplimiento de las recomendaciones dadas por la norma ISO 27033 en % 9	86
Tabla 68. Nivel de cumplimiento de las recomendaciones dadas por la norma ISO 27033 en % 10	87
Tabla 69. Stakeholders	91
Tabla 70. Matriz de poder de los Stakeholders	92
Tabla 71. Nivel de compromiso de los Stakeholders	93
Tabla 72. Cronograma de Despliegue del Diseño de Red Informática.....	97
Tabla 73. Tiempo estimado de instalación de la etapa de Planificación	102
Tabla 74. Funciones del Director del Proyecto	103
Tabla 75. Funciones del Administrador de la Red	104
Tabla 76. Funciones del Jefe de Ejecución	105
Tabla 77. Formulario de Control de Actividades.....	106
Tabla 78. Formulario de Control de Subsistemas.....	107
Tabla 79. Costo de los enlaces de Internet.....	114
Tabla 80. Costo de los equipos de Seguridad.....	115
Tabla 81. Costo de la solución End Point	115
Tabla 82. Descripción del Plan de Pruebas	117
Tabla 83. Descripción del Plan de Pruebas	119
Tabla 84. Descripción del Plan de Pruebas	123
Tabla 85. Descripción de los hosts de navegación.....	125

Tabla 86. <i>Plan de Pruebas del Caso Navegación Insegura</i>	126
Tabla 87. <i>Descripción de los hosts de prueba</i>	132
Tabla 88. <i>Plan de Pruebas del Caso Update</i>	133
Tabla 89. <i>Lista de Indicadores, Métricas y Logros</i>	138
Tabla 90. <i>Cantidad de Controles recomendados por la norma ISO 27033</i>	146
Tabla 91. <i>Nomenclatura de la fórmula</i>	148
Tabla 92. <i>Duración de las actividades del proceso de Planificación</i>	149
Tabla 93. <i>Valor del PERT</i>	151

ÍNDICE DE FIGURAS

<i>Figura 1.</i> Problema Reportado en el Sistema Web	4
<i>Figura 2.</i> Gráfica del consumo del ancho de banda del Sistema Web en el año 2016	5
<i>Figura 3.</i> Gráfica del consumo del ancho de banda del Sistema Web en el año 2017	6
<i>Figura 4.</i> Estándares de la familia 27000.....	12
<i>Figura 5.</i> Interface Gráfica de Virus Total.....	16
<i>Figura 6.</i> Interface Gráfica de MxToolbox	17
<i>Figura 7.</i> Proceso para lograr seguridad de la red.....	19
<i>Figura 8.</i> Zonas de peligro de una red	22
<i>Figura 9.</i> Ubicación de los equipos de Red en el Data Center del Call Center	33
<i>Figura 10.</i> Ubicación de los usuarios en sus módulos de trabajo	34
<i>Figura 11.</i> Interacción de los usuarios y la Web	35
<i>Figura 12.</i> Tasación del Riesgo en la red Call Center.....	67
<i>Figura 13.</i> Puntos cumplidos por el Call Center que recomienda la norma ISO 27033 1 ..	74
<i>Figura 14.</i> Puntos cumplidos por el Call Center que recomienda la norma ISO 27033 2 ..	76
<i>Figura 15.</i> Puntos cumplidos por el Call Center que recomienda la norma ISO 27033 3 ..	78
<i>Figura 16.</i> Puntos cumplidos por el Call Center que recomienda la norma ISO 27033 4 ..	79
<i>Figura 17.</i> Puntos cumplidos por el Call Center que recomienda la norma ISO 27033 5 ..	81
<i>Figura 18.</i> Puntos cumplidos por el Call Center que recomienda la norma ISO 27033 6 ..	82
<i>Figura 19.</i> Puntos cumplidos por el Call Center que recomienda la norma ISO 27033 7 ..	83
<i>Figura 20.</i> Puntos cumplidos por el Call Center que recomienda la norma ISO 27033 8 ..	85
<i>Figura 21.</i> Puntos cumplidos por el Call Center que recomienda la norma ISO 27033 9 ..	86
<i>Figura 22.</i> Puntos cumplidos por el Call Center que recomienda la norma ISO 27033 10 ..	87
<i>Figura 23.</i> EDT del Proyecto	98
<i>Figura 24.</i> Diagrama de Desglose Analítico	99
<i>Figura 25.</i> Organización.....	102
<i>Figura 26.</i> Propuesta de la Nueva Red para el Call Center.....	111
<i>Figura 27.</i> Correo SPAM	118
<i>Figura 28.</i> Análisis del Contenido del correo	120
<i>Figura 29.</i> Política de bloqueo contra el correo SPAM	121
<i>Figura 30.</i> Interface Gráfica de Windows Xp Virtual.....	122

<i>Figura 31.</i> Portal de Pagos Paypal	125
<i>Figura 32.</i> Circuito de Análisis	127
<i>Figura 33.</i> Interface Gráfica del Splunk.....	127
<i>Figura 34.</i> Interface Gráfica del Pcap	128
<i>Figura 35.</i> Interface Gráfica de Virus Total.....	129
<i>Figura 36.</i> Interface Gráfica de Detección de Virus Total.....	129
<i>Figura 37.</i> Interface Gráfica de Url Query	130
<i>Figura 38.</i> Descripción de la redirección en Url Query	131
<i>Figura 39.</i> Topología de Prueba del Antivirus	133
<i>Figura 40.</i> Interface de la Pc de prueba sin Antivirus.....	134
<i>Figura 41.</i> Interface de la Pc de prueba con Antivirus.....	134
<i>Figura 42.</i> Resultados de la Infección en el host sin Kaspersky	135
<i>Figura 43.</i> Resultados de la navegación con Kaspersky	136
<i>Figura 44.</i> Medidor del Indicador 1	139
<i>Figura 45.</i> Activos de información por fase.....	140
<i>Figura 46.</i> Cantidad de Riesgos según el Nivel	143
<i>Figura 47.</i> Gráfica Esperada del Indicador	144
<i>Figura 48.</i> Medidor del Indicador 3	145
<i>Figura 49.</i> Resultados de la Métrica evaluada	147
<i>Figura 50.</i> Gráfico de PERT	149

ÍNDICE DE FIGURAS

Anexo 1. Clasificación de Activos según su Integridad, Confiabilidad y Disponibilidad	158
Anexo 2. Cláusulas de la Norma ISO 27033	160
Anexo 3. Anexo C de la norma ISO 27033	179
Anexo 4. Matriz de Riesgos de los Activos de la Información	185
Anexo 5. Gestión de Riesgos.....	189

1 INTRODUCCIÓN:

1.1 Motivación del Tema

Según el experto Federico Santi, Director de Seguridad de Hewlett Packard Italia, la aplicación de los conceptos de Seguridad de Información será el corazón de la correcta gestión de eventos de seguridad debido a la velocidad a la que cambia el escenario de las amenazas cibernéticas.

Hoy en día, la implementación de Seguridad tiene un costo de hasta 10 veces inferior al de los componentes de un negocio de cualquier giro. Por este motivo, se debe aprovechar al máximo sus alcances de trabajo en términos de prevención con el objetivo de identificar actividades sospechosas.

Se trata de todo un reto en la carrera de los profesionales de la ingeniería de redes demostrar lo aprendido en sus años de estudio. Proponer una red con la visibilidad de todos sus componentes IT que protejan los activos de la información del negocio y que eviten el daño a su reputación que podría ser irreversible o difícil de recuperar.

En los siguientes capítulos, se describirán, también, los conceptos claves que se deben tener en cuenta para elegir los lineamientos básicos antes y después de la puesta en marcha del diseño de la nueva red. Por ejemplo, la utilización del IPS y del IDS junto con los impactos de la nueva red del Call Center.

1.2 Organización Objetivo

La empresa para la que se diseña la solución es un Call Center con sedes en diversos países y un aproximado de 160,000 colaboradores. Sus soluciones combinan el accionar de personas, plataformas telefónicas y servicios web todas destinadas a responder a clientes en América Latina, USA y Europa siendo los principales focos los que se encuentran en Sur América..

La empresa se unió en febrero de 2011 al Pacto Mundial de las Naciones Unidas que establece incorporar los 10 principios que permitan transformar nuestro mundo creando una economía global sostenible e inclusiva que beneficie a todas las personas, comunidades y mercados.

Mediante su política "Eco- eficiente se pone como objetivo optimizar los recursos naturales a través del uso de medios digitales, como los sistemas web, en lugar de avisos de papel para reducir la tala indiscriminada de árboles y el mejor uso de nuestro ambiente. Se preocupa por el desarrollo sostenible de las comunidades donde tienen oficinas, siendo este un factor fundamental para su estrategia corporativa. Se esmera por realizar políticas que permitan a sus trabajadores respetar los sectores ambientales y culturales en los que trabajan. Como resultado de esto, los lazos con sus usuarios o consumidores se ven afianzados y permite transformarlos en socios estratégicos lo cual permite cumplir de mejor forma con las crecientes expectativas de los consumidores a nivel mundial.

El Call Center tiene como lineamientos:

- Visión: Volverse el socio de Negocios más grande de Latinoamérica y generador de soluciones en servicios. Así mismo, en un centro de crecimiento humano que desarrolle los talentos de su personal colaborador.
- Misión: Generar servicios de alta calidad anticipándose a las necesidades de sus clientes o socios de negocio haciéndolos más rentables.

1.3 Campo de Acción en la Organización Objetivo

En Perú, el Call Center comenzó a trabajar desde el año 1999 y en la actualidad cuenta con 3 oficinas en la ciudad de Lima y, hasta la fecha, se ha convertido en el Call Center más importante de la industria en el país con más de 8.000 posiciones de atención y 14,500 empleados. Todo el estudio del documento se enfocará en el “Local Principal o Cabecera” ya que en esta última se aloja el sistema Web y donde se realizan las tres principales funciones de la Empresa: Gestión de Logros, Gestión de IT y Gestión del Negocio.

1.3.1 Gestión de Logros

- El Manejo o gestión de Logros es una política en la que la empresa busca establece metas y logros para que el colaborador desarrolle sus habilidades. Posee el programa "Employment and job-skills training" que permite a los trabajadores recibir una capacitación y así, mediante sus actividades, encontrar las habilidades que pueda tener y que no esté consiente de ellas que le puedan servir para obtener

un mejor puesto y/o en su vida personal. La empresa dedicó cerca de 13.3 millones de horas al "training" en 2014.

- La empresa es un agente relevante a nivel económico ya que contrata a minorías con dificultades para colocarlos en el ámbito laboral. Adicionalmente implementó el voluntariado corporativo, campañas sociales y humanitarias.

1.3.2 Gestión del Negocio

En Gestión del Negocio, el Call Center busca desarrollarse como socio estratégico de muchas empresas de Telecomunicaciones, banca y finanzas. Uno de sus principales clientes es un proveedor de servicios de telefonía Móvil para el cual el Call Center tiene la misión de vender paquetes de internet vía llamadas telefónicas.

1.3.3 Gestión de TI

- El Call Center provee de un sistema WEB que sirve de interface entre su cliente, el proveedor de servicios telefonía, y los usuarios móviles para comprar, pagar o cancelar líneas telefónicas.
- Las ventajas de este sistema web son:
 - Acceso de millones de usuarios a través de un punto de Internet.
 - Permite obtener los servicios de una forma más rápida.
 - Posibilidad de obtener beneficios adicionales por el uso de este medio innovador.
 - Si el cliente no habla el idioma, el sistema web es intuitivo y, de esta manera, más efectivo que un teleoperador.
 - Acceso a más productos y servicios.

1.4 Situación Problemática

1.4.1 Primer Problema: Caída del sistema web

Desde su fundación en 1999, la principal herramienta del call center ha sido el Sistema WEB dirigido a su principal cliente en Perú: Un Proveedor de telefonía Móvil. Esta experiencia ha servido al Call Center para cumplir exitosamente con sus políticas internas de VISIÓN e MISIÓN y consolidar su relación con su principal cliente en un vínculo comercial de más de 15 años. Sin embargo, desde su implementación, el sistema WEB ha estado fuera de servicio en muchas ocasiones.

Los operadores y usuarios manifiestan que desde sus dispositivos móviles y computadoras de escritorios reciben el mensaje:

Figura 1. Problema Reportado en el Sistema Web

Fuente: Elaboración Propia

Se hizo descartes con el proveedor de servicios de internet con pruebas a nivel WAN encontrándose numerosas consultas a la IP del sistema WEB en un determinado intervalo de tiempo.

Figura 2. Gráfica del consumo del ancho de banda del Sistema Web en el año 2016

Fuente: Sistema de Monitoreo del Cliente

El sistema web recibe un enorme flujo de mensajes y solicitudes provenientes de IPs de diferentes países lo que conduce a una sobrecarga del sistema y lo fuerza a cerrarse. Concluyéndose que se trata de un ataque de Negación de Servicios.

Como resultado, los operadores del Call Center tienen que asumir la actividad de cobranza y venta que hacía el sistema web para no perder las ventas ni las cobranzas las líneas telefónicas de su principal cliente.

Figura 3. Gráfica del consumo del ancho de banda del Sistema Web en el año 2017

Fuente: Sistema de Monitoreo del Cliente

Sin embargo, esta medida afecta el rendimiento de los teleoperadores ya que se ven en la necesidad de ampliar su jornada de trabajo y al Call Center ya que se aumentan los pagos por concepto de horas extras y se perjudican los SLA con otros clientes.

1.4.2 Segundo Problema: Lentitud en todos los terminales de los teleoperadores

Los trabajadores experimentan lentitud no solo al conectarse al sistema web, sino a aplicativos internos del Call Center. Esto se debe a la simplicidad de la topología de la red ya que no ha cambiado desde su implementación en el año 1999. Su composición es básica (router, switch y dispositivos periféricos). Existen otros equipos conectados en el mismo segmento de red que las computadoras de los teleoperadores como cámaras de vigilancia que hacen actualización de sus sistemas operativos que consumen el ancho de banda del enlace. La principal razón de no invertir en un mejor esquema de red es por el giro del negocio. Se prefiere invertir en más cubículos o estaciones de trabajo para los teleoperadores y no en una red escalable capaz de adaptarse a nuevos escenarios o topologías.

1.4.3 Tercer Problema: El uso incorrecto de los usuarios de red y estaciones de trabajo

- Los teleoperadores trabajan en turnos rotativos con usuarios de red o del sistema operativo compartidos. El uso indebido de los usuarios de red para iniciar sesión en horario laboral ocasiona lo siguientes:
- Suplantación de identidades de un trabajador con otro.
- Posible exposición de información sensible del Call Center a terceros.
- Ingreso de usuarios con diferentes niveles de conocimiento a la red de datos.
- Exposición a la información sensible de la empresa a códigos maliciosos.
- Acceso a Datos o archivos que no les corresponde usar o de diferentes áreas de trabajo.

1.5 Problema Por Resolver

De los tres problemas detectados, se concluye que el más crítico es la caída del sistema WEB del Call Center debido a los constantes ataques informáticos que recibe y a la ausencia de sistemas que lo protejan; así mismo, la caída del sistema WEB aumenta la carga laboral de otras áreas.

1.6 Objetivo General

Diseñar una red de Seguridad de Informática basada en los requisitos brindados por la norma ISO 27033 que permita determinar las acciones requeridas para proteger el Sistema Web de un Call Center ante ataques Informáticos.

1.7 Objetivos Específicos

- OE1: Desarrollar el análisis de riesgos del Call Center que permita:
 - Clasificar los principales activos de información que soportan el Sistema Web del Call Center.
 - Determinar las amenazas y vulnerabilidades del Sistema Web del Call Center.
- OE2: Realizar un análisis de brecha que permita determinar el nivel de cumplimiento de la web del Call Center con respecto a los requisitos de seguridad indicado por norma ISO 27033.

- OE3: Elaborar el plan de implementación del Diseño de Red Informática para el Call Center.

1.8 Indicadores de Logro de Objetivos

Tabla 1.

Comparativa entre los Objetivos Específicos, Indicadores y Métricas

	OBJETIVO ESPECIFICO		INDICADOR DE LOGRO	MÉTRICA
OE1:	Desarrollar el análisis de riesgos del Call Center que permita:	Clasificar los principales activos de información que soportan el Sistema Web del Call Center.	Matriz de valorización de activos de información.	Porcentaje de activos de información considerados como críticos.
		Determinar las amenazas y vulnerabilidades del Sistema Web del Call Center.	Informe de análisis de riesgos.	Número de riesgos que supera el nivel de riesgo aceptable.
OE2:	Realizar un análisis de brecha que permita determinar el nivel de cumplimiento de la web del Call Center con respecto a los requisitos de seguridad indicado por norma ISO 27033.		Informe de análisis de Brecha.	Número de controles requeridos por el anexo A de la norma ISO 27033.
OE3:	Elaborar el plan de implementación del Diseño de Red Informática para el Call Center.		Plan de acción.	Tiempo de implementación de actividades.

Fuente: Elaboración Propia

1.9 Justificación del Proyecto

Todas empresas se exponen a numerosas amenazas informáticas cuya complejidad ha evolucionado desde sus primeras versiones. Por esta razón, nos vemos en la necesidad de implementar redes informáticas sean capaces de mitigar ataques externos o que puedan mitigar actividades maliciosas y que puedan ser escalables o adaptables a situaciones más complejas. Cabe mencionar, que la inversión en esta solución es necesaria y no aleja a la empresa de su principal giro de negocio. Por este motivo, el diseño de una red basada en normas Seguridad Informática se presenta como una alternativa útil y con beneficios ante la problemática actual.

El presente proyecto no solo presenta el diseño de una red basada en Seguridad de la Información, sino que sigue las recomendaciones de la norma ISO 27033 aplicando el modelo Defensa en Profundidad en beneficio para el Call Center. Los beneficios se describen de la siguiente manera:

1.9.1 Valor Tecnológico

- Las nuevas plataformas informáticas que aparecen hacen necesario la adopción de nuevas tecnologías que modernicen la infraestructura de la red y que otorguen un enlace escalable y del alto rendimiento, que motive a los trabajadores y que renueve la imagen de la empresa ante las de otras.
- Existe la necesidad de diseñar el sistema de Seguridad Informática para proteger al Call Center de ataques informáticos cada vez más sofisticados.

1.9.2 Valor Práctico

- El diseño de Red servirá como marco de referencia a todo personal de Tecnologías de la Información para la solución práctica de los problemas de esta naturaleza.

1.9.3 Valor Metodológico

- Es una referencia de fácil comprensión para la solución de problemas en Call Center o empresas de similar rubro.

1.9.4 Valor Productivo

- Se podrán evitar sobre carga de trabajo a los teleoperadores.
- Reducción de pérdidas económicas.
- La implementación de la red de seguridad de la información permitirá conocer la importancia de la información administrada de tal manera.

1.10 Estado del Arte

Según el Director del Centro Nacional de Protección de las Infraestructuras Críticas (CNPIC), la adopción de las tecnologías emergentes ayuda a crear sistemas estratégicos de defensa en las compañías en términos relacionados con la ciberseguridad para evitar caer en los crecientes ciberataques que se perciben en la actualidad.

En sus declaraciones, define como "Infraestructuras Críticas" aquellos equipos físicos o servicios que al ser interrumpidos repercuten de manera significativa la seguridad o el bienestar económico del individuo o empresa vinculada.

En el trabajo de investigación, destaca como "Infraestructuras Críticas" el sistema web ya que su servicio y sus equipos físicos al sufrir una interrupción impacta seriamente en el desempeño económico del Call Center.

A continuación, se incluye el libro académico necesario para el desarrollo del proyecto. Es un libro con todos conceptos referentes que se pueden utilizar en el proyecto y que nos ayudará a elegir una metodología o normativa para la solución.

1.10.1 International Standarization Organization

La International Standarization Organization o ISO es la entidad internacional independiente, no gubernamental conformado por 162 organismos que desarrollan normas o estándares basados en los consensos relevantes para la innovación y desafíos globales en todo el mundo.

Existen muchas normas ISO, se agrupan por familias o series y cada una de ellas posee una nomenclatura específica. Las cuatro categorías fundamentales son:

1.10.2 Finalidades de las normas ISO

- Ofrecer orientación, simplificación y unificación de criterios en las empresas y organizaciones con el objetivo de reducir costos y aumentar la productividad.
- Buscan estandarizar las normas de productos y servicios en las organizaciones.
- Homogenizan los parámetros de calidad y seguridad de los productos y servicios.

1.10.3 Ventajas

- Prestigio y enorme seguimiento alcanzado. Las normas ISO proporcionan elementos para que una organización pueda alcanzar y mantener mayores niveles de calidad sus productos y servicios.
- Ayudan a satisfacer las necesidades de un cliente cada vez más exigente.
- Constituye ventaja competitiva sobre otras empresas.
- Reduce incidencias en la producción.
- Implementa procesos de mejora continua.

1.10.4 ISO/IEC serie 27000

Las normas ISO/IEC 27000 series son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC).

La serie contiene las mejores recomendaciones o prácticas para desarrollar, implementar y mantener los Sistemas de Gestión de la Seguridad de la Información (SGSI):

- ISO/IEC 27000.- Es el vocabulario del estándar para el SGSI.
- ISO/IEC 27001.- Es la norma más importante de la familia. Norma que especifica los requisitos para la implementación del SGSI. Es la certificación que deben obtener las organizaciones.
- ISO/IEC 27002.- Es código de las buenas prácticas para la gestión de seguridad de la información.
- ISO/IEC 27003.- Son directrices para la implementación del SGSI. Es el soporte de la norma ISO/IEC 27001.

- ISO/IEC 27004.- Corresponden a las métricas para la gestión de la seguridad de la información. Proporciona recomendaciones de quién, cuándo y cómo realizar mediciones de seguridad de la información.
- ISO/IEC 27005.- Trata la gestión de riesgos en la seguridad de la información. Recomendando y alineando métodos y técnicas de evaluación de riesgos de Seguridad en la Información.
- ISO/IEC 27006:2007. - Requisitos para la acreditación de las organizaciones que proporcionan la certificación de los sistemas de gestión de la seguridad de la información.
- ISO/IEC 27033:2009. - Guía completa para el desarrollo de seguridad de las diferentes redes y servicios que existen en la red.

Figura 4. Estándares de la familia 27000

Fuente: Elaboración Propia

1.10.5 Aplicación de las Principales normas en el Proyecto

Luego de evaluar la problemática del Call Center, se determina que la norma más apropiada para el Diseño de la Red de Seguridad Informática para la protección del Sistema Web es la ISO 27033 ya que es una norma dedicada a la seguridad en las redes. Está compuesta por 6 partes que van desde los conceptos generales, directrices de diseño e implementación de seguridad en las redes, aseguramiento de las comunicaciones entre redes y VPN; así como, seguridad de redes Wireless.

2 MARCO TEÓRICO

2.1 IPS

Un Sistema de Prevención de Intrusos o IPS es un dispositivo de seguridad que monitoriza el tráfico de red y las actividades en un sistema en busca de actividades maliciosas.

2.1.1 Funciones del IPS

- Identifica la actividad maliciosa y la detiene
- Puede alertar al administrador ante la detección de intrusiones o actividad maliciosa
- Establece políticas de seguridad para proteger a la red de un ataque.

Los IPS se clasifican en cuatro diferentes tipos:

- Basados en Red LAN (NIPS):
- Basados en Red Wireless (WIPS):
- Análisis de comportamiento de red (NBA)
- Basados en Host (HIPS)

Los IPS categorizan el tráfico malicioso:

- Detección basada en firmas: Igual que un antivirus.
- Detección basada en políticas: Se requiere que se declaren políticas de seguridad.
- Detección basada en anomalías: Según el patrón de comportamiento del tráfico de red.
- Detección basada en firmas: Reconoce una determinada cadena de bytes en cierto contexto, y entonces lanza una alerta.

2.1.2 Estrategias

Detección honey pot (jarra de miel): Se configura un equipo de prueba que llame la atención de los atacantes.

2.2 IDS

Un sistema de detección de intrusiones o IDS es un programa de detección de accesos no autorizados a un host o a una red.

El IDS puede comportarse como un sniffer de red para obtener datos externos sobre las anomalías que pueden ser indicio de la presencia de ataques y falsas alarmas.

2.2.1 Tipos de IDS

- HIDS (HostIDS): Sirve para rastrear los rastros de los intrusos y sus de sus actividades en el host atacado.
- NIDS (NetworkIDS): Es un IDS basado en red que detecta ataques a todo el segmento de la red. Su interfaz debe funcionar en modo promiscuo para capturar todo el tráfico de la red.

2.2.2 Comparación con el Firewall

- Un IDS difiere de un Firewall en que este último generalmente examina intrusiones externas para evitar que estas ocurran, pero no determina un ataque que pueda estar ocurriendo internamente en la red.
- Un IDS examina la intrusión cuando esta toma lugar y genera una alarma y examina ataques que se originan dentro del sistema mediante heurística o patrones conocidos como firmas.

2.2.3 Mecanismos de Detección de Ataque

Un IDS usa alguna de las 3 siguientes técnicas para determinar que un ataque se encuentra en curso:

- Patrón
- Heurística
- Implementación

2.2.4 Diferencias entre el IPS e IDS

Para realizar una correcta gestión de amenazas y vulnerabilidades son prioridades absolutas en un análisis de red, es más importante para los profesionales de la seguridad conocer la funcionalidad de las herramientas de defensa contra intrusos con el fin de tomar buenas decisiones a la hora de implementar la solución.

Un IDS o Sistema de Defensa contra Intrusos y un IPS o Sistemas de Prevención de Intrusiones son productos similares. Sin embargo, no son lo mismo. Es importante empezar con el entendimiento de que IDS e IPS son herramientas muy, muy diferentes. A pesar de que tienen una base común, que se colocan en sitios de la red diferentes, tienen diferentes funciones, y resuelven problemas diferentes.

- El IDS usa tecnologías para prevenir los problemas de seguridad y es de carácter reactivo. Mientras que un IPS es de carácter proactivo en base a políticas desarrolladas que permiten el tráfico "a través de".
- Los IPS's son dispositivos de control. Se colocan entre dos redes y controlar el tráfico que pasa a través de ellos. Esto significa que el IPS está en el lado de la política de seguridad de la red del cliente.

Existe una afinidad entre los Firewalls y los IPS's por eso podemos encontrar ambos dispositivos incorporados en una solución permitiendo de esta manera bloquear y permitir tráfico.

La razón principal para tener un IPS es para bloquear ataques conocidos a través de una red.

2.3 Herramientas Web de Análisis

Se considera muy importante la elección de herramientas web para analizar archivos descargados, tráfico o dominios posiblemente maliciosos que refuercen la seguridad en la red. Los criterios que se han seguido corresponden a los siguientes:

- Reputación.
- Costos.
- Interface de administración amigable.

2.3.1 Virus Total

Virus Total es un portal en el web creado por Hispasec Sistemas con la finalidad de analizar en forma gratuita archivos y páginas web de contenido malicioso. Su sede central está en Andalucía, España y consta de 55 antivirus y 61 motores de detección en línea.

