UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS

FACULTAD DE INGENIERÍA

**PROGRAMA ACADÉMICO DE INGENIERÍA DE SISTEMAS DE
INFORMACIÓN**

**Modelo de gestión de riesgos de seguridad de TI para pymes del sector
comercial que dependen de proveedores críticos**

TESIS

Para optar el título profesional de Ingeniero de Sistemas de Información

AUTOR(ES)

Flores Huamani, Vladimir (0000-0001-5501-0175)

Chavez Rios, Manuel Junior (0000-0003-2516-2746)

ASESOR

Mansilla Lopez, Juan Pablo Jesus (0000-0003-0039-6044)

Lima, 02 de Julio de 2020

DEDICATORIA

El presente trabajo está dedicado a nuestros padres por haber sido nuestro principal apoyo a lo largo toda la carrera universitaria. Asimismo, a todas las personas especiales que nos acompañaron durante esta gran etapa, aportando a nuestra formación tanto profesional como de ser humano.

AGRADECIMIENTOS

Agradecemos a Dios por bendecirnos y guiarnos a lo largo de nuestras vidas, ser el apoyo y fortaleza en aquellos momentos de dificultad y debilidad.

De igual manera, queremos agradecer a todas las personas que nos guiaron y apoyaron a la realización exitosa de este proyecto. De manera especial a nuestro asesor de tesis Juan Pablo Mansilla, principal colaborador durante todo este proceso, quien con su dirección, conocimiento, enseñanza y colaboración permitió el desarrollo de este trabajo.

RESUMEN EJECUTIVO

La seguridad de la información se ha convertido en un área importante, ya que las organizaciones diariamente administran activos de TI valiosos que dependen de proveedores críticos; tales como: bases de datos, servicios, aplicaciones, hardware, etc. Estos activos están sometidos a riesgos de una gran variedad, como: desastres naturales, ciberataques, fraudes, etc. que pueden afectar de forma crítica a la organización.

Estudios realizados sobre organizaciones en Europa y EE. UU revelan que las Pymes se caracterizan por la falta de la dedicación necesaria a la seguridad de TI. Esto debido principalmente a que la seguridad de la información no forma parte de sus necesidades internas. En el Perú, las empresas no se encuentran preparadas para afrontar situaciones de riesgo, debido a que la mayoría de las organizaciones carecen de políticas de seguridad y sistemas de evaluación de riesgos.

El presente proyecto plantea el desarrollo de un modelo de gestión de riesgos de seguridad de TI que tiene como objetivo incrementar el nivel de madurez y disminuir el nivel de riesgo en los procesos y activos de TI de las Pymes que dependen de proveedores críticos. Esto mediante una serie de controles y planes de seguridad basados en la metodología Magerit y estándares de seguridad como la ISO/IEC 27001:2013. Con esto, buscamos cubrir la principal necesidad identificada en las Pymes, la cual es reducir el nivel de impacto ocasionado por los riesgos que afectan los activos y procesos de TI soportados por terceros, y que además puedan contar con un adecuado plan de continuidad.

Palabras clave: Gestión del riesgo; Estándares de gestión del riesgo; Pyme; Magerit; Activos de TI; ISO

ABSTRACT

Information security has become an important area as organizations daily manage valuable IT assets that depend on critical providers; such as: databases, services, applications, hardware, etc. These assets are subject to risks of a wide variety, such as: natural disasters, cyberattacks, fraud, etc. that can critically affect the organization.

Studies carried out on organizations in Europe and USA reveal that SMEs are characterized by the lack of dedication necessary to IT security. This is mainly because information security is not part of their internal needs. In Peru, companies are not prepared to face risk situations, since most organizations lack security policies and risk assessment systems.

This project proposes the development of an IT security risk management model that aims to increase the level of maturity and decrease the level of risk in the IT processes and assets of SMEs that depend on critical providers. This through a series of controls and security plans based on the Magerit methodology and security standards such as ISO / IEC 27001: 2013. With this, we seek to cover the main need identified in SMEs, which is to reduce the level of impact caused by the risks that affect IT assets and processes supported by third parties, and that may also have an adequate continuity plan.

Keywords: Risk management; Risk management standards; SME; Magerit; IT assets; ISO

TABLA DE CONTENIDOS

Introducción.....	13
CAPITULO 1 DEFINICIÓN DEL PROYECTO.....	14
1.1 OBJETO DE ESTUDIO	15
1.2 DOMINIO DEL PROBLEMA.....	15
1.3 PLANTEAMIENTO DE LA SOLUCIÓN.....	17
1.4 OBJETIVOS DEL PROYECTO	17
1.5 INDICADORES DE ÉXITO	18
1.6 PLANIFICACIÓN DEL PROYECTO	18
1.6.1 Alcance	19
1.6.2 Plan de Gestión de Tiempo.....	20
1.6.3 Plan de Gestión de Recursos Humanos	22
1.6.4 Plan de Gestión de Comunicaciones	25
1.6.5 Plan de Gestión de Riesgos	25
CAPITULO 2 LOGROS DE LOS STUDENT OUTCOMES	27
2.1 STUDENT OUTCOMES.....	28
2.1.1 Student Outcome 1	28
2.1.2 Student Outcome 2	29
2.1.3 Student Outcome 3	30
2.1.4 Student Outcome 4	31
2.1.5 Student Outcome 5	33
2.1.6 Student Outcome 6	35
2.1.7 Student Outcome 7	36
CAPITULO 3 MARCO TEÓRICO	41
3.1 COMERCIO.....	42
3.2 SEGURIDAD.....	46
3.3 RIESGO	47
3.4 ACTIVO DE INFORMACIÓN	51
3.5 AMENAZA	52
3.6 ESTANDAR ISO.....	54
3.7 LEY DE PROTECCIÓN DE DATOS PERSONALES	63
CAPITULO 4 DESARROLLO DEL PROYECTO	69
4.1 ANÁLISIS DE LA PROPUESTA.....	70
4.1.1 Benchmarking	70
4.1.2 Metodologías para la gestión de riesgos	70
4.1.3 Estándares para la gestión de seguridad de la información	80
4.2 DISEÑO DEL MODELO DE REFERENCIA	85
4.2.1 Descripción.....	85
4.2.2 Modelo de referencia.....	85
CAPITULO 5 RESULTADO DEL PROYECTO	114
5.1 VALIDACIÓN DEL MODELO	115
5.1.1 Juicio de expertos	115

5.1.2 Aplicación del modelo en un caso de estudio.....	125
5.2 PLAN DE CONTINUIDAD DEL PROYECTO.....	138
5.2.1 Etapas del modelo de referencia	138
5.2.2 Estrategia de continuidad del modelo	141
5.2.3 Implementación del modelo.....	152
5.2.4 Actualización del modelo	155
5.3 COSTOS Y PRESUPUESTOS	159
CAPITULO 6 GESTIÓN DEL PROYECTO.....	164
6.1. GESTIÓN DEL PROYECTO	165
6.1.1 Gestión del tiempo.....	165
6.1.2 Gestión de los Recursos Humanos	165
6.1.3 Gestión de las Comunicaciones	167
6.1.4 Gestión de los Riesgos	168
6.1.5 Lecciones Aprendidas	168
CONCLUSIONES.....	170
RECOMENDACIONES	171
GLOSARIO	172
SIGLARIO	174
BIBLIOGRAFÍA.....	175
ANEXOS	177
Anexo A – WASC	177
Anexo B – Benchmarking	196
Anexo C - Resultados de la encuesta Juicio de expertos	203
Anexo D - Cuestionario Assessment.....	211
Anexo E - Cartera de Proyectos	227

INDICE DE TABLAS

Tabla 1: Tabla de necesidades y causas	16
Tabla 2: Descripción de Indicadores de éxito del proyecto	18
Tabla 3: Tabla de Gestión del tiempo	22
Tabla 4: Tabla de Roles y responsabilidades	24
Tabla 5: Tabla de riesgos del proyecto.....	26
Tabla 6: Criterios de selección y exclusión.....	38
Tabla 7: Estructura del sector comercial	45
Tabla 8: Probabilidad de ocurrencia.....	53
Tabla 9: Degradación del valor	53
Tabla 10: Modelo de PDCA aplicado a procesos de BCMS.....	58
Tabla 11: Alcance del ISO 19011 - 2011	61
Tabla 12: Comparativa de metodologías de gestión de riesgos	79
Tabla 13: Comparativa de estándares de gestión de seguridad de la información.....	84
Tabla 14: Nivel de madurez de la gestión de Riesgos y seguridad de TI.....	97
Tabla 15: Criterio: Seguridad de la información de la empresa.....	99
Tabla 16: Criterio: Seguridad de la información asociado a proveedores críticos.....	100
Tabla 17: Criterio: Procesos asociados a proveedores críticos de TI.....	101
Tabla 18: Criterio: Activos críticos de TI asociado a proveedores críticos.....	102
Tabla 19: Criterio: Amenazas asociadas a los activos de TI.....	103
Tabla 20: Criterio: Impacto y riesgo	105

Tabla 21: Criterio: Planes de tratamiento.....	106
Tabla 22: Criterio: Establecimiento de controles	107
Tabla 23: Criterio: Monitoreo y control.....	109
Tabla 24: Criterio: Auditoria.....	110
Tabla 25: Herramienta de evaluación.....	112
Tabla 26: Herramienta de evaluación (Puntajes por pregunta)	113
Tabla 27: Expertos para evaluación de criterios	118
Tabla 28: Instrumento de evaluación	119
Tabla 29: Calificación experto 1	120
Tabla 30: Calificación experto 2	121
Tabla 31: Calificación experto 3	122
Tabla 32: Calificación experto 4	122
Tabla 33: Calificación experto 5	123
Tabla 34: Evaluación AS-IS del nivel de madurez	129
Tabla 35: Controles para Gestión del riesgo	130
Tabla 36: Controles para Gestión de Seguridad de información.....	131
Tabla 37: Controles para la continuidad del negocio	132
Tabla 38: Evaluación TO-BE del nivel de madurez.....	133
Tabla 39: Indicadores de éxito del nivel de madurez.....	134
Tabla 40: Lista de riesgos potenciales de Kukyflor	136
Tabla 41: Controles propuestos para los activos críticos de TI.....	136

Tabla 42: Lista de riesgo residual de Kukyflor	137
Tabla 43: Comparativa: Riesgo inherente vs Riesgo residual.....	137
Tabla 44: Indicador de éxito del nivel de riesgo Kukyflor.....	138
Tabla 45: Costo de Investigación y desarrollo del modelo	160
Tabla 46: Costo de Implementación del modelo.....	161
Tabla 47: Costo de soporte externo del modelo	162
Tabla 48: Matriz de riesgos del proyecto	168

ÍNDICE DE FIGURAS

Figura 1: Gestión de RRHH del proyecto	23
Figura 2: Proceso sistemático de revisión de la literatura	39
Figura 3: Índice sector comercio en el Perú.....	44
Figura 4: Componentes del análisis de gestión de riesgos	50
Figura 5: Modelo de PDCA aplicado a procesos de BCMS	58
Figura 6: Proceso metodología Octave	72
Figura 7: Componentes de la evaluación de riesgos Magerit.....	73
Figura 8: Fases del método EBIOS	75
Figura 9: Fases del método CORAS	77
Figura 10: Mapa de miembros ISO	81
Figura 11: Modelo PDCA en BS 7799.....	82
Figura 12: Proceso de gestión de riesgos en SP 800-39.....	83
Figura 13: Modelo de gestión de riesgos de seguridad de TI.....	92
Figura 14: Criterios de validación del modelo	93
Figura 15: Elementos clave de la gestión de riesgos.....	94
Figura 16: Nivel de madurez de gestión de riesgos y seguridad de TI.....	96
Figura 17: Proceso de Juicio de Expertos	116
Figura 18: Resultado por Categoría	124
Figura 19: Resultado por Fases del modelo	125
Figura 20: Proceso de validación del modelo en un caso de estudio	127

Figura 21: Puntaje por criterios AS-IS	128
Figura 22: Puntaje por criterios TO-BE	133
Figura 23: Mapa de calor del nivel de riesgo	135
Figura 24: Ciclo PDCA.....	141
Figura 25: Actividades típicas de auditoría.....	151
Figura 26: Cronograma de actividades implementación del modelo	154
Figura 27: Pasos a seguir para la implementación del modelo	154
Figura 28: Plan de continuidad del modelo de gestión de riesgos de seguridad de TI.....	158
Figura 29: Flujo de Caja.....	163
Figura 30: Plan de trabajo del proyecto	165

INTRODUCCIÓN

El objetivo principal del presente proyecto consiste en la implementación de un “**Modelo de Gestión de Riesgos de Seguridad de TI para Pymes del Sector Comercial que dependen de proveedores críticos**”. Por tal motivo, el presente documento detallará la descripción completa del proyecto, según la estructura brindada por la Universidad Peruana de Ciencias Aplicadas (UPC). La finalidad de este proyecto es permitir a las organizaciones (PYMES) tomar conciencia de los riesgos a los que se encuentran sus activos de tecnologías de información que dependen de proveedores críticos, y tomar acciones que puedan reducir el nivel de impacto causados por estos; el cual les permitirá operar de forma continua.