The screenshot displays the Virus Total web interface. At the top, the Virus Total logo is on the left, and a description of the service is on the right. Below the logo, there is a section for community reputation, showing that 2 users have said the sample is 'goodware' and 0 have said it is 'malware'. The file details section shows the file name 'cdbxp_setup_4.3.7.2356.exe', submission date '2010-08-20 11:34:23 (UTC)', and current status 'analysing'. A progress bar is shown below the status. To the right of the file details, there is a 'VT Community' section with a green smiley face icon, the word 'goodware', and a 'Safety score: 100.0%'. Below these sections is a table with four columns: 'Antivirus', 'Version', 'Last Update', and 'Result'. The table lists several antivirus engines and their results for the analyzed file.

Antivirus	Version	Last Update	Result
AhnLab-V3	2010.08.20.01	2010.08.20	-
AVG	9.0.0.851	2010.08.20	-
BitDefender	7.2	2010.08.20	-
ClamAV	0.96.2.0-git	2010.08.20	-
Emsisoft	5.0.0.37	2010.08.20	-
eSafe	7.0.17.0	2010.08.19	-
F-Secure	9.0.15370.0	2010.08.20	-
Fortinet	4.1.143.0	2010.08.20	-

Figura 5. Interface Gráfica de Virus Total

Fuente: Virus Total

2.3.2 Mxtoolbox

Es una herramienta de gestión licenciada que permite analizar Ip's de dominios y encontrar actividad maliciosa que conlleve a un fraude.

Figura 6. Interface Gráfica de MxToolbox

Fuente: MxToolBox

2.4 ISO/IEC 27033:2009

Da una visión general de seguridad de la red y de los conceptos asociados. Aporta orientación de la gestión de la Seguridad de la Red. El alcance de la norma puede modificarse a medida que el estándar sigue desarrollando; puede estudiarse o dividirse en los siguientes dominios:

Tabla 2.

Dominios de la norma ISO 27033

ISO / IEC 27033-1	Describe los conceptos asociados con seguridad de la red. Incluye una descripción general de la seguridad de la red de datos y las definiciones relacionadas, así como una guía sobre cómo identificar y analizar los riesgos de seguridad de la red y en base a todos los requisitos. También describe cómo lograr arquitecturas de seguridad de buena calidad y los aspectos de riesgo, diseño y control asociados con los escenarios típicos de red.
Conceptos para la seguridad de la red.	
ISO / IEC 27033-2	Ayuda a definir como las organizaciones deberían alcanzar arquitecturas de calidad técnica en material de seguridad, diseños e implementaciones que garanticen la seguridad de la red adecuada para sus entornos empresariales.
Pautas para el diseño e implementación de redes.	
ISO / IEC 27033-3	Define los riesgos específicos, técnicas de diseño y los problemas de control asociados de la red de datos.
Riesgos	
ISO / IEC 27033-4	Tiene como objetivo definir los riesgos específicos, las técnicas de diseño y los problemas de control para asegurar los flujos de información entre redes que utilizan gateway de seguridad.
Comunicación entre Redes	
ISO / IEC 27033-5	Define los riesgos específicos, las técnicas de diseño y los problemas de control para asegurar las conexiones que se establecen utilizando redes privadas virtuales (VPN).
Acceso Remoto	
ISO / IEC 27033-6	Define los riesgos específicos, las técnicas de diseño y los problemas de control para proteger las redes inalámbricas IP.
VPN	

Fuente: elaboración Propia

La estructura de este documento se organiza de la siguiente manera:

2.4.1 Descripción General

Los avances en seguridad de la información en los últimos años se han vuelto cada vez más importante. La Norma ISO / IEC 27033 se ocupa específicamente de la planificación e implementación de seguridad de la red mediante sus directrices y medidas.

El tema de este trabajo es una comparación entre los dominios que componen la norma ISO/IEC 27033 en la protección de del sistema Web del Call Center.

El siguiente gráfico describe la estructura de la norma ISO / IEC 27033-1 y su visión general del proceso de planificación de la seguridad de la red y su gestión.

Figura 7. Proceso para lograr seguridad de la red

Fuente: Norma ISO 27033:2009

2.4.2 Procesos

Tabla 3.

Procesos de la norma ISO 27033

Análisis de riesgos y la selección de las medidas	Este procedimiento consiste en "Determinar el Contexto o Alcance y, luego, "La Evaluación de los Riesgos". Se debe reunir toda la información necesaria sobre la situación actual y la configuración de la red dentro de la empresa e identificar los riesgos asociados.
Identificación de Controles	Estos controles pueden ser a la vez técnicas y administrativas y se dan con el fin de implementar la seguridad en la red y mantener las medidas de apoyo.
Identificación de Arquitectura Técnica de Seguridad y Controles	El contenido de esta etapa del proceso es establecer la arquitectura de seguridad de la red técnica adaptables a las necesidades de la empresa y documentarlo sobre la base de los objetivos corporativos.
Desarrollo, implementación, puesta a prueba, verificación y medición	El contenido de esta etapa del proceso consiste en "desarrollar, implementar, probar, verificar y medir la solución a desarrollarse.

Fuente: Elaboración Propia

2.4.2.1 Análisis de Riesgos y Selección de Medidas

Esta sección trata de la identificación de riesgos de la red e identificación de los controles de seguridad.

2.4.2.1.1 Inventario de Red

- El primer paso es recoger toda la información asociada con la red. Para esto es necesarios los documentos que detallen los componentes que intervienen en la red.
- El segundo paso es enlistar las aplicaciones, servicios, tipos de conexiones y otras características en este punto.
- El tercer paso es documentar los tipos de conexión de redes.
- Finalmente, el último paso consiste en reunir información relacionada con la seguridad de la red.

Después de reunir toda la información que pueda ser relevante para la seguridad de red, deben ser objeto de evaluación todos los riesgos que puedan causar perturbación o interferencia de acuerdo con lo que dicte la norma ISO / IEC 27033-1:

- Pérdida de confidencialidad.
- Integridad.
- Disponibilidad.
- No repudio.

Figura 8. Zonas de peligro de una red

Fuente: Norma ISO 27033

Para ser capaz de seleccionar las medidas de seguridad adecuadas, los riesgos y peligros deben ser reconocidos y evaluados. Sólo con este conocimiento, las medidas pueden ser seleccionadas para la protección de la red.

Por lo que el siguiente paso es evaluar la información que se ha recogido en los pasos anteriores.

2.4.2.1.2 Análisis de Riesgos

- La determinación de la importancia de la información y de los servicios.
- Identificación y evaluación de la probabilidad o niveles de amenazas contra la información y de los servicios.
- Identificación y evaluación del grado de gravedad o niveles de vulnerabilidades que podrían ser explotadas por las amenazas detectadas.
- La evaluación de las medidas de los riesgos basados en los potenciales impactos adversos sobre las operaciones comerciales y el nivel de amenazas y vulnerabilidades.

2.4.2.2 Identificación de Controles

La norma ISO / IEC 27033-1 describe 8 Controles de apoyo de carácter técnico y no técnico.

1) Actividades de gestión de la seguridad de la red

- Una política de seguridad documentado con arquitectura de seguridad técnica adjunta.
- Realice comprobaciones de seguridad para garantizar que las medidas implementadas fueron suficiente.
- Documentar las condiciones que deben cumplirse en la red antes de realizarse una conexión.
- Las condiciones de seguridad necesarias para usuarios remotos.
- Plan de emergencia.

2) Responsabilidades

ISO / IEC 27033-1 exige estricta división de responsabilidades para reforzar la seguridad de la red de una organización.

3) Política de Seguridad de la red

De acuerdo con la norma ISO / IEC 27033-1 se debe ocupar específicamente de los requisitos de seguridad de la red para el uso de los recursos, servicios y aplicaciones deben

estar presentes. Debe tenerse en cuenta las consecuencias que vienen con cualquier uso indebido.

4) SecOps red

SecOps red son documentos que describen el apoyo que debe recibir la política de seguridad de los operadores o actores involucrados en las operaciones diarias. Del mismo modo, estos documentos incluyen la asignación de responsabilidades.

5) Verificación de las Correcciones en la seguridad de la red

La norma requiere que la regularidad de la seguridad de la red necesita ser comprobada. El testeo de la eficiencia de las medidas es una parte importante para el mantenimiento y la mejora continua de la seguridad de la información.

6) Las condiciones de seguridad para las conexiones de red

La transferencia de información a otros puntos finales (por ejemplo, internet) posee el riesgo que en el otro extremo de la comunicación no se implementen los requisitos para la seguridad de su propia organización.

7) Las condiciones de seguridad documentados para usuarios remotos

Documentar las de políticas de seguridad para el uso de las VPN.

8) Gestión de incidentes

La protección básica se tratará en los sucesivos capítulos.

2.4.2.3 Identificación de la Arquitectura Técnica de Seguridad y Controles

ISO / IEC 27033 proporciona una guía para crear y documentar una arquitectura de seguridad de la red. Esta sección es de carácter técnico y se refiere específicamente a las redes y sus partes que las componen, y como puede ser desarrollada y documentada.

La norma recomienda la elaboración de los siguientes documentos:

- Documento de arquitectura de seguridad o diseño técnico de la red. Este documento describe la arquitectura o componentes de la seguridad técnica.

- Documento de acceso a la puerta de enlace en términos de seguridad que incluyan firewalls y políticas de seguridad, IDS, IPS.
- Documento de Secops o Procedimientos Operativos de Seguridad.
- Documento que detalle las condiciones de seguras para la conexión a la red para terceros.
- Documento de directrices para los usuarios.

El desarrollo y documentación de una arquitectura de seguridad de la red se divide en los siguientes pasos:

- La preparación para el diseño técnico y la aplicación de seguridad de la red:
 - Inicio del proyecto de seguridad.
 - Requisitos para la seguridad de la red: Compruebe que el hardware y software que componen la red de la organización son apropiados.
 - Revisión de la arquitectura existente: Toda la arquitectura técnica existentes deberían ser descritos, y los requisitos funcionales.
 - Identificación de Activos de información: Identificación de los valores de la empresa.
 - Confirmación de los resultados de la evaluación de gestión de riesgos de seguridad, la revisión de los controles de seguridad de red existentes y/o previstos en el contexto de esos resultados, y selección de posibles controles de seguridad: La comprobación para verificar la eficacia de las medidas y, posiblemente, seleccionar las medidas adecuadas, como resultado de la evaluación de riesgos.
 - La revisión de los requisitos de rendimiento de red y confirmación de criterios. Los requisitos de desempeño necesitan ser revisados junto con las consultas y los criterios de rendimiento requeridos que deben cumplirse en la arquitectura técnica. Por tanto, se requiere de datos para permitir las configuraciones de líneas de comunicación, servidores, gateways de seguridad y demás que asegure la disponibilidad del servicio requerido.
 - Revisión de los requisitos para el desempeño de la red.
- Diseño técnico de seguridad de red: Preparación de la arquitectura de seguridad técnica.
- El uso de "gateway".

- El uso de modelos, marcos y otros.
 - Selección del producto asociado con el diseño de la red de la arquitectura de seguridad basada en factores como idoneidad técnica, rendimiento, capacidad de crecimiento, seguridad lógica y, por supuesto, trayectoria del proveedor.
 - La selección de los productos.
 - Se recomienda una prueba de concepto.
 - Finalizar la Seguridad de la Red Técnica (Arquitectura / Diseño) y la documentación relacionada. Completar y documentar la preparación de la arquitectura de seguridad técnica.
- Preparación para la prueba. Un documento de estrategia de seguridad que deben adoptarse para demostrar la arquitectura técnica de seguridad de red. Principalmente se concentra en cómo los controles de seguridad técnicas deben ser probados y abarca incluso en las pruebas a realizar, por quién y desde dónde. Los preparativos para probar la arquitectura de seguridad deben llevarse a cabo.
- Cierre Formal de la arquitectura de seguridad técnica.
- La aceptación formal de la arquitectura de seguridad técnica.

2.4.2.4 Desarrollo, Implementación, Puesta a Prueba, Verificación y Medición

1. Implementación y prueba

El 27033-1 norma ISO / IEC describe el proceso y todas las medidas correspondientes para lograr una arquitectura de red segura. Debe ser desplegado primero en un entorno de modo de prueba. Si es necesario se deberá cotejarse con las especificaciones contenidas en los diversos documentos elaborados como Políticas de Seguridad, Plan de Continuidad de Negocio, Arquitectura de Seguridad Técnica, etc.). Estas pruebas deben ser predefinidas en un documento. Si se han completado las pruebas, los resultados se debe documentar y debe ser aprobado por la dirección.

2. El funcionamiento de la arquitectura de seguridad técnica

Si la arquitectura de seguridad técnica ha sido aceptada por la administración y si se producen nuevos componentes o cambios significativos, entonces se recomienda ser reexaminados.

3. Supervisión y revisión

Para tener una visión general del estado actual de la arquitectura de seguridad técnica, esta tiene que ser supervisada y vigilante constantemente o de manera anual.

2.4.3 Anexo A de la norma ISO 27033

Tabla 4.

Anexos del Estándar 27033

Anexo A	Temáticas de Tecnología - Riesgos, Técnicas de Diseño y Cuestiones de Control
A.1	Redes de área local
A.2	Redes de área amplia
A.3	Conexiones inalámbricas
A.4	Radio Networks
A.5	Redes de Banda ancha
A.6	Gateway de seguridad
A.7	Redes privadas virtuales
A.8	Redes de voz
A.9	La convergencia IP
A.10	Alojamiento web
A.11	Correo electrónico de Internet
A.12	Acceso enrutado a terceras organizaciones
A.13	Intranet para Data Center

Elaboración Propia

2.4.3.1 Controles sugeridos por el anexo A de la norma ISO 27033

Tabla 5.

Anexo A.1 del Estándar 27033

A.1	Red de Área Local
	Energía
	Proporcionar UPS con apagado automático para dispositivos de red y de usuario críticos.
	Hardware y Software
	Instalar software que detecte código malicioso (incluyendo anti-virus) y actualizarlo periódicamente de forma automática.
	Desactivar unidades extraíbles como unidad de CD-ROM y puertos USB para prevenir la pérdida o fuga de información.
	Eliminar el software obsoleto o que no sean necesarios a las funciones de las aplicaciones.
	Procedimientos
	Se recomienda documentar la configuración del software de seguridad para usarlas en las nuevas estaciones de trabajo.
	Programar la descarga periódica de parches relacionados con la seguridad y sus respectivas actualizaciones.
	Se recomienda crear discos de arranque o reparación de emergencia y almacenarlos en una ubicación segura.
	Implementar registros para los problemas de mantenimiento y el mal uso de las estaciones de trabajo.
	Presentar toda la documentación correspondiente a las estaciones de trabajo (manuales y discos) para el uso del personal técnico.
	Garantizar que todos los router, switches y dispositivos de comunicaciones han cambiado las contraseñas periódicamente.
	Garantizar el cifrado del tráfico de red.
	Implementar procedimientos para la auditoría de red y gestión de sistemas.
	Programar la instalación periódica de actualizaciones de firmware.
	Probar vulnerabilidades de todos los dispositivos conectados a internet.

Fuente: Elaboración Propia

Tabla 6.

Anexo A.2 del Estándar 27033

A.2	Redes de Área Amplia
	Sustitución de los Protocolos intrínsecamente inseguros tales como Telnet y FTP por SSH o TFTP.
	El cifrado del tráfico de red.
	Implementar notificaciones SNMP para la autenticación segura para acceder a los dispositivos WAN.
	Implementar enlaces de contingencia para salidas y entrada de consultas.
	Asignación de dispositivos de red para identificar dispositivos no autorizados dentro de la red.
	La obtención de garantías de servicio del proveedor de servicios que busquen minimizar latencia y jitter en sus enlaces.
	Implementación de auditoría para el acceso a los dispositivos WAN.
	Uso de cortafuegos para descartar tráfico inesperado que entra a la red.
	Uso de software para evitar código malicioso como troyanos, virus, gusanos y spyware.
	Uso de IDS para identificar el tráfico sospechoso dentro de una red.
	Asegurar los lugares de gestión de redes físicamente seguros.
	Asegurar que los dispositivos de red están respaldados.

Fuente: Elaboración Propia

Tabla 7.

Anexo A.6 del Estándar 27033

A.6	Gateways de Seguridad
	Separación virtual de las redes.
	Proporcionar un único punto controlado y manejo de entrada a la red.
	Cumplir con la política de seguridad de la organización en cuanto a las conexiones de red.
	Proporcionar un único punto de acceso para el registro de ingreso.

Fuente: Elaboración Propia

Tabla 8.

Anexo A.10 del Estándar 27033

A.10	Alojamiento web
	Zonificación para limitar el efecto de un ataque exitoso.
	Instalación de los diferentes tipos de firewall para contrarrestar posibles vulnerabilidades de firewall.
	El diseño debe ser examinado hasta encontrar los posibles puntos de fallo y estos deben ser eliminados.
	Instalar carga de conmutación por fallo para proteger contra un falla del equipo.
	Proxy de servicios para limitar el acceso a sitios web.
	Instalación de software anti-malware (incluyendo antivirus) para controlar la importación de malware.
	Plan de direccionamiento IP para limitar el número de direcciones públicas al mínimo.
	Encriptación de los enlaces de gestión.
	Copia de seguridad de todos los registros de transacciones y de eventos de cada servidor y luego copiarlos en un medio de seguridad.
	Implementar un servicio de sincronización de tiempo para analizar el acceso no autorizado y ser capaz de seguir el rastro a través de los archivos de registro.
	Reserva de direcciones IP y MAC.
	Servicio de copia de seguridad.
	Dispositivos que puedan soportar operaciones de 24 horas los 7 días de la semana.
	Los sistemas operativos de apoyo deben ser sometidos a pruebas de seguridad para garantizar que todos los dispositivos están completamente fortificados.
	Implementar aplicaciones robustas cuyo código de programación ha sido verificado.

Fuente: Elaboración Propia

Tabla 9.

Anexo A.13 del Estándar 27033

A.13	Centro de Datos de la Intranet
	Gateways de seguridad para controlar el acceso al centro de datos.
	Uso de IPS e IDS en el centro de datos.
	Código anti-maliciosos (incluyendo antivirus) en los servidores.
	Gestión de dispositivos de infraestructura.
	Servicio de registro y de auditoría en todos los componentes en el centro de datos.
	Plan de continuidad de las fallas.
	Diseño que se adecue a los cambios o necesidades a futuro.
	Comprobaciones de integridad regulares para cambios no autorizados a los datos.
	VLAN para separar los servicios dentro del centro de datos para proteger los servicios más sensibles.
	Dispositivos LAN configurados para controlar los cambios no autorizados a direcciones MAC.
	Uso de protocolos de seguridad.

Fuente: Elaboración Propia

3 DEFINICIÓN DEL PROBLEMA

Se define el problema identificado, su alcance, el impacto en la organización y su causa. Así mismo, se describe el entorno donde será desplegado la solución y los interesados utilizando lenguaje de ingeniería.

3.1 Entorno de Despliegue

En este capítulo, se muestran la situación actual del Call Center, sus elementos presentes y carencias que nos llevarán a realizar los documentos y consideraciones para el diseño de la red de Seguridad Informática acorde a las recomendaciones de la norma ISO 27033.

3.1.1 Situación Actual de la Red

3.1.1.1 Acceso Físico al Data Center

El Data Center del Call Center es una oficina independiente y se encuentra ubicada en el primer piso del local de Ate Vitarte. No existe personal que lo resguarde ante ingresos por actividades (Mantenimiento Preventivo o Correctivo de parte de los Proveedores). Los gabinetes que alojan los dispositivos de red y servidores no cuentan con puertas que aseguren la integridad de los dispositivos. Se diseñó esta solución en un principio para proveer de la suficiente ventilación a la granja de servidores.

Figura 9. Ubicación de los equipos de Red en el Data Center del Call Center

Fuente: Elaboración Propia

3.1.1.2 Acceso Físico a Equipos

Con respecto a las estaciones de trabajo, las computadoras son equipos compartidos entre los usuarios que las usan de acuerdo con el horario de trabajo y a la hora de llegada. Desde cada uno de los computadores, se puede ingresar a las bases de datos y repositorios alojados en los servidores:

- Se llega a dar los casos en las que un usuario por error no cierra su sesión dejando el acceso de su información que solo ellos deben manejar a usuarios no autorizados.
- La información corporativa que el usuario del primer turno maneja se puede obtener ingresando al perfil del usuario.

Figura 10. Ubicación de los usuarios en sus módulos de trabajo

Fuente: Elaboración Propia

3.1.1.3 Sistema Web del Call Center

El sistema web del Call Center se queda fuera de servicio constantemente debido a los ataques sufridos. Luego, experimenta de experimentar una saturación en el enlace. La plataforma tecnológica de esta empresa tiene un modelo básico: Servidor con Antivirus y antimalware.

Figura 11. Interacción de los usuarios y la Web

Fuente: Elaboración Propia

Según estadísticas de la universidad de Veracruz, el lenguaje de programación Java (el sistema Web fue desarrollado en esta plataforma), se encuentra en el cuarto lugar entre los lenguajes de desarrollo más vulnerables (Ver Tabla)

Tabla 10.

Estadísticas de Fallos

ÍTEM	NOMBRE	NÚMERO DE FALLOS
1	Classic ASP	1.686 fallos por megabyte (1.112 fallos críticos por megabyte)
2	ColdFusion	262 fallos por megabyte (227 fallos críticos por megabyte)
3	PHP	184 fallos por megabyte (47 fallos críticos por megabyte)
4	Java	51 fallos por megabyte (5.2 fallos críticos por megabyte)
5	.NET	32 fallos por megabyte (9.7 fallos críticos por megabyte)
6	C ++	26 fallos por megabyte (8.8 fallos críticos por megabyte)
7	iOS	23 fallos por megabyte (0.9 fallos críticos por megabyte)
8	Android	11 fallos por megabyte (0.4 fallos críticos por megabyte)
9	aScript	8 fallos por megabyte (0.09 fallos críticos por megabyte)

Fuente: Universidad de Veracruz

3.2 Metodología

El Sistema Web del Call Center en un entorno de producción enfrenta situaciones problemáticas de distinta naturaleza. Estos inconvenientes pueden originarse cuando sus vulnerabilidades son atacadas o las situaciones amenazadoras se cumplen dentro de su red como desde fuera de la misma. Cuando estas amenazas atacan directamente las vulnerabilidades se produce el Riesgo.

El Call Center tiene la obligación de identificar, analizar y evaluar los riesgos para determinar las necesidades y requerimientos que el Sistema Web necesita para ser protegido.

La Gestión del Riesgo presenta 5 actividades que consecutivamente se ejecutan:

Tabla 11.

Metodología de la Gestión de Riesgos

Proceso	Fases	Actividades
Gestión de Riesgos	Preparación	Parametrización
	Valorización	Inventario de Activos
		Análisis de Riesgos
	Tratamiento	Evaluación de Riesgos
		Tratamiento de Riesgos

Fuente: Elaboración Propia

3.2.1 Parametrización

3.2.1.1 Nivel de Aceptación del Riesgo:

Se aplican los siguientes niveles de Riesgo en la red del Call Center: Extremo, Alto, Medio y Bajo; en donde, los riesgos Extremo y Alto son catalogados como No Aceptable.

3.2.2 Inventario de Activos

Se inicia la identificación de los activos de la información que soportan el sistema Web del Call Center.

Se recomienda realizar el inventario de activos que soportan esta plataforma informática y su valoración según una escala cuantitativa y cualitativa con el objetivo de determinar el impacto que tendría en la empresa (Call Center) de su pérdida. Por este motivo, se procede a elaborar la Matriz de riesgos para visualizar las diferentes escalas en la que cae su importancia y los riesgos que corren.

3.2.2.1 Preguntas que nos ayudarán a realizar el Inventario de Activos de la Información

- ¿Qué tipo de activo es? Software, Hardware, Servicios, Datos, Humano.
- ¿Ha sido declarado público o Privado?
- ¿Es crítico para las operaciones internas?
- El activo de la información debe estar expuesto al público.

Tabla 12.

Símbolos de los Activo de la Información

SIMBOLO	CATEGORÍA DE ACTIVO DE INFORMACIÓN
D	Datos
Hw	Hardware
Sw	Software
T	Trabajador
U	Ubicación
S	Servicios
E	Equipos de Telecomunicaciones

Fuente: Elaboración Propia

El Call Center presenta en sus 3 ambientes anteriormente descritos (Estaciones de Trabajo, Sistema Web y Data Center) presenta los siguientes Activos de la Información y son clasificados y detallados de la siguiente manera (Ver Anexo 4 para los detalles teóricos):

Tabla 13.

Clasificación de los Activos de Información según la Ubicación

CLASIFICACIÓN	ACTIVO DE LA INFORMACIÓN
INTERNO	Estaciones de Trabajo.
	Servidores.
	Periféricos y pendrives.
	Oficinas e instalaciones.
	Gabinets o Racks
	Teleoperadores.
	Personal Técnico.
	Aplicaciones Informáticas.
	Sistemas Operativos.
	Equipos de Comunicaciones.
	Cámaras de Vigilancia.
	Bases de datos.
	Suministros Eléctricos.
EXTERNO	Usuario Final.
	Proveedores.

Fuente: Elaboración Propia

Tabla 14.

Clasificación de los Activos de Información según su Pertenencia

CLASIFICACIÓN	DETALLE
Público	Recursos que pueden ser accedidos por personas ajenas a una empresa o dentro de la misma, pero el término "Área Autorizada" no aplica.
Privado	Recursos que no están disponibles a la comunidad, pero si a los miembros dentro de la empresa o por personal específico de un área.

Fuente: Elaboración Propia

3.2.2.2 Identificación de los Activos de la Información del Sistema Web del Call Center

Tabla 15.

Activos de la Información identificados en el Call Center 1

Información del Activo						
ID	Símbolo	Categoría	Nombre del Activo de Información	Pertenencia	Descripción	Ubicación
1	H	Servidor	SERVIDOR BLADE	Privado	Servidor principal	Interno
2	H	Servidor	SERVIDOR BLADE	Privado	Servidor Contingencia	Interno
3	H	Servidor	SERVIDOR BLADE	Privado	Servidor bases de datos.	Interno
4	E	Sistema de Vigilancia	Camaras de Vigilancia	Privado	Polycom	Interno
5	H	Dispositivos de almacenamiento	NAS, SYNOLOGY	Privado	Unidad de respaldo de Backups	Interno
6	Pw	UPS	UPS 15KVA	Privado	Unidad de poder para los equipos de cómputo	Interno
7	E	Equipo de Ruteo	Router	Privado	Equipo de Internet del Proveedor	Externo
8	E	Equipo de Switching	Switch	Privado	Equipo de Internet del Proveedor	Interno

Fuente: Elaboración Propia

Tabla 16.

Activos de la Información identificados en el Call Center 2

Información del Activo						
ID	Símbolo	Categoría	Nombre del Activo de Información	Pertenencia	Descripción	Ubicación
9	H	Estaciones de Trabajo	Computadoras	Privado	Computadoras de los Teleoperadores	Interno
10	Sw	Sistema Operativo	Windows Server	Privado	Sistema operativo Equipos Servidor backup	Interno
11	Sw	Sistema Operativo	Windows Server	Privado	Sistema operativo Servidor Principal	Interno
12	Sw	Base de Datos	Base de Datos	Privado	Motor de bases de datos para el Sistema Web	Interno
13	Sw	IDS	Antivirus	Privado	Sistema End point de protección antimalware.	Interno
14	S	Servicio de Internet	Internet	Público	Salida a la World Wide Web	Externo
15	S	Servicio Web	Servicio Web	Privado	Sistema de Ventas entre el Call Center y el ISP.	Interno
16	T	Trabajadores	Teleoperadores	Privado	Personal que ingresa los datos al Sistema Web	Interno
17	T	Proveedores	Técnicos	Público	Personal de otras empresas que ingresan al Data Center por trabajos programados.	Externo

Fuente: Elaboración Propia

Todos estos componentes tendrán un valor en base a los criterios de Integridad Confidencialidad y Disponibilidad.

3.2.2.3 Valorización de Activos

El valor de un activo se calcula al sumar los valores numéricos del nivel de relevancia respecto a la Integridad Confidencialidad y Disponibilidad.

Valor del Activo = (Integridad + Confidencialidad + Disponibilidad)

3

A continuación, se debe valorizar cada una de los factores que influyen en el Activo de la información:

Tabla 17.

Valor del Activo de Información

VALOR	DESCRIPCIÓN	CONFIDENCIAL	DISPONIBILIDAD	INTEGRIDAD
5	Crítico	El activo de la información maneja datos o información a los que solo las máximas autoridades del Call Center pueden acceder ya que su divulgación podría afectar irreversiblemente al Call Center.	El activo de la información siempre debe estar disponible ya que su ausencia afectaría irreversiblemente al Call Center.	No se admiten alteraciones en la estructura del activo de la información ya que esto podría dañar irreversiblemente al Call Center.
4	Alto	El activo de la información maneja datos que están restringidos a un proyecto específico y solo el personal de esta área puede acceder a esta información ya que su divulgación podría afectar gravemente al Call Center.	El activo de la información puede estar indisponible una hora y su ausencia afectaría gravemente al Call Center.	Se admite un mínimo de alteraciones en el activo de la información ya que cambios severos afectarían gravemente al Call Center.
3	Medio	El activo de la información maneja datos confidenciales y solo el personal de las áreas internas al proceso pueden acceder a esta información ya que su divulgación podría afectar considerablemente al Call Center.	El activo de la información puede estar indisponible por un día y su ausencia afectaría considerablemente al Call Center.	Se pueden admitir alteraciones en un máximo del 50 % en los componentes del Activo de la Información ya que impactaría considerablemente al Call Center.

2	Bajo	El activo de la información maneja es propia del Call Center y solo su personal pueden acceder ya que su divulgación podría afectar parcialmente al Call Center.	El activo de la información puede estar indisponible por una semana y su ausencia afectaría parcialmente al Call Center.	Se pueden admitir alteraciones en la mayoría de los componentes del Activo de la Información ya que impactaría parcialmente al Call Center.
1	Muy Bajo	El activo de la información es de carácter público y su divulgación no impacta al Call Center.	El activo de la información puede estar indisponible de manera indefinida ya que su ausencia no impacta al Call Center.	Se pueden admitir alteraciones en toda la estructura del Activo de la Información en su totalidad ya que no impacta a los procesos del Call Center.

Fuente: Elaboración Propia

Se debe seleccionar aquellos activos cuyo valor de tasación resulte Alto o Muy alto en base al promedio obtenido de los valores de la Confidencialidad, Integridad y Disponibilidad del activo de la información para ser considerados en la etapa de Análisis.

Tabla 18.

Valor de Tasación de los Activo de Información

Valor	Tasación
4.0-5.0	Crítico
3.0-4.0	Alto
2.0-3.0	Medio
1.0-2.0	Bajo
1.0-1.0	Muy Bajo

Fuente: Elaboración Propia

3.2.3 Análisis de Riesgos

Después de realizar el inventario de activos de la información se realiza el Análisis de Riesgos seleccionando solo aquellos cuyo valor de tasación resulten elevados llegando incluso a ser considerados muy altos. La obtención de los riesgos saldrá del análisis u obtención de las vulnerabilidades y amenazas.

A continuación, se analizan los Riesgo a los que está expuesto el Call Center para luego analizar el impacto que tendrían sobre los Activos de la Información en caso de que sucedan.

El riesgo se produce cuando las amenazas atacan las vulnerabilidades existentes sobre los activos de la Información:

$$\text{Riesgo} = \text{Vulnerabilidad} * \text{Amenaza}$$

En donde se detalla el valor y descripción correspondiente a cada factor.

3.2.3.1 Amenazas detectadas en el Call Center (Ver Anexo 4)

El siguiente análisis representa el catálogo de amenazas sobre los Activos de Información del Call Center. Todas las amenazas detectadas se presentan en los cuadros siguientes:

3.2.3.1.1 Amenazas de los Enlaces de Comunicaciones

Tabla 19.

Amenazas a los enlaces de Comunicaciones 1

Repudio	
Tipos de Activos de la Información Afectados: 1.- Equipos de comunicaciones. 2.- Equipos Informáticos.	Dimensiones (CID) afectados: 1.- Disponible. 2.- Trazabilidad
Descripción: Negación a posteriori de actuaciones o compromisos adquiridos en el pasado. Repudio de Origen: Negación legal de ser el remitente u origen de un mensaje o comunicación. Repudio de Recepción: Negación de haber recibido un mensaje o comunicación. Repudio de Entrega: Negación de haber recibido un mensaje para su entrega a otro. Ocasionado por: NEGACIÓN DE ACCIONES	

Fuente: Elaboración Propia

Tabla 20.

Amenazas a los enlaces de Comunicaciones 2

Interceptación de Información	
Tipos de Activos de la Información Afectados: 1.- Redes de Comunicaciones.	Dimensiones (CID) afectados: 1.- Confidencialidad.
Descripción: El atacante llega a tener acceso a información que no le corresponde. Ocasionado por: ESCUCHA PASIVA	

Fuente: Elaboración Propia

Tabla 21.

Amenazas a los enlaces de Comunicaciones 3

Denegación de Servicios	
Tipos de Activos de la Información Afectados: 1.- Personal Interno. 2.- Equipos Informáticos. 3.- Redes de Comunicaciones.	Dimensiones (CID) afectados: 1.- Disponibilidad.
Descripción: No existen recursos suficientes que impiden la caída del Sistema Web cuando la carga de trabajo es desmesurada. Ocasionado por: SATURACIÓN DEL SISTEMA INFORMÁTICO.	

Fuente: Elaboración Propia

Tabla 22.

Amenazas a los enlaces de Comunicaciones 4

Ingeniería Social	
Tipos de Activos de la Información Afectados: 1.- Personal Interno.	Dimensiones (CID) afectados: 1.- Confidencialidad. 2.- Integridad. 3.- Disponibilidad.
Descripción: Abuso de la confianza del público para que realicen actividades que interesan a posibles agresores. Ocasionado por: SUSTRACCIÓN DE INFORMACIÓN.	

Fuente: Elaboración Propia

Tabla 23.

Amenazas a los enlaces de Comunicaciones 5

Análisis de Tráfico	
Tipos de Activos de la Información Afectados: 1.- Equipos de comunicaciones.	Dimensiones (CID) afectados: 1.- Confidencialidad.
Descripción: El atacante informático puede analizar el contenido de las comunicaciones y puede extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de las comunicaciones.	
Ocasionado por: SATURACIÓN DEL SISTEMA INFORMÁTICO	

Fuente: Elaboración Propia

Tabla 24.

Amenazas a los enlaces de Comunicaciones 6

Caída del sistema por Agotamiento de Recursos	
Tipos de Activos de la Información Afectados: 1.- Servicios. 2.- Equipos Informáticos (Hardware). 3.- Equipos de Comunicaciones.	Dimensiones (CID) afectados: 1.- Disponibilidad.
Descripción: La carencia de recursos informáticos provoca la caída del sistema cuando la carga de trabajo es desmesurada.	
Ocasionado por: SATURACIÓN DEL SISTEMA INFORMÁTICO	

Fuente: Elaboración Propia

3.2.3.1.2 Amenazas del Hardware

Tabla 25.

Amenazas a los dispositivos del Call Center 1

Robo	
Tipos de Activos de la Información Afectados:	Dimensiones (CID) afectados:
1.- Equipos Informáticos (hardware). 2.- Soportes de Información. 3.- Equipamiento auxiliar.	1.- Disponibilidad. 2.- Confidencialidad.
Descripción <p>La pérdida de dispositivos afecta directamente la Disponibilidad de los servicios. Son los problemas más habituales en las empresas. La situación se empeora si los dispositivos hospedan datos ya que se puede sufrir una fuga de información.</p> Ocasionado por: RECUPERACIÓN DE SOPORTES RECICLADOS O DESECHADOS	

Fuente: Elaboración Propia

Tabla 26.

Amenazas a los dispositivos del Call Center 2

Degradación de los Soportes de almacenamiento de la Información	
Tipos de Activos de la Información Afectados:	Dimensiones (CID) afectados:
1.- Equipos de comunicaciones	1.- Disponible.
Descripción: <p>Degradación por el transcurso del tiempo.</p> Ocasionado por: FALLA DE FUNCIONAMIENTO DE HARDWARE.	

Fuente: Elaboración Propia

3.2.3.1.3 Amenazas de la Información

Tabla 27.

Amenazas a la Información del Call Center 1

Mantenimiento y Actualización de Programas	
Tipos de Activos de la Información Afectados: 1.- Aplicaciones (Software).	Dimensiones (CID) afectados: 1.-Disponibilidad. 2.- Integridad.
Descripción: Las actualizaciones del código permiten a los programas o a los componentes del Sistema Web puedan ser utilizados y reparados por el fabricante.	
Ocasionado por: FALLA DE FUNCIONAMIENTO DEL SOFTWARE PERJUICIO A LA MANTENIBILIDAD DEL SISTEMA DE INFORMACIÓN	

Fuente: Elaboración Propia

Tabla 28.

Amenazas a la Información del Call Center 2

Revelación de Información	
Tipos de Activos de la Información Afectados: 1.- Información. 2.- Claves criptográficas. 3.- Servicios. 4.- Aplicaciones (Software). 5.- Equipos de Comunicaciones. 6.- Instalaciones.	Dimensiones (CID) afectados: 1.- Confidencialidad
Descripción Revelación de información.	
Ocasionado por: DIVULGACIÓN. COPIA ILEGAL DE SOFTWARE.	

Fuente: Elaboración Propia

Tabla 29.

Amenazas a la Información del Call Center 3

Vulnerabilidades de los Programas	
Tipos de Activos de la Información Afectados: 1.- Aplicaciones (Software).	Dimensiones (CID) afectados: 1.-Disponibilidad. 2.- Integridad. 3.- Confidencialidad.
Descripción: Con lleva a la falle en la compilación del sistema Web con consecuencias sobre la Disponibilidad, Integridad y Confidencialidad de los datos y la capacidad de operar del proceso. Ocasionado por:	

Fuente: Elaboración Propia

Tabla 30.

Amenazas a la Información del Call Center 4

Difusión de Software con Código Malicioso	
Tipos de Activos de la Información Afectados: 1.- Aplicaciones (Software).	Dimensiones (CID) afectados: 1.-Disponibilidad. 2.- Integridad. 3.- Confidencialidad.
Descripción: Esta actividad propaga software malicioso como virus, spyware, troyanos etc. Ocasionado por:	

Fuente: Elaboración Propia

3.2.3.1.4 Amenazas del Personal

Tabla 31.

Amenazas provenientes del Personal del Call Center 1

Indisponibilidad del Personal	
Tipos de Activos de la Información Afectados:	Dimensiones (CID) afectados:
1.- Personal Interno	1.- Disponibilidad.
Descripción La inasistencia accidental del puesto de trabajo conlleva a la indisponibilidad y falta de atención del servicio. Ocasionado por: DAÑO A LA DISPONIBILIDAD DEL PERSONAL.	

Fuente: Elaboración Propia

Tabla 32.

Amenazas provenientes del Personal del Call Center 2

Abuso de Privilegios de Acceso	
Tipos de Activos de la Información Afectados:	Dimensiones (CID) afectados:
1.- Personal Interno 2.- Claves criptográficas. 3.- Servicios. 4.- Aplicaciones (Software). 5.- Equipos informáticos (Hardware). 6.- Equipos de comunicaciones.	1.- Confidencialidad. 2.- Integridad. 3.- Disponibilidad
Descripción Todos los usuarios en la red poseen un nivel de privilegios para una determinada función en la red. Cuando el usuario abusa de estos privilegios surgen los peligros en la red. Ocasionado por: DAÑO A LA DISPONIBILIDAD DEL PERSONAL.	

Fuente: Elaboración Propia

Tabla 33.

Amenazas provenientes del Personal del Call Center 3

Errores de los Usuarios	
Tipos de Activos de la Información Afectados: 1.- Información. 2.- Claves criptográficas. 3.- Servicios. 4.- Aplicaciones (Software). 5.- Equipos informáticos (Hardware).	Dimensiones (CID) afectados: 1.- Disponibilidad. 2.- Integridad. 3.- Confidencialidad.
Descripción Errores de los teleoperadores cuando usan los servicios. Ocasionado por: ERROR HUMANO	

Fuente: Elaboración Propia

Tabla 34.

Amenazas provenientes del Personal del Call Center 4

Errores de los Proveedores	
Tipos de Activos de la Información Afectados: 1.- Información. 2.- Claves criptográficas. 3.- Servicios. 4.- Aplicaciones (Software). 5.- Equipos de comunicaciones.	Dimensiones (CID) afectados: 1.- Disponibilidad. 2.- Integridad. 3.- Confidencialidad.
Descripción Errores de los proveedores durante el mantenimiento o instalación de nuevos servicios. Ocasionado por: ERROR HUMANO	

Fuente: Elaboración Propia

3.2.3.1.5 Amenazas del Data Center

Tabla 35.

Amenazas al Data Center del Call Center 1

Fuego	
Tipos de Activos de la Información Afectados:	Dimensiones (CID) afectados:
1.- Equipos de comunicaciones. 2.- Equipos Informáticos. 3.- Soportes de Información. 4.- Equipos Auxiliares. 5.- Instalaciones.	1.- Disponible.
Descripción: Posibilidad de que el incendio destruya los Activos de Información. Ocasionado por: INCENDIO	

Fuente: Elaboración Propia

Tabla 36.

Amenazas al Data Center del Call Center 2

Contaminación Mecánica	
Tipos de Activos de la Información Afectados:	Dimensiones (CID) afectados:
1.- Equipos Informáticos. 2.- Soportes de Información. 3.- Equipos Auxiliares.	1.- Disponible.
Descripción: Polvo, Suciedad, Ruido, Vibraciones. Ocasionado por: CONTAMINACIÓN	

Fuente: Elaboración Propia

Tabla 37.

Amenazas al Data Center del Call Center 3

Contaminación Electromecánica	
Tipos de Activos de la Información Afectados:	Dimensiones (CID) afectados:
1.- Equipos Informáticos. 2.- Soportes de Información. 3.- Equipos Auxiliares.	1.- Disponible.
Descripción: Luz Ultravioleta, Campos Magnéticos. Ocasionado por: EMISIONES ELECTROMAGNÉTICAS.	

Elaboración Propia

Tabla 38.

Amenazas al Data Center del Call Center 4

Avería de Origen Físico o Lógico	
Tipos de Activos de la Información Afectados:	Dimensiones (CID) afectados:
1.- Aplicaciones. 2.- Equipos informáticos. 3.- Soportes de Información. 4.- Equipos Auxiliares.	1.- Disponible.
Descripción: Los errores de fábrica ocasionan fallos en los equipos, aplicaciones y en el Sistema Web. Ocasionado por: AVERÍA DEL HARDWARE.	

Fuente: Elaboración Propia

Tabla 39.

Amenazas al Data Center del Call Center 5

Falla en los Servicios de Comunicaciones	
Tipos de Activos de la Información Afectados: 1.- Equipos de comunicaciones	Dimensiones (CID) afectados: 1.- Disponible.
Descripción: Esto conlleva al cese de la transmisión datos a las oficinas remotas o al proveedor y se debe al fallo físico del medio de transmisión. Ocasionado por: PERDIDA DEL ENLACE DE COMUNICACIÓN.	

Fuente: Elaboración Propia

Tabla 40.

Amenazas al Data Center del Call Center 6

Interrupción de otros Servicios y Suministros esenciales	
Tipos de Activos de la Información Afectados: 1.- Equipos Auxiliares.	Dimensiones (CID) afectados: 1.- Disponible.
Descripción: Equipos o funciones dentro del Call Center separados o dependientes del sistema Web. Por ejemplo, servicio de impresión. Ocasionado por: PERDIDA COMUNICACIÓN INTERNA.	

Fuente: Elaboración Propia

Tabla 41.

Amenazas al Data Center del Call Center 7

Condiciones Inadecuadas de Temperatura	
Tipos de Activos de la Información Afectados:	Dimensiones (CID) afectados:
1.- Soportes de Información. 2.- Equipos informáticos. 3.- Equipos Auxiliares.	1.- Disponible.
Descripción: El excesivo calor o humedad que tiene el Call Center afectan el rendimiento de los equipos de cómputo y comunicación. Ocasionado por: FALLAS EN LA CLIMATIZACIÓN	

Fuente: Elaboración Propia

Tabla 42.

Amenazas al Data Center del Call Center 8

Corte de Suministro Eléctrico	
Tipos de Activos de la Información Afectados:	Dimensiones (CID) afectados:
1.- Soportes de Información. 2.- Equipos informáticos. 3.- Equipos Auxiliares.	1.- Disponible.
Descripción: Cese de la energía eléctrica. Ocasionado por: PÉRDIDA DE SUMINISTRO ELÉCTRICO.	

Elaboración Propia

3.2.3.2 Vulnerabilidades detectadas en el Call Center

El siguiente análisis representa el catálogo de vulnerabilidades sobre los Activos de Información del Call Center. Todas las vulnerabilidades detectadas se presentan en el cuadro siguiente:

Tabla 43.

Vulnerabilidades del Data Center del Call Center

DATA CENTER	Protección física inadecuada del Data Center.
	Protección física inadecuada de la sala de llamadas.
	Falta de controles de acceso al data Center.
	Falta de controles de acceso a las salas de llamadas.
	Inestabilidad en el abastecimiento de energía eléctrica.
	Falta de abastecimiento de aire.
	Falta de extintores contra Incendio.
	Falta de mantención del Data Center.

Fuente: Elaboración Propia

Tabla 44.

Vulnerabilidades del Hardware del Call Center

HARDWARE	Falla de las estaciones de trabajo y sus componentes
	Falla de las Cámaras de Vigilancia.
	Degradación de los medios de almacenamiento de Datos.
	Temperatura elevada en los equipos de comunicaciones.
	Exposición de las computadoras a agentes externos dañinos (Líquidos, comidas).
	Falta de mantención a las estaciones de trabajo.
	Obsolescencia de componentes de cómputo.
	Inestabilidad en el abastecimiento de energía eléctrica.

Fuente: Elaboración Propia

Tabla 45.

Vulnerabilidades en la Información del Call Center

INFORMACIÓN	Testeo insuficiente de software.
	Uso de contraseñas débiles.
	Falta de gestión de contraseñas.
	Falta de controles sobre Instalación y Desinstalación de software.
	Falta de documentación del software instalado.
	Falta de uso de parches de software
	Inadecuada gestión de encriptación.
	Falta de protección contra virus y código malicioso

Fuente: Elaboración Propia

Tabla 46.

Vulnerabilidades en los enlaces de Comunicaciones del Call Center

ENLACES DE COMUNICACIONES	Falta de enlaces de Contingencia.
	Cableado de red en mal estado.
	Falta de equipos de Seguridad.
	Protección inadecuada de tráfico sensible.
	Inadecuada administración de red.
	Inadecuada protección para el acceso público.

Fuente: Elaboración Propia

Tabla 47.

Vulnerabilidades del Personal del Call Center

PERSONAL	Poco personal técnico.
	Inadecuado de sistema de reclutamiento de personal.
	Roles indefinidos sobre responsabilidades.
	Falta de medidas de seguridad.
	Falta de políticas de Seguridad de la Información.

Fuente: Elaboración Propia

3.2.3.3 Riesgos Detectados en el Call Center

Tabla 48.

Riesgos en todos los activos de la Información del Call Center

ACTIVO DE LA INFORMACIÓN	RIESGO DEL BIEN O ACTIVO DE LA INFORMACIÓN
Estaciones de Trabajo o Computadoras	Propagación de código malicioso.
	Robo de equipos de cómputo.
Información	Robo de Información
	Intromisiones de otros usuarios a la estación de trabajo.
Redes	Acceso por entidades externas a información sensible o privada del Call Center.
	Propagación de código malicioso en la red del Call Center.
Servidor	Acceso no autorizado a los servidores del Call Center
Soporte Técnico	Acceso y manipulación a redes privadas
	Acceso y manipulación a información privada

Fuente: Elaboración Propia

Tabla 49.

Riesgos en todos los activos de la Información del Call Center (Continuación)

ACTIVO DE LA INFORMACIÓN	RIESGO DEL BIEN O ACTIVO DE LA INFORMACIÓN
Proveedores	Robo de información
	Alteración, Manipulación y Destrucción de información.
Bases de Datos del Sistema Web	Alteración, Manipulación y Destrucción de información.
	Acceso a la Base de Datos del Sistema Web por usuarios no autorizados o ajenos del Call Center.
	Acceso a información sensible del Call Center.
Sistema de Respallos	Alteración, Manipulación y Destrucción de información de respaldo.
	Acceso a los Sistemas de Respaldo por usuarios no autorizados.
Sistemas de Autenticación	Exposición de credenciales de sistemas importantes a usuarios no autorizados.
Salida a Internet	Divulgación de información confidencial del Call Center.

Fuente: Elaboración Propia

3.2.4 Evaluación de Riesgos

En esta sección se evalúa el riesgo con los datos obtenidos en la sección 13.13.3 Riesgos Detectados en el Call Center. Posteriormente se valoriza el impacto sobre los activos de la información que soportan el sistema web del Call Center,

3.2.4.1 Impacto sobre el Call Center

Se valoriza el impacto que tendrán las amenazas identificadas sobre los activos. Así mismo, el valor número se obtiene al promediar el valor de los aspectos como imagen Institucional, Operacional y Legal:

Tabla 50.

Impacto de los Riesgos en todos los activos de la Información del Call Center

VALOR	IMPACTO		
	IMAGEN INSTITUCIONAL PERDIDA DE IMAGEN	OPERACIONAL PARALIZACION EN LAS OPERACIONES	LEGAL INCUMPLIMIENTO DE CONTRATO
Catastrófica (4)	El Call Center pierde su imagen institucional.	Las Operaciones se paralizan y no se pueden recuperar.	Penalizaciones que ponen en riesgo el vínculo entre el Call Center y su cliente.
Significativa (3)	Personal con alto cargo en el Call Center se ve perjudicado.	Las Operaciones se paralizan, pero se recuperan después de unos meses de inactividad.	Penalizaciones que ponen en riesgo el vínculo entre el personal de alto cargo del Call Center y su cliente.
Moderada (2)	El área encargada resulta perjudicada.	Las Operaciones se paralizan, pero se recuperan después de unos días de inactividad.	Penalizaciones que ponen en riesgo el vínculo entre el área del Call Center y su cliente.
Menor (1)	El personal del Call Center resulta perjudicado.	Las Operaciones del Call Center resultan dañados en un nivel mínimo a tal punto que se puede seguir operando.	Penalizaciones que ponen en riesgo el vínculo entre cierto personal del Call Center y su cliente.

Fuente: Elaboración Propia

3.2.4.2 Nivel de Exposición al Riesgo

El nivel de exposición al riesgo se obtiene del producto de los siguientes valores:

- Probabilidad de Ocurrencia del Riesgo.
- Impactos del Riesgo.

Nivel de Exposición al Riesgo = (Probabilidad del Riesgo * Impactos del Riesgo)

Tabla 51.

Probabilidad de Ocurrencia del Riesgo en la red Call Center

PROBABILIDAD DE OCURRENCIA DEL RIESGO		
VALOR	DETALLE	OCURRENCIA
5	Muy alta Probabilidad.	Ha sucedido varias veces en 1 semana.
4	Alta Probabilidad.	Ha sucedido 1 vez al mes en promedio.
3	Media Probabilidad.	Ha sucedido 1 vez por año en promedio.
2	Baja Probabilidad.	Ha sucedido cada 5 años en promedio.
1	Muy baja Probabilidad.	Ha sucedido 1 vez cada 15 años en promedio.

Fuente: Elaboración Propia

3.2.4.3 Tasación de Exposición al Riesgo

El Call Center se expone a diferentes niveles de riesgo. Estos niveles representan los diferentes resultados que tendrían dependiendo de qué tipo de activo de la información impacten o el tipo de vulnerabilidad esté expuesta:

Tabla 52.

Tasación de la Exposición del Riesgo en la red Call Center

VALOR	DESCRIPCIÓN
Riesgo Extremo 15-20	El valor es Muy Alto ya que daños a la Integridad, Confidencialidad y Disponibilidad del activo de la información ocasionaría daños irreparables al proceso del Call Center.
Riesgo Alto 11-14	El valor es Alto ya que daños a la Integridad, Confidencialidad y Disponibilidad del activo de la información ocasionaría daños considerables al proceso del Call Center.
Riesgo Moderado 8-10	El valor es Medio ya que daños a la Integridad, Confidencialidad y Disponibilidad del activo de la información ocasionaría daños medios al proceso del Call Center.
Riesgo Menor 4-6	El valor es Bajo ya que daños a la Integridad, Confidencialidad y Disponibilidad del activo de la información ocasionaría daños menores al proceso del Call Center.
Riesgo Insignificante 1-3	El valor es Muy Bajo ya que daños a la Integridad, Confidencialidad y Disponibilidad del activo de la información ocasionaría daños leves al proceso del Call Center.

Fuente: Elaboración Propia

Figura 12. Tasación del Riesgo en la red Call Center

Fuente: Elaboración Propia

De esta forma, se selecciona los riesgos cuyo valor es Alto y Extremo para la aplicación de controles.

Tabla 53.