La estructura de este documento se encuentra distribuida en los siguientes seis capítulos:

Capítulo 1

Describe el proyecto de forma general, presenta el problema, el objeto de estudio, objetivos del proyecto, la propuesta de solución y la gestión del proyecto durante los ciclos 2018-02 y 2019-01.

Capítulo 2

Describe los logros del proyecto en base a los Students Outcomes, regida a la acreditación de ABET.

Capítulo 3

Describe el marco teórico que fundamentará el proyecto en base al planteamiento del problema realizado. Este capítulo contempla puntos muy importantes para la solución del problema.

Capítulo 4

Contiene el desarrollo del proyecto; el cual contempla el análisis y diseño de la propuesta que forman parte de los objetivos específicos.

Capítulo 5

Se desarrolla el resultado final del proyecto; en el cual se describe la validación y el plan de continuidad del proyecto.

Capítulo 6

Detalla todos los documentos de gestión del proyecto haciendo uso de la metodología PMBOK.

Finalmente, se incluirán todas las fuentes investigadas durante el proyecto y anexos al documento.

CAPITULO 1   DEFINICIÓN DEL PROYECTO

En el capítulo 1 se describen los aspectos generales del proyecto. Se describen la problemática, el objetivo general, los objetivos específicos, la solución propuesta, los indicadores de éxito con los que se medirá el cumplimiento del proyecto. Por otro lado, se detallan los planes elaborados con relación a la gestión del proyecto, los cuales son el Alcance del proyecto, Plan de Gestión del Tiempo, Plan de Gestión de Recursos Humanos, Plan de Comunicaciones y el Plan de Gestión de Riesgos.

1.1 OBJETO DE ESTUDIO

El proyecto consiste en el desarrollo de un **"Modelo de Gestión de Riesgos de Seguridad de TI para Pymes del Sector Comercial que dependen de proveedores críticos"**, el cual estará basado principalmente por la metodología MAGERIT y el estándar ISO 27001:2013. Asimismo, otras herramientas como los estándares y normas: ISO 22301:2012, ISO 19011:2011, la Ley de protección de datos personales y las Circulares de la Superintendencia de Banca y Seguros (SBS) los cuales se usaron como soporte para el modelo. Esta propuesta permitirá a una organización reducir el nivel del impacto causado por cualquier amenaza que afecte los procesos y activos de TI que dependen de proveedores críticos.

1.2 DOMINIO DEL PROBLEMA

De acuerdo con la Norma Internacional de Información Financiera (NIIF), las PYMES se caracterizan por ser aquellas entidades que publican estados financieros con fines de información general para usuarios externos y no tienen responsabilidad pública; esta definición se basa en la naturaleza de una entidad y no en su tamaño.

Según Dimopoulos, considera que la gestión de la seguridad de la información a través de una evaluación de riesgos formal en las PYMES encuentra dificultades de implementación debido a los siguientes factores:

- i)** El desarrollo de la seguridad de la información no forma parte de las necesidades internas de las PYMES;
- ii)** Debido a la falta de experiencia, en las PYMES hay errores de percepción de la situación actual de la seguridad de la información y el nivel de exposición a las amenazas de seguridad;
- iii)** Las PYMES tienen percepciones que requieren un enfoque principalmente en actividades relacionadas con negocios.

Estos factores se han validado y confirmado a través de diferentes estudios; mientras tanto, Lopes et al, de un estudio realizado en 307 pymes, concluyeron que solo en el 9% de ellas se puede considerar que existe una cultura organizacional sobre la seguridad de la información. Gordas sugiere que las PYMES requieren un enfoque estructurado para el monitoreo y la gestión exitosa

y el gobierno de la seguridad de la información, mediante el uso de modelos apropiados de gestión de riesgos de seguridad. (Author (s): Montenegro, 2016)

Según una encuesta de PwC Global State of the Information Security Survey 2018, aplicado a más de 9,500 ejecutivos de negocios y tecnología en 122 países, los participantes del estudio reconocen la importancia de prevenir los riesgos cibernéticos: el 40% cita a la interrupción de las operaciones como la principal consecuencia de un ataque cibernético, seguida por el acceso a información confidencial (39%), daños a la calidad de los productos (32%) y daños a la vida humana (22%)”.

No obstante, muchas empresas con riesgo de sufrir ataques cibernéticos aún están insuficientemente preparadas para hacerle frente a esta problemática. El 44% de encuestados afirma no tener una estrategia de seguridad de la información, mientras que 48% no cuenta con programas de concientización y capacitación en seguridad para los empleados y el 54% no ha implementado un proceso de respuesta a incidentes. (Gestión D. , 2017)

Un estudio reciente de la Universidad de Texas revela que solo el 6% de empresas que sufren pérdidas catastróficas de datos logran sobrevivir. En el estudio se visibilizó que una paralización no controlada de más de ocho horas en una empresa causa una pérdida irreversible al negocio.

Pero la mayoría de las compañías no cuentan con adecuados planes de continuidad para enfrentarlos y superarlos sin comprometer la vida de los negocios.” (Gestión, 2018)

Necesidad	Causas
Reducir el nivel de impacto ocasionado por los riesgos que afectan a los activos y procesos de TI en las Pymes que dependen de proveedores críticos	• Falta de seguimiento del cumplimiento de los controles de seguridad que se deben realizar a los proveedores. (PWC, 2017) • No existe implementación de controles adecuados debido a que no cuentan con un área de gestión de riesgos o tienen deficiencias en las mismas. (Gestión D. , 2017) • Deficiencia de auditorías de la empresa a los proveedores que permita asegurar el cumplimiento de los Acuerdos de nivel de servicio (SLA's) establecidos por los proveedores. (Comercio, 2017) • Falta de controles adecuados hacia los proveedores con acceso a los activos de información de la empresa. (PWC, 2017)

Tabla 1: Tabla de necesidades y causas

Fuente: Elaboración propia

1.3 PLANTEAMIENTO DE LA SOLUCIÓN

La solución que el proyecto plantea es el desarrollo de un “Modelo de Gestión de Riesgos de Seguridad de TI para Pymes del Sector Comercial que dependen de proveedores críticos”. Este modelo se desarrollará a partir de la recolección de información sobre metodologías de gestión de riesgos y estándares de gestión de seguridad de la información publicados, así como también el uso de estándares como: ISO 22301:2012, ISO 19011:2011, la Ley de protección de datos personales y las Circulares de la Superintendencia de Banca y Seguros (SBS)

Con el proyecto, se busca garantizar la seguridad de las TI en las Pymes del sector comercial que dependen de proveedores críticos, y en su defecto estas tengan un mínimo nivel de impacto ante cualquier amenaza ya sea de tipo interno o externo reestableciendo sus operaciones en el menor tiempo posible.

1.4 OBJETIVOS DEL PROYECTO

- **Objetivo General**

OG: Implementar un Modelo de Gestión de Riesgos de Seguridad de TI en una Pyme del Sector Comercial que dependa de proveedores críticos.

- **Objetivos Específicos**

OE1: Analizar metodologías y estándares de gestión de riesgos de seguridad de la información que permitan el diseño del modelo de gestión de riesgos de seguridad de TI.

OE2: Diseñar un modelo de gestión de riesgos de seguridad de TI para Pymes del sector comercial basados en la metodología y estándares seleccionados.

OE3: Validar el modelo de gestión de Riesgos de Seguridad de TI en una Pyme del sector comercial que dependa de proveedores críticos.

OE4: Elaborar un Plan de Continuidad que garantice un adecuado nivel de seguridad a los activos y procesos de TI vinculados a proveedores críticos y la escalabilidad del modelo.

1.5 INDICADORES DE ÉXITO

A continuación, se describen los indicadores para medir el éxito del proyecto a través del logro de los objetivos específicos ya planteados.

Objetivos	Indicador de éxito	Objetivo específico
<i>IE1</i>	Acta de aprobación por parte del cliente sobre el análisis de las metodologías y estándares de gestión de riesgos de seguridad de la información.	OE1
<i>IE2</i>	Acta de aprobación por parte del cliente sobre el diseño del modelo de gestión de riesgos de seguridad de TI basado en la metodología y estándares seleccionados.	OE2
<i>IE3</i>	Acta de aprobación por parte del cliente y el responsable de la entidad comercial sobre la validación del modelo de gestión de riesgos de seguridad de TI en la Pyme del sector comercial seleccionada.	OE3
<i>IE4</i>	Acta de aprobación por parte del cliente sobre el plan de continuidad elaborado.	OE4

Tabla 2: Descripción de Indicadores de éxito del proyecto

Fuente: Elaboración propia

1.6 PLANIFICACIÓN DEL PROYECTO

Elaborar un Plan de Gestión del Proyecto está enfocado en realizar una gestión eficiente del mismo, tomando en cuenta el tiempo asignado para las actividades del proyecto, los recursos necesarios a emplear, humanos y materiales, limitaciones del proyecto, riesgos, entre otros. En esta sección, se explica la elaboración del Plan de la Gestión del Proyecto, desde la fase inicial hasta la fase final. Se expondrá el Plan de Gestión del

Alcance, el Plan de Gestión del Tiempo, Plan de Gestión de Recursos Humanos, Plan de Gestión de Comunicaciones y el Plan de Gestión de Riesgos.

1.6.1 Alcance

El alcance del proyecto considera lo siguiente:

- Definición de gestión de Riesgos
  - Importancia de la gestión de riesgos
  - Gestión del riesgo
  - Análisis del riesgo
- Análisis de metodologías de Gestión del Riesgo
  - Metodologías de Gestión del Riesgo
  - MAGERIT
  - OCTAVE
  - EBIOS
  - CORAS
  - MEHARI
- Análisis de estándares de TI
  - ISO 27001
  - ISO 22301
  - ISO 19011
- Metodología MAGERIT
  - Concepto
  - Pasos a seguir
  - Plan de actividades
- Modelo de gestión de riesgos de seguridad de TI
  - Diseño del modelo de gestión de riesgos en base a las metodologías y estándares seleccionados
  - Aprobación del modelo de gestión de riesgos de TI
- Validación del modelo de gestión de riesgo
  - Aplicación del modelo desarrollado de acuerdo con los procesos de la empresa comercial
  - Análisis situacional del sector comercial
  - Activos, procesos y proveedores críticos
  - Identificación de amenazas

- Levantamiento y diagnóstico situacional de la entidad comercial
- Evaluación mediante encuestas enviadas a la empresa del sector comercial
- Evaluación de Riesgos de seguridad de TI asociados a proveedores críticos
- Tratamiento de riesgos de seguridad de TI asociados a proveedores críticos
- Valoración del Riesgo residual
- Nivel de madurez de la empresa en gestión de riesgos de seguridad de TI
- Indicadores luego de la implementación del modelo
- Evaluación a través de juicio de expertos
- Plan de continuidad para el modelo de gestión de riesgos
  - Seguimiento y revisión de riesgos de seguridad de TI asociados a proveedores críticos
    - Programa de auditoría de seguimiento a los controles establecidos en el modelo de gestión de riesgos asociados a proveedores críticos
    - Determinación de las competencias de los auditores
    - Establecimiento de criterios de evaluación del auditor
- Acta de Aceptación y cierre
- Memoria Final del Proyecto
- Poster del proyecto

1.6.2 Plan de Gestión de Tiempo

Se encuentra orientado en gestionar el tiempo que se emplea en el proyecto para lograr el cumplimiento de las actividades establecidas en el cronograma. A continuación, se detallan las fechas de entrega que han sido planificadas para los entregables del proyecto, según las fases acordadas.

Fase del Proyecto	Hito del proyecto	Fecha Estimada	Entregables incluidos	Prioridad
	Validación del Capítulo 2 (Plan).	Semana 2 2018-02	Documento de los Outcomes de ABET	Alta

Inicio	Aprobación del Project Charter	Semana 3 2018-02	Project Charter	Alta
	Aprobación del marco teórico (capítulo 4).	Semana 6 2018-02	Memoria del Proyecto (Capítulo 4 – Marco Teórico)	Alta
	Aprobación del Estado del Arte.	Semana 10 2018-02	Memoria del Proyecto (Capítulo 3 – Estado del Arte)	Alta
Planificación	Ejecución del Capítulo 7 (Artefactos de PM).	Semana 6 2018-02	Documento de los Artefactos del PM.	Alta
Ejecución	Aprobación del Objetivo 1.	Semana 11 2018-02	Benchmarking de metodologías y estándares de gestión de riesgos de seguridad de información	Alta
	Aprobación del Objetivo 2.	Semana 14 2018-02	Diseño del modelo de gestión de riesgos de seguridad de TI	Alta
	Aprobación del Objetivo 3.	Semana 23 2019-01	Criterios de validación del modelo	Alta

	Revisión del Capítulo 05 (Desarrollo del proyecto)	Semana 23 2019-01	Memoria del Proyecto (Capítulo 5 – Desarrollo del proyecto)	Alta
	Aprobación de la Cartera de Proyectos.	Semana 25 2019-01	Acta de aprobación de la Cartera de Proyectos	Alta
Control	Aprobación del Objetivo 04.	Semana 27 2019-01	Documento del Plan de Continuidad del modelo	Alta
	Aprobación del Capítulo 02 -	Semana 30 2019-01	Documento de los Outcomes de ABET	Alta
Cierre	Aprobación de los artefactos del proyecto, por parte del profesor cliente o gerente.	Semana 31 2019-01	• Poster del proyecto • Acta de conformidad del proyecto	Alta

Tabla 3: Tabla de Gestión del tiempo

Fuente: Elaboración propia

1.6.3 Plan de Gestión de Recursos Humanos

Tiene como fin identificar a los involucrados en el proyecto, está compuesto por el Comité de dirección, equipo de trabajo y los recursos internos o externos que serán parte del mismo para el

cumplimiento de las actividades planificadas. Además, se detallan los roles y responsabilidades que cumplen a lo largo del desarrollo del proyecto.