Principales Riesgos detectados

Activo de la Información	Riesgo Detectado	Tolerancia	I	P	R	Apetito de Riesgo
Estaciones de Trabajo o Computadoras	Propagación de código malicioso.	Riesgo Extremo	4	5	20	Riesgo No aceptable
Redes	Propagación de código malicioso en la red del Call Center.	Riesgo Extremo	4	5	20	Riesgo No aceptable
Información	Robo de Información	Riesgo Alto	4	3	12	Riesgo No aceptable
Redes	Acceso por entidades externas a información sensible o privada del Call Center.	Riesgo Alto	4	3	12	Riesgo No aceptable
Proveedores	Robo de información	Riesgo Alto	4	3	12	Riesgo No aceptable
Salida a Internet	Divulgación de información confidencial del Call Center.	Riesgo Alto	4	3	12	Riesgo No aceptable

Fuente: Elaboración Propia

3.2.5 Tratamiento de Riesgos

A continuación, se determinará un control de riesgos según los datos obtenidos en el análisis de riesgo. Este control de riesgo va a ser la base para poder mitigar, implementar y controlar los riesgos extremos o con mayor probabilidad de daño. No se analizarán los riesgos de menor impacto ya que su control innecesario.

Se deberá decidir qué acciones se tomarán con los activos que están sujetos a los riesgos detectados. Se aplicará una de las siguientes estrategias: Modificar, Aceptar, Evitar o Compartir.

Tabla 54.

Tasación del Riesgo en la red Call Center

Medidas frente al Riesgo	
Aceptar	Tomar el riesgo sin recurrir a medios para protegerse.
Reducir	Implementar controles
Evitar	Se utiliza cuando los niveles del riesgo son demasiado altos para el Call Center.
Transferir	Esta medida surge cuando no se puede aplicar controles de protección sobre los activos de la información. La única alternativa restante es traspasar el impacto de los riesgos a una tercera organización.

Fuente: Elaboración Propia

Tabla 55.

Tratamiento de Riesgos según los controles propuestos

SEGURIDAD											
Riesgo Presente	Tasación del Riesgo	Acción	C	D	I	Control ISO 27033	Control de Mitigación	I	P	R	Riesgo Residual
Propagación de código malicioso.	Riesgo Extremo	Reducir			x	Anexo A: 8.7 Protección contra código malicioso	Configurar las estaciones de trabajo con acceso limitado	4	5	20	Riesgo Insignificante
							Bloquear panel de configuración de antivirus para evitar manipulación de los usuarios finales				
							Mantener el antivirus activado en todas las estaciones de trabajo.				
							Actualizar antimalware o antivirus en las estaciones de trabajo.				
							Adquirir antimalware o antivirus con licenciamiento empresarial.				
Propagación de código malicioso en la red del Call Center.	Riesgo Extremo	Reducir			x	Anexo A: 8.7 Protección contra código malicioso	Configurar las estaciones de trabajo con acceso limitado a redes.	4	5	20	Riesgo Menor
							Monitorear los puertos TCP/UDP.				

Fuente: Elaboración Propia

Tabla 56.

Tratamiento de Riesgos según los controles propuestos

SEGURIDAD											
Riesgo Presente	Tasación del Riesgo	Acción	C	D	I	Control ISO 27033	Control de Mitigación	I	P	R	Riesgo Residual
Robo de Información	Riesgo Alto	Reducir	x	x		10.5Gestión de la vulnerabilidad Técnicas	Encriptar información en los discos duros del Call Center.	4	3	1 2	Riesgo Insignificante
							Respaldar información periódicamente en servidores del Call Center.				
							Implementar contraseña de arranque en la BIOS de las estaciones de trabajo del Call Center.				
							Implementar contraseña de inicio de sesión en las estaciones de trabajo del Call Center.				
Acceso por entidades externas a información sensible o privada del Call Center.	Riesgo Alto	Reducir	x			10.5Gestión de la vulnerabilidad Técnicas	Monitorear las conexiones activas.	4	3	1 2	Riesgo Menor
							Monitorear la modificación de los archivos del Call Center.				
							Monitorear los puertos TCP/UDP.				

Fuente: Elaboración Propia

Tabla 57.

Tratamiento de Riesgos según los controles propuestos

SEGURIDAD											
Riesgo Presente	Tasación del Riesgo	Acción	C	D	I	Control ISO 27033	Control de Mitigación	I	P	R	Riesgo Residual
Robo de información	Riesgo Alto	Reducir	x	x		7.8Protección del equipo contra robos	Monitorear los puertos TCP/UDP.	4	3	12	Riesgo Insignificante
Divulgación de información confidencial del Call Center.	Riesgo Alto	Reducir	x			10.5 Gestión de la vulnerabilidad Técnicas	Bloquear el acceso a páginas de internet no seguras o de dudosa reputación.	4	3	12	Riesgo Menor
							Uso de firewalls para la protección de tráfico hacia y desde Internet.				
							Monitorear los puertos TCP/UDP.				
							Desarrollar Políticas de Seguridad para el acceso a internet.				

Fuente: Elaboración Propia

3.3 Desarrollo de Análisis de Brechas (GRAP ANALYST)

A continuación, se presenta la comparativa Gráfica entre las Cláusulas de las normas ISO 27033 y su cumplimiento por el Call Center. Se aclara que esta comparativa se hace tomando como referencia 7 cláusulas de las 13 dictadas en el Anexo A de la norma ISO 27033:

Tabla 58.

Cláusulas que se usarán en el Diseño de la Red Informática

Anexo A	Temáticas de Tecnología - Riesgos, Técnicas de Diseño y Cuestiones de Control
A.1	Redes de área local
A.2	Redes de área amplia
A.6	Gateway de seguridad
A.10	Alojamiento web
A.12	Acceso enrutado a terceras organizaciones
A.13	Intranet para Data Center

Fuente: Elaboración Propia

Figura 13. Puntos cumplidos por el Call Center que recomienda la norma ISO 27033 1

Fuente: Elaboración Propia

Tabla 59.

Nivel de cumplimiento de las recomendaciones dadas por la norma ISO 27033 en % 1

Redes de Área Local	OBJETIVO	ACTUAL
Gabinetes seguros para Equipos de Comunicaciones	100	50
UPS para equipos críticos	100	100
Software antimalware	100	0
Desactivación de Unidades Extraíbles	100	30
Eliminar el Software Obsoleto.	100	50
Documentación de software instalado en cada Estación de Trabajo.	100	30
Descarga periódica de Parches de Seguridad	100	10
Discos de Arranque o de Emergencia	100	10
Registros de problemas de las estaciones de trabajo.	100	10
Manuales y discos para el uso del personal técnico.	100	0
Cambio de contraseñas para equipos de comunicación	100	0
Cifrado del tráfico de red.	100	0
Procedimientos para la auditoría de Red y gestión de sistemas.	100	50
Instalación periódica de actualizaciones de firmware.	100	50
Prueba de vulnerabilidades de todos los dispositivos conectados a internet.	100	0

Fuente: Elaboración Propia

Figura 14. Puntos cumplidos por el Call Center que recomienda la norma ISO 27033 2

Fuente: Elaboración Propia

Tabla 60.

Nivel de cumplimiento de las recomendaciones dadas por la norma ISO 27033 en % 2

Redes de Área Amplia	OBJETIVO	ACTUAL
Sustitución de los Protocolos Inseguros.	100	0
Cifrado del tráfico de red.	100	10
Implementación de notificaciones SNMP en dispositivos WAN.	100	100
Implementación de enlaces de contingencia.	100	0
Dispositivos de red para identificar dispositivos no autorizados dentro de la red.	100	0
Garantías del ISP del servicio que busque minimizar latencia y jitter en sus enlaces.	100	0
Implementación de auditoría para el acceso a los dispositivos WAN.	100	100
Uso de cortafuegos para descartar tráfico inesperado que entra a la red.	100	100
Uso de software para evitar código malicioso como troyanos, virus, gusanos y spyware.	100	0
Uso de IDS para identificar el tráfico sospechoso dentro de una red.	100	0
Asegurar los lugares de gestión de redes físicamente seguros.	100	40

Fuente: Elaboración Propia

Anexo A.6 Gateways de seguridad

Figura 15. Puntos cumplidos por el Call Center que recomienda la norma ISO 27033 3

Fuente: Elaboración Propia

Tabla 61.

Nivel de cumplimiento de las recomendaciones dadas por la norma ISO 27033 en % 3

Gateways de Seguridad	OBJETIVO	ACTUAL
Separación virtual de las redes.	100	10
Proporcionar un único punto controlado y manejo de entrada a la red.	100	100
Cumplir con la política de seguridad de la organización en cuanto a las conexiones de red.	100	10
Proporcionar un único punto de acceso para el registro de ingreso.	100	100

Fuente: Elaboración Propia

Anexo A.10 Alojamiento web

Anexo A.10.1 Tráfico de Salida a Internet

Figura 16. Puntos cumplidos por el Call Center que recomienda la norma ISO 27033 4

Fuente: Elaboración Propia

Tabla 62.

Nivel de cumplimiento de las recomendaciones dadas por la norma ISO 27033 en % 4

Tráfico de Salida a Internet	OBJETIVO	ACTUAL
Listas negras y blancas (para acceso a Internet).	100	0
Instalar un servidor proxy saliente y un filtro de contenido.	100	40
Instalar un servidor de detección de código malicioso.	100	40
Acceso a los equipos con usuario de lectura.	100	40
Eliminar o aislar ordenadores infectados en la red.	100	10
Capacitar al personal para no descargar y ejecutar software desde Internet.	100	50

Fuente: Elaboración Propia

Anexo A.10.2 Acceso entrante desde Internet

Figura 17. Puntos cumplidos por el Call Center que recomienda la norma ISO 27033 5

Fuente: Elaboración Propia

Tabla 63.

Nivel de cumplimiento de las recomendaciones dadas por la norma ISO 27033 en % 5

Acceso entrante desde Internet	OBJETIVO	ACTUAL
Instalar las medidas de autenticación.	100	0
Instalar un servidor externo web configurado en su propia DMZ fuera de Internet frente al firewall.	100	0
Instalar un servidor apropiado para proporcionar acceso eficiente a los escritorios de los usuarios.	100	0
Instalar un servidor proxy entrante (y de selección de contenido).	100	0
Sistema periódico de instalación de parches de seguridad.	100	50
Actualizaciones de software en servidores.	100	100
Integrar múltiples detectores código malicioso.	100	0
Uso de IDS / IPS.	100	0

Fuente: Elaboración Propia

Anexo A.10.3 Acceso a Internet para empleados

Figura 18. Puntos cumplidos por el Call Center que recomienda la norma ISO 27033 6

Fuente: Elaboración Propia

Tabla 64.

Nivel de cumplimiento de las recomendaciones dadas por la norma ISO 27033 en % 6

Servicios de Acceso a Internet para los Empleados	OBJETIVO	ACTUAL
Política de Seguridad.	100	50
Comunicaciones y Operaciones administrativas.	100	100
Control de acceso.	100	0

Fuente: Elaboración Propia

Anexo A.12 Acceso enrutada a terceras organizaciones

Anexo A.12.1 Servicios al Cliente

Figura 19. Puntos cumplidos por el Call Center que recomienda la norma ISO 27033 7

Fuente: Elaboración Propia

Tabla 65.

Nivel de cumplimiento de las recomendaciones dadas por la norma ISO 27033 en % 7

Negocio para los servicios al cliente	OBJETIVO	ACTUAL
La autenticación mediante certificados digitales, contraseñas, datos biométricos o tarjetas inteligentes.	100	100
Uso de cortafuegos y Listas de Control de Acceso para evitar el acceso de usuarios no autorizados.	100	0
Control de acceso basado en roles para limitar la función del usuario.	100	100
Revisión del registro de Aplicación Web para la identificación de ataques y su contención.	100	50
Cifrado de la información almacenada.	100	100
Uso de protocolos TLS para la seguridad entre los navegadores y servidores web.	100	0
Protección de mensajes SOAP para la comunicación de objetos pertenecientes a servicios Web.	100	0
Archivo de datos de verificación / integridad utilizando algoritmos: como picadillo / sumas de comprobación, certificados	100	0

Fuente: Elaboración Propia

Anexo A.12.2 Servicios Empresariales

Figura 20. Puntos cumplidos por el Call Center que recomienda la norma ISO 27033 8

Fuente: Elaboración Propia

Tabla 66.

Nivel de cumplimiento de las recomendaciones dadas por la norma ISO 27033 en % 8

Negocio de Servicios Empresariales	OBJETIVO	ACTUAL
Política de Seguridad para la Gestión de Acceso.	100	50
Roles y responsabilidades claramente identificados.	100	100
Acceso basado en roles y con límite de privilegios.	100	0
Cifrado de datos.	100	0
Autenticación de identidad tanto de receptores como emisores de información.	100	0
Uso de VPN o Redes Privadas Virtuales.	100	0
Certificados Digitales.	100	0

Fuente: Elaboración Propia

Anexo A.13 Intranet para Data Center

Anexo A.13.1 Entornos Altamente Sensibles

Figura 21. Puntos cumplidos por el Call Center que recomienda la norma ISO 27033 9

Fuente: Elaboración Propia

Tabla 67.

Nivel de cumplimiento de las recomendaciones dadas por la norma ISO 27033 en % 9

Entornos Altamente Sensibles	OBJETIVO	ACTUAL
Adecuada segmentación de la red mediante el uso de tecnologías de redes privadas virtuales.	100	50
Se recomienda encriptar datos almacenados a nivel de aplicación.	100	0

Fuente: Elaboración Propia

Anexo A.13.2 Segmentación de la Red

Figura 22. Puntos cumplidos por el Call Center que recomienda la norma ISO 27033 10

Fuente: Elaboración Propia

Tabla 68.

Nivel de cumplimiento de las recomendaciones dadas por la norma ISO 27033 en % 10

Segmentación de la red para el Cumplimiento de los Requisitos específicos de cada país en las Organizaciones Internacionales	OBJETIVO	ACTUAL
Instalar gateways de seguridad	100	5
Instalar proxies a nivel de aplicación.	100	5
Aplicar técnicas de control de acceso.	100	5

Fuente: Elaboración Propia

3.4 Nivel de Cumplimiento de la Norma ISO 27033

El Call Center no cuenta con una política de seguridad de la información. Posee un mecanismo de mitigación de riesgo dentro del proceso de apoyo al sistema Web estos fueron determinados de acuerdo a una opinión técnica sin ningún apoyo de una norma internacional. Motivos por los cuales, se necesita actualizar a la norma ISO-27033.

Existe un gobierno de TI básico. Las funciones de gestión de tecnologías de la información son realizadas por el soporte técnico local y el administrador de la sede u oficina, pero este no incluye la formalización de la estructura organizativa, responsabilidades, procedimientos y planificación de actividades sobre la gestión de seguridad y privacidad de la información.

Así mismo, existe una metodología de gestión del riesgo en el Call Center. El área de Calidad identifica y gestiona los riesgos.

Existe un documento donde se tiene clasificado los activos de información con una revisión anual.

Cada proceso del Call Center se encuentra representado por las matrices de identificación de riesgo.

Cabe mencionar que las matrices de riesgo no incluyen riesgos de seguridad de la información para los procesos propios del Call Center ni para la administración del sistema Web. Se encontraron evidencia análisis de riesgos operativos tecnológico.

No existen controles implantados para seguridad de red o comunicaciones locales. Recientemente se adquirió una herramienta de monitoreo que permite ver al administrador de red cuando se produce una caída total del enlace, saturación del enlace, pero no cuando sufre de ataques informáticos para el análisis proactivo que amenace al sistema web. Se cuenta como medida de contingencias para dicho sistema Web. Existen una correcta segmentación de la red mediante vlans para personal administrativo y teleoperadores y controles de acceso con validación MAC.

No hay Tele-workers ni acceso a VPN. Por estos motivos, no existen técnicas criptográficas y de ciframiento para uso de conexiones remotas. Tampoco se observa políticas de manejo de contraseñas fuertes o expiración de claves.

El sistema Web del Call Center se encuentra respaldado por el proveedor de servicios de Internet (ISP) con un contrato de confiabilidad del 99,99%. Se trata de un enlace dedicado con disponibilidad del 1:1 sin servicios de seguridad de appliance. El contrato debe ser revisado con el proveedor para cambiarlo por un enlace de Servicios Gestionados o Seguridad desde La Nube que permita crear un sistema de alarmas y vulnerabilidades.

La gestión de incidentes de seguridad se realiza sobre la misma herramienta de gestión de incidentes del Outsourcing de Helpdesk, y existen formatos para la recolección de información de incidentes eventos, pero estos no se encuentran registrados en el sistema documental. Se hace necesario la constitución de una base de conocimiento especializada para seguridad de la información, en la cual se pueda tener la información aplicada de los incidentes para realizar identificación de vulnerabilidades y análisis de problemas. No se cuenta con procedimientos formalizados para la recolección de pruebas de incidentes y eventos y cadena de custodia.

En cuanto a la seguridad física, los equipos de comunicaciones se encuentran distribuidos en un rack de 2 columnas junto con los equipos de infraestructura. La ausencia de un ingeniero de redes o infraestructura dentro del área de sistemas trae como resultado la ausencia de un responsable del acceso a la data center o de monitoreo que garantice sustentabilidad operacional. El soporte técnico del Call Center cubre aproximadamente el 10% de las funciones que hostea la data center incluyendo el sistema de CCTV.

En cuanto a la gestión de privacidad de datos personales, la entidad es consciente de la importancia del tratamiento de privacidad de sus activos de información, por lo cual contrató la ejecución de una consultoría sobre manejo de datos personales con una empresa externa con experticia en tratamiento de información en el sector salud. La consultoría se encuentra en etapa de planeación.

Se tiene un plan de continuidad de negocio operativo y se realizan periódicamente análisis de impacto de negocio (BIA) para algunas áreas críticas, pero no se estableció en un Plan de continuidad de Negocio.

La capacitación en seguridad de la información no está formalizada. Se evidencian boletines y correos para generar concienciación sobre la Seguridad Informática dirigida a todo el personal del Call Center.

3.5 EDT y Registro de Interesados

La Gestión de los interesados del proyecto se convierte en una función que cada vez adquiere mayor relevancia ya que logra la participación eficaz de los interesados.

Por este motivo, debemos partir de la identificación y mantenimiento de un registro de los mismos. Toda esta información está guardada en este documento, la organización a la que pertenecen, categorías, nivel de interés e influencia sobre el proyecto entre otros aspectos. Así mismo, se presenta la siguiente leyenda de los términos a usar:

Influencia: I: Inicio; P: Planificación; E: Ejecución; S: Supervisión y Control; C: Cierre, F: Favorable; N: Neutra / A: Alta; M: Media; B: Baja

3.5.1 Registro de Interesados

Tabla 69.

Stakeholders

ORGANIZACIÓN	CARGO	REQUISITOS SOBRE SISTEMA DE SEGURIDAD INFORMÁTICA	INFLUENCIA					INFLUENCIA SOBRE EL DISEÑO DE LA RED DE SEGURIDAD INFORMATICA	Nivel interés (Bajo, Medio, Alto)
			I	P	E	S	C		
Call Center	Gerente General del Call Center	Administra el buen funcionamiento de los recursos que tiene el Call Center.	FA	FA	FA	FA	FA	Gestión de compromisos Y requerimientos administrativos, operativos y legales	A
Call Center	Jefe de Infraestructura de Red	Proveer del espacio y otras necesidades dentro del data center para la nueva solución.	FB	FB	FB	NB	NB	Gestión de requerimientos técnicos y operativos	A
Call Center	Jefe de Compras	Proveer del capital necesario para la compra de la solución.	NB	NB	AB	AB	AB	Gestión de compra de cara a proveedores de servicios	A
Call Center	Teleoperadores	Personal que usará el sistema web.	NB	NB	AB	AB	AB	Cumplir con la habilitación de los servicios en los tiempos comprometidos por cada etapa	B

Fuente: Elaboración Propia

3.5.2 Matriz de Poder

Tabla 70.

Matriz de poder de los Stakeholders

		Autoridad sobre el Proyecto	
		Alta	Baja
Alta	1.	Jefe de Infraestructura	
	2.	Jefe de Compras	
Baja			3. Tele operadores

Fuente: Elaboración Propia

3.5.3 Nivel de Compromiso de Interesados

Tabla 71.

Nivel de compromiso de los Stakeholders

TÍTULO	ÁREA	ROLES	REQUISITOS	EXPECTATIVAS
Jefe de Infraestructura de Red	Jefe de Infraestructura de Red	Proveer del espacio y otras necesidades dentro del data center para la nueva solución de seguridad informática.	Gestión de requerimientos técnicos y operativos	Evitar la sobre carga de actividades del área de los teleoperadores por la caída del portal web del call center.
Jefe de Compras	Dpto. de Compras	Compra de todas las soluciones necesarias para la red de seguridad informática.	Cumplir con la política de adquisiciones.	Cumplimiento del proyecto dentro de la fecha de compromiso.
Teleoperadores	Teleoperadores	Vender a través del sistema web.	Cumplir con la gestión de entrega de equipos microondas.	Liberarse de las tareas de vender a través del sistema web cuando la aplicación queda fuera de servicio

Fuente: Elaboración Propia

3.6 Hitos Principales del Proyecto

- Inicio del proyecto.
- Presentación y Aprobación del Proyecto DISEÑO DE UNA RED DE SEGURIDAD INFORMATICA PARA LA PROTECCIÓN DEL SISTEMA WEB DE UN CALL CENTER.
- Revisión de los Requerimientos.
- Evaluación Técnica 1.
- Entrega del Plan de Pruebas.
- Revisión de los Casos de Prueba.

3.7 Recopilación y Priorización de Requerimientos

- Los requerimientos se relevarán en reuniones conjuntas entre los usuarios solicitantes y el equipo del proyecto.
- El equipo de proyecto documentará los requerimientos en el documento correspondiente y el líder usuario los revisará y validará para luego firmarlos en señal de aceptación.
- La recopilación será planificada en reuniones de trabajo cuyas fechas de realización serán consensuadas con el líder usuario para comprometer los recursos humanos con el conocimiento detallado del proceso y poder optimizar el grado de certeza del requerimiento.

3.8 Principales Consideraciones para la Implementación de la Red de Seguridad Informática

- La red debe ser capaz de recopilar información sobre el tipo de ataque al que fue víctima el sistema web.
- La red debe ser capaz de registrar la hora a la que sucedió el ataque. Esto servirá para el control del personal e información para el área de sistemas.
- La red debe permitir generar reportes sobre los resultados del análisis y tipo de acción correctiva.

3.9 Descripción de los Entregables del Proyecto

- Acta de constitución, Plan de dirección de proyecto
- Modelos Propuestos o Prototipos.
- Integración de partes de la nueva red.
- Plan de pruebas e Informe de pruebas.
- Plan de Capacitación e Informe de cierre.

3.10 Procedimiento para la Elaboración del EDT

- El EDT del proyecto será estructurado utilizando la herramienta de Descomposición. Identificándose inicialmente los entregables de las fases del proyecto.
- Se considerarán cuatro (04) fases para el proyecto: Planificación, Análisis, Diseño y, Pruebas y Capacitación.
- Se asignará dueños y responsables para cada fase.
- En la etapa de planificación se recopilarán los requerimientos para armar el cronograma y los alcances del proyecto
- En la fase de planificación se recogen las especificaciones, un cronograma de trabajo y un registro de interesados.
- En la fase de análisis se analizan los riesgos a los que está expuesto el Call Center debido a la distancia a la que se encuentra de las sugerencias dadas por la norma ISO 27033.
- En la fase de diseño se crea el plan de implementación.
- En la fase de pruebas y Capacitación tendremos las pruebas realizadas y sus resultados.
- Todas las fases serán revisadas con los stakeholders para estar de acuerdo con los tiempos planteados y el desarrollo del proyecto.

3.11 Procedimiento para Elaborar un Diccionario de la EDT

- Se colocarán las métricas
- La estimación de costos
- Entradas, salidas y puntos de control.
- Declaración de responsables.

3.12 Procedimiento de Validación del Alcance

- Al término de elaboración de cada entregable, éste debe ser presentado al Jefe del Proyecto, el cual se encargará de aprobar o presentar las observaciones del caso. Si el entregable es aprobado, es enviado al cliente.
- Los alcances irán alineados con los objetivos y requerimientos planteados por el cliente en las primeras reuniones de recopilación de información.
- Reuniones con el cliente para revisar las actas de los avances para validar el correcto avance del proyecto y el desarrollo de las políticas necesarias para proteger los Assets del Call Center.

Tabla 72.

Cronograma de Despliegue del Diseño de Red Informática

ID	Nombre de Tarea	Duración en Días
1	Aspectos Introductorios	6
2	Descripción general de la empresa de estudio.	0.5
3	Estudio del valor económico adquirido desde su aparición en el mundo.	0.5
4	Análisis del problema que lo afecta.	2
5	Presentación de su solución.	2
6	Definición de los objetivos de la solución y sus Indicadores de logro.	1
7	Estado del Arte	5
8	Recolección de información teórica necesaria para desarrollar el Diseño de Red Informática para la protección del sistema web del Call Center.	2
9	Descripción de estándares internacionales, normativas nacionales y metodologías que se usarán en el desarrollo del proyecto.	3
10	Definición del Problema	7
11	Analizar el entorno de despliegue.	2
12	Especificaciones y Justificación del Proyecto.	2
13	Criterios tomados en cuenta para la elaboración del Diseño de la Red Informática para la protección del sistema Web del Call Center.	2
14	EDT y Registro de Interesados.	1
15	Diseño de Solución	3
16	Esquematizar y plantear el desarrollo de la solución propuesta.	1
17	Identificar el hardware y software del mercado que cumpla con las especificaciones de la solución.	2
18	Evaluación y Validación de la Propuesta	5
19	Evaluar la propuesta de solución financieramente y en los otros alcances que involucran a las partes interesadas.	1
20	Establecer el método de validación.	1
21	Evaluación de Impactos.	2
22	Plantear las conclusiones y recomendaciones asegurando la profundidad, relevancia y unidad de las mismas con el propósito de la tesis.	1

Fuente: Elaboración Propia

3.13 EDT del Proyecto

Figura 23. EDT del Proyecto

Fuente: Elaboración Propia

3.14 Plan de Implementación del Proyecto

El plan de implementación será la guía de apoyo en el proceso de Instalación del Sistema de Seguridad Informática basadas en las recomendaciones de la norma ISO 27033 en el Call Center. Se establecen las guías que se deben seguir a lo largo del proceso de implementación.

El plan se divide en 2 etapas:

- Planificación.
- Organización.

Así mismo, se detalla el personal necesario para llevar a cabo el evento de implementación y, también, los respectivos controles que se necesitarán para la protección del Sistema Web del Call Center.

3.14.1 Planificación

Analiza las actividades a realizar y la programación de actividades con sus respectivos tiempos, así como el personal que debe intervenir.

Diagrama de Desglose Analítico

Figura 24. Diagrama de Desglose Analítico

Fuente: Elaboración Propia

3.14.1.1 Planificación del Proyecto

Para la preparación del proyecto se realizarán las siguientes actividades:

3.14.1.1.1 Asignación del director del proyecto

Se decide qué persona será el encargado de dirigir la implementación del sistema.

Tiempo estimado de Duración: 7

3.14.1.1.2 Asignación del administrador de la red

Se selecciona a la persona que estará a cargo de la red que se implementará en el Call Center.

Tiempo estimado de Duración: 7

3.14.1.1.3 Asignación del jefe de ejecución

Será encargado de supervisar las actividades que permitan el cambio entre el sistema actual y el sistema a implementar.

Tiempo estimado de Duración: 7 días

Se calcula un total de una semana para encontrar al personal que reúna las destrezas necesarias para liderar el proyecto.

3.14.1.2 Acondicionamiento de instalaciones

Se sugieren las siguientes actividades para acondicionar el espacio físico dentro del Call center que permitan la Implementación de la Red de Seguridad Informática:

3.14.1.2.1 Acondicionamiento del espacio físico dentro del Call Center

- Evaluación de las condiciones del espacio físico del Call Center
- Diseñar la distribución del equipo informático dentro del local o Data Center.
- Adecuación del Data Center del Call Center
 - Existencia de aire acondicionado en las áreas de mayor concentración de equipo.
 - El Tablero Eléctrico debe contar con puesta a tierra.
 - Infraestructura física que ofrezca seguridad al equipo contra situaciones climatológicas u otras que afecten el buen funcionamiento de este.
- Integración de nuevo enlace Principal o de Contingencia.
- Instalación de nuevos equipos de comunicaciones
- Segmentación de Nueva Red.
- Integración de la nueva Red y de la antigua red.

- Instalación del Software anti-Malware Server.
- Instalación del Software anti-Malware en la Estación de Trabajo.

Tiempo estimado de Duración: 60 días.

3.14.1.3 Pruebas

- Para la realización de pruebas del Diseño de Red Informática para el Call Center se desarrollarán las siguientes fases:
- Diseño de las Pruebas. Esto permitirá encontrar errores en el desarrollo de la Red Informática.
- Ejecución de las Pruebas. Dentro de las Cuales se observan las siguientes etapas:
 - Comunicación de las estaciones de trabajo con el Sistema Web
 - Comunicación del Sistema Web con los nuevos equipos de comunicación.
 - Análisis de los resultados para las correcciones correspondientes.

Tiempo estimado de Duración: 7 días

3.14.1.4 Capacitación del Personal

Para la capacitación del Call Center, se recomiendan las siguientes actividades:

- Preparación de la capacitación.
 - Diseño de la capacitación para los distintos niveles de usuarios.
 - Reproducción del material a utilizar en la capacitación.
- Preparación de los grupos a capacitar.
- Capacitación del Personal.

Tiempo estimado de Duración: 7 días

3.14.1.5 Puesta en Marcha

- Operación paralela del sistema

Mantener ambos sistemas de Red operativos, de manera paralela para que los usuarios se familiaricen poco a poco con el nuevo sistema.

- Análisis de resultados
- Puesta en Marcha

La nueva Red de Seguridad informática quedará operando después de 30 días y después de corregir los errores encontrados.

Tiempo estimado de Duración: 15 días.

Tabla 73.

Tiempo estimado de instalación de la etapa de Planificación

ID	Etapa Planificación	Tiempo estimado en Días
E1	Planificación del Proyecto	7
E2	Acondicionamiento de instalaciones	60
E3	Pruebas	7
E4	Capacitación del Personal	7
E5	Puesta en Marcha	15

Fuente: Elaboración Propia

3.14.2 Organización

Se sugiere un marco organizativo que sirva como plataforma para la guía de la ejecución del proyecto. Aquí se recomienda una unidad ejecutora, una matriz de responsabilidades juntos con sus funciones.

Figura 25. Organización

Fuente: Elaboración Propia

- Director de Proyecto, el cual será el responsable de dirigir todo el proceso.
- Administrador de la red
- Jefe de ejecución del proyecto quienes también supervisarán la parte de instalación de la red.

3.14.2.1 Descripción de funciones

Tabla 74.

Funciones del Director del Proyecto

Puesto: Director del proyecto	
Rol	Administrar las actividades a realizar para la implementación del sistema.
Jefe Inmediato Superior	Director del instituto
Funciones:	Planificar todas las actividades que permitan implementar la Red de Seguridad Informática.
	Planificar las actividades del Administrador de la Red.
	Definir un plan de contingencia ante problemas que se presenten durante la implementación del proyecto.
	Asignar los recursos a cada personal dentro del plan de implementación.
	Analizar los resultados obtenidos.

Fuente: Elaboración Propia

Tabla 75.

Funciones del Administrador de la Red

Puesto: Administrador de la red	
Rol	Administrar la red del Call Center incluyendo el Sistema Web, los equipos de comunicaciones y las estaciones de trabajo.
Jefe Inmediato Superior	Director del proyecto
Funciones	Verificar la correcta instalación del software antimalware.
	Instalar el software tanto en el servidor como en las estaciones de trabajo.
	Apoyar en la capacitación al personal del Call Center.
	Crear cuentas de acceso a usuarios del sistema con roles limitados.
	Resolver los problemas que se presenten en el ante durante y después de la migración a la nueva Red que tengan los usuarios con el sistema instalado

Fuente: Elaboración Propia

Tabla 76.

Funciones del Jefe de Ejecución

Puesto: Jefe de ejecución	
Descripción:	Será el encargado de llevar a cabo la capacitación del personal del Call Center y, también, hará seguimiento cercano al funcionamiento e implementación de la Nueva Red de Seguridad Informática.
Jefe Inmediato Superior	Director del proyecto
Funciones:	Imparte capacitación al personal que interactuará en la nueva Red de Seguridad Informática.
	Organiza los grupos de usuarios para su capacitación tomando en cuenta el nivel que tendrán estos dentro de la Red de Seguridad Informática.
	Diseña el plan de pruebas que permitan verificar el rendimiento de la Red de Seguridad Informática.
	Hace entrega de un informe al Director del Proyecto de los resultados analizados en las pruebas realizadas en la nueva Red de Seguridad Informática.
	Brinda apoyo al Director del Proyecto en las actividades surgidas durante la ejecución del proyecto.

Fuente: Elaboración Propia

3.15 Control del Diseño de Red

El control significa hacer un seguimiento cercano de tal forma que conlleve a la ejecución del proyecto según lo planificado. En esta parte, existen formularios que permitirán verificar el desarrollo y el progreso de las actividades que se ejecutan.

Estos documentos deberán ser completados por el Director del Proyecto quien a su vez dará informe al Director con los respectivos avances de cada una de las actividades que a su vez se contraponen con los avances esperados.

Con esta metodología no solo se logra detallar las actividades y sus progresos, sino, también, permiten ser clasificados y almacenados por el Director del Proyecto para llevar control de los sistemas que compondrán el Desarrollo de la Red Informática para el Call Center.

3.15.1 Formulario de Control de Actividades

Debe ser llenado por el responsable de la actividad luego de terminarse. Debe usarse para el seguimiento de cada una de las actividades.

Tabla 77.

Formulario de Control de Actividades

IMPLEMENTACIÓN DE DISEÑO DE RED DE SEGURIDAD INFORMÁTICA PARA EL CALL CENTER			
FORMULARIO DE CONTROL DE ACTIVIDADES			
Elaborado por:			
Fecha de Elaboración:			
Periodo del informe:	Inicio:		Fin:
Responsable de las actividades:			
ID	ACTIVIDAD	PORCENTAJE AVANZADO	PORCENTAJE OBJETIVO
OBSERVACIONES			
REVISADO POR		FECHA DE REVISIÓN	/ /

Fuente: Elaboración Propia

3.16 Formulario de Control de Subsistemas

Solo puede ser llenado por el Director del Proyecto y se utilizará para hacer seguimiento de cada uno de los subsistemas dentro del plan de implementación.

Tabla 78.

Formulario de Control de Subsistemas

IMPLEMENTACIÓN DE DISEÑO DE RED DE SEGURIDAD INFORMÁTICA PARA EL CALL CENTER				
FORMULARIO DE CONTROL DE SUBSISTEMAS				
Elaborado por:				
Fecha de Elaboración:				
Periodo del informe:			Inicio:	Fin:
Nombre del Proceso				
Responsable del Proceso				
ID	NOMBRE DEL SUBSISTEMA	ESTADO		
		TERMINADO	PENDINTE	
Grado de Avance:	Actividades Esperadas:	Cantidad	Porcentaje	
	Actividades Realizadas:	Cantidad	Porcentaje	
	Actividades Pendientes:	Cantidad	Porcentaje	
OBSERVACIONES				
REVISADO POR			FECHA DE REVISIÓN	/ /

Fuente: Elaboración Propia

3.17 Índices de Evaluación.

El índice permite medir el avance del proyecto y llevar un buen control del desarrollo del proyecto. A continuación, se describen los índices a utilizar:

3.17.1 Índice de actividades programadas ejecutadas

El índice de actividades programadas ejecutadas permite conocer el grado de avance del proyecto. Se calcula de la siguiente manera:

$$\frac{\sum \text{Duración de las Actividades Programadas Ejecutadas}}{\sum \text{Duración de Todas las Actividades}}$$

Explicación de la Fórmula:

- Los resultados menores a 1 indican que es un estado aceptable
- Los resultados mayores a 1 indican que se deben tomar medidas correctivas. Por ejemplo, reducción de tiempos en actividades siguientes.

3.17.2 Índice de duración de actividades

Este índice permite conocer el grado de diferencia entre el tiempo real de una actividad y el tiempo que se tenía programado para la misma. Se describe de la siguiente manera:

$$\frac{\text{Duración real de la actividad}}{\text{Tiempo Programado para la Actividad}}$$

Explicación de la Fórmula:

- Los resultados menores a 1 indican un resultado aceptable.
- Los resultados mayores a 1 sugieren la toma de medidas correctivas tales como reducción de tiempos en las actividades.

3.17.3 Índice de actividades programadas retrasadas

Nos ayuda a conocer el grado de retraso del proyecto. Este índice viene dado por la fórmula:

$$\frac{\sum \text{Tiempo de Retraso de las Actividades}}{\sum \text{Duración de Todas las Actividades}}$$

Explicación de la Fórmula:

- Un resultado cercano a Cero señala niveles aceptables.
- Un resultado mayor que 1 indican retrasos y por consiguiente la toma de medidas correctivas.

4 DISEÑO DE LA RED INFORMÁTICA

Después de realizar el análisis de red actual, sus vulnerabilidades y riesgos; se recomienda realizar los siguientes cambios en la red del Call Center:

4.1 Implementación de la Gestión Unificada de Amenazas: UTM

Se necesita la instalación de un dispositivo firewall o equipo UTM con funcionalidades de IPS (Sistema de Prevención de Intrusos) licenciado que contenga las firmas actualizadas de los nuevos ataques informáticos.

4.2 Zona Desmilitarizada: DMZ

Es menester la creación de una Zona Desmilitarizada para publicar físicamente los Servidores donde se aloja el sistema Web y el equipo UTM o firewall mediante reglas de DNAT o SNAT. La implementación de la Zona Desmilitarizada servirá para que los usuarios puedan hacer uso del Sistema Web desde Internet.

4.2.1 Beneficios de la Implementación una DMZ

- En caso se produzca un ataque informático, el atacante no podrá ingresar y comprometer los otros segmentos de red del Call Center.
- Así mismo, el firewall de la DMZ protegerá los servidores donde se aleja la base de datos y el Sistema Web del Call Center de los usuarios internos y solos permitirles el ingreso a los servicios a los que están autorizados.
- IPS y Monitoreo de Red.
- Escalabilidad.

4.3 Uso de Diferentes IP Públicas

Se recomienda tener una IP pública diferente para la salida del servicio Web y para la navegación de los usuarios del Call Center como medida de control y seguridad.

Figura 26. Propuesta de la Nueva Red para el Call Center

Fuente: Elaboración Propia

4.4 Recomendaciones a aplicar para la la Red Propuesta

4.4.1 Perímetro Lógico

- Firewall.
- Antivirus.

4.4.2 Red Interna

- Vlan
- ACL
- Accesos SSH

4.4.3 Servidores

- Uso de contraseñas robustas.
- Parches de Seguridad
- Antimalware
- Segmentación de Red
- Contraseñas Complejas para Usuarios Administrativos.
- Contraseñas complejas para usuarios estándar.
- Contraseñas complejas.

4.4.4 Aplicación

- Ambiente de red interna de desarrollo.
- Proceso de creación para parches.

4.4.5 Políticas de seguridad para Servidores y Estaciones de Trabajo

- Deberán recibir actualizaciones de software periódicamente. Esto incluye depuración de bitácoras siendo respaldadas semanalmente.
- Deberán recibir mantenimiento cada 6 meses que incluya la revisión de su configuración.

- Deberán ser ubicados en un área física que cumpla las recomendaciones para un Centro de Datos.
- Acceso restringido.
- Temperatura adecuada.

4.4.6 Protección contra descargas eléctricas.

- Mobiliario adecuado que garantice la seguridad de los equipos.
- El personal con acceso de red deberá renovar sus credenciales con las siguientes condiciones:
- Contraseñas fuertes o robustas.
- Cuando el usuario sospeche que su cuenta ha sido hackeada deberá notificarlo.
- El personal de red, debe notificar ante las siguientes anomalías del servidor:
- Si observa cualquier comportamiento anormal en el servidor.
- Si tiene problemas en el acceso a los servicios proporcionados por el servidor.

4.4.7 Políticas de Cuentas de Usuario

- A todos los trabajadores de la red se les debe proporcionar una charla inductiva donde se les mencione las formas de proteger y manejar los recursos informáticos de la institución.
- Conocer y aplicar las políticas y procedimientos apropiados en relación al manejo de la información y de los sistemas informáticos.
- Todo usuario debe respetar la confidencialidad y derechos individuales de los demás usuarios.
- No divulgar información confidencial del Call Center ni permitir el uso de sus sistemas a personal externo.
- No utilizar los recursos informáticos que no estén directamente vinculadas con el trabajo realizado en el Call Center.
- Proteger sus credenciales de la vista y posterior robo de otro personal.
- No podrán crear programas tendientes a alterar los sistemas institucionales académicos, administrativos o contables.

4.4.8 Políticas de clave de acceso a los programas administrativos

- Todo usuario que requiera utilizar un programa administrativo debe de contar con un usuario y una clave para acceder a dicho recurso.
- Los usuarios administrativos no deben dar a conocer la clave a nadie.
- Los usuarios administrativos deben modificar periódicamente su clave.

4.5 Costos de la Solución Planteada

Tabla 79.

Costo de los enlaces de Internet

COSTO DE LÍNEAS DE INTERNET			COSTOS		
ID	Medio de Transmisión	BW (Mbps)	CAPEX \$	OPEX Mantenimiento	Total
1	Internet - Principal	10	800	\$0.00	800
2	Internet - Backup	10	800	\$0.00	800
Costo mensual de Servicio de Internet en Dólares					1600
Costo mensual de Servicio de Internet en Soles					5232

Fuente: Elaboración Propia

Tabla 80.

Costo de los equipos de Seguridad

ID	EQUIPAMIENTO/ SERVICIO	DESCRIPCIÓN	COSTO TOTAL		
			UNITARIO \$	QTY	Total \$ al Mes
1	Firewall Fortinet	Fortigate 100E + Licencia por 3 años	250	4	1000
2	Protección DDoS Fortinet	FortiDDoS 200B	638	1	638
3	FC-10-02H01-247-02-12 FortiDDoS-200B	Licencia y soporte para 3 años	436	1	436
Costo mensual de equipos de Seguridad en Dólares					2074
Costo mensual de equipos de Seguridad en Soles					6782

Fuente: Elaboración Propia

Tabla 81.

Costo de la solución End Point

ID	PRODUCTO	DESCRIPCIÓN	COSTO TOTAL	
			QTY	TOTAL \$
1	Kaspersky Antivirus	Solución Endpoint Security for Business + licencia de 2 años	63	2312.3

Fuente: Elaboración Propia

Se calcula una inversión total de S./19575 soles en el primer mes y luego una inversión de S./12793 en el segundo mes hasta el mes 36

4.6 Efectividad de la Solución

A continuación, se genera 2 niveles para determinar la efectividad de la red propuesta como solución: Red WAN y End Point. Cada escenario estará compuesto por elementos de seguridad propios que otorgan seguridad específica a la red del Call Center.

4.7 Nivel WAN

El primer nivel de defensa de la propuesta de red está desarrollado en un entorno real. La red está expuesta a un ataque y servirá como escenario para analizar el comportamiento del código malicioso y como provenirnos de ellos. El principal componente de este escenario será un equipo Fortinet que será instalado y configurado después de detectado el ataque.

De esta manera, replicaremos el control frente a riesgos similares o de la misma naturaleza del Centro De Atención Telefónica (Call Center) cuando la vulnerabilidad es atacada desde fuera de la red.

Así mismo, se describen el Plan de pruebas y el Método de Análisis:

- Plan de Pruebas

El Plan de Pruebas permite tener una visión específica de las actividades a realizarse. Expresa la relación entre el proceso a evaluar y las partes interesadas. También, permite obtener una primera idea de cuál es el impacto en las operaciones, funciones y participantes del Call Center. El plan de Pruebas propuesto presenta la relación entre la organización, los individuos involucrados en la solución y los proveedores. El plan de Pruebas consta del siguiente formato que será llenado en cada escenario a estudiarse:

Tabla 82.

Descripción del Plan de Pruebas

Preguntas	Participantes	
	Proyecto	Cliente
¿Quiénes participan?		
¿Quiénes lo implementan?		
¿Dónde se desarrolla?		
¿Cuándo se desarrolla?		
¿Cuáles son los recursos a usar?		
¿Quiénes son los Proveedores que lo implementan?		

Fuente: Elaboración Propia

En esta etapa, es primordial la participación y buen juicio del soporte técnico o usuario de la plataforma de seguridad que evalúe los módulos de seguridad y los posibles puntos vulnerables.

- Métodos de Análisis

Se hará un análisis del resultado obtenidos luego de aplicar el cambio de las reglas de seguridad del dispositivo de seguridad del Call Center luego de recibir el ataque haciendo preguntas de Troubleshooting de Nivel 1 y 2:

- ¿Cuál es la Ip del Host infectado?
- ¿Cuál es el nombre del host infectado?
- ¿Cuál es la MAC del host infectado?
- ¿Cuál es la IP del dominio comprometido?
- ¿Cuál es el nombre del dominio comprometido?
- ¿Cuál es la IP del dominio que redirecciona al dominio comprometido?

4.7.1 Caso de Ataque de SPAM:

La red del cliente ha recibido el siguiente mensaje:

Figura 27. Correo SPAM

Fuente: Elaboración Propia

Según la traducción, el atacante menciona que la cuenta ha sido infectada y luego de entrar a la misma, ha notado alguna conducta que el usuario quiera ocultar. Por este motivo, el atacante solicita una cantidad de dinero para mantener el anonimato el tipo de información que el usuario maneja. El usuario cuenta con una solución BITDEFENDER ENDPOINT SECURITY TOOLS con el cual se monitorea la presencia de código malicioso en los correos. Sin embargo, la solución falló dejando pasar el correo.

4.7.1.1 Esquema de Trabajo

Tabla 83.

Descripción del Plan de Pruebas

Preguntas	Participantes	
	Proyecto	Call Center
¿Quiénes participan?	Analista	Usuario- Teleoperador
¿Quiénes lo implementan?	Jefe del Proyecto	-
¿Dónde se desarrolla?	Servidor de Correos del Trabajo	Estación de trabajo
¿Cuándo se desarrolla?	Al final del Proyecto	-
¿Cuáles son los recursos para usar?	Gateway de seguridad, enlace de Internet	Estación de trabajo
¿Quiénes son los Proveedores que lo implementan?	Fortinet	-
Objetivos Específicos a Medir	OE2	-
Indicadores a usar	IOE2	-

Fuente: Elaboración Propia

4.7.1.2 Resolución del Problema

Con la finalidad de realizar un mayor análisis de lo reportado, se analiza el encabezado del correo donde se detalla la IP pública donde proviene el correo y otros parámetros adicionales. Se adjunta un ejemplo de encabezado de correo.

```
Received: from 81.202.181.5.dyn.user.ono.com (81.202.181.5) by
mail.abisacorp.com (10.10.10.2) with Microsoft SMTP Server id 14.1.438.0;
Fri, 8 Mar 2019 06:41:36 -0500
Message-ID: <5C826303.4030405@abisacorp.com>
Date: Fri, 8 Mar 2019 12:41:39 +0000
From: <postmaster@abisacorp.com>
User-Agent: Mozilla/5.0 (Windows NT 6.0; rv:15.0) Gecko/20120824 Thunderbird/15.0
MIME-Version: 1.0
To: <postmaster@.com>
Subject: Fraudsters known your old passwords. Access data must be changed.
Content-Type: text/plain; charset="IBM852"; format=flowed
Content-Transfer-Encoding: 8bit
Return-Path: postmaster@.com
X-MS-Exchange-Organization-AuthSource: DC001.abisa.local
X-MS-Exchange-Organization-AuthAs: Anonymous
X-MS-Exchange-Organization-PRD: com
X-MS-Exchange-Organization-SenderIdResult: TempError
Received-SPF: TempError (DC001.abisa.local: error in processing during
lookup of postmaster@com: DNS timeout)
X-EndpointSecurity-Oxide81-EV: v:6.6.8.119, d:int, a:n, w:t, t:0, sv:1552032831, ts:1552045297
X-Auto-Response-Suppress: DR, OOF, AutoReply
```

Figura 28. Análisis del Contenido del correo

Fuente: Elaboración Propia

4.7.1.3 Resultado del Análisis

De acuerdo con lo analizado, los correos recibidos provienen de servidores de otros países:

- IP publica que envía: 81.202.181.5 (España) (correo 1 dominio original: 81.202.181.5.dyn.user.ono.com).
- IP publica que envía: 14.248.196.59 (Vietnam) (correo 2 dominio original: static.vnpt.vn).

Para evitar que estos correos spam lleguen al servidor de correo es necesario tomar medidas correctivas:

- Tener un antispam en la red para evitar la recepción de correo malicioso. En caso de contar con un gateway de seguridad, se tendría que aplicar reglas para filtrar esos tipos de correos y colocarlos en listas negras.
- Cambiar las contraseñas de todas las cuentas de correos de los usuarios por claves más robustas
- Mantener actualizados los últimos parches de seguridad de su servidor de correo local.

Figura 29. Política de bloqueo contra el correo SPAM

Fuente: Elaboración Propia

Se puede observar que el contador de tráfico se encuentra en 24.95Gb lo cual indica que el equipo de seguridad está cumpliendo su función de AntiSpam.

4.8 Nivel End Point

Constituye el último nivel de nuestra red y está desarrollada en un entorno virtual que servirá como escenario para analizar el comportamiento del código malicioso y como provenirnos de ellos. Los componentes de este escenario serán máquinas virtuales en VMWare que emulan estaciones de trabajo con sistemas operativos Windows Xp.

Después de instaladas las máquinas virtuales, se instalan las herramientas que nos servirán para implementar la última línea de defensa de nuestra solución propuesta.

De esta manera, replicamos el riesgo cuando la vulnerabilidad proviene del usuario o de sus actividades. Así mismo, se describen el Plan de pruebas y el Método de Análisis:

Figura 30. Interface Gráfica de Windows Xp Virtual

Fuente: VMWare

- Plan de Pruebas

El Plan de Pruebas permite tener una visión específica de las actividades a realizarse. Expresa la relación entre el proceso a testear y las partes interesadas. También, permite obtener una primera idea de cuál es el impacto en las operaciones, funciones y participantes que se desarrollan en el Call Center. El plan de Pruebas propuesto presenta la relación entre la organización, los individuos involucrados en la solución y los proveedores. El plan de Pruebas consta del siguiente formato que será llenado en cada escenario a estudiarse:

Tabla 84.

Descripción del Plan de Pruebas

Preguntas	Participantes	
	Proyecto	Cliente
¿Quiénes participan?		
¿Quiénes lo implementan?		
¿Dónde se desarrolla?		
¿Cuándo se desarrolla?		
¿Cuáles son los recursos a usar?		
¿Quiénes son los Proveedores que lo implementan?		

Fuente: Elaboración Propia

En algunos escenarios, se cuenta con un analista de seguridad que hace posible evaluar los módulos de seguridad y los posibles puntos vulnerables. En otros, contaremos solo con la presencia del usuario que, con poca experiencia en el uso de Internet, visitará intencionalmente una página web con contenido malicioso. En ambos casos, ambas partes serán asistidos por la solución propuesta.

- Métodos de Análisis

Se hará un contraste entre los resultados obtenidos entre los elementos de la red antes y después de implementar la nueva red del Call Center cuando se visitan los sitios web haciendo preguntas de Troubleshooting de Nivel 1 y 2:

- ¿Cuál es la Ip del Host infectado?
- ¿Cuál es el nombre del host infectado?
- ¿Cuál es la MAC del host infectado?
- ¿Cuál es la IP del dominio comprometido?
- ¿Cuál es el nombre del dominio comprometido?
- ¿Cuál es la IP del dominio que redirecciona al dominio comprometido?

4.8.1 Caso de Navegación Insegura

El siguiente escenario consiste en un trabajador que está en horario laboral (dentro de la red) y que usa un sistema operativo Windows Xp Professional Service Pack 3. Está personal necesitó hacer el pago de sus servicios personales a través de una página web: PayPal. Como no recordaba el dominio de la empresa, colocó en google el nombre del dominio “PayPal” y escogió el resultado “billinggoldspal.com”.

Tabla 85.

Descripción de los hosts de navegación

Cantidad	Sistema Operativo	Descripción
1	Windows Xp Professional Service Pack 3	Hosts de Prueba
1	Windows 64bit	Servidor

Fuente: Elaboración Propia

Figura 31. Portal de Pagos Paypal

Fuente: VMWare

4.8.1.1 Esquema de Trabajo

En esta parte del diseño, se presenta el esquema funcional de la red de datos en un entorno virtual lo que le permite al analista total libertad para ejecutar sus pruebas. De esta manera, se obtiene ventajas adicionales como gestión de riesgos y mejora continua en caso se vea alguna deficiencia de la red propuesta. El teleoperador hace la solicitud desde el entorno virtual, pasa el firewall (html request) hasta llegar al router. Luego, llega a internet donde se genera la consulta y respuesta.

Tabla 86.