Figura 1: Gestión de RRHH del proyecto

Fuente: Elaboración propia

El equipo del proyecto estará conformado por:

Rol	Miembro	Responsabilidades
Comité de Proyectos	Rosario Villalta Jimmy Armas Pedro Shiguihara Daniel Subauste	- Aprobar proyectos profesionales. - Evaluar el avance del proyecto. - Verificar el cumplimiento de los entregables - Decidir continuidad de proyectos.
Gerente General de Empresas Virtuales	Alfredo Barrientos	- Gestionar todos los proyectos que tiene a su cargo, dando su aprobación
Gerente General de IT Consulting	Daniel Burga	- Gestionar todos los proyectos que están dentro de la empresa IT Consulting
Gerente Profesor de IT Consulting	Esther Aliaga	- Asesorar y dar seguimiento a los proyectos de la empresa. - Facilitar la comunicación con las empresas virtuales. - Monitorear los avances del proyecto. - Brindar recomendaciones en cuanto al desarrollo del proyecto.
Profesor Cliente	Juan Pablo Mansilla	- Dar los requerimientos del Proyecto. - Dar conformidad a los entregables del proyecto. - Asesorar a los jefes de proyecto.
Jefe de Proyecto 1 y 2	Vladimir Flores Manuel Chávez	- Gestionar proyecto para cumplir con los objetivos, cronograma y alcance del mismo. - Coordinar reuniones con el cliente. - Apoyar en la investigación del proyecto. - Acordar con las autoridades involucradas en el proyecto. - Responsables del resultado del proyecto - Monitorear el desarrollo del proyecto. - Gestionar recursos

Tabla 4: Tabla de Roles y responsabilidades

Fuente: Elaboración propia

1.6.4 Plan de Gestión de Comunicaciones

Tiene como objetivo acordar criterios para la comunicación interna y externa sobre el proyecto, con el propósito de informar a los involucrados los avances, así como las eventualidades que puedan existir en el desarrollo del mismo.

Además, permite normalizar las formas de comunicación, con lo cual, será de conocimiento por parte de equipo de proyecto, los procedimientos y medios de comunicación a usarse según se requiera.

Para más información, revisar los documentos:

- MGRSTI_Plan de Gestión de Comunicaciones_v1.0
- MGRSTI_Registros de Interesados_v1.0

Todas las reuniones deben seguir las siguientes pautas:

- Se manejará una agenda para cada reunión de acuerdo a los temas de interés a tratarse, así como también las tareas pendientes de reuniones anteriores. Para este caso, se debe tener en cuenta el entregable a realizar según el diccionario EDT.
- Cada punto de la agenda contará con un nivel de prioridad a ser tratado.
- Se cuenta con un horario específico para cada reunión, que en este caso será los sábados a las 11:00am; sin embargo, será necesario confirmar/recordar la reunión vía correo electrónico un día antes como máximo.
- En caso se deba postergar una reunión, se deberá justificar y además acordar el nuevo día de esta de manera formal a través de un correo electrónico.
- Al finalizar cada reunión se deberá recopilar lo tratado, resaltando los acuerdos para posteriormente elaborar el acta de reunión.
- Todas las actas de reunión deberán ser firmadas por el cliente, jefe de proyecto1 y jefe de proyecto2.

1.6.5 Plan de Gestión de Riesgos

Permite identificar los posibles riesgos durante el desarrollo del proyecto, de tal manera se establece el impacto y la criticidad de los mismos, con lo que se plantea estrategias de mitigación ante la posible materialización del riesgo. La siguiente tabla detalla los riesgos identificados, su probabilidad y su impacto en el proyecto:

#	Riesgo	Probabilidad	Impacto	Estrategia de mitigación
1	Poca disponibilidad de tiempo por parte del cliente	Alta	Alto	Mantener una comunicación constante con el cliente para coordinar reuniones con anticipación.
2	Elaboración y presentación de los entregables del proyecto fuera del tiempo planificado.	Baja	Alto	Registrar fechas de revisión de documentación con el cliente.
3	Cambio del alcance del proyecto	Baja	Alto	Revisar el avance del proyecto junto al cliente y validar las fases e hitos a cumplir.
4	Incumplimiento y falta de compromiso por parte del recurso de QS.	Medio	Alta	Se debe realizar el seguimiento de las tareas asignadas al recurso enviadas a través de correo electrónico.
5	Falta de información sobre el tema de investigación	Baja	Medio	Realizar una constante búsqueda de fuentes confiables.
6	Recursos QS no disponibles	Baja	Medio	Realizar las solicitudes de recursos lo más pronto posible.

Tabla 5: Tabla de riesgos del proyecto

Fuente: Elaboración propia

CAPITULO 2   LOGROS DE LOS STUDENT OUTCOMES

En el capítulo 2, se contempla el cumplimiento de los Student Outcomes de la carrera de Ingeniería de Sistemas de Información, los cuales permiten que el proyecto se realice de acuerdo a los objetivos y al perfil del ingeniero de sistemas de información de la Universidad Peruana de Ciencias Aplicadas.

2.1 STUDENT OUTCOMES

Para la carrera de Ingeniería de Sistemas de Información, los Student Outcomes a lograr están dadas por la Comisión de Ingeniería de ABET. En las siguientes secciones se presentarán como se realizó con éxito cada uno de estos Student Outcomes.

2.1.1 Student Outcome 1

La capacidad de identificar, formular y resolver problemas complejos de ingeniería aplicando los principios de ingeniería, ciencia y matemática.

La necesidad identificada está referido a reducir el nivel de impacto ocasionado por los riesgos que afectan a los activos de TI de las Pymes del sector comercial que dependen de proveedores críticos. Esta necesidad se sustenta mediante la investigación realizada en diferentes fuentes de información confiables como: revistas especializadas, informes, artículos los cuales contienen estadísticas que demuestran que las Pymes no se encuentran preparadas para afrontar situaciones de riesgo. Para resolver la necesidad planteada se apoyó de diferentes herramientas como los estándares: ISO 27001, ISO 19011, ISO 22301, normativas nacionales, leyes y metodologías de gestión de riesgos. Todos ellos con la finalidad de diseñar un modelo el cual permitirá mitigar los riesgos identificados y que la empresa esté preparada para afrontarlos.

Asimismo, para la formulación de la necesidad se apoyó de la investigación de fuentes confiables donde se analizan estadísticas e indicadores, así como también las causas del problema identificado. Para la solución del problema o necesidad se empleó de manera apropiada la aplicación de aportes científicos de los artículos como: **“Aplicación de la metodología MAGERIT en una empresa agroindustrial”**, **“Enfoques de modelado de activos complejos vs. simples para Evaluación de riesgos de seguridad de la información”**. De cada uno de los artículos se identificó los aspectos más relevantes que nos sirvieron como base para el desarrollo del modelo. Aspectos como: conceptos teóricos, la aplicación del modelo en un caso de estudio y resultados finales; Todos ellos, nos apoyaron para realizar el diseño del modelo de gestión de riesgos de seguridad de TI el cual ayudará a resolver el problema o necesidad identificado.

Para la solución de la necesidad se diseñó el Modelo de gestión de riesgos de seguridad de TI. Este fue realizado con base a las comparativas que se hicieron respecto a metodologías de gestión de riesgos de seguridad de la información y estándares de gestión de seguridad de la información.

Luego del cual se seleccionó la metodología y el estándar más adecuado que serán los componentes principales del modelo de referencia.

Para el diseño del modelo de referencia se apoyó en la metodología MAGERIT, el cual permite hacer un análisis del nivel de riesgo de sistemas de información a través de dos métodos: cualitativo y cuantitativo. Ambos métodos usan cálculos matemáticos al relacionar el impacto y la probabilidad, garantizando así una disminución del nivel de riesgo. También, para una adecuada gestión de los riesgos MAGERIT tiene como componente principal a los activos de TI, por lo que la metodología tiene un proceso a seguir para identificar los activos críticos de TI, estos representan los de mayor valor para la organización y deben ser protegidos adecuadamente ante cualquier amenaza.

Asimismo, se siguió una serie de etapas las cuales fueron analizadas y desarrolladas según un plan de trabajo que mide el esfuerzo, costo, tiempo etc. Se inició con el análisis de metodologías de gestión de riesgos, y análisis de estándares de gestión de seguridad de información. Se prosiguió con el diseño del modelo de gestión de riesgos. Luego se realizó la validación del mismo en una Pyme del sector comercial cuyo resultado final fueron las recomendaciones o controles propuestos. Para una correcta solución del problema, es necesario que la organización cumpla con todas las regulaciones, estándares y metodología incluidos en el modelo. También puede aplicar mejores prácticas que no estén contempladas en el modelo de referencia. Todo ello ayudará a gestionar de manera óptima los riesgos que afectan a los activos de TI asociados a proveedores críticos.

2.1.2 Student Outcome 2

La capacidad de aplicar el diseño de ingeniería para producir soluciones que satisfagan necesidades específicas con consideración de salud pública, seguridad y bienestar, así como factores globales, culturales, sociales, ambientales y económicos

Para la solución que satisfaga la necesidad identificada de las Pymes del sector comercial se diseñó el modelo de gestión de riesgos de seguridad de TI. Ello se hizo tomando como referencia las buenas prácticas de estándares y notaciones aplicados a otros modelos en diferentes artículos de investigación.

Los componentes principales del modelo son: la metodología de gestión de riesgos de seguridad de la información MAGERIT, y el estándar ISO 27001:2013 Sistema de gestión de seguridad de la información.

Para el diseño del modelo se hizo un análisis de las principales metodologías y estándares de gestión de riesgos de seguridad de la información que aportarán a la elaboración de la propuesta de solución. Este análisis tendrá como resultado un comparativo (benchmarking) de estas técnicas de gestión de riesgos usando criterios de selección definidos y puntajes asignados a estos, que nos ayudará a elegir la mejor metodología y estándar de gestión de riesgos.

El modelo permitirá a la empresa estar en la capacidad de afrontar los eventos ocurridos y gestionarlos de manera adecuada reduciendo así los riesgos que las afectan. Ello permitirá a la misma pasar a un siguiente del nivel de madurez respecto a la gestión de riesgos y seguridad de TI. Además, el modelo fue diseñado para ser aplicado a empresas del sector comercial y cuenta con viabilidad económica lo que permite a estas poder implementarlo sin ningún inconveniente.

Asimismo, el proyecto fue diseñado de acuerdo a restricciones económicas, tiempo, recursos humanos. Todo ello previo a un análisis que se ve reflejado en el entregable Project Charter. La duración del proyecto es de 1 año durante el cual sigue una serie de etapas las cuales son: Análisis, Diseño, Validación y Plan de continuidad del modelo de referencia. El proyecto se llevó a cabo cumpliendo estándares y buenas prácticas siguiendo la metodología PMBOK, el cual nos da directrices para un correcto desarrollo del mismo.

Finalmente, durante la implementación del modelo, cualquier proceso de negocio de la organización debe alinearse al modelo de gestión de riesgos de seguridad de TI. Ello permitirá una implementación más eficiente y una adecuada gestión de los riesgos asociados a proveedores críticos.

2.1.3 Student Outcome 3

La capacidad de comunicarse efectivamente con un rango de audiencias

Durante los ciclos 2018-02 y 2019-01, año de elaboración del proyecto, se realizarán en varias oportunidades exposiciones presenciales ante el comité, el profesor gerente y cliente. También, en la validación y ejecución del caso de estudio del proyecto, se tendrá que realizar presentaciones a los expertos en el tema. Para realizar una buena presentación se debe seguir una serie de recomendaciones que nos ayudaran a realizar exposiciones que además de dejar una buena

impresión al jurado, nos permitirá vencer en el tiempo las dificultades más comunes. Estas recomendaciones pueden ser: grabarse uno mismo, practicar en grupo, exponer ante otra persona, conocer al público, mantener un contacto visual, etc.