Plan de Pruebas del Caso Navegación Insegura

Preguntas	Participantes	
	Proyecto	Call Center
¿Quiénes participan?	Analista	Usuario-Teleoperador
¿Quiénes lo implementan?	Jefe del Proyecto	-
¿Dónde se desarrolla?	Ambiente de Pruebas	Estación de trabajo
¿Cuándo se desarrolla?	Al final del Proyecto	-
¿Cuáles son los recursos a usar?	Firewall, Router, enlace de Internet y Servidor Web	Estación de trabajo
¿Quiénes son los Proveedores que lo implementan?	Software Libre, Splunk y Wireshark	-
Objetivos Específicos a Medir	OE	-
Indicadores a usar	IOE1	-

Fuente: Elaboración Propia

Figura 32. Circuito de Análisis

Fuente: Elaboración Propia

4.8.1.2 Resolución del Problema

A continuación, nuestro analista recoge los archivos y logs como resultado de la consulta hecha por el usuario al dominio malicioso. La primera aplicación alojada en nuestro servidor de aplicaciones es Splunk, el sistema de alarmas. Con esto, vamos a demostrar la eficiencia de nuestra Red Propuesta.

Figura 33. Interface Gráfica del Splunk

Fuente: Elaboración Propia

Seguidamente se monitorea la red a través del programa Wireshark que genera un archivo Pcap a estudiar.

Figura 34. Interface Gráfica del Pcap

Fuente: Elaboración Propia

Como siguiente paso, analizamos las Ips y consultas más sospechosas en un portal web gratuito. Esta herramienta se llama Virus Total y fue descrita en el capítulo 2 del presente documento.

Figura 35. Interface Gráfica de Virus Total

Fuente: Elaboración Propia

Figura 36. Interface Gráfica de Detección de Virus Total

Fuente: www.virustotal.com

El análisis confirma que ha sido observado por dos herramientas de seguridad: Snort y Suricata. Los dominios maliciosos que arrojan los dos gestores son:

- billinggoldspal.com
- billinggoldspal.com/cola/153b7ff4a55eb44e549bcd88c8c11368/index/web/Login/index.php

Como paso de seguridad, aplicamos el principio de Sandox. Es decir, en un entorno aislado o virtual, abrimos la consulta o el URL malicioso en un torno virtual. Para esto nos valemos de otra herramienta: URlquery.

The screenshot displays the URlquery web interface. The browser address bar shows the URL: <https://urlquery.net/report.php?id=1468621163443>. The interface includes a navigation bar with links for 'urlQuery', 'Search', 'Statistics', and 'About'.

Overview

URL	billinggoldspal.com/cola/153b7ff4a55eb44e549bcd88c8c11368/index/web/Login/index.php
IP	81.194.91.203
ASN	A551167 Contabo GmbH
Location	Germany
Report completed	2016-07-16 00:37:32 CET
Status	Report complete
urlQuery Alerts	No alerts detected

Settings

UserAgent	Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.13) Gecko/20101203 Firefox/3.6.13
Referer	
Pool	
Access Level	public

Intrusion Detection Systems

Snort /w Sourcefire VRT	No alerts detected
Suricata /w Emerging Threats Pro	No alerts detected

Blacklists

Fortinet's Web Filter / fortiguard.com	No alerts detected
MDL / malwaredomainslist.com	No alerts detected
DNS-BH / malwaredomains.com	No alerts detected
memoronic secure DNS / memoronic.no	No alerts detected
OpenPhish / openphish.com	No alerts detected
PhishTank / phishtank.com	No alerts detected
Spamhaus DBL / spamhaus.org	No alerts detected

Figura 37. Interface Gráfica de Url Query

Fuente: www.urlquery.com

https://urlquery.net/report.php?id=1468621163443

HTTP Transactions (11)

Request	Response
GET /cola/153b7f4a55eb44e549bcd88c8c11368/index/web/login/index.php HTTP/1.1 Host: billinggoldspal.com	91.194.91.283 HTTP/1.1 302 Found Content-Type: text/html; charset=iso-8859-1
GET /cgi-sys/suspendedpage.cgi HTTP/1.1 Host: billinggoldspal.com	91.194.91.283 HTTP/1.1 200 OK Content-Type: text/html
GET /Bilder/logo_contabo.jpg HTTP/1.1 Host: www.contabo.de	184.20.9.162 HTTP/1.1 301 Moved Permanently Content-Type: text/html; charset=iso-8859-1
GET /Bilder/logo_contabo.jpg HTTP/1.1 Host: contabo.de	184.20.9.162 HTTP/1.1 302 Found Content-Type: text/html; charset=iso-8859-1
POST / HTTP/1.1 Host: ocsf.comodoca4.com	178.255.83.1 HTTP/1.1 200 OK Content-Type: application/ocsp-response
POST / HTTP/1.1 Host: ocsf.comodoca4.com	178.255.83.1 HTTP/1.1 200 OK Content-Type: application/ocsp-response
POST / HTTP/1.1 Host: ocsf.usertrust.com	178.255.83.1 HTTP/1.1 200 OK Content-Type: application/ocsp-response
GET /Bilder/logo_contabo.jpg HTTP/1.1 Host: contabo.de	184.20.9.162 HTTP/1.1 200 OK Content-Type: image/jpeg
GET /favicon.ico HTTP/1.1 Host: billinggoldspal.com	91.194.91.283 HTTP/1.1 302 Found Content-Type: text/html; charset=iso-8859-1
GET /favicon.ico HTTP/1.1 Host: billinggoldspal.com	91.194.91.283 HTTP/1.1 302 Found Content-Type: text/html; charset=iso-8859-1

Figura 38. Descripción de la redirección en Url Query

Fuente: www.urlquery.com

4.8.1.3 Resultado del análisis

El host del usuario fue el Windows Xp-PC1 y su dirección IP fue la 172.16.155.149 junto con su dirección MAC del usuario: 00:0C:29:41:C4:27.

La explicación que se da es que el usuario visitó una página con un inicio de sesión falso del portal web PayPal alojado en el dominio malicioso: billinggoldspal.com.

Llenó un formulario con información personal y el portal web lo envió redirigido al sitio real de PayPal.

Lo que vino después fue un correo con una URL falsa de la página a través de un correo electrónico de phishing para terminar de recolectar sus credenciales personales.

Las Ip's que se muestran en el archivo Pcap muestran que el usuario navegó en unas cuantas páginas web después de enviar el formulario de PayPal falso.

4.8.2 Caso de UPDATE del Sistema Operativo en las Estaciones de Trabajo

El siguiente caso consiste en un usuario Windows Xp Professional Service Pack 3 que durante la ejecución de sus labores encontró un dominio que le solicitaba realizar un Windows Update dado a que su sistema operativo está desactualizado y necesita actualizarlo.

Como se mencionó anteriormente, uno de los problemas que tiene el Call center, es que los teleoperadores suelen instalar programas o aplicaciones de sitios web no legítimos.

Los componentes de la topología virtual serán trabajados en una plataforma VMWare con dos hosts de prueba. Uno contiene un antivirus propuesto y el otro no:

4.8.2.1 Esquema de Trabajo

Este es otra parte del diseño en la que se presenta el esquema funcional de la red de datos con dos computadores. Solo uno está asegurado con Kaspersky. Se presenta a la red trabajando sin la intervención de nuestros analistas y pasando nuestros Firewalls de Seguridad de la red propuesta (pueden tratarse de dominios maliciosos recientes que no están en las bases de datos de los sistemas de seguridad). La solicitud entra a un circuito de trabajo virtual. Se trata de una solicitud de navegación web (HTML request) pasando nuestro sistema de seguridad hasta llegar al router. Luego, llega a internet donde se genera la consulta y respuesta.

Tabla 87.

Descripción de los hosts de prueba

Cantidad	Sistema Operativo	Descripción
1	Windows Xp Professional Service Pack 3	Contiene el antivirus que protegerá el host de las mismas amenazas que el host de prueba.
1	Windows Xp Professional Service Pack 3	El host navegará por dominios maliciosos para medir la reacción de Kaspersky

Fuente: Elaboración Propia

Tabla 88.

Plan de Pruebas del Caso Update

Preguntas	Participantes	
	Proyecto	Call Center
¿Quiénes participan?	-	Usuario- Teleoperador
¿Quiénes lo implementan?	Jefe del Proyecto	-
¿Dónde se desarrolla?	-	Estación de trabajo
¿Cuándo se desarrolla?	Al final del Proyecto	-
¿Cuáles son los recursos a usar?	-	Estación de trabajo
¿Quiénes son los Proveedores que lo implementan?	-	Kaspersky
Objetivos Específicos a Medir	OE1	-
Indicadores a usar	IOE1	-

Fuente: Elaboración Propia

Figura 39. Topología de Prueba del Antivirus

Fuente: Elaboración Propia

Figura 40. Interface de la Pc de prueba sin Antivirus

Fuente: VMWare

Figura 41. Interface de la Pc de prueba con Antivirus

Fuente: VMWare

4.8.2.2 Resolución del Problema

Por efectos de prueba, se hará una solicitud al siguiente dominio malicioso:

- fakewindowsupdate.com/gb/xpindex.html

Después de la consulta, se obtiene una interface similar de actualización del sistema operativo:

Figura 42. Resultados de la Infección en el host sin Kaspersky

Fuente: VMWare

Como se puede apreciar, se trata de una actualización falsa que no se detiene al llegar al 100%.

El host está exponiéndose a daños en las librerías y archivos del sistema.

Figura 43. Resultados de la navegación con Kaspersky

Fuente: VMWare

4.8.2.3 Resultado del análisis:

El host del usuario fue el Windows Xp-PC1 y su dirección IP fue la 172.16.155.149 junto con su dirección MAC del usuario: 00:0C:29:41:C4:27.

La explicación que se da es que el usuario visitó una página web que le solicitó realizar un Windows Update ilegítimo en un dominio malicioso.

Los firewalls de la nueva red propuesta no poseían en su base de datos las firmas de estos ataques.

Lo que vino después fue una actualización del sistema operativo falsa que no se detenían a pesar de que llegaron al 100% entrando de esta manera a un loop lógico en el sistema operativo.

Este resultado no se vio en el host que contenía el antivirus Kaspersky ya que la solicitud era detenida al momento de lanzarse. Ver Ilustración 43

5 PRUEBAS, RESULTADOS Y VALIDACIÓN

A continuación, se procede con la medición de los indicadores vinculados con los objetivos específicos presentados en el capítulo 1 a fin de evaluar el rendimiento de la nueva red propuesta. Cada uno de los indicadores, nos ayudará a verificar el nivel de protección dado al Call Center, y, también, a señalar los escenarios o puntos que conviene mejorarse a fin de maximizar el nivel de protección de la red según los resultados obtenidos de cada uno de los indicadores. Así mismo, se presentan los indicadores que ayudarán a evaluar el cumplimiento de los objetivos del presente documento

Tabla 89.

Lista de Indicadores, Métricas y Logros

	OBJETIVO ESPECIFICO		INDICADOR DE LOGRO	MÉTRICA	LOGRO ESPERADO
OE1:	Desarrollar el análisis de riesgos del Call Center que permita:	Clasificar los principales activos de información que soportan el Sistema Web del Call Center.	Matriz de valorización de activos de información.	Porcentaje de activos de información considerados como críticos.	No mayor al 40%.
		Determinar las amenazas y vulnerabilidades del Sistema Web del Call Center.	Informe de análisis de riesgos.	Número de riesgos que supera el nivel de riesgo aceptable.	No mayor al 15%
OE2:	Realizar un análisis de brecha que permita determinar el nivel de cumplimiento de la web del Call Center con respecto a los requisitos de seguridad indicado por norma ISO 27033.		Informe de análisis de Brecha.	Número de Controles recomendados por la normativa ISO 27033 Cumplidos	No menor al 60%.
OE3:	Elaborar el plan de implementación del Diseño de Red Informática para el Call Center.		Plan de acción.	Tiempo de implementación de actividades.	Que se encuentra en un promedio de 4 meses.

Fuente: Elaboración Propia

5.1 Pruebas y Resultados del Indicador 1: Matriz de Valorización de Activos de Información.

El siguiente indicador permite evaluar los activos de la información (anexo 3) que sirven de apoyo al sistema Web. Su valor Fue obtenido del análisis del punto 3.2.2.3 Valorización de Activos.

- Objetivo: Determinar la cantidad de equipos cuyo nivel de importancia los sitúa en una situación de extrema importancia para el Call Center.
- Pruebas para el Análisis: El indicador será medido de la siguiente manera:

$$\text{Porcentaje de Activos Críticos} = \frac{\text{Cantidad de Activos Críticos} * 100\%}{\text{Cantidad Total de Activos}}$$

Donde:

- Mayor al 40% = Crítico
- Menor al 40% Aceptable

Figura 44. Medidor del Indicador 1

Fuente: Elaboración Propia

Figura 45. Activos de información por fase

Fuente: Elaboración propia

Los activos de la información que soportan el sistema Web fueron analizados en su totalidad y, según el estudio, su valor de criticidad oscila en valores que van de la siguiente manera:

- El 41% de los activos de la información son considerados dentro de un nivel críticos ya que comprometen procesos del Call Center que ponen en riesgo su situación financiera o que de ser afectados arriesgarían la imagen del Call Center de manera catastrófica.

- El 18% de los activos de la información son considerados dentro de un nivel alto ya que comprometen Operaciones que si se paralizan ponen en riesgo el vínculo entre el personal de alto cargo del Call Center y su cliente, pero se recuperan después de unos meses de inactividad.
- El 18 % de los activos de información son de nivel de criticidad medio. Sus Operaciones se paralizan, pero se recuperan después de unos días de inactividad.
- El 23% de los activos de la información poseen un nivel de criticidad bajo y esto conlleva a que las Operaciones del Call Center resultan dañados en un nivel mínimo a tal punto que se puede seguir operando.

Conclusión de la Prueba

La situación actual de los activos de la información es crítica. Los componentes que interactúan con el sistema Web deben ser atendidos ya que si alguna vulnerabilidad es explotada obtendría penalizaciones contractuales que ponen en riesgo el vínculo entre el Call Center y su cliente.

5.2 Pruebas y Resultados del Indicador 2: Riesgos que sobrepasan el Nivel de Tolerancia
Este indicador toma como datos de entrada los riesgos a los que está expuesto el Call Center que se observaron en la sección 3.2.3.3: Riesgos Detectados en el Call Center:

- Objetivo: Evaluar los riesgos que sobrepasan el umbral de riesgos que sobrepasan el nivel de tolerancia. Se miden los riesgos que pasan su condición a no aceptable pues tanto el apetito de riesgo como el nivel de tolerancia pueden variar en el tiempo. En consecuencia, es necesario poder medir aquellas desviaciones en los riesgos
- Pruebas para el Análisis: El indicador será medido de la siguiente manera:

$$\text{Porcentaje de Riesgos} = \frac{\sum \text{Riesgos por encima del Apetito de Riesgo} * 100\%}{\sum \text{Riesgos Aceptables}}$$

Los resultados del indicador serán medidos de la siguiente manera:

- Riesgos Aceptables:
- Riesgos No Aceptables:

El resultado nos permitirá conocer la cantidad de riesgos que la organización puede tolerar ya que los riesgos no aceptables no deben superar el 14%. De esta forma, se comprueba la efectividad del Plan de tratamiento de riesgos del Call Center.

Hallazgos

Riesgos encima del apetito de Riesgo: 2

Riesgos Aceptables: 16

Figura 46. Cantidad de Riesgos según el Nivel

Fuente: Elaboración Propia

$$\text{Porcentaje de Riesgos} = \frac{2 * 100\%}{16}$$

$$\text{Porcentaje de Riesgos} = 12.5\%$$

Conclusión de la Prueba

De acuerdo a lo evidenciado se observa que, de un universo de 18 riesgos, dos son considerados críticos. Es decir, su ocurrencia daña a la Integridad, Confidencialidad y Disponibilidad del activo de la información expuesto y ocasionaría daños irreparables al proceso del Call Center. Esto representa el 12.5% del total de riesgos sobrepasan el nivel de tolerancia.

5.3 Pruebas y Resultados del Indicador 3: Número de Controles recomendados por la normativa ISO 27033 Cumplidos

El presente indicador hará uso como fuente de información el Informe de análisis de brechas desarrollado en el punto 3.3: Desarrollo de Análisis de Brechas.

Así mismo, el indicador representará los resultados mediante la siguiente gráfica que reúne la totalidad de controles en comparativa de la cantidad de los que se cumplen. De esa manera se muestra en qué nivel de cumplimiento de las recomendaciones brindadas por la norma ISO 27033 se encuentra el Call Center:

Figura 47. Gráfica Esperada del Indicador

Fuente: Elaboración Propia

- Objetivo del indicador: Determinar el nivel de madurez de los controles existentes en el Call Center.
- Pruebas para el Análisis: El indicador será medido de la siguiente manera:

$$\text{Nivel de Madurez de Controles} = \frac{\text{Cantidad de Controles Cumplidos} \times 100\%}{\text{Cantidad Total de Controles Sugeridos}}$$

Características del indicador

5: Nivel Óptimo Alcanzado: Si los controles se cumplen al 100%

4: Nivel Deseado: Si los controles se cumplen al 80%

3: Nivel Controles Existentes: Si los controles se cumplen al 60%

2: Nivel Básico: Si los controles se cumplen al 40%

1: Nivel Crítico: Si los controles se cumplen al 20%

Figura 48. Medidor del Indicador 3

Fuente: Elaboración Propia

Este indicador nos ayuda a evaluar el nivel de madurez inicial en el que se encuentra el Call Center

Hallazgos

Existen 6 dominios que pueden ser aplicados al Call Center (Ver 3.3 Desarrollo de Análisis de Brechas) al cual llamaremos Universo.

Cada uno de estos dominios sugiere controles aplicables y variables (dependiendo del tipo de red y el tipo de negocio al que se dedica).

De esta manera, se ha reunido la siguiente información:

Tabla 90.

Cantidad de Controles recomendados por la norma ISO 27033

Anexo A	Dominios	Total de Controles	Cantidad Actual	Porcentaje de Cumplimiento
A.1	Redes de área local	15	1	7%
A.2	Redes de área amplia	11	3	27%
A.6	Gateways de seguridad	4	2	50%
A.10	Alojamiento web	17	2	12%
A.12	Acceso Enrutado	15	4	27%
A.13	Intranet para Data Center	5	3	60%
Total Controles		67	15	22%

Fuente: Elaboración Propia

$$\text{Nivel de Madurez de Controles} = \frac{15 \times 100\%}{67} = 22\%$$

Nivel de Madurez = Básico

Figura 49. Resultados de la Métrica evaluada

Fuente: Elaboración Propia

Conclusión de la Prueba

De acuerdo con lo evidenciado se observa que de un universo de 67 controles aplicables al Call Center, solo se cumplen 15 representando el 22% de Madurez. Se encuentra con un nivel de madurez básico bordeando lo crítico (Entre el 20% y el 40%).

Los resultados se posicionan en el medidor anaranjado de nuestra escala de valor (Medidor) ya que no existen políticas, procedimientos y lineamientos de seguridad de la información. Se propone practicar este procedimiento luego de implementar el diseño de la Red de Seguridad Informática a fin de evaluar la evolución de este indicador.

5.4 Pruebas y Resultados del Indicador 4: Cálculos de tiempo en proyectos de seguridad de la información

El siguiente indicador reúne los datos obtenidos de nuestro Plan de Implementación del Diseño de la Red de Seguridad Informática. Con estos datos conoceremos el tiempo necesario para desarrollarlo.

- Objetivo del indicador: Evaluar la efectividad de los proyectos que se detallan en el punto 3.13 Plan de Implementación del Proyecto.
- Fórmula de Cálculo:

$$\text{Evaluación PERT } (Te) = \frac{15 \times Ta + 4Tm + Tb}{6} + \frac{Tb - Ta}{6}$$

Donde:

Tabla 91.

Nomenclatura de la fórmula

Ta	Es el tiempo optimista al menor tiempo que puede durar una actividad.
Tm	Es el tiempo probable que pudiera durar una actividad.
Tb	Es el tiempo mayor que puede durar una actividad.
Te	Corresponde al tiempo esperado para una actividad.

Fuente: Elaboración Propia

- Características del indicador: 2 meses < 4 meses < 6 meses
- Periodo de 2 meses: El proyecto se desarrolla dentro de los plazos establecidos y con normalidad.
- Periodo de 4 meses: El proyecto llega al margen del tiempo establecido.
- Periodo de 6 meses: El proyecto no se ha cumplido.
- La evaluación de esta métrica será mensual. De esta forma, mediremos los avances de la implementación de la red.

Hallazgos

Tabla 92.

Duración de las actividades del proceso de Planificación

ID	Etapla Planificación	Duración Optimista	Duración más Probable	Duración Pesimista
E1	Planificación del Proyecto	7	14	30
E2	Acondicionamiento de instalaciones	60	67	90
E3	Pruebas	7	10	14
E4	Capacitación del Personal	7	10	14
E5	Puesta en Marcha	15	16	18

Fuente: Elaboración Propia

Figura 50. Gráfico de PERT

Fuente: TODOPMP.COM

- Existe un 99.73% de probabilidad que la actividad esté comprendida entre la media ± 3 desviación estándar σ
- Existe un 95.46% de probabilidad que la actividad esté comprendida entre la media ± 2 desviación estándar σ
- Existe un 68,26% de probabilidad que la actividad esté comprendida entre la media ± 1 desviación estándar σ

Estimaciones para la actividad Planificación del Proyecto:

$$\text{Duración de la actividad E1} = (7 + 4(14) + 30) / 6 = 16 \text{ días}$$

$$\text{Desviación estándar } (\sigma) = (30 - 7) / 6 = 3.8$$

$$\text{Varianza} = \sigma^2 = 14.44$$

Estimaciones para la actividad Acondicionamiento de instalaciones:

$$\text{Duración de la actividad E2} = (60 + 4(67) + 90) / 6 = 70 \text{ días}$$

$$\text{Desviación estándar } (\sigma) = (90 - 60) / 6 = 5$$

$$\text{Varianza} = \sigma^2 = 25$$

Estimaciones para la actividad Pruebas:

$$\text{Duración de la actividad E3} = (7 + 4(10) + 14) / 6 = 10 \text{ días}$$

$$\text{Desviación estándar } (\sigma) = (14 - 7) / 6 = 1.67$$

$$\text{Varianza} = \sigma^2 = 2.79$$

Estimaciones para la actividad Capacitación del Personal:

$$\text{Duración de la actividad E4} = (7 + 4(10) + 14) / 6 = 10 \text{ días}$$

$$\text{Desviación estándar } (\sigma) = (14 - 7) / 6 = 1.67$$

$$\text{Varianza} = \sigma^2 = 2.79$$

Estimaciones para la actividad Puesta en Marcha:

$$\text{Duración de la actividad E5} = (15 + 4(16) + 18) / 6 = 16 \text{ días}$$

$$\text{Desviación estándar } (\sigma) = (18 - 15) / 6 = 0.5$$

$$\text{Varianza} = \sigma^2 = 0.25$$

A continuación, procedemos a calcular la duración del proyecto con una precisión de 95.46%:

Cabe mencionar, que se consideran que las actividades son secuenciales. Es decir, todas forman parte de la ruta crítica, De esta manera, para estimar la duración total del proyecto se deben sumar los valores de la columna PERT:

Tabla 93.

Valor del PERT

I D	Etapas Planificación	Duración Optimista	Duración más Probable	Duración Pesimista	PERT	σ	σ^2
E1	Planificación del Proyecto	7	14	30	16	3.8	14.44
E2	Acondicionamiento de instalaciones	60	67	90	70	5	25
E3	Pruebas	7	10	14	10	1.67	2.79
E4	Capacitación del Personal	7	10	14	10	1.67	2.79
E5	Puesta en Marcha	15	16	18	16	0.5	0.25
TOTAL			117		122		45.27

Fuente: Elaboración Propia

El tiempo estimado para este proyecto es de 122 días (4 meses).

Por otro lado, se tiene que sumar la varianza de cada actividad y obtener la desviación estándar total:

$$\text{Desviación Estándar} = \sqrt{45.27} = 6.73$$

Finalmente:

$$2 \text{ Sigmas} = 95.46\%:$$

$$\text{Menor tiempo probable: } 122 \text{ días} - 2(6.73) = 108.54$$

$$\text{Mayor tiempo probable: } 122 \text{ días} + 2(6.73) = 135.46$$

Conclusión de la Prueba

De acuerdo con lo evidenciado se observa que la implementación del proyecto podría realizarse en un periodo máximo de 135 días con condiciones adversas. Esta seguridad se tiene con un 95.46% según el índice de PERT.

6 COMETARIOS

El diseño de Red de Seguridad Informática estableció los principales lineamientos para una adecuada protección de la red de datos y componentes del Sistema Web del Call Center.

Toda la propuesta, en los despliegues de red virtual o en producción y en sus Niveles WAN y End Point, ha demostrado eficacia en cuando a proteger la red de consultas a dominios con contenido malicioso e, incluso, de ataques que ha aparecido en el transcurso del tiempo. Así mismo, la red, una vez se implemente, nuevamente pasará por un proceso de Análisis de Riesgos, Brechas e Inventario de Activos para comprobar:

- El nuevo nivel obtenido y si se garantiza la Confidencialidad, Integridad y Disponibilidad (CID) de la Información y, también, los sistemas implicados en su tratamiento.
- La escalabilidad y adaptabilidad de nuevas tecnologías que aparezcan en el transcurso del tiempo.

7 CONCLUSIONES DE LOS OBJETIVOS ESPECÍFICOS DESARROLLADOS

- 1) Se logró valorizar los Activos de la Información que soportan el Sistema Web del Call Center para mejorar la gestión de riesgos. Cerca del 60% de los componentes llegan a niveles de riesgo altos y hasta críticos, lo cual significaría que su divulgación, falta de disponibilidad o alguna alternación podría ocasionar daños graves y hasta irreversibles a la imagen del Call Center.
- 2) Se identificó todos los principales riesgos de seguridad de la información a los que está expuesto el Call Center. Siendo que el 12.5% del total de riesgos sobrepasan el nivel de tolerancia a los que los administradores del Call Center están dispuestos a asumir como línea de negocios. Así mismo, se otorga un control obtenido del anexo A de la norma ISO 27033 para tratar las vulnerabilidades que dan origen a los riesgos.
- 3) Se determinó los controles existentes en el Call Center así como su nivel de madurez frente a todas los requisitos que recomienda la norma ISO 27033 mostrándose que solo se cumple el 22% de lo recomendado por la norma. Su nivel de madurez es básico. Se sugiere el realizar nuevamente el análisis después de la implementación de la red de Seguridad Informática para calcular el nuevo nivel alcanzado.
- 4) Se ha desarrollado el Plan de Implementación del Diseño de la Red de Seguridad Informática para el Call Center estableciéndose que el proyecto puede ser implementado en 4 meses y una semana lo cual sale ligeramente de lo esperado como proyecto. Así mismo, se simularon todos los escenarios posibles de ataque a los que está expuesto la empresa con el fin de comprobar el correcto funcionamiento de los niveles de seguridad y su interacción con los usuarios.