Luego de las exposiciones se procedió al feedback de los interesados los cuales consistieron en realizar correcciones a la presentación como: disminuir los textos de las presentaciones, agregar más gráficos, sustentar mejor los indicadores. Todas estas observaciones fueron levantadas luego de la asesoría con el profesor cliente y posteriormente presentadas a los demás interesados. Además, estas observaciones fueron tomadas como experiencia de mejora para las siguientes sustentaciones con los interesados del proyecto.

La comunicación también se dio durante las reuniones con todos los interesados del proyecto. Con el profesor gerente en el dictado de clases, con los recursos que apoyaron a realizar diferentes tareas, con el Comité de proyectos para cualquier consulta o tramite, con los representantes de la empresa donde se hizo la validación y con el profesor cliente el cual fue nuestro principal apoyo. Todas estas reuniones se evidenciaron con las actas de reunión que se tuvieron a lo largo del proyecto.

Para la parte escrita, en la documentación se usaron las plantillas proporcionadas por la universidad para mantener una estructura organizada y entendible. Además, la redacción de la documentación será revisada por distintos profesores para validar que sea entendible para el lector.

Finalmente, los resultados de la implementación del modelo serán comunicados de manera oral y escrita a la alta gerencia de la empresa donde se realizó la validación. Específicamente al Gerente general y al Gerente de TI los cuales tienen diferentes especialidades. Esto se hizo a través de un documento escrito, y también mediante una exposición oral en las instalaciones de la organización.

2.1.4 Student Outcome 4

La capacidad de reconocer responsabilidades éticas y profesionales en situaciones de ingeniería y hacer juicios informados, que deben considerar el impacto de las soluciones de ingeniería en contextos globales, económicos, ambientales y sociales

Por derechos de autor y respeto a la propiedad intelectual, la información recopilada y analizada en el presente documento cuenta con las referencias y citas apropiadas de los respectivos modelos,

artículos, definiciones, reportes, estándares e incluso imágenes que no sean de elaboración propia. Además, en el modelo propuesto se tomará en cuenta la Ley de protección de datos personales para el tratamiento de riesgos, con la finalidad de mantener uno de los mayores pilares que sostienen a las organizaciones, los clientes. Asimismo, para la elaboración del presente documento los autores respetan la propiedad intelectual y la confidencialidad de la información entregada por la empresa en donde se hizo la validación y de ser necesario se mantendrá en estricta reserva la información confidencial que se recopile de las empresas materia de análisis; esto a través de un acuerdo de confidencial de parte de la empresa y los jefes de proyecto.

Asimismo, como futuros ingenieros reconocemos el papel del: Institute of Electrical and Electronics Engineers - IEEE y la Association for Computing Machinery - ACM para promover la creatividad, desarrollo, integración, compartir y aplicar los avances de la tecnología de la información en beneficios de la sociedad en general y de los mismos profesionales. Esto a través de la publicación de informes y artículos científicos relacionados con nuestro proyecto de desarrollo. Por otra parte, para el correcto desarrollo del proyecto se han cumplido los códigos de ética y conducta profesional de la IEEE y la ACM. Esto se evidencia en el manejo adecuado de la información, respeto hacia los interesados del proyecto, fomentar el conocimiento a la ciudadanía, liderazgo profesional y evaluación de los recursos.

Asimismo, la responsabilidad profesional se demuestra mediante el cumplimiento de las tareas establecidas en el plan de trabajo, la cual tiene una duración de 1 año y que es revisada periódicamente por todos los interesados del proyecto para su correcto desarrollo. En caso de cualquier inconveniente surgido para el cumplimiento de las tareas se realizan reuniones con los interesados a fin de llegar a un acuerdo para el cumplimiento de los objetivos establecidos en el plan de trabajo.

Para la comprensión del aspecto social, nuestra propuesta se enfoca en las Pymes del sector comercial que dependen de proveedores críticos. Por ello, luego de la implementación del modelo de gestión de riesgos de seguridad de TI, se emiten los resultados finales, esto a través de indicadores de éxito sobre gestión de riesgos. Esto conllevará a la identificación de controles y recomendaciones para reducir los riesgos que afectan a los activos de TI de las Pymes.

En cuanto al aspecto económico, los indicadores de éxito muestran estadísticas de la disminución de los riesgos que afectan a las Pymes de sector comercial que dependen de proveedores críticos y en consecuencia generan beneficios económicos. Asimismo; estudios realizados indican que las Pymes no tienen gran capacidad económica como otras grandes empresas para invertir gran

capital en tecnología. Por ello, a través del estudio de costos y presupuestos se demostró que el proyecto es viable para su implementación por lo que cualquier Pyme del sector comercial podrá aplicarlo sin ningún inconveniente generando un retorno de inversión dentro de un año luego de su implementación.

Finalmente, el modelo de referencia genera un impacto ambiental de manera indirecta a través de algunos controles o recomendaciones propuestos que hacen que se pueda usar los recursos computacionales de manera eficiente minimizando el impacto ambiental y maximizando la viabilidad económica de las organizaciones.

2.1.5 Student Outcome 5

La capacidad de funcionar efectivamente en un equipo cuyos miembros juntos proporcionan liderazgo, crean un entorno de colaboración e inclusivo, establecen objetivos, planifican tareas y cumplen objetivos

a) Participa en equipos multidisciplinarios con eficacia, eficiencia y objetividad, en el marco de un proyecto en soluciones de sistemas de información

Durante el desarrollo del proyecto, además de las reuniones con el profesor gerente, asesor de paper y profesor cliente, reuniones que siempre se registraron en actas; se pactó y ejecutó varias reuniones con diferentes profesionales en materia de tecnologías de la información, riesgos y seguridad de la información, tanto para la fase de levantamiento de información (análisis), como para la fase de validación de los componentes del modelo en una empresa de estudio. Durante este periodo nosotros, en calidad de jefes de proyectos, lideramos una simulación de implementación del modelo propuesto en una pyme del sector comercial denominada Kukyflor. Para lograr la aplicación de la metodología se trabajó junto con el especialista de TI y el analista de seguridad de la empresa quienes, en todo momento a través de entrevistas y encuestas, nos brindaron la información necesaria para identificar, evaluar y tratar los riesgos de los procesos y activos de TI asociados a los proveedores críticos de la empresa. Por otro lado, se mantuvo reuniones con el gerente general de la empresa Kukyflor para la presentación de avances de la aplicación del modelo; además de reuniones de conformidad sobre las recomendaciones y métricas obtenidas producto de la aplicación de este mismo. Reuniones la cuales, también fueron registradas en actas. Adicionalmente, se realizó una reunión con la analista contable de la empresa a fin de estimar el presupuesto con la que esta contaba para la implementación de nuestra propuesta, además de los gastos anuales producto de incidentes de seguridad.

El equipo de profesionales con los que se trabajó está conformado por:

- Comité de proyectos
- Portfolio Manager
- Asesor de Paper
- Asesor / Cliente
- Jefes de proyecto
- Gerente general de Kukyflor (Administrador)
- Gerente TI de Kukyflor
- Analista de seguridad de Kukyflor
- Analista contable de Kukyflor

b) Conoce al menos un sector empresarial o dominio de aplicación de soluciones de tecnologías de la información.

Durante la etapa inicial, ambos jefes de proyecto realizamos actividades de investigación y análisis para identificar la necesidad o problemática en las pymes en el marco de la gestión de riesgos y seguridad de TI, proponer alguna solución para satisfacer esta necesidad y dominar la teoría del tema a tratar. Para ello, nos valimos de fuentes confiables tales como páginas web de noticias internacionales, informes, libros, tesis y papers. Estos últimos debidamente indexados en revistas especializadas y provenientes de bases de datos científicos como: Scopus y Web of Science (WOS). Producto de la investigación en este sector empresarial, se pudo concluir que las pymes dedican la mayor parte de sus recursos y presupuesto a los procesos relacionados a la actividad principal de la organización, es decir la que genera mayor cantidad de ingresos, descuidando así la gestión de riesgos y más aún la seguridad de TI y, por consiguiente, la mayoría de estas empresas no cuentan con una adecuada cultura organizacional relacionada a estas materias.

Además, para el dominio del tema a tratar, se revisó las últimas versiones de las principales metodologías de gestión de riesgos, tales como OCTAVE, MAGERIT, EBIOS, CORA Y MEHARI y los principales estándares de gestión de seguridad de la información tales como la ISO 27001, BS 7799 y NIST 800-39. Esto con la finalidad de diseñar la propuesta que satisfaga la necesidad identificada y conocer toda la teoría relacionada. Todo lo anteriormente mencionado se demostró durante el desarrollo del Project Charter, el Marco teórico y el Estado del Arte.

c) Conocimientos de nuevos métodos de colaboración y comunicación

Durante el desarrollo del proyecto, las principales formas de trabajo colaborativo y coordinación entre los miembros del equipo fueron mediante reuniones presenciales, llamadas de teléfono móvil y envío de correos electrónicos. Sin embargo, entre los jefes de proyecto, pudimos utilizar herramientas modernas para el trabajo remoto, tales como Google Drive y Microsoft Sharepoint para la compartición y edición de documentación online y Hangouts para videollamadas.

2.1.6 Student Outcome 6

La capacidad de desarrollar y llevar a cabo la experimentación adecuada, analizar e interpretar datos, y usar el juicio de ingeniería para sacar conclusiones

a) Diseño de experimentos

Para la fase de validación y verificación de los componentes del modelo propuesto, se realizó un caso de estudio en una pyme del sector comercial denominada Kukyflor. Mediante reuniones con el gerente general de la empresa se desarrolló un plan para la simulación de la implementación de modelo, ya que debido al limitado tiempo académico una implementación real no sería posible. Esta simulación se ejecutaría paulatinamente durante reuniones semanales con los especialistas de tecnología y seguridad de la pyme en un tiempo aproximado de un mes. Para validar esta simulación, se diseñaron encuestas para la captura de información, métricas de medición como, la escala del nivel de madurez y el nivel de riesgo producto de la probabilidad y el impacto de las amenazas, hojas de trabajo para dar forma a estas métricas y obtener resultados, además de indicadores de éxito para medir el desempeño.

b) Desarrollo de experimentos

Para ejecutar la validación y verificación se aplicaron las fases del modelo en la empresa de estudio. Valiéndonos de las encuestas elaboradas, entrevistas y observaciones en sitio, se identificaron los riesgos de los procesos y activos de TI que dependen de proveedores críticos; luego, haciendo uso de las hojas de trabajo preparadas previamente se valoraron y estimaron el impacto de estos riesgos a través de datos cuantitativos, para así proponer controles o recomendaciones para mitigar o remediar estos hallazgos. Controles basados principalmente en la metodología MAGERIT y los estándares ISO 27001 e ISO 22301. El cálculo realizado mediante las hojas de trabajo obtuvo como resultado un nivel de madurez inicial en lo que respecta al gobierno de gestión de riesgos y seguridad de TI de la empresa y un nivel de riesgo inicial

(inherente) en los activos de TI, ambos asociados a proveedores críticos. Finalmente, se realizó la simulación del estado futuro de la empresa luego de haber implementado los controles y recomendaciones valiéndonos de las mismas métricas y hojas de cálculo usadas durante la etapa de evaluación del estado inicial.

c) Análisis e interpretación de datos/resultados

Luego de realizar la simulación de la implementación de recomendaciones mediante nuestra herramienta de trabajo (Libros de Excel), se demostró que la empresa aumentó su nivel de madurez en el gobierno de gestión de riesgos y seguridad de TI en un 86.49% y disminuyó el nivel de riesgo de los activos de TI en un 79.46% (ambos asociados a proveedores críticos). Se llegó a esta conclusión haciendo uso estas métricas y mediante el uso de indicadores de éxito, con los cuales se pudo comprobar cuantitativamente en cuanto porcentaje mejoró la empresa con respecto a su estado inicial, demostrando así la efectividad del modelo propuesto.

2.1.7 Student Outcome 7

Capacidad de adquirir y aplicar nuevos conocimientos según sea necesario, utilizando estrategias de aprendizaje apropiadas

a) Actualiza conceptos y conocimientos necesarios para su desarrollo profesional y en especial para su proyecto en soluciones de tecnologías de la información

Durante la etapa de análisis, se investigaron las principales metodologías y estándares de gestión de riesgos y seguridad de la información que, posteriormente mediante una herramienta de benchmarking se evaluaron y seleccionaron las más adecuadas para solucionar la necesidad de las pymes, la cual hace referencia a disminuir el nivel del riesgo de los procesos y activos de TI que dependen de proveedores críticos. La principal metodología y estándar seleccionados fueron MAGERIT y la ISO 27001 respectivamente, ya que son las que mejor se complementan y adaptan a esta necesidad. En ese sentido, el modelo propuesto se diseñó en base a esa metodología y estándar, para su posterior validación y verificación en un caso de estudio. Para este caso de estudio, se eligió una pyme del sector comercial que no contaba con procedimientos de gestión de riesgos y seguridad de TI correctamente establecidos; además de tener una pobre cultura organizacional en estos temas. Durante la ejecución de la validación de los componentes del modelo, se aplicó la metodología MAGERIT para identificar, evaluar y tratar los riesgos de los activos de TI la organización, siendo este último procedimiento complementado por la ISO 27001.

Durante el planeamiento de esta ejecución, nos dimos cuenta de que sería importante medir la efectividad del modelo, tanto a nivel de procesos de TI como a nivel de activos de TI, por ello se decidió utilizar como métricas el nivel de madurez y el nivel de riesgo. Una vez que se obtuvo los resultados de estas métricas, se realizó una simulación de implementación de los controles propuestos en la pyme con la finalidad de estimar el estado futuro de la empresa y poder medir el éxito de la aplicación del modelo mediante indicadores.

Para la búsqueda de la literatura que aportó a nuestra investigación, se siguió la metodología propuesta en el paper: “UNA REVISIÓN SISTEMÁTICA DE LA LITERATURA SOBRE LA ELICITACIÓN DE REQUISITOS DE SOFTWARE” de David Mauricio y otros autores. Se realizó una revisión sistemática de la literatura teniendo en cuenta las siguientes fases:

- Planificación de la revisión: en esta fase se elaboran las preguntas de investigación y se define el protocolo de revisión.
- Desarrollo de la revisión: en esta fase los estudios primarios se seleccionan de acuerdo con los criterios de selección y exclusión.

Planificación de la revisión:

Para lograr el propósito de la búsqueda, se proponen las siguientes preguntas de investigación:

- ¿Qué metodologías son las más utilizadas para gestionar los riesgos de seguridad de la información?
- ¿Qué estándares o normas son las más usadas para gestionar los riesgos de seguridad de la información?
- ¿Qué propuestas existen para la gestión de riesgos de TI?

Se realizó una búsqueda especializada de estudios científicos sobre investigaciones de otros países que aporten al tema de interés. Las bases de datos de esta búsqueda fueron principalmente Scopus, en su calidad de metabuscador, y la Web of Science. Se utilizaron principalmente las siguientes cadenas de búsqueda en las fuentes de información:

- Risk Management Model
- Information Security Risk Management
- IT Risk Management
- Information Security Risk Management Method

- Information Security Risk Management Standard

Estas se aplicaron al título del artículo, resumen y palabras clave para una mejor calidad en los documentos obtenidos. Después de eso, se aplicaron los criterios de selección y exclusión mostrados en la Tabla 6.

Criterios de Selección	Criterios de Exclusión
Estudios relacionados al estado del arte y la motivación.	El lenguaje de estudio es diferente de inglés.
Documentos relacionados a las diferentes propuestas de gestión de riesgos de seguridad de la información: frameworks, modelos, metodologías, estándares, etc.	Papers que no sean artículos de journals ni conference papers (Este se seleccionará en última instancia).
Papers relacionados a la gestión de riesgos de seguridad de TI.	Documentos fuera del rango de años del 2016 al 2019 (Se seleccionará estudios del 2015 en última instancia).
Estudios relacionados a la gestión de riesgos de seguridad de la información.	Estudios que no estén orientados a la gestión de riesgos.
Priorizar estudios con enfoques cuantitativos.	

Tabla 6: Criterios de selección y exclusión

Fuente: Elaboración propia

Desarrollo de la revisión:

Los primeros resultados obtenidos en el proceso de búsqueda pasaron primero por los criterios de exclusión establecidos en la Tabla 6. Luego, se revisaron los resúmenes, introducciones y conclusiones utilizando los criterios de selección dando como resultado una cantidad de papers. Finalmente, se revisó rápidamente los papers obtenidos hasta el momento y se eligieron los más resaltantes o que aportan más a la investigación basándonos nuevamente en los criterios de selección. A continuación, se muestra un proceso de revisión de referencia:

Figura 2: Proceso sistemático de revisión de la literatura

Fuente: Elaboración propia

b) Reconoce la necesidad del aprendizaje permanente para el desempeño profesional y el desarrollo de proyectos en soluciones de tecnologías de la información

Durante el desarrollo del proyecto nos dimos cuenta de que existe una gran oportunidad de desarrollo profesional en las áreas de gestión de proyectos y las de gestión de riesgos y seguridad de la información tanto en empresas reconocidas como en consultoras independientes, por ello luego de graduarnos estaríamos interesados en apuntar a alguna de estas áreas profesionales. En ese sentido, el plan sería ingresar a una empresa que nos permita desarrollarnos en alguna de estas áreas profesionales y en paralelo adquirir los conocimientos necesarios mediante cursos o especializaciones para luego obtener certificaciones que validen lo aprendido a partir de entidades de renombre internacional (ISACA, PMI, SGS, Bureau Veritas) para finalmente postular a alguna empresa de prestigio internacional donde podamos desarrollar nuestro máximo potencial y seguir

aprendiendo de manera permanente. Esto, considerando otros estudios complementarios, como los de inglés y áreas de conocimiento necesarias según el tipo de empresa donde nos desempeñemos.

CAPITULO 3   MARCO TEÓRICO

El capítulo tres describe el marco que fundamentará el proyecto en base al planteamiento del problema. Este capítulo comprende puntos importantes para una adecuada gestión del riesgo. En un inicio se define el concepto de comercio que abarca la definición y tipos, así como estadísticas de este sector. En segundo lugar, se describe el concepto de seguridad y las dimensiones que abarca. En tercer lugar, el riesgo y los tipos de riesgo que existen. En cuarto lugar, se menciona a los activos de información, que son parte fundamental de una organización. Seguidamente se define el concepto de amenaza y su respectiva clasificación. Luego, se definen los estándares ISOS que serán parte del desarrollo del proyecto. Finalmente, se describirá la Ley de protección de datos personales. Todos estos conceptos mencionados, ayudarán en gran medida en el desarrollo del proyecto.

3.1 COMERCIO

3.1.1 Definición

Es la actividad económica que consiste en la compra y venta al por mayor y menor de bienes nuevos o usados sin alterar o transformar su estado original, y la prestación de servicios accesorios a la venta de esos productos. Esta relación comercial pone en contacto al productor (oferta) con el consumidor (demanda).

Comprende también mantenimiento y reparación de vehículos, este servicio se brinda tanto a vehículos automotores, motocicletas y mototaxis. (INEI Peru, 2015)

Fuentes de Información

- Superintendencia Nacional de Aduanas y Administración Tributaria (SUNAT)
- Instituto Nacional de Estadística e Informática (INEI)
- Encuesta Económica Anual del Sector Comercio y Servicios

Es una de las 14 grandes actividades económicas del Perú, representa alrededor del 10,8% del PBI total y es una actividad importante como generadora de empleo. (Comercio D. E., 2018)

3.1.2 Clasificación del sector comercial

Según el Instituto Nacional de Estadísticas e Informática (INEI), el sector comercio abarca tres divisiones:

- Comercio al por mayor
- Comercio al por menor o retail
- Venta, mantenimiento y reparación de vehículos automotores y motocicletas, venta al por menor de combustible para automotores

La actividad comercio al por mayor y al por menor, consiste en la compra y venta de bienes nuevos o usados sin alterar o transformar su estado original. (Camara de Comercio, 2016)

a) Comercio al por mayor

El comercio al por mayor comprende aquellos establecimientos cuyas ventas se pueden destinar a comerciantes al por menor, a usuarios industriales, a otros mayoristas, y a quienes actúan en calidad de agente o corredor en la compra o venta de mercancías.

b) Comercio al por menor o retail

El comercio al por menor comprende aquellos establecimientos cuyas ventas se destinan al público en general para su consumo o uso personal. (MTPE, 2006)

Las actividades cuyas ventas tienen un mayor aporte en el comercio al por menor o llamado “**comercio retail**” son cuatro: las que provienen de tiendas por departamentos y supermercados, mejoramiento para el hogar electrodomésticos, boticas y farmacias y libros, periódicos y otros productos. (Camara de Comercio, 2016)

3.1.3 Datos estadísticos

Índice Sector Comercio en el Perú

El sector comercio en el segundo trimestre del 2018 mostró un crecimiento de 3,2%, como resultado favorable del subsector comercio al por mayor y menor (3,3%); y el subsector mantenimiento y reparación de vehículos automotores (1,5%).

Entre los departamentos que presentaron un buen desempeño en el sector comercio destacaron principalmente: Lima (4,3%) debido a las ventas al por mayor de otros enseres domésticos tales como electrodomésticos de entretenimiento (televisión y equipos de sonido), productos de aseo personal y hogar por aumento en la demanda, aunado al incremento de la publicidad y descuentos. Asimismo; subió la venta al por mayor de combustibles para los sectores construcción y minería; también el abastecimiento a estaciones de servicio y distribuidores de gas minorista. Del mismo modo, se incrementó la venta al por mayor y menor de alimentos, bebidas y tabaco, ante el lanzamiento de nuevos productos y alta temporada de consumo; La Libertad (2,2%) presentó mayores ventas al por mayor de computadoras, equipo periférico y programas informáticos por ejecución de proyectos tecnológicos; Piura (2,2%) aumentó las ventas al por mayor de vehículos automotores (livianos, pesados) y motocicletas, por mejoras crediticias y apertura de sedes comerciales; Lambayeque (2,0%) logró mayores ventas al por mayor de materias primas agropecuarias y de animales vivos; y Arequipa (1,6%) reflejó más ventas al por mayor de alimentos, bebidas y tabaco, producto de la mejora en la distribución y buen manejo de políticas de ventas.

También se incrementaron los departamentos de Cusco (2,7%), Loreto (2,3%), Áncash (2,5%), Cajamarca (2,1%), Ica (1,5%) y Huánuco (2,6%), entre otros.

En el primer semestre de 2018, el sector comercio acumuló un crecimiento de 3,0%, sustentado en la mayor actividad del subsector comercio al por mayor y menor (3,0%) y del subsector mantenimiento y reparación de vehículos automotores (2,6%). A nivel departamental, estuvo influenciado principalmente por Lima (3,7%), Piura (3,1%), Lambayeque (2,5%), La Libertad (2,5%) y Arequipa (2,4%). (INEI, Indicador de la Actividad Productiva departamental, 2018)

Figura 3: Índice sector comercio en el Perú

Fuente: INEI - Directorio Central de Empresas y Establecimientos.

3.1.4 Estructura empresarial

El análisis del Directorio Central de Empresas y Establecimientos permite conocer la estructura empresarial del país a través del número de empresas formales, su especialización productiva, tipo

de organización, tamaño y análisis de densidad empresarial por habitante y superficie, que constituye información indispensable para el conocimiento de la realidad empresarial.

Determinación del sector empresarial

La Micro y Pequeña Empresa se definió según el artículo 3 del Decreto Legislativo 1086 que aprueba la Ley de Promoción de la Competitividad, Formalización y Desarrollo de la Micro y Pequeña Empresa y del Acceso al Empleo Decente. Emitido el 28 de junio de 2008.

La Mediana Empresa según la Ley 30056. Ley que modifica diversas leyes para facilitar la inversión, impulsar el desarrollo productivo y el crecimiento empresarial. Emitido el 2 de julio 2013. (INEI, Directorio central de empresas y establecimientos, 2015)

Una nueva clasificación de las empresas peruanas que toma como referencia el monto de sus ventas anuales y ya no el número de sus trabajadores se contempla en la Ley 30056 denominada “Ley de Impulso al Desarrollo Productivo y al Crecimiento Empresarial”, promulgada por el Ejecutivo el 02 de Julio del 2013. Esta norma forma parte del paquete de medidas para facilitar la inversión, impulsar el desarrollo productivo y el crecimiento empresarial.

La Ley N° 30056 elimina el número máximo de trabajadores como parámetro para calificar como una MYPE. El incluir esta variable incidía negativamente en el mercado de trabajo. Por ello, su eliminación resulta acertada, pues fomentará el uso del factor trabajo frente al factor capital.

Así las cosas, con la modificación realizada por la Ley N° 30056, el nivel de ventas anuales queda como el único factor de categorización empresarial.

Segmento empresarial	Unidades Impositivas Tributarias (UIT)	N° de Trabajadores
Microempresa	Hasta 150 - S/.592,500	No hay límite
Pequeña empresa	Mayor de 150 (S/.592,500) hasta 1700 (S/.6'715,000)	No hay límite
Mediana empresa	Mayor de 1700 (S/.6'715,000) hasta 2300 (S/.9'085,000)	No hay límite
Gran empresa	Mayor de 2300 (S/.9'085,000)	No hay límite

Tabla 7: Estructura del sector comercial

Fuente: INEI

Se determina la “**Gran Empresa**” en base al límite superior de la Mediana Empresa

Nota: 1 UIT = S/4,150.00

3.2 SEGURIDAD

Seguridad es la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o y de los servicios que dichas redes y sistemas ofrecen. (MAGERIT, 2012)

El objetivo a proteger es la misión de la Organización, teniendo en cuenta las diferentes dimensiones de la seguridad que interesan de un activo; estas según Magerit son:

- **Disponibilidad:** Disposición de los servicios a ser usados cuando sea necesario. La carencia de disponibilidad supone una interrupción del servicio. La disponibilidad afecta directamente a la productividad de las organizaciones.
- **Integridad:** Mantenimiento de las características de completitud y corrección de los datos. Contra la integridad, la información puede aparecer manipulada, corrupta o incompleta. La integridad afecta directamente al correcto desempeño de las funciones de una Organización.
- **Confidencialidad:** Que la información llegue solamente a las personas autorizadas. Contra la confidencialidad o secreto pueden darse fugas y filtraciones de información, así como accesos no autorizados.