8 RECOMENDACIONES

- 1) Con respecto al OE1, Informe de Análisis de Riesgos, la norma ISO 27033 otorga recomendaciones mínimas para la gestión de riesgos. Por lo tanto, se recomienda revisar la norma ISO 27001 para tener un mayor alcance en el tratamiento de riesgos.
- 2) Con respecto al OE2, se recomienda realizar un segundo Informe de Análisis de Brecha después de la implantación de la Red de Seguridad Informática para recalcular el nuevo nivel de madurez que tendrá el Call Center.
- 3) Dar a todos los trabajadores técnicos y teleoperadores capacitación sobre el uso de la nueva tecnología que se implementará de tal forma que se fomente un uso apropiado y se aproveche al máximo sus capacidades.
- 4) Establecer diagramas de red y procedimientos al personal técnico que permita administrar y diagnosticar problemas en la red.
- 5) Actualizar periódicamente todos los controles sugeridos en este documento y contrastarlos con las futuras necesidades del negocio. De esta manera se logrará proteger de nuevos ataques que surjan con el avance de las tecnologías de la información.

9 REFERENCIAS

- 1) Universidad de Valencia. (2018). ¿Qué es la seguridad informática y cómo puede ayudarme? Recuperado de <https://www.universidadviu.com/la-seguridad-informatica-puede-ayudarme/> [Consulta: 30 de diciembre de 2018].
- 2) Norma ISO 27033. (2015). ISO/IEC 27033-1:2015(en) Recuperado de <https://www.iso.org/standard/63461.html> [Consulta: 05 de enero de 2019].
- 3) Kaspersky Anti-Virus. (2019). Endpoint Security for Business Recuperado de <https://latam.kaspersky.com/small-to-medium-business-security/endpoint-select> [Consulta: 26 de marzo de 2019].
- 4) Fortinet. (2018). Segmentación de red que escala Recuperado de <https://www.fortinet.com/lat/solutions/enterprise-midsize-business/scalable-flexible-segmentation.html> [Consulta: 26 de marzo de 2019].
- 5) Eset. (2015). IDS, Firewall y Antivirus: ¿qué debes tener instalado? Recuperado de <https://www.welivesecurity.com/la-es/2015/04/24/ids-firewall-antivirus-debes-instalar/> [Consulta: 5 de febrero de 2019].
- 6) Edureka. (2016). What is Docker & Docker Container. Recuperado de <https://www.edureka.co/blog/what-is-docker-container> [Consulta: 26 de marzo de 2019].
- 7) Universidad Nacional Autónoma de México. (2019). FIREWALLS, CONTROLANDO EL ACCESO A LA RED. Recuperado de <https://revista.seguridad.unam.mx/numero-04/firewalls-controlando-el-acceso-la-red> [Consulta: 5 de marzo de 2019].
- 8) SANTOS, Omar (2007) End-to-end Network Security: Defense-in-depth.USA: Cisco Press® Networking Technology Serie.
- 9) CHACON C. Delfor (2016) Metodología de Gestión de Riesgos de Seguridad de la Información. Lima: Ministerio de Economía y Finanzas.
- 10) TORRES O. Paola Isabel (2011) Tesis Diseño e Implementación de un Sistema de Seguridad Perimetral para la Red de Comercializadora Internacional Oceanos S.A. Cartagena: Universidad Tecnológica de las Indias

- 11) RIVADENEIRA G. Carlos Alberto (2008) Tesis Diseño de una Red Inalámbrica con Tecnología WI-FI para el Cyber Café @Lejonet. Quito: Escuela Politécnica Nacional
- 12) VERDEZOTO V. Byron Omar (2015) Tesis Diseño de una Red LAN para el Transport de Voz, Datos y Video para el Municipio del Cantón Valencia Provincia de los Rios. Quito: Escuela Politécnica Nacional
- 13) LUZARDO S. Jessica Maria (2010) Sistema de Control de Procesos Empresariales por medio de Indicadores de Gestión aplicado al Departamento de Servicio al Cliente en el Proceso de Facturación y Atención de Reclamos de la empresa PLÁSTICOS S.A. ubicada en la ciudad de Guayaquil. Guayaquil: Escuela Politécnica Nacional
- 14) BARRENECHEA Z. Taylor Iván (2011) Tesis Diseño de una Red LAN Inalámbrica para una Empresa en Lima. Lima: Pontificia Universidad Católica del Peru
- 15) ROMERO M. Andres Felipe (2017) Tesis Diseño de un Plan de Tratamiento de Riesgos de Seguridad de la Información para Campañas Electorales con Presupuesto Ajustado. Bogotá: Institución Universitaria Politécnica Grancolombiano
- 16) REEVES, Silvio Hudgson (2018) Tesis PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. Santo Domingo: Institución Nacional de Formación Técnica Profesional
- 17) VELURTAS, Facundo (2009) Tesis Optimización de Enlaces en Redes IP y Control de tráfico. La Plata: Universidad Nacional de La Plata
- 18) ARIGANELLO, Ernesto / BARRIENTOS, Enrique (2010) Redes Cisco a Fondo. Madrid: RA-MA
- 19) BOYLE, Randall (2009) Applied Information Security. EE.UU:Prentice Hall
- 20) LAMMLE, Todd (2008) Seguridad de Redes. EE.UU:Sybex
- 21) BOYLES, Tim (2010) CCNA Security. EE.UU:Wiley Publishing
- 22) KHANDELWAL, Dr B.C. Punmia K. (2002) Project Planning and Control with Pert and CPM. India: Motilal UK Books.

10 ANEXOS

Anexo 1. Clasificación de Activos según su Integridad, Confiabilidad y Disponibilidad

INTEGRIDAD	
Información:	<p>Perdida de la precisión o exactitud del activo de información.</p> <p>Ejemplo: Errores de compilación o procesamiento del Sistema Web.</p>
Hardware:	<p>Alteración, pérdida o manipulación del Activo de la Información que produce que el activo físico no efectúe correctamente sus actividades o sus funciones.</p> <p>Ejemplo: Daño de los componentes del activo de un componente del Call Center.</p>
Software:	<p>Perdida de la precisión o exactitud del activo de información.</p> <p>Ejemplo: Modificación de la configuración del software con lleva a errores de compilación o procesamiento del Sistema Web.</p>
Servicio:	<p>Perdida de la precisión o exactitud del activo de información.</p> <p>Ejemplo: El servicio brindado no se presta en las condiciones óptimas y acordadas por el Call Center.</p>
Teleoperadores:	Los teleoperadores introducen errores, datos incompletos o manipulen información según criterios equivocados.
Descripción	Explicación
ALTO	La pérdida de exactitud del Activo de la Información otorga un gran impacto significativo en la prestación de servicios del Call Center.
Medio	La pérdida de exactitud del Activo de la Información otorga un gran impacto moderado en la misión y los objetivos del Call Center.
Baja	La pérdida de exactitud del Activo de la Información puede tener un impacto pequeño en la prestación de servicios del Call Center.

CONFIDENCIALIDAD	
Información:	Personal no autorizado accede al activo de información.
Hardware:	Personal no autorizado conoce la configuración del Sistema Web y accede al Activo de Información sin autorización.
Software:	Personal no autorizado conoce o accede a la configuración del Activo de Información.
Servicios:	Alguien conoce su existencia o configuración o hace uso no autorizado del activo.
Teleoperador:	La información a la que se tiene acceso es usada inadecuadamente o se le da otro uso.
Descripción	Explicación
ALTO	La divulgación no autorizada de la información de este activo impacta gravemente la imagen del Call Center.
Medio	La divulgación no autorizada de la información de este activo tiene un impacto medio en la imagen del Call Center.
Bajo	La divulgación no autorizada de la información puede ocasionar un impacto pequeño o no daña la misión y los objetivos del Call Center.

DISPONIBILIDAD	
Información:	El personal autorizado no tiene acceso al bien o Activo de Información.
Hardware:	El personal autorizado no tiene acceso al bien o Activo de Información.
Software:	El personal autorizado no tiene acceso al bien o Activo de Información.
Servicio:	El personal autorizado no tiene acceso al bien o Activo de Información.
Personal:	El personal autorizado no tiene acceso al bien o Activo de Información.
Descripción	Explicación
ALTO	La indisponibilidad del bien o Activo de la Información produce un gran impacto en la prestación del servicio del Call Center.
Medio	La indisponibilidad del bien o Activo de la Información impacta negativamente los servicio del Call Center.
Bajo	La indisponibilidad del bien o Activo de la Información daña levemente los servicio del Call Center.

7 Identificación de Riesgos y Preparación para Identificar los Controles de Seguridad

7.1 Introducción

Como se mencionó en la anterior parte, la primera etapa es recopilar información sobre el entorno de red actual o futuro. La siguiente etapa es identificar y evaluar los riesgos de seguridad de red.

7.2 La información actual o futura de las Redes

7.2.1 Requisitos de seguridad en la Política empresarial de Seguridad de la Información

La Política de Seguridad de una empresa puede incluir declaraciones sobre las necesidades de Confidencialidad, Integridad, No Repudio y Disponibilidad, así como los tipos de amenazas y riesgos con la finalidad de aplicar los controles de seguridad en la red que deben ser implementados. Así, el primer paso debe ser revisar la Política de Seguridad de la Información de la empresa.

Por ejemplo, una política podría afirmar que la disponibilidad de ciertos tipos de información es importante o que ningún tipo de pago sea válido sin firma digital.

Estos requisitos son importantes en la evaluación y gestión de riesgos ya que permiten definir los aspectos de la arquitectura o el diseño de seguridad técnicas y los potenciales controles de seguridad.

7.2.2 La información sobre la actual / Planificación de Redes

7.2.2.1 Introducción

El siguiente paso debe ser recopilar y revisar la información en la red actual. Es decir, la arquitectura, aplicaciones, servicios, tipos de conexión y otras características. Esto influenciará en la identificación y evaluación de riesgos:

7.2.2.2 Arquitecturas de red, aplicaciones y servicios

Dependiendo del área que cubren, se puede clasificar como sigue:

Enlaces LAN, Storage Area Network (SAN) y almacenamiento conectado a red (NAS) para enlaces locales

Enlaces WAN o Global de Red de Área (GAN) para enlaces de larga distancia.

Protocolos multimedia.

Protocolos de control de acceso. Por ejemplo, de esto incluyen IEEE 802.1x y WPA.

Protocolos MPLS que permite a una red central ser compartido por múltiples redes privadas.

7.2.2.3 Tipos de conexión de red

Algunos de estos tipos de conexión se pueden realizar a través de redes privadas y otros podrían estar través de redes públicas para conectarse a servicios como correo electrónico, Internet, Intranet o Extranet. Cada uno de los tipos de conexión puede tener diferentes vulnerabilidades y riesgos de seguridad.

Una forma de clasificar los tipos genéricos de conexión de red que pueden ser necesarios para realizar negocios es el siguiente:

Interconexión entre diferentes partes de la misma organización.

Interconexión entre oficinas regionales.

Cualquier tipo de conexión en el entorno de red actual o futuro deben ser revisados por sus implicaciones en la seguridad y la información obtenida se deben utilizar en el proceso de identificación y evaluación de los riesgos de seguridad y los controles asociados.

7.2.2.4 Otras características de la red

Red de Datos.

Red de Voz.

Híbrido que abarca tanto la red de datos y voz, y posiblemente de vídeo.

7.3 Información de Riesgos de Seguridad y Control de Potencial Áreas

Como se refleja anteriormente, la mayoría de las organizaciones hoy en día dependen de la utilización de las redes y sistemas de información para apoyar sus operaciones

comerciales. Cuando se realiza una conexión a otra red, se debe tener cuidado que la conexión no está expuesta a riesgos adicionales.

Algunos de estos riesgos pueden estar relacionados con asegurar el cumplimiento con la legislación y la regulación correspondiente. Dependiendo de la legislación nacional respectiva, tales controles pueden imponer obligaciones a los que procesan y difunden la información personal a través de redes. De este modo, los riesgos que se enfrentan en este escenario podrían estar relacionados con el acceso no autorizado a la información, el envío de información no autorizada, la descarga de código malicioso, la negación de la conexión de servicio, y la falta de disponibilidad de información y servicio.

Por este motivo, una revisión de la gestión de riesgos de seguridad de red debe llevarse a cabo para identificar y confirmar los controles técnicos de seguridad y los aspectos técnicos del diseño de seguridad, junto con el apoyo a los controles de seguridad no técnicos de acuerdo con las buenas prácticas de seguridad reconocidas en la familia de normas ISO / IEC 27001.

Esto implica cinco actividades principales:

La determinación de las medidas de la importancia de la información y de servicios expresados en términos de los potenciales impactos adversos sobre las operaciones comerciales.

Identificación y evaluación de la probabilidad de ocurrencia o niveles de amenazas en contra de la información y de servicios.

Evaluar los controles de riesgos basado en las medidas determinadas sobre los impactos sobre las operaciones comerciales y los niveles de amenazas y vulnerabilidades.

Identificación de los aspectos del diseño de seguridad técnica que se requieren para asegurar que los riesgos evaluados se mantienen dentro de límites aceptables.

Los principales procesos de evaluación y de gestión de riesgos de seguridad de red se muestran en la figura 6 a continuación.

En la Figura las dos primeras filas de cajas “Establecimiento de Revisión del límite / Scope” e “Identificación de los Activos” indican las actividades preparatorias. Las siguientes dos filas de indican las actividades de evaluación de riesgos, y dos filas finales indican la selección de control de Seguridad de la Información y las actividades de aceptación de riesgo residual.

8 Controles de Apoyo

8.1 Introducción

Esta cláusula proporciona una visión general de los controles que soportan arquitecturas técnicas de seguridad de red y sus controles técnicos relacionados. Los controles que son especialmente importantes en relación con el uso de las redes se amplían en la cláusula 8.2 a 8.9 y abordan la gestión de seguridad de la red: Gestión de la Seguridad de la Red, Funciones y Responsabilidades en la Seguridad de Red, Monitoreo Evaluación de Seguridad de Red etc.

8.2 Gestión de seguridad de la red

8.2.1 Fondo

La gestión de seguridad de la red debe llevarse a cabo con la debida consideración de los diferentes protocolos y servicios de seguridad relacionados.

8.2.2 Actividades de gestión de seguridad de red

8.2.2.1 Introducción

Un requisito clave para cualquier red es que es apoyada por las actividades de manejo seguras, lo que iniciar y controlar la implementación y operación, de la seguridad. Estas actividades deben llevarse a cabo para garantizar la seguridad de todos los sistemas de información de una organización / de la comunidad. actividades de gestión de la seguridad de la red deben incluir:

Definición de todas las responsabilidades relacionadas con la seguridad de la red y la designación de un administrador de seguridad con la responsabilidad general.

Política de seguridad de la red debidamente documentada y acompañando de documentados de arquitectura de seguridad técnica.

Procedimientos operativos de seguridad de red documentados.

Pruebas de seguridad que garanticen la seguridad de la red.

Documentos que señalen las condiciones de seguridad que deben cumplirse antes de permitir la conexión por organizaciones internas y externas.

Documentos con las condiciones de seguridad mínimas que deben cumplir los usuarios de la red remota

Documentos y planes de recuperación de la continuidad de negocio ante desastres.

8.2.2.2 Política de Seguridad de la red

La administración es responsable de apoyar la política de seguridad de la red en la organización. Esta política de seguridad abarcan declaraciones claras sobre los siguientes puntos:

Postura de organización con respecto a uso de la red.

Reglas para el uso de los recursos específicos de la red, servicios y aplicaciones.

Penalizaciones por el incumplimiento de las normas de seguridad.

Los documentos Secops deben ser desarrolladas como un apoyo a la Política de Seguridad donde se detallen los procedimientos de operación cotidiana a la seguridad de la red y quién es responsable de su gestión. Una plantilla de ejemplo se muestra en el Anexo C.

8.2.2.4 Comprobación del Cumplimiento de Seguridad de Red

Se debe comprobar los controles especificados para todas las redes en los siguientes documentos:

- La política de seguridad de la red.
- Procedimientos operativos de seguridad.
- Arquitectura de seguridad técnica.
- Políticas de Seguridad aplicados a los Gateway de Acceso.
- Plan de continuidad de negocio ante desastres.
- Condiciones mínimas de Seguridad para la conexión.

Esto debe ocurrir antes de poner en marcha el funcionamiento de cualquier red o de realizar una nueva versión. Cabe mencionar que se debe realizar pruebas de seguridad con

las normas reconocidas, con una estrategia de pruebas de seguridad y los planes relacionados producidos de antemano que se indique con lo que se han de realizar, con las pruebas de qué, dónde y cuándo; con una combinación de análisis de vulnerabilidad y pruebas de penetración compatible con la legislación del país de origen. Después de la prueba, los informes deben indicar los detalles de las vulnerabilidades encontradas y las correcciones necesarias y en qué prioridad.

8.2.2.5 Condiciones de seguridad para varias conexiones de red en la Organización

Condiciones de seguridad para la conexión con segundas o terceras organizaciones deben estar pactadas contractualmente aceptando los riesgos asociados con el otro extremo de una conexión de red fuera de su dominio (riesgos relacionados con la protección de la privacidad de datos).

8.2.2.6 Condiciones de seguridad documentados para usuarios de red remota

Las condiciones de seguridad para los usuarios de la red remotos deben ser descritas en un documento. Esto debe describir las responsabilidades del usuario con los componentes del sistema de red y su seguridad.

8.2.2.7 Gestión de la Red de Seguridad de incidentes

Los incidentes de Seguridad de la Información poseen mayor probabilidad de ocurrencia junto con los impactos adversos e implicaciones legales significativos. Por este motivo, una organización con conexiones de red debe tener un sistema de gestión de incidentes correctamente documentado capaz de responder con rapidez para minimizar su impacto y prevenir la ocurrencia.

8.2.3 Los roles y responsabilidades de seguridad de red

Los roles y responsabilidades que deben ponerse en marcha asociados con la gestión de seguridad de la red son los siguientes.

Gerencia senior:

- Definición de los objetivos de seguridad de la empresa.
- Comenzar, aprobar, publicar y ejecutar la Política de Seguridad de la Organización junto con sus normas y procedimientos.
- Políticas de garantizar la seguridad y de uso aceptable.
- Administración de redes:
- Desarrollar detalladamente y aplicar la Política de Seguridad de la red.
- Gestionar los servicios externos para garantizar la conformidad con las políticas internas y externas de seguridad de red.
- Asegurarse de que la responsabilidad operacional de las redes se separe de las operaciones de cómputo
- Mantener las herramientas y componentes de seguridad de red actualizados según la evolución de las amenazas de red.
- Configuraciones de seguridad de red como listas de acceso
- Monitorización de la actividad de la red, en respuesta a incidentes de seguridad o alarma etc.

Usuarios de la red:

- Comunicar sus requisitos de seguridad.
- Cumplir con la política de seguridad de la empresa.
- Cumplir con las políticas de uso aceptable corporativos para los recursos de red.
- Proporcionar información sobre la eficacia de la seguridad de red.

8.2.4 Red de Monitoreo

La supervisión de la red es una parte muy importante en la gestión de seguridad de la red.

8.2.5 La evaluación de seguridad de la red

La seguridad de la red es una tarea cotidiana ya que el personal de seguridad debe garantizar que las redes sigan trabajando con los parches de seguridad más actuales y los arreglos disponibles de los fabricantes.

Así mismo, deben tomarse medidas para auditar periódicamente los controles de seguridad existentes con puntos de referencia establecidos mediante pruebas de seguridad.

8.3 Gestión de la Vulnerabilidad Técnica

Las vulnerabilidades técnicas están presentes en las redes. Su explotación, técnicas puede tener graves consecuencias en la seguridad de las redes informáticas. La gestión de vulnerabilidad debe cubrir los siguientes componentes:

- Obtención de Información oportuna sobre las vulnerabilidades técnicas.
- Evaluación de la exposición de las redes a tales vulnerabilidades.
- Definición de los controles apropiados de seguridad como medida contra los riesgos en la red.
- Implementación y verificación de los controles de seguridad definidos en los documentos.

Un requisito previo para la gestión de la vulnerabilidad técnica debe ser contar con un inventario completo de todos los componentes de la red incluyendo tipo de dispositivo, fabricante, números de versión de hardware, firmware y las personas responsables.

8.4 Identificación y autenticación

Es importante ser capaz de restringir el acceso a las conexiones a personal autorizado (ya sea interno o externo a la empresa) a determinados servicios de red y a su información. Se recomienda la instalación de 3 zonas de control de seguridad que podrían ser relevantes para el uso de las redes y sistemas de información:

- Inicio de Sesión Remota.- Puede darse el caso por personal autorizado que trabajan fuera de la organización a distancia o personal de otras organizaciones que son

conexiones establecidas por socios contractuales a través de redes públicas. Cada tipo de inicio de conexión remota debe tener una seguridad adicional controles apropiados a la naturaleza de la red.

- Mejoras de autenticación.- Los sistemas de credenciales basadas en ID/contraseña de usuario pueden resultar fáciles de adivinar. Por este motivo, se deben emplear formas más seguras de autenticación. Por ejemplo, cualquier PIN relacionado o perfil biométrico o dos factores de autenticación.

8.5 Registro de Auditoría y Supervisión de la Red

Los registros de auditoría son importantes para garantizar la eficacia de la seguridad de la red junto con un seguimiento permanente que conlleven a una rápida detección y respuesta a eventos de seguridad. Sin esta actividad, no será posible constatar que los controles de seguridad de red son efectivos.

Sin embargo, se tiene presente que el almacenaje de una enorme cantidad de información de auditoría puede tornar el análisis más difícil de manejar. Incluso el análisis tiene que ser realizado en tiempo real. Los registros de auditoría deben incluir los siguientes tipos de eventos:

- Intentos fallados de conexiones remotas con fechas y horas exactas.
- Trafico que cruce el gateway de seguridad.
- Alertas de duplicidad de IP.

Los registros para la auditoría proceden de fuentes como routers, firewalls, IDS y son enviados a un servidor de auditoría central para consolidar y analizar la información. Los registros de auditoría pueden ser examinados:

- En tiempo real ya que permiten alertarnos de posibles ataques.
- Fuera de línea que son esenciales ya que esto permite el análisis de sus tendencias.

Todos estos registros de auditoría deben mantenerse en un lugar seguro y por un período de tiempo acordado respaldado y archivado de una forma que asegure la Integridad, Disponibilidad y la Confidencialidad.

Se hace hincapié en que la monitorización de red debe llevarse a cabo de una manera totalmente compatible con la legislación y reglamentación nacional e internacional en la materia (Ley de Protección de Datos).

Otro punto importante, es que el monitoreo debe llevarse a cabo de manera responsable y no para revisar el comportamiento de los empleados donde las leyes de privacidad sean muy limitadas.

8.6 La detección y prevención de intrusiones

Con el aumento de las redes informáticas, aumentan los métodos más avanzados de ataque con base en herramientas disponibles en Internet. Incluso, muchas de estas herramientas pueden ser fáciles de usar por personas con experiencia mínima en informática.

Un IDS escucha todo el tráfico al interior de una red e identifica el intento de una intrusión o la ocurrencia de una. Incluso, puede responder a las intrusiones, así como alertar al personal apropiado.

Un IPS comprueba todo el tráfico antes de que ingrese a las redes internas y bloquea automáticamente todos los ataques reconocidos proporcionando una respuesta activa.

8.7 Protección contra código malicioso

Por lo general, el código malicioso no puede ser detectado antes de ocurrir el daño. Por este motivo, los sistemas que nos previenen de estos ataques deben mantenerse siempre se mantiene al día a través de las actualizaciones diarias. El software de código anti-maliciosos para escanear los datos y programas y eventualmente identificar patrones sospechosos asociados con malware deben ser actualizada a intervalos regulares para cuando se presenten nuevas firmas estén disponibles las alertas de malware de alto riesgo.

8.8 Servicios de Cifrado

Los controles de encriptación deben ser considerados para cifrar la información que pasa a través de redes para preservar la confidencialidad de la información. Los controles de integridad de la firma o mensajes digitales si es que se busca la preservación de la

integridad. Los controles de firma digital pueden proporcionar una protección similar a los controles de autenticación de mensajes y, también, tienen políticas de no repudio.

La decisión de utilizar el cifrado, firma digital, la integridad de mensajes u otros controles basados en cifrado debe tener en cuenta las leyes y regulaciones gubernamentales pertinentes.

Una técnica de cifrado utilizado comúnmente se conoce como un cifrado de bloques y formas para protección de cifrado. Otra forma son los de integridad de mensaje conocida como códigos de autenticación de mensajes (o MACs).

8.9 Gestión de Continuidad de Negocio

Es importante que los controles estén en su lugar para asegurar el curso del negocio en caso de un desastre para recuperar cada parte de la actividad ante una interrupción en la red. La Gestión de Continuidad del Negocio debe tener procesos con etapas que abarcan revisión impacto, revisión de evaluación de riesgos, el establecimiento de requisitos de recuperación de negocios, formulación de estrategias de continuidad de negocio, producción plan de continuidad de negocio, la prueba del plan de continuidad de negocio, sensibilización del personal ante la continuidad del negocio, el mantenimiento del plan de continuidad de negocio en curso, y la reducción del riesgo. Sólo siguiendo todas las etapas se puede asegurar que los plazos requeridos del negocio están alineados con las necesidades del negocio.

Desde la perspectiva de la red, se debe implementar conexiones alternativas con capacidad suficiente para recuperar de las conexiones posterior a los eventos no deseados. Estos requisitos deben basarse en la importancia de las conexiones para el funcionamiento del negocio y los impactos comerciales adversos previstos en caso de interrupción. Mientras que la conectividad puede permitirse muchas ventajas a una organización, en el caso de una interrupción esto podría representar un “puntos únicos de fallo”.

9 Directrices para el Diseño e Implementación de Seguridad de Red

9.1 Fondo

Esta cláusula se ocupa de los diversos aspectos del diseño de la red de seguridad y los aspectos técnicos y de control. Los controles propuestos deben ser revisados a fondo en el contexto de las arquitecturas de red. Es decir, se deben ajustar según sea necesario como base para el desarrollo, implementación y prueba de la solución.

9.2 Arquitectura o Diseño de Seguridad de Red Técnico

La documentación de las propuestas de la arquitectura de seguridad técnica o diseño e implementación proporciona un medio para examinar las diferentes soluciones. Esto da base para la resolución de problemas asociados a las restricciones técnicas de la empresa.

La documentación debe tener en cuenta los requisitos de la política de seguridad de la información de la empresa (véase el numeral 7.2.1), la arquitectura de red, aplicaciones, servicios, tipos de conexión y otras características (véase el numeral 7.2.2), y la lista de posibles controles identificados en la evaluación de riesgos (véase el apartado 7.3). Después de revisar las propuestas se debe acordar y documentar el documento técnico de la seguridad.

Los datos de entradas para Diseñar la red técnica de Seguridad incluyen lo siguiente:

- Requisitos del servicio que da la empresa.
- Documentación de cualquier arquitectura o diseño existente o previsto.
- Política de Seguridad de la Red actual.
- Activos de Información de deben ser protegidos.