A estas dimensiones canónicas de la seguridad se pueden añadir otras derivadas que se acerquen a la percepción de los usuarios de los sistemas de información:

- **Autenticidad:** Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. Contra la autenticidad de la información podemos tener manipulación del origen o el contenido de los datos.

Contra la autenticidad de los usuarios de los servicios de acceso, podemos tener suplantación de identidad.

- **Trazabilidad:** Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento. La trazabilidad es esencial para analizar los incidentes, perseguir a los atacantes y aprender de la experiencia. La trazabilidad se materializa en la integridad de los registros de actividad.

3.3 RIESGO

3.3.1 Concepto

El riesgo es el "**efecto de la incertidumbre en los objetivos**". Un efecto es una desviación de lo esperado. Puede ser positivo, negativo o ambos y puede abordar, crear o generar oportunidades y amenazas. Los objetivos pueden tener diferentes aspectos y categorías (como los objetivos financieros, de salud y seguridad y medioambientales), y se pueden aplicar a diferentes niveles (por ejemplo, estratégico, de toda la organización, proyecto, producto y proceso). (ISO 31000, 2018)

Se dice también que el riesgo es la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a una organización.

El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente. Es importante saber qué características son de interés en cada activo, así como saber en qué medida estas características están en peligro, es decir, analizar el sistema. (MAGERIT, 2012)

3.3.2 Tipo de Riesgo

Las organizaciones están expuestas a diversos tipos de riesgo empresarial. Estos riesgos se pueden clasificar de varias maneras. Sin embargo, a pesar de la categorización de los riesgos, las organizaciones deben ser capaces de enfrentar todo tipo de riesgos, independientemente de la forma en que se clasifiquen, estos riesgos son:

- **Riesgo financiero:** En el campo de las finanzas, el riesgo no es una incertidumbre abstracta o posibilidad de falla o variabilidad del resultado. Es la probabilidad de que el rendimiento real de una inversión sea diferente de lo esperado.

- **Riesgo operacional:** Surge de la ejecución de las funciones comerciales, por lo que existe en todas las organizaciones en una serie de formas y existe independientemente del tamaño de la organización. Como tal, es un concepto muy amplio que incluye riesgos de salud y seguridad, riesgo físico, riesgo de fraude, riesgo de recursos humanos y riesgo de subcontratación.
- **Riesgo estratégico:** El impacto actual y prospectivo en las ganancias o el capital derivado de decisiones comerciales adversas, la implementación incorrecta de las decisiones o la falta de respuesta a los cambios de la industria.
- **Riesgo reputacional:** El impacto actual y prospectivo sobre las ganancias y el capital derivado de la publicidad negativa en relación con las prácticas comerciales de una institución.
- **Riesgo de cumplimiento legal y normativo:** El riesgo de cumplimiento generalmente se considera como parte del riesgo operacional, pero hoy en día está ganando fuerza por sí mismo.
- **Riesgo de los sistemas de información:** Se reconoce cada vez más como una categoría importante de riesgo empresarial por derecho propio en lugar de incluirse en otras categorías, como los riesgos estratégicos y operativos. (Silva, 2012)

3.3.3 Gestión del Riesgo

Los riesgos que afectan a las organizaciones pueden tener consecuencias en términos de rendimiento económico y reputación profesional, así como de los resultados ambientales, de seguridad y sociales. Por lo tanto, administrar el riesgo de manera efectiva ayuda a las organizaciones a desempeñarse bien en un ambiente lleno de incertidumbre.

Sneza realiza un estudio sobre las PYMES considerando los resultados del análisis de riesgos como clave para garantizar que las políticas y procedimientos son realmente necesarios, llegando a la conclusión de que las PYMES deben guiarse por el riesgo de pérdidas de activos derivado del análisis de riesgos. Se debe persuadir a los propietarios de las PYMES de emprender un escenario formal basado en el análisis de riesgos y la protección de los activos de información. Los recientes

hallazgos de la seguridad de la información han puesto de manifiesto una fuerte correlación entre el proceso formal de evaluación de riesgos y los gastos de la seguridad de la información.

Se debe tener en cuenta que el análisis de riesgos es un proceso costoso que no se puede repetir cada vez que se realiza una modificación. Por eso es importante desarrollar metodologías específicas que permitan mantener los resultados del análisis de riesgos.

El desarrollo de la gestión de riesgos se puede hacer de dos maneras. Primero, la organización desarrolla la administración de riesgos, mejorando gradualmente cada grado subsiguiente de realización en comparación con el anterior. Puede ser solo la mejora del proceso de gestión de riesgos o el componente de crecimiento de la madurez de la gestión del sistema, la organización, el equipo. Segundo, la administración de riesgos puede mejorarse en ciertas acciones del sistema durante la implementación.

Por lo tanto, se puede decir que la gestión general de riesgos es una actividad de coordinación, la tarea es dirigir y controlar las actividades de la organización y el proceso teniendo en cuenta los riesgos notables. Todo el proceso complejo se puede expresar en la secuencia de eventos que justifican y demuestran la necesidad de un análisis de riesgo.

El proceso típico de gestión de riesgos de seguridad de la información comúnmente incluye las fases de establecimiento del contexto, identificación de riesgos y análisis de riesgos. Cada una de estas fases suele estar formada por una serie de actividades y subprocesos.

Figura 4: Componentes del análisis de gestión de riesgos

Fuente: Larionovs, A., Teilans, A., Grabusts, P.

3.3.4 Metodologías de gestión de riesgo

Existen diferentes metodologías para gestionar los riesgos de seguridad de Tecnologías de información, cada una con diferentes enfoques. En el mercado hay una amplia variedad de metodologías disponibles para administrar, evaluar y tratar los riesgos, evidentemente es de mucha ayuda para las organizaciones. Al tener numerosas opciones, las organizaciones pueden adoptar uno o una combinación de los métodos que mejor se adapten a sus necesidades y se adapten a la estructura y cultura respectivas de la empresa. Los diferentes métodos tendrán diferentes usos, enfoques, propósitos y pueden enfatizar un conjunto diferente de aspectos. Existen muchos métodos de análisis de riesgos disponibles en la actualidad, y la tarea principal de una organización es determinar cuál usar. (Agrawal, Vivek, 2017)

Las principales metodologías para la gestión de riesgos son:

- Octave (Evaluación de amenazas, activos y vulnerabilidad operacionalmente crítica)
- Magerit (Methodology for Information Systems Risk Analysis and Management)
- Ebios
- Coras
- Mehari

La descripción detallada de cada una se mencionará en el capítulo 4, donde se realiza una comparativa de estas y se elegirá la más adecuada para la elaboración del modelo de gestión de riesgos de seguridad de TI.

3.4 ACTIVO DE INFORMACIÓN

Son los componentes o funcionalidades de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Estos incluyen: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos. (MAGERIT, 2012)

3.4.1 Clasificación de los activos de Información

La metodología Magerit clasifica los activos de información de la siguiente manera:

- Equipos informáticos (Hardware)
- Aplicaciones (Software)
- Servicios
- Instalaciones
- Redes de comunicación

Se debe tener en cuenta que para el desarrollo del proyecto solo abarcará activos relacionados a Tecnologías de Información los cuales son: servicios, aplicaciones, datos y hardware; y a su vez estén asociados a procesos críticos que dependen de proveedores críticos.

3.4.2 Valoración del activo

La valoración se puede ver desde la perspectiva de la necesidad de proteger, pues cuanto más valioso es un activo (activo crítico), mayor nivel de protección se requiere en la dimensión (o dimensiones) de seguridad que sean pertinentes. Cada activo en cada dimensión recibe un valor en la escala V que indica Magerit.

Los activos de información reciben una valoración en cada una de las dimensiones de la seguridad.

3.5 AMENAZA

Las amenazas son “**cosas que ocurren**”. Y, de todo lo que puede ocurrir, interesa lo que puede pasarles a los activos de información y causar un daño.

Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización. (MAGERIT, 2012)

3.5.1 Identificación de las amenazas

Según Magerit las amenazas se clasifican en:

- **De origen natural**

Hay accidentes naturales (terremotos, inundaciones, etc.). Ante esos avatares el sistema de información es víctima pasiva, pero de todas formas tendremos en cuenta lo que puede suceder.

- **Del entorno (de origen industrial)**

Hay desastres industriales (contaminación, fallos eléctricos, ...) ante los cuales el sistema de información es víctima pasiva; pero no por ser pasivos hay que permanecer indefensos.

- **Defectos de las aplicaciones**

Hay problemas que nacen directamente en el equipamiento propio por defectos en su diseño o en su implementación, con consecuencias potencialmente negativas sobre el sistema. Frecuentemente se denominan vulnerabilidades técnicas o, simplemente, ‘vulnerabilidades’.

- **Causadas por las personas de forma accidental**

Las personas con acceso al sistema de información pueden ser causa de problemas no intencionados, típicamente por error o por omisión.

- **Causadas por las personas de forma deliberada**

Las personas con acceso al sistema de información pueden ser causa de problemas

intencionados: ataques deliberados; bien con ánimo de beneficiarse indebidamente, bien con ánimo de causar daños y perjuicios a los legítimos propietarios.

No todas las amenazas afectan a todos los activos, sino que hay una cierta relación entre el tipo de activo y lo que le podría ocurrir.

3.5.2 Valoración de las amenazas

Cuando un activo es víctima de una amenaza, no se ve afectado en todas sus dimensiones, ni en la misma cuantía. Para la valoración, Magerit toma en cuenta dos aspectos:

- **Probabilidad de ocurrencia (Frecuencia):** Cuán probable o improbable es que se materialice la amenaza. Para medir la probabilidad Magerit hace uso de la frecuencia esperada de ocurrencia (ARO – Annual rate Of Occurrence). La frecuencia de una amenaza es un valor real superior a cero.

ID	Valor	Descripción
MA	100	A diario
A	10	Mensualmente
M	1	Una vez al año
B	0.1	Cada varios años
MB	0.01	Siglos

Tabla 8: Probabilidad de ocurrencia

Fuente: Magerit

- **Degradación:** Cuando un activo es víctima de una amenaza, una parte de su valor se pierde. Se habla de un “**porcentaje de degradación del activo**”, de forma que se puede perder entre un 0% y un 100%.

ID	Nombre	Degradación	Descripción
MA	Muy alto	Casi seguro	Fácil
A	Alto	Muy alto	Medio
M	Medio	Posible	Difícil
B	Bajo	Poco probable	Muy difícil
MB	Muy bajo	Muy raro	Extremadamente difícil

Tabla 9: Degradación del valor

Fuente: Magerit

3.6 ESTANDAR ISO

3.6.1 ISO

ISO (Organización Internacional de Normalización) es una federación mundial de organismos nacionales de normalización (organismos miembros de ISO). El trabajo de preparación de las Normas Internacionales normalmente se realiza a través de los comités técnicos de ISO. Cada organismo miembro interesado en una materia para la cual se haya establecido un comité técnico tiene el derecho de estar representado en dicho comité. Las organizaciones internacionales públicas y privadas en coordinación con ISO, también participan en el trabajo. ISO colabora estrechamente con la Comisión Electrotécnica Internacional (IEC) en todas las materias de normalización electrotécnica.

Las normas internacionales se redactan de acuerdo con las reglas establecidas en la Parte 2 de las directivas ISO/IEC.

La tarea principal de los comités técnicos es preparar Normas Internacionales. Los Proyectos de Normas Internacionales adoptados por los comités técnicos se envían a los organismos miembros para votación. La publicación como Norma Internacional requiere la aprobación por al menos del 75% de los organismos miembros que emiten voto.

Se llama la atención sobre la posibilidad de que algunos de los elementos de este documento puedan estar sujetos a derechos de patente. ISO no asume la responsabilidad por la identificación de cualquiera o todos los derechos de patente. (ISO 19011, 2012)

3.6.2 ISO 27001 – 2013

3.6.2.1 Definición

Especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información dentro del contexto de la organización. También incluye requisitos para la evaluación y el tratamiento de riesgos de seguridad de la información adaptados a las necesidades de la organización.

Los requisitos establecidos en ISO/IEC 27001:2013 son genéricos y están destinados a ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza. (ISO 27001 O. , 2013)

El sistema de gestión de la seguridad de la información preserva la confidencialidad, la integridad y la disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos y da confianza a las partes interesadas de que los riesgos se gestionan adecuadamente.

Es importante que el sistema de gestión de la seguridad de la información sea parte e integre con los procesos de la organización y la estructura de gestión general, y que la seguridad de la información se considere en el diseño de procesos, sistemas de información y controles. Se espera que la implementación del sistema de gestión de la seguridad de la información se adapte a las necesidades de la organización.