Las salidas del proceso de Diseño de Red son los siguientes:

- Documento de seguridad técnica de la red.
- Requisitos mínimos de seguridad de acceso al servicio, gateways de seguridad o firewall.
- Procedimientos operativos de seguridad (Secops).

- Requisitos mínimos de seguridad para el acceso para terceros. Requisitos mínimos de seguridad para el acceso de contratistas o outsourcing.

Una vez que el diseño de la red ha sido documentado se deben llevar a cabo dicha implementación y en el proceso se pueden ajustar nuevos controles a la luz de los problemas encontrados durante las pruebas

La información sobre cada una de las siguientes actividades está prevista en la norma ISO / IEC 27033-2:

- Preparación para el diseño técnico de la seguridad de la red y su aplicación.
- Iniciación del proyecto de Seguridad de Red.
- Confirmando los requisitos generales de la organización.
- La revisión de la arquitectura existente o propuesta.
- Identificación de activos.
- Confirmación de resultados de evaluación y gestión de riesgos de seguridad, revisión de los controles de seguridad de red existentes.
- Revisión de los requisitos de rendimiento de la red y la confirmación de criterios. (Configuraciones de líneas de comunicación, servidores, gateways de seguridad, etc. que garanticen la disponibilidad de servicio requerido).
- Uso de modelos o marcos de referencia.
- Selección del producto basado en criterios de idoneidad técnica, rendimiento, capacidad de expansión, seguridad lógica trayectoria del proveedor, etc.
- Documento final con el Diseño de la Seguridad de la Red y la documentación relacionada.
- Documento de estrategia de pruebas de seguridad.

Se recuerda nuevamente que el Diseño de la Seguridad de la Red debe estar plenamente documentado y revisado antes de finalizar la lista de controles de seguridad para su implementación.

10 Escenarios de Red de Referencia - Riesgos, diseño, técnicas y cuestiones de control

10.1 Introducción

La norma ISO / IEC 27033-3 describe los riesgos, técnicas de diseño y los problemas de control asociados con las redes informáticas. Proporciona una guía detallada sobre los riesgos de seguridad y las técnicas de diseño de seguridad y controles necesarios para mitigar esos riesgos en todos los escenarios especificados.

10.2 Servicios de Acceso a Internet para Empleados

La prestación de estos servicios a los empleados debe considerar el acceso con fines identificados y autorizados. Se debe definir una política específica donde se detalle los servicios que se brindan y con qué fines. El acceso a Internet está permitido normalmente por razones de laborales y puede estar permitido el uso privado del servicio en forma limitada. También hay que determinar qué servicios se permiten. Por ejemplo, canales de chat, foros de colaboración, correo etc. De esta manera, los riesgos que se tratan dentro de un escenario específico.

El principio básico del servicio brindado a los trabajadores es satisfacer las necesidades de la empresa.

10.3 Servicios de colaboración mejoradas

Los entornos de mayor auge en las empresas son los de colaboración o mensajería instantánea, videoconferencia y entornos para compartir documentos. Estos servicios de colaboración se presentan de dos formas básicas:

- Utilizarlos como servicios internos mas no con los socios externos.
- Utilizarlos como los servicios internos y servicios externos a la empresa. Este último escenario ofrece mucho más beneficio, pero al mismo tiempo traen mayores riesgos de seguridad.

10.4 Negocio para Servicios comerciales

Internet y sus tecnologías proporcionan más opciones de negocio a las comercios, pero también introducen nuevos riesgos de Seguridad de la Información. Se ven afectados la Disponibilidad y la Fiabilidad.

Si se utiliza el Internet como una conexión de red, los requisitos como la Disponibilidad y Fiabilidad deben ser manejados de manera diferente mediante medidas como la Calidad de Servicio.

10.5 Negocio a Servicios al Cliente

Estos negocios incluyen el comercio electrónico y la banca electrónica. Los requisitos de Seguridad de la Información incluyen la Confidencialidad (para el servicio de Banca Electrónica), Autenticación. Estos métodos reducen en el riesgos de pérdida financiera, pérdida de reputación comercial o credibilidad).

10.6 Servicios de Outsourcing

Algunas empresas utilizan servicios externos o han externalizado algunas de sus funciones de manera total o parcialmente con el apoyo de su infraestructura de TI. Así mismo, estos se tienen que adecuar a las necesidades de ambos lados para proporcionar acceso directo a sus sistemas, accesos permanentes o acceso temporal. En algunos casos, los servicios subcontratados necesitan derechos de acceso altamente privilegiados con el fin de cumplir con las tareas específicas de gran nivel.

10.7 La segmentación de la red

La legislación de un país en particular pueden requerir una protección específica de los datos del cliente mientras que otros prohíben la transferencia de dichos datos a otros países. Las organizaciones internacionales suelen hacer negocios con un número de diferentes países. Estos organismos tienen la obligación de cumplir con las diversas

legislaciones específicas de cada país mientras crean sus diferentes requisitos de seguridad de la información.

Por este motivo, se hacen segmentación de una red para cubrir las diferentes necesidades de seguridad de la información de cada país lo que puede ser una solución amplia efectiva. Por ejemplo, aplicar técnicas de Defensa en Profundidad además del control de acceso de nivel de aplicación.

10.8 Comunicaciones móviles

Este escenario de red hace mención a dispositivos personales como los Smartphone o laptops. La orientación de los aspectos de seguridad de las comunicaciones a tales dispositivos se proporciona en la norma ISO 27033-7 " Seguridad de las Comunicaciones a través de Redes Inalámbricas y de Radio.

Estos dispositivos presentan nuevas características disponibles como el crecimiento de las capacidades de la memoria y permanencia en línea a través de Internet que significa un riesgo significativo de seguridad de información similar las situaciones en las que una persona utiliza su estación de trabajo para uso privado o con fines no laborales.

10.9 Soporte de red para usuarios que viajan

Los usuarios que viajan esperan las mismas facilidades de conectividad que los que tienen en ubicaciones fijas. Sin embargo, este tipo de conexiones o solicitudes a la red ofrecen nuevos riesgos a la Intranet si no está implementado con controles apropiados.

10.10 Soporte para Redes Domésticas y Pequeñas Oficinas Comerciales

Las redes pequeñas domésticas o a menudo requieren ingresar a la Intranet de una organización. Los costos de las ampliaciones de la red hacia la red doméstica es un tema crítico ya que se entran en temas como los costo / beneficio. Esto significa de coste de los controles de seguridad que deben utilizarse para asegurar tales conexiones a la red y, por lo

general, esto impide el uso de los controles de seguridad de redes ya establecidos y utilizados en la Intranet.

En muchos escenarios hogar o pequeña empresa de la infraestructura también se puede utilizar para uso privado, así como para fines comerciales - que puede dar lugar a riesgos adicionales de seguridad de la información. Los riesgos de seguridad se definen y se describen consejos sobre técnicas de diseño de seguridad y controles para mitigar esos riesgos.

11 Temáticas de "Tecnología" - Riesgos, Técnicas de diseño y problemas de control

Los detalles de los riesgos de seguridad, técnicas de diseño y problemas de control asociados con los temas de tecnología se muestran en el Anexo A de la norma ISO 27033. Los temas que se aplican al caso de estudio han sido de tallados en la presente tesis. Así mismo, los temas tratados son en la norma son los siguientes:

- Redes de Área Local (véase A.1 en la norma).
- Redes de Área Ancha (ver A.2 en la norma).
- Redes Inalámbricas (véase A.3 en la norma).
- Redes de Radio (véase A.4 en la norma).
- Redes de Banda Ancha (véase A.5 en la norma).
- Gateways de Seguridad (véase A.6 en la norma).
- Redes Privadas Virtuales (véase A.7 en la norma).
- Redes de Voz (véase A.8 en la norma).
- Convergencia IP (véase A.9 en la norma).
- Alojamiento Web (ver A.10 en la norma).
- Correo Electrónico de Internet (ver A.11 en la norma).
- Acceso Enrutado a Organizaciones de Terceros (ver A.12 en la norma).
- Centro de Datos (ver A.13 en la norma).

Anexo 3. Anexo C de la norma ISO 27033

Ejemplo de Plantilla para un Documento SecOPs

- 1 Introducción
- 1.1 Visión General
- 1.2 Estructura del documento
- 2 Alcance
- 2.1 Ubicaciones
- 2.2 Infraestructura técnica
- 2.2.1 Entorno de TI
- 2.2.2 Red de arquitectura
- 2.2.3 Situación 1
- 2.2.4 Situación 2
- 2.2.5 Situación 3
- 2.2.6 Conexiones externas
- 3 Política de seguridad
- 4 Organizador Seguridad de la Información
- 4.1 Introducción
- 4.2 Gestión de Seguridad Estructura y responsabilidades
- 4.2.1 Oficial de Seguridad de la Organización
- 4.2.2 Oficial Adjunto de Seguridad de la Organización
- 4.2.3 Organización Oficial de Seguridad de Información
- 4.2.5 Equipo de Soporte de TI (según el caso)
- 4.2.6 Gerentes de área de Negocio

- 4.2.7 Personal
- 4.2.8 Organigrama de Gestión
- 4.3 Incidentes de Seguridad de la Información y Reporte de debilidades de Información
- 4.4 Distribución de los Procedimientos Operativos de Seguridad (SecOPs)
- 4.5 Evaluación de los riesgos asociados con las partes externas
- 4.6 Acuerdos sobre acceso externo (Terceros)
- 4.7 Outsourcing
- 5 Gestión de Activos
 - 5.1 Inventario de Activos
 - 5.2 El uso aceptable de la información y otros activos
 - 5.3 Clasificación de la Información
- 6 Seguridad de Recursos Humanos
 - 6.1 Cantidad mínima de Personal de Seguridad y sus Requisitos
 - 6.2 Términos y Condiciones
 - 6.3 Sensibilización y Formación Seguridad de la Información
 - 6.4 Proceso disciplinario
 - 6.5 Monitoreo de Personal
 - 6.6 Terminación del contrato
 - 6.7 Tarjetas de Acceso de Seguridad o Pases para Edificios
 - 6.8 El acceso físico a las Redes y sistemas de TI
- 7 Seguridad Física y Ambiental
 - 7.1 Implementación física y Control de Seguridad Ambiental
 - 7.2 Perímetro de seguridad física
 - 7.3 Controles físico de entrada

- 7.4 Trabajando en habitaciones / Áreas clave
- 7.5 Emplazamiento de equipo
- 7.6 Teclas y combinaciones
- 7.7 Alarmas de detección de intrusos
- 7.8 Protección del equipo contra robos
- 7.9 Retiro de equipos
- 7.10 Controles de acceso a hardware
- 7.11 Detección de Manipulaciones
- 7.12 Mantenimiento y reparación
- 7.13 Seguridad de energía
- 7.14 Seguridad contra incendios
- 7.15 Agua / Seguridad Líquido
- 7.16 Las alertas de seguridad
- 7.17 Seguridad de PC o estaciones de trabajo
- 8 Gestión de comunicaciones y operaciones
 - 8.1 Procedimientos y responsabilidades operacionales
 - 8.1.1 Cambiar Procedimientos de Control
 - 8.1.2 La segregación de funciones y áreas de responsabilidad
 - 8.2 Planificación y aceptación del sistema
 - 8.2.1 Planificación de capacidad
 - 8.2.2 La aceptación del sistema
 - 8.3 Protección Contra Código malicioso y móvil
 - 8.3.1 Prevención
 - 8.3.2 Detección

- 8.3.3 Recuperación
- 8.3.4 Código móvil
- 8.4 Copia de seguridad y recuperación
- 8.5 Componentes de TI (incluyendo Red), Puesta en Marcha y Cierre
- 8.6 Seguridad de Medios (incluyendo documentos)
 - 8.6.1 Gestión de medios extraíbles
 - 8.6.2 Salidas Impresas
 - 8.6.3 Reutilización Segura
- 8.7 Intercambio de Información
- 8.8 Vigilancia
 - 8.8.1 Contabilidad y Auditoría
 - 8.8.2 Libros de Registros Contables
 - 8.8.3 Sincronización del reloj
- 8.9 Registros del Operador
- 8.10 Registro de Fallos
- 8.11 TI y Planes de Comunicación
- 9 Control de Acceso
 - 9.1 Gestión de Cuentas de Usuario
 - 9.1.1 Solicitudes de Cuentas de Usuario
 - 9.1.2 Creación de Cuentas de Usuario
 - 9.1.3 Revisión, Desactivación y Eliminación de Cuentas de Usuario
 - 9.2 Configuración de Control de Acceso
 - 9.3 Gestión de Contraseñas
 - 9.3.1 Control y Aplicación

- 9.3.2 Generación de contraseñas
- 9.3.3 Almacenamiento y Transmisión de Contraseña
- 9.3.4 Cambio de Contraseñas
- 9.3.5 Revisión de Contraseñas
- 9.3.6 Mantenimiento de Contraseñas
- 9.3.7 Contraseñas de los Usuarios Privilegiados de Supervisión / Sistemas de Gestión
- 9.4 Tokens de Seguridad de Acceso
- 9.5 Control de Acceso a la Red
 - 9.5.1 General
 - 9.5.2 Conexiones Externas
- 9.6 Condiciones de Seguridad para la Conexión
- 9.7 Acceso remoto
- 9.8 Control de Acceso a Sistema Operativo, Aplicaciones e Información
- 9.9 Informática móvil y Teletrabajo
 - 9.9.1 General
 - 9.9.2 Seguridad Portátil
 - 9.9.3 Seguridad PDA
- 10 Sistemas de Información Adquisición, desarrollo y Mantenimiento
 - 10.1 Seguridad de los Ficheros del sistema
 - 10.1.1 El control de Software de Operación
 - 10.1.2 Protección de datos de prueba del sistema
 - 10.1.3 Protección de Código Fuente
 - 10.2 Seguridad en el desarrollo y apoyo a los procesos
 - 10.2.1 Integridad de Software de Sistema y Aplicación

- 10.2.2 Desarrollo de Software Tercerizado
 - 10.3 Mantenimiento del software
 - 10.4 Registro de Fallas de software
 - 10.5 Gestión de la vulnerabilidad Técnicas
 - 11 Gestión de la Incidentes de Seguridad de Información
 - 11.1 Incidentes de Seguridad de Información y Debilidades
 - 11.2 TI y Fallas en la Red
 - 12 Gestión de Continuidad de Negocio
 - 12.1 Planificación de la Continuidad del Negocio
 - 12.2 Procedimientos de Respaldo
 - 12.3 Emergencias y Averías
 - 12.3.1 Falles de Hardware
 - 12.3.2 Falles de Software
 - 12.3.3 Evacuación del Edificio ante Incendios
 - 13 Conformidad
 - 13.1 Cumplimiento de requisitos legales
 - 13.2 El cumplimiento de Políticas de Seguridad y Normas Técnicas y Conformidad
 - 13.3 Protección de Herramientas de Auditoría del Sistema
 - 14 Configuración de Documentos
 - 14.1 Feedback
 - 14.2 Cambios en el SecOPs
- Apéndice A - Referencias

Anexo 4. Matriz de Riesgos de los Activos de la Información

Información del Activo					Clasificación de activos de información				Ubicación		Pertenencia		Propiedad	
ID	Tipo	Subcategoría	Nombre del Activo de Información	Descripción	C	I	D	Valor Críticidad	Interno	Externo	Público	Privado	Propietario	Custodio
1	Hardware	Servidor	SERVIDOR BLADE	Servidor principal	4	4	1	3	I			Privado	Jefe de Área	Soporte Técnico
2	Hardware	Servidor	SERVIDOR BLADE	Servidor Continencia	4	4	1	3	I			Privado	Jefe de Área	Soporte Técnico
3	Hardware	Servidor	SERVIDOR BLADE	Servidor bases de datos	4	4	4	4	I			Privado	Jefe de Área	Soporte Técnico
4	Hardware	Dispositivos de almacenamiento	NAS, SYNOLOGY	Unidad de respaldo de Backus .	4	4	4	4	I			Privado	Jefe de Área	Soporte Técnico
5	Energía	UPS	UPS TITAN , 15KV A	Unidad de poder para los equipos de cómputo	1	4	5	3	I			Privado	Jefe de Área	Soporte Técnico

Información del Activo					Clasificación de activos de información				Ubicación		Pertenencia		Propiedad	
ID	Tipo	Subcategoría	Nombre del Activo de Información	Descripción	C	I	D	Valor Críticidad	Interno	Externo	Público	Privado	Propietario	Custodio
6	Equipo de Comunicación	Equipo de Ruteo	Router	Equipo de Internet del Proveedor	5	5	5	5		E		Privado	Jefe de Área	Soporte Técnico
7	Equipo de Comunicación	Equipo de Switching	Switch	Equipo de Internet del Proveedor	5	5	5	5	I			Privado	Jefe de Área	Soporte Técnico
8	Equipo de Comunicación	Sistema de CCTV.	Cámaras de Vigilancia	Polycom	5	1	1	2		E		Privado	Jefe de Área	Soporte Técnico
9	Servicios	Servicio de Internet	Internet	Salida a la World Wide Web	5	5	5	5		E		Privado	Jefe de Área	Soporte Técnico
10	Hardware	Estaciones de Trabajo	Computadoras	Computadoras de los Teleoperadores	5	1	1	2	I			Privado	Jefe de Área	Soporte Técnico

Información del Activo					Clasificación de activos de información				Ubicación		Pertenencia		Propiedad	
I D	Tipo	Subcategoría	Nombre del Activo de Información	Descripción	C	I	D	Valor Crítico dad	Inter no	Exter no	Públi co	Priva do	Propiet ario	Custo dio
1 1	Softw are	Sistema Operativ o	Window s Server	Sistema operativ o Servidor Principa l	5	5	5	5	I			Priva do	Jefe de Área	Sopor te Técni co
1 2	Softw are	Sistema Operativ o	Window s Server	Sistema operativ o Equipos Servidor backup	5	5	5	5	I			Priva do	Jefe de Área	Sopor te Técni co
1 3	Softw are	Base de Datos	Oracle	Motor de bases de datos para el Sistema Web	5	5	5	5	I			Priva do	Jefe de Área	Sopor te Técni co
1 4	Softw are	Antivirus	Norton Antiviru s	Sistema End point de protecci ón antimal ware.	1	5	5	4	I			Priva do	Jefe de Área	Sopor te Técni co

Información del Activo					Clasificación de activos de información				Ubicación		Pertenencia		Propiedad	
ID	Tipo	Subcategoría	Nombre del Activo de Información	Descripción	C	I	D	Valor Crítica	Interno	Externo	Público	Privado	Propietario	Custodio
15	Servicios	Servicio Web	Servicio Web	Sistema de Ventas entre el Call Center y el ISP.	5	5	5	5	I		Público		Jefe de Área	Soporte Técnico
16	Trabajadores	Teleoperadores	Teleoperadores	Personal que ingresa los datos al Sistema Web	5	1	1	2		E	Público		Jefe de Área	Soporte Técnico
17	Trabajadores	Proveedores	Técnicos	Personal de otras empresas que ingresan al Data Center por trabajos programados.	5	1	1	2		E	Público		Jefe de Área	Soporte Técnico

Anexo 5. Gestión de Riesgos

SEGURIDAD												
Activo de la Información	Riesgo Presente	Tasación del Riesgo	Acción	C	D	I	Control ISO 27033	Control de Mitigación	I	P	R	Riesgo Residual
Estaciones de Trabajo o Computadoras	Propagación de código malicioso.	Riesgo Extremo				x	Anexo A: 8.7 Protección contra código malicioso	Configurar las estaciones de trabajo con acceso limitado a redes.	4	5	20	Riesgo Insignificante
								Bloquear panel de configuración de antivirus para evitar manipulación de los usuarios finales				
								Mantener el antivirus activado en todas las estaciones de trabajo.				
								Actualizar antimalware o antivirus en las estaciones de trabajo.				
								Adquirir antimalware o antivirus con licenciamiento empresarial.				

SEGURIDAD												
Activo de la Información	Riesgo Presente	Tasación del Riesgo	Acción	C	D	I	Control ISO 27033	Control de Mitigación	I	P	R	Riesgo Residual
Estaciones de Trabajo o Computadoras	Robo de equipos de cómputo.	Riesgo Insignificante				x	Anexo A: 8.2.2.2 Política de Seguridad de la red	Restringir entrada y salida de equipos de cómputo al Call Center.	1	1	1	Riesgo Insignificante
								Adquirir seguros contra robo de equipos de cómputo.				
								Diseñar formato de reportes de pérdida de equipos.				
								Usar cadena y candado de seguridad de equipo contra robo.				
								Cifrar la información sensible ubicada en las estaciones de trabajo.				

SEGURIDAD												
Activo de la Información	Riesgo Presente	Tasación del Riesgo	Acción	C	D	I	Control ISO 27033	Control de Mitigación	I	P	R	Riesgo Residual
Información	Robo de Información	Riesgo Alto	Reducir	x	x		10.5Gestión de la vulnerabilidad Técnicas	Encriptar información en los discos duros del Call Center.	4	3	12	Riesgo Insignificante
								Respaldar información periódicamente en servidores del Call Center.				
								Implementar contraseña de arranque en la BIOS de las estaciones de trabajo del Call Center.				
								Implementar contraseña de inicio de sesión en las estaciones de trabajo del Call Center.				

SEGURIDAD												
Activo de la Información	Riesgo Presente	Tasación del Riesgo	Acción	C	D	I	Control ISO 27033	Control de Mitigación	I	P	R	Riesgo Residual
Información	Intromisiones de otros usuarios a la estación de trabajo.	Riesgo Menor	Aceptar	x			9.1.3 Revisión, Desactivación y Eliminación de Cuentas de Usuario	Educar al usuario en medidas de Seguridad de la Información básica.	1	5	5	Riesgo Insignificante
							9.3.7 Contraseñas de los Usuarios Privilegiados de Supervisión / Sistemas de Gestión	Configurar las estaciones de trabajo con acceso limitado a redes.				
								Mejorar la estructura de ID y contraseñas.				

SEGURIDAD												
Activo de la Información	Riesgo Presente	Tasación del Riesgo	Acción	C	D	I	Control ISO 27033	Control de Mitigación	I	P	R	Riesgo Residual
Redes	Acceso por entidades externas a información sensible o privada del Call Center.	Riesgo Alto	Reducir	x			10.5Gestión de la vulnerabilidad Técnicas	Monitorear las conexiones activas.	4	3	12	Riesgo Menor
								Monitorear la modificación de los archivos del Call Center.				
								Monitorear los puertos TCP/UDP.				
	Propagación de código malicioso en la red del Call Center.	Riesgo Extremo	Reducir				x	Anexo A: 8.7 Protección contra código malicioso	Configurar las estaciones de trabajo con acceso limitado a redes.	4	5	20
							Monitorear los puertos TCP/UDP.					

SEGURIDAD												
Activo de la Información	Riesgo Presente	Tasación del Riesgo	Acción	C	D	I	Control ISO 27033	Control de Mitigación	I	P	R	Riesgo Residual
Servidor	Acceso no autorizado a los servidores del Call Center	Riesgo Moderado	Reducir	x	x	x	7.10Control es de acceso a hardware	Monitorear los puertos TCP/UDP.	3	3	9	Riesgo Menor
Soporte Técnico	Acceso y manipulación a redes privadas	Riesgo Menor	Aceptar	x		x	7.11Detección de Manipulaciones	Monitorear los puertos TCP/UDP.	2	3	6	Riesgo Insignificante
	Acceso y manipulación a información privada	Riesgo Menor	Aceptar	x		x	9.2Configuración de Control de Acceso	Determinar los niveles de responsabilidad.	2	3	6	Riesgo Insignificante
							9.2Configuración de Control de Acceso	Planificar las tareas del personal de soporte técnico.				Riesgo Insignificante
Proveedores	Robo de información	Riesgo Alto	Reducir	x	x		7.8Protección del equipo contra robos	Monitorear los puertos TCP/UDP.	4	3	12	Riesgo Insignificante
	Alteración, Manipulación y Destrucción de información.	Riesgo Menor	Aceptar		x	x	7.11Detección de Manipulaciones	Planificar las tareas del proveedor.	4	1	4	Riesgo Insignificante

SEGURIDAD												
Activo de la Información	Riesgo Presente	Tasación del Riesgo	Acción	C	D	I	Control ISO 27033	Control de Mitigación	I	P	R	Riesgo Residual
Bases de Datos del Sistema Web	Alteración, Manipulación y Destrucción de información.	Riesgo Menor	Aceptar		x	x	7.11Detección de Manipulaciones	Actualizar periódicamente los respaldos de seguridad.	4	1	4	Riesgo Menor
	Acceso a la Base de Datos del Sistema Web por usuarios no autorizados o ajenos del Call Center.	Riesgo Menor	Aceptar	x			7.11Detección de Manipulaciones	Mejorar la estructura de ID y contraseñas.	4	1	4	Riesgo Menor
	Acceso a información sensibles del Call Center.	Riesgo Menor	Aceptar	x			7.11Detección de Manipulaciones	Encriptar de datos sensibles del proceso.	2	3	6	Riesgo Menor

SEGURIDAD												
Activo de la Información	Riesgo Presente	Tasación del Riesgo	Acción	C	D	I	Control ISO 27033	Control de Mitigación	I	P	R	Riesgo Residual
Sistema de RespalDOS	Alteración, Manipulación y Destrucción de información de respaldo.	Riesgo Insignificante	Aceptar		x	x	7.11Detección de Manipulaciones	Actualizar periódicamente los respaldos de seguridad.				Riesgo Insignificante
								Capacitar al personal técnico respectivo en el proceso de restauración de los datos del sistema Web.	1	1	1	
	Acceso a los Sistemas de Respaldo por usuarios no autorizados.	Riesgo Insignificante	Aceptar	x			7.10Controles de acceso a hardware	Determinar los niveles de acceso al sistema Web por personal externo no autorizado.	1	1	1	Riesgo Insignificante

SEGURIDAD												
Activo de la Información	Riesgo Presente	Tasación del Riesgo	Acción	C	D	I	Control ISO 27033	Control de Mitigación	I	P	R	Riesgo Residual
Sistemas de Autenticación	Exposición de credenciales de sistemas importantes a usuarios no autorizados	Riesgo Insignificante	Aceptar	x		x	9.3.3 Almacenamiento y Transmisión de Contraseña	Encriptar la información del sistema de autenticación.	1	3	3	Riesgo Menor
Salida a Internet	Divulgación de información confidencial del Call Center.	Riesgo Alto	Reducir	x			10.5 Gestión de la vulnerabilidad Técnicas	Bloquear el acceso a páginas de internet no seguras o de dudosa reputación.	4	3	12	Riesgo Menor
								Uso de firewalls para la protección de tráfico hacia y desde Internet.				
								Monitorear los puertos TCP/UDP.				
								Realizar Políticas de Seguridad para el acceso a internet.				