Este Estándar Internacional puede ser utilizado por partes internas y externas para evaluar la capacidad de la organización para cumplir con los requisitos de seguridad de la información propios de la organización.

El orden en que los requisitos se presentan en esta norma internacional no refleja su importancia ni implica el orden en el que se implementarán. Los elementos de la lista se enumeran solo con fines de referencia. (ISO 27001 O. , 2013)

Según la ISO 27001, la seguridad de la información hace referencia a:

- **Confidencialidad:** Es la propiedad de prevenir que se divulgue la información a personas o sistemas no autorizados. (ISO 27001, 2015)
- **Integridad:** Es la propiedad que busca proteger que se modifiquen los datos libres de forma no autorizada. (ISO 27001, 2015)
- **Disponibilidad:** Es una característica, cualidad o condición de la información que se encuentra a disposición de quien tiene que acceder a esta, bien sean personas, procesos o aplicaciones. (ISO 27001, 2015)

3.6.3 ISO 22301 – 2012

3.6.3.1 Definición

Esta Norma Internacional para la gestión de la continuidad del negocio especifica los requisitos para planificar, establecer, implementar, operar, supervisar, revisar, mantener y mejorar continuamente un sistema de gestión documentado para protegerse, reducir la probabilidad de que ocurra, prepararse, responder y recuperarse de problemas incidentes cuando surgen.

Los requisitos especificados en esta norma internacional son genéricos y están destinados a ser aplicables a todas las organizaciones, o partes de ellas, independientemente del tipo, tamaño y naturaleza de la organización. El grado de aplicación de estos requisitos depende del entorno operativo y la complejidad de la organización.

Esta Norma Internacional es aplicable a todos los tipos y tamaños de organizaciones que deseen:

- a) establecer, implementar, mantener y mejorar un BCMS,
- b) garantizar la conformidad con la política de continuidad del negocio establecida,
- c) demostrar conformidad con otros,
- d) solicitar la certificación / registro de su BCMS por un organismo de certificación de un tercero acreditado, o
- e) hacer una autodeterminación y auto declaración de conformidad con esta Norma Internacional.

Este Estándar Internacional se puede usar para evaluar la capacidad de una organización para cumplir con sus propias necesidades y obligaciones de continuidad. (ISO 22301, 2012)

3.6.3.2 Business Continuity Management System (BCMS)

Esta Norma Internacional especifica los requisitos para la configuración y administración de un Sistema de Gestión de Continuidad del Negocio (BCMS) efectivo.

Un BCMS enfatiza la importancia de:

- comprender las necesidades de la organización y la necesidad de establecer políticas y objetivos de gestión de la continuidad del negocio
- implementar y operar controles y medidas para gestionar la capacidad general de una organización para gestionar incidentes disruptivos
- monitorear y revisar el desempeño y la efectividad del BCMS, y
- mejora continua basada en la medición objetiva.

Un BCMS, como cualquier otro sistema de gestión, tiene los siguientes componentes clave:

- a) una política;
- b) personas con responsabilidades definidas;
- c) procesos de gestión relacionados con
  - 1) política,
  - 2) planificación,
  - 3) implementación y operación,
  - 4) evaluación del desempeño,
  - 5) revisión de la gestión, y
  - 6) mejora;
- d) documentación que proporciona pruebas auditables; y
- e) cualquier proceso de gestión de la continuidad del negocio relevante para la organización.

La continuidad del negocio contribuye a una sociedad más resiliente. La comunidad más amplia y el impacto del entorno de la organización en la organización y, por lo tanto, en otras organizaciones, pueden necesitar participar en el proceso de recuperación. (ISO 22301, 2012)

3.6.3.3 El modelo Plan-Do-Check-Act (PDCA)

Esta Norma Internacional aplica el modelo "Planificar, Hacer, Verificar, Actuar" (PDCA, por sus siglas en inglés) para planificar, establecer, implementar, operar, monitorear, revisar, mantener y mejorar continuamente la efectividad del BCMS de una organización.

Esto garantiza un grado de consistencia con otros estándares de sistemas de gestión, tales como ISO 9001 Sistemas de gestión de calidad, ISO 14001 Sistemas de gestión ambiental, ISO/IEC 27001 Sistemas de gestión de seguridad de la información, ISO/IEC 20000-1 Tecnología de la información - Gestión de servicios, e ISO 28000, Especificación para sistemas de gestión de seguridad para la cadena de suministro, apoyando así la implementación y el funcionamiento coherentes e integrados con los sistemas de gestión relacionados.

La Figura 5 ilustra cómo un BCMS toma como insumos a las partes interesadas, requisitos para la gestión de la continuidad y, a través de las acciones y procesos necesarios, produce resultados de continuidad (es decir, continuidad del negocio administrado) que cumplen esos requisitos. (ISO 22301, 2012)

Figura 5: Modelo de PDCA aplicado a procesos de BCMS

Fuente: ISO 22301 – 2012

Plan (Establecer)	Establecer una política de continuidad del negocio, objetivos, metas, controles, procesos y procedimientos relevantes para mejorar la continuidad del negocio a fin de entregar resultados que se alineen con las políticas y objetivos generales de la organización.
Do (Implementar y operar)	Implementar y operar la política de continuidad del negocio, controles, procesos y procedimientos.
Check (Monitorear y revisar)	Monitoree y revise el desempeño en relación con la política y objetivos de continuidad del negocio, informe los resultados a la gerencia para su revisión, y determine y autorice acciones para remediar y mejorar.
Act (Mantener y mejorar)	Mantener y mejorar el BCMS mediante la adopción de medidas correctivas, sobre la base de los resultados de la revisión de la administración y la nueva evaluación del alcance del BCMS y la política y objetivos de continuidad del negocio.

Tabla 10: Modelo de PDCA aplicado a procesos de BCMS

3.6.3.4 Términos y definiciones

- **Actividad**

Proceso o conjunto de procesos realizados por una organización (o en su nombre) que produce o admite uno o más productos y servicios. (ISO 22301, 2012)

- **Auditoría**

Proceso sistemático, independiente y documentado para obtener evidencia de auditoría y evaluarla objetivamente para determinar el grado en que se cumplen los criterios de auditoría

- **Continuidad del negocio**

Capacidad de la organización para continuar la entrega de productos o servicios a niveles predefinidos aceptables después de un incidente disruptivo.

- **Gestión de continuidad del negocio**

proceso holístico de gestión que identifica amenazas potenciales para una organización y los impactos en las operaciones comerciales que esas amenazas, si se realizan, pueden causar, y que proporciona un marco para construir resiliencia organizacional con la capacidad de una respuesta efectiva que salvaguarde los intereses de sus partes interesadas clave, reputación, marca y actividades creadoras de valor.

- **Sistema de gestión de la continuidad del negocio (BCMS)**

Parte del sistema de gestión general que establece, implementa, opera, monitorea, revisa, mantiene y mejora la continuidad del negocio.

- **Plan de negocios continuo**

Procedimientos documentados que guían a las organizaciones a responder, recuperar, reanudar y restaurar a un nivel predefinido de operación después de la interrupción.

- **Programa de continuidad del negocio**

Un proceso continuo de gestión y gobierno respaldado por la alta dirección y con los recursos adecuados para implementar y mantener la gestión de la continuidad del negocio.

- **Mejora continua**

Actividad recurrente para mejorar el rendimiento.

- **Corrección**

Acción para eliminar una no conformidad detectada

- **Acción correctiva**

Acción para eliminar la causa de una inconformidad y prevenir la recurrencia. (ISO 22301, 2012)

3.6.4 ISO 19011 – 2011

3.6.4.1 Definición

Esta Norma Internacional proporciona orientación sobre la auditoría de los sistemas de gestión, incluyendo los principios de la auditoría, la gestión de un programa de auditoría y la realización de auditorías de sistemas de gestión, así como orientación sobre la evaluación de la competencia de los individuos que participan en el proceso de auditoría, incluyendo a la persona que gestiona el programa de auditoría, los auditores y los equipos auditores.

Las organizaciones pueden operar más de un sistema de gestión formal. Para simplificar la legibilidad de esta Norma Internacional, se prefiere la forma singular de “sistema de gestión”, el usuario puede adaptar la implementación de la orientación a su propia situación particular. Esto también aplica al uso de “persona” y “personas”, “auditor” y “auditores”.

Esta Norma Internacional se aplica a un amplio rango de usuarios potenciales, incluyendo auditores, organizaciones que implementan sistemas de gestión y organizaciones que necesitan realizar auditorías de sistemas de gestión por razones contractuales o reglamentarias.

Esta Norma Internacional introduce el concepto de riesgo en la auditoría de sistemas de gestión. El enfoque adoptado se refiere tanto a los riesgos del proceso de auditoría para alcanzar sus objetivos como al riesgo potencial de la auditoría para interferir con las actividades y procesos del auditado. No proporciona orientación específica para los procesos de gestión del riesgo de la organización, pero reconoce que las organizaciones pueden centrar el esfuerzo de auditoría en cuestiones de importancia para el sistema de gestión.

Esta Norma Internacional adopta el enfoque de que cuando se auditan juntos dos o más sistemas de gestión de distintas disciplinas, esto se denomina “auditoría combinada”. Cuando estos sistemas están integrados en un único sistema de gestión, los principios y procesos de auditoría son los mismos que para una auditoría combinada. (ISO 19011, 2012)

3.6.4.2 Alcance

Esta Norma Internacional no establece requisitos, sino que proporciona orientación sobre la gestión de un programa de auditoría, sobre la planificación y realización de una auditoría del sistema de gestión, así como sobre la competencia y evaluación de un auditor y un equipo auditor.

Auditoría interna	Auditoría externa	
	Auditoría al proveedor	Auditoría de tercera parte
A veces llamada auditoría de primera parte	A veces llamada auditoría de segunda parte	Para propósitos legales, reglamentarios y similares

Tabla 11: Alcance del ISO 19011 - 2011

Fuente: ISO 19011 – 2011

3.6.4.3 Términos y condiciones

- **auditoría**

Proceso sistemático, independiente y documentado para obtener evidencias de la auditoría y evaluarlas de manera objetiva con el fin de determinar el grado en que se cumplen los criterios de auditoría. (ISO 19011, 2012)

Las auditorías internas, denominadas en algunos casos auditorías de primera parte, se realizan por la propia organización, o en su nombre, para la revisión por la dirección y para otros propósitos internos (por ejemplo, para confirmar la eficacia del sistema de gestión o para obtener información para la mejora del sistema de gestión). Las auditorías internas pueden formar la base para una auto declaración de conformidad de una organización. En muchos casos, particularmente en organizaciones pequeñas, la independencia puede demostrarse al estar libre el auditor de responsabilidades en la actividad que se audita o al estar libre de sesgo y conflicto de intereses.

Las auditorías externas incluyen auditorías de segunda y tercera parte. Las auditorías de segunda parte se llevan a cabo por partes que tienen un interés en la organización, tal como los clientes, o por otras personas en su nombre. Las auditorías de tercera parte se llevan a cabo por organizaciones auditoras independientes, tales como las autoridades reglamentarias o aquellas que proporcionan la certificación.

- **criterios de auditoría**

Conjunto de políticas, procedimientos o requisitos usados como referencia frente a la cual se compara la evidencia de la auditoría.

- **hallazgos de la auditoría**

Resultados de la evaluación de la evidencia de la auditoría recopilada frente a los criterios de auditoría.

- **conclusiones de la auditoría**

Resultado de una auditoría, tras considerar los objetivos de la auditoría y todos los hallazgos de la auditoría

- **cliente de la auditoría**

Organización o persona que solicita una auditoría

- **auditado**

Organización que es auditada

- **auditor**

Persona que lleva a cabo una auditoría

- **equipo auditor**

Uno o más auditores que llevan a cabo una auditoría, con el apoyo, si es necesario, de expertos técnicos.

- **programa de auditoría**

Detalles acordados para un conjunto de una o más auditorías planificadas para un periodo de tiempo determinado y dirigido hacia un propósito específico

- **alcance de la auditoría**

Extensión y límites de una auditoría

- **plan de auditoría**

Descripción de las actividades y de los detalles acordados de una auditoría

- **conformidad**

Cumplimiento de un requisito

- **no conformidad**

Incumplimiento de un requisito

- **sistema de gestión**

Sistema para establecer la política y los objetivos y para lograr dichos objetivos.

Un sistema de gestión de una organización puede incluir diferentes sistemas de gestión, tales como un sistema de gestión de la calidad, un sistema de gestión financiera o un sistema de gestión ambiental. (ISO 19011, 2012)

3.7 LEY DE PROTECCIÓN DE DATOS PERSONALES

3.7.1 Definición

Es una normativa peruana definida como Ley N° 29733 publicada el 3 de Julio del 2011 en el diario oficial “**El Peruano**” cuyo objetivo es garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen. (LEY 29733, 2011)

La norma de manera general establece que son de aplicación a los datos personales contenidos (o destinados a ser contenidos) en bancos de datos personales cuyo tratamiento se realice en el Perú, entendiéndose por "datos personales" a toda información sobre una persona natural que la identifica o la hace identificable y a "bancos de datos personales" como el conjunto organizado de datos personales, independientemente del soporte y cualquiera sea la forma o modalidad de su creación, formación, almacenamiento, organización y acceso. (Gestion, 2015).

La ley N° 29733, tiene como objetivo garantizar el derecho fundamental a la protección de los datos personales, es decir, toda información sobre la persona que lo identifica, a través de un adecuado tratamiento, en un marco de respeto de los derechos fundamentales que corresponden.

3.7.2 Ámbito de aplicación

La presente ley es de aplicación a los datos personales contenidos o ser contenidos en bancos de datos personales, de administración pública o privada, cuyo tratamiento se realiza en el territorio nacional. Son objetivo de especial protección los datos sensibles y no aplican a los siguientes datos personales:

- Bancos de datos personales creados por personas naturales para fines exclusivamente relacionados con su vida privada o familiar.
- Bancos de datos de administración pública solo en tanto su tratamiento resulte necesario para el estricto cumplimiento de las competencias asignadas por ley a las respectivas entidades públicas, para la defensa nacional, seguridad pública, y para el desarrollo de actividades en materia penal para la investigación y represión del delito.

3.7.3 Términos y definiciones

1. Banco de datos personales. Conjunto organizado de datos personales, automatizado o no, independientemente del soporte, sea este físico, magnético, digital, óptico u otros que se creen, cualquiera fuere la forma o modalidad de su creación, formación, almacenamiento, organización y acceso.

2. Banco de datos personales de administración privada. Banco de datos personales cuya titularidad corresponde a una persona natural o a una persona jurídica de derecho privado, en cuanto el banco no se encuentre estrictamente vinculado al ejercicio de potestades de derecho público.

3. Banco de datos personales de administración pública. Banco de datos personales cuya titularidad corresponde a una entidad pública.

4. Datos personales. Toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados.

5. Datos sensibles. Datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos, opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual.

6. Encargado del banco de datos personales. Toda persona natural, persona jurídica de derecho privado o entidad pública que sola o actuando conjuntamente con otra realiza el tratamiento de los datos personales por encargo del titular del banco de datos personales. (LEY 29733, 2011)

7. Entidad pública. Entidad comprendida en el artículo I del Título Preliminar de la Ley 27444, Ley del Procedimiento Administrativo General, o la que haga sus veces. (LEY 29733, 2011)

8. Flujo transfronterizo de datos personales. Transferencia internacional de datos personales a un destinatario situado en un país distinto al país de origen de los datos personales, sin importar el soporte en que estos se encuentren, los medios por los cuales se efectuó la transferencia ni el tratamiento que reciban.

9. Fuentes accesibles para el público. Bancos de datos personales de administración pública o privada, que pueden ser consultados por cualquier persona, previo abono de la contraprestación correspondiente, de ser el caso. Las fuentes accesibles para el público son determinadas en el reglamento.

10. Nivel suficiente de protección para los datos personales. Nivel de protección que abarca por lo menos la consignación y el respeto de los principios rectores de esta Ley, así como medidas técnicas de seguridad y confidencialidad, apropiadas según la categoría de datos de que se trate.

11. Persona jurídica de derecho privado. Para efectos de esta Ley, la persona jurídica no comprendida en los alcances del artículo I del Título Preliminar de la Ley 27444, Ley del Procedimiento Administrativo General.

12. Procedimiento de anonimización. Tratamiento de datos personales que impide la identificación o que no hace identificable al titular de estos. El procedimiento es irreversible.

13. Procedimiento de disociación. Tratamiento de datos personales que impide la identificación o que no hace identificable al titular de estos. El procedimiento es reversible.

14. Titular de datos personales. Persona natural a quien corresponde los datos personales.

15. Titular del banco de datos personales. Persona natural, persona jurídica de derecho privado o entidad pública que determina la finalidad y contenido del banco de datos personales, el tratamiento de estos y las medidas de seguridad.

16. Transferencia de datos personales. Toda transmisión, suministro o manifestación de datos personales, de carácter nacional o internacional, a una persona jurídica de derecho privado, a una entidad pública o a una persona natural distinta del titular de datos personales.

17. Tratamiento de datos personales. Cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales. (LEY 29733, 2011)

3.7.4 Principios de la Ley 29733

Esta ley tiene definido diferentes principios, los cuales se detallarán a continuación:

- **Principio de legalidad:** El tratamiento de los datos personales se hace conforme a lo establecido en la ley. Es decir, se prohíbe la recopilación de los datos personales por medios fraudulentos.
- **Principio de consentimiento:** Todo tratamiento de los datos personales debe ser con previo consentimiento de su titular.
- **Principio de finalidad:** Los datos personales deben ser recopilados para una finalidad determinada, explícita y lícita. El tratamiento de los datos personales no debe extenderse a otra finalidad que no haya sido la establecida de manera inequívoca como tal al momento de su recopilación, excluyendo los casos de actividades de valor histórico, estadístico o científico cuando se utilice un procedimiento de disociación o anonimización.

- **Principio de proporcionalidad:** Todo tratamiento de datos personales debe ser adecuado, relevante y no excesivo a la finalidad para la que estos hubiesen sido recopilados.
- **Principio de calidad:** Los datos personales que vayan a ser tratados deben ser veraces, exactos y en la medida de lo posible, actualizada, necesaria, pertinente y adecuada respecto de la finalidad para la que fueron recopilados. Deben conservarse de forma tal que se garantice su seguridad y solo por el tiempo necesario para cumplir con la finalidad del tratamiento.
- **Principio de seguridad:** El titular del banco de datos personales y el encargado de su tratamiento deben adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la categoría de datos personales de que se trate.
- **Principio de disposición de recurso:** Todo titular de datos personales debe contar con las vías administrativas o jurisdiccionales necesarias para reclamar y hacer valer sus derechos, cuando estos sean vulnerados por el tratamiento de sus datos personales.
- **Principio de nivel de protección adecuado:** Para el flujo transfronterizo de datos personales, se debe garantizar un nivel suficiente de protección para los datos personales que se vayan a tratar o, por lo menos equiparable a lo previsto por esta Ley o por los estándares internacionales de esta materia.

3.7.5 Artículo 13. Alcance sobre el tratamiento de datos personales

- **13.1** El tratamiento de datos personales debe realizarse con pleno respeto de los derechos fundamentales de sus titulares y de los derechos que esta Ley les confiere. Igual regla rige para su utilización por terceros.
- **13.2** Las limitaciones al ejercicio del derecho fundamental a la protección de datos personales solo pueden ser establecidas por ley, respetando su contenido esencial y estar justificadas en razón del respeto de otros derechos fundamentales o bienes constitucionalmente protegidos.
- **13.3** Mediante reglamento se dictan medidas especiales para el tratamiento de los datos personales de los niños y de los adolescentes, así como para la protección y garantía de sus derechos. Para el ejercicio de los derechos que esta Ley reconoce, los niños y los adolescentes actúan a través de sus representantes legales, pudiendo el reglamento

determinar las excepciones aplicables, de ser el caso, teniendo en cuenta para ello el interés superior del niño y del adolescente.

- **13.4** Las comunicaciones, telecomunicaciones, sistemas informáticos o sus instrumentos, cuando sean de carácter privado o uso privado, solo pueden ser abiertos, incautados, interceptados o intervenidos por mandamiento motivado del juez o con autorización de su titular, con las garantías previstas en la ley. Se guarda secreto de los asuntos ajenos al hecho que motiva su examen. Los datos personales obtenidos con violación de este precepto carecen de efecto legal.
- **13.5** Los datos personales solo pueden ser objeto de tratamiento con consentimiento de su titular, salvo ley autoritativa al respecto. El consentimiento debe ser previo, informado, expreso e inequívoco.
- **13.6** En el caso de datos sensibles, el consentimiento para efectos de su tratamiento, además, debe efectuarse por escrito. Aun cuando no mediara el consentimiento del titular, el tratamiento de datos sensibles puede efectuarse cuando la ley lo autorice, siempre que ello atienda a motivos importantes de interés público.
- **13.7** El titular de datos personales puede revocar su consentimiento en cualquier momento, observando al efecto los mismos requisitos que con ocasión de su otorgamiento.
- **13.8** El tratamiento de datos personales relativos a la comisión de infracciones penales o administrativas solo puede ser efectuado por las entidades públicas competentes, salvo convenio de encargo de gestión conforme a la Ley 27444, Ley del Procedimiento Administrativo General, o la que haga sus veces. Cuando se haya producido la cancelación de los antecedentes penales, judiciales, policiales y administrativos, estos datos no pueden ser suministrados salvo que sean requeridos por el Poder Judicial o el Ministerio Público, conforme a ley.
- **13.9** La comercialización de datos personales contenidos o destinados a ser contenidos en bancos de datos personales se sujeta a los principios previstos en la presente Ley.

CAPITULO 4   DESARROLLO DEL PROYECTO

En este capítulo se desarrollan los dos primeros objetivos específicos del proyecto. Estos representan las etapas trabajadas para el análisis y diseño del Modelo de gestión de riesgos de seguridad de TI. Primero, se realiza un benchmarking de diferentes herramientas (metodologías y estándares) de gestión de riesgos de seguridad de la información que permitirán diseñar el modelo. Luego, se plantea el diseño del modelo basado en la metodología MAGERIT y el estándar ISO/IEC 27001:2013; además de otras herramientas de soporte como son: ISO 22301:2012, ISO 19011:2011, la Ley de protección de datos personales y las Circulares de la Superintendencia de Banca y Seguros (SBS). Esto con la finalidad de resolver la necesidad identificada.

4.1 ANÁLISIS DE LA PROPUESTA

4.1.1 Benchmarking

El objetivo principal es proporcionar información práctica para las organizaciones que desean iniciar o mejorar su proceso de gestión de riesgos. Esto se logrará estudiando y comparando en detalle las diferentes metodologías existentes para la gestión de riesgos de seguridad de información y los diferentes estándares de gestión de seguridad de la información.

Se realizó dos estudios comparativos, una correspondiente a **“metodologías de gestión de riesgos”** y otra correspondiente a **“estándares de seguridad de información”**.

La comparativa identifica lo que cada metodología tiene para ofrecer, los temas que aborda y su proceso para gestionar el riesgo. Al tener claro los puntos fuertes (sus principales ventajas con respecto a las otras metodologías) y flaquezas de cada metodología, será más sencillo seleccionar la más adecuada para resolver la necesidad identificada.

Todos los estándares que se mencionarán tienen el objetivo común de garantizar un adecuado nivel de seguridad en los activos de información. Sin embargo, no existen puntos de referencia o guías que ayuden a las organizaciones a determinar qué estándar es el mejor para ser aplicado dentro de la organización.

Además, para efectos de este proyecto, se tomó en cuenta principalmente las etapas de tratamiento, seguimiento y monitoreo de los riesgos de seguridad de la información para complementar la metodología de gestión de riesgos seleccionada en el análisis previo.

4.1.2 Metodologías para la gestión de riesgos

4.1.2.1 Información general

Hay una lista extensa de metodologías para gestionar los riesgos de los sistemas de información y que pueden causar confusión al elegir el apropiado. Para evitar esta dificultad, es útil elegir el método de gestión de riesgo que se adecue a la organización. Este apartado explora diferentes tipos de metodologías de gestión de riesgo como: OCTAVE, MAGERIT, EBIOS, CORAS y MEHARI. Después de comparar estas

metodologías, se eligió la más adecuada para su posterior implementación en una empresa (PYME) correspondiente al sector comercial.

4.1.2.2 Metodologías

A. OCTAVE (Evaluación de amenazas, activos y vulnerabilidad operacionalmente crítica)

Es una metodología utilizada para identificar y evaluar los riesgos de seguridad de la información. OCTAVE está destinado a ayudar a la compañía en términos de:

- Desarrollar un criterio de evaluación de riesgo cualitativo que describa la tolerancia de riesgo operacional de la compañía.
- Identificar los activos que son importantes para la misión de la empresa.
- Identificar vulnerabilidades y amenazas a esos activos.
- Determinar y evaluar las posibles consecuencias para la empresa si se produce la amenaza.

Hay 3 variantes de OCTAVE que pueden ser utilizadas. Las variantes son el método OCTAVE, OCTAVE-S y OCTAVE Allegro. Estos tres métodos no son un método complementario o que se sustituyan entre sí. El uso de estos tres métodos está destinado a satisfacer las necesidades específicas de los usuarios de OCTAVE que desean realizar una evaluación de riesgos.

Los objetivos que debe alcanzar OCTAVE Allegro es una evaluación integral del entorno de riesgo operacional de una organización con el objetivo de producir mejores resultados sin la necesidad de un amplio conocimiento en términos de evaluación de riesgos. Este enfoque difiere del enfoque OCTAVE, que OCTAVE Allegro se enfoca en los activos de información dentro del contexto de cómo se utilizan, dónde se almacenan, transportan y procesan, y cómo se ven afectados por la amenaza, la vulnerabilidad y la interrupción como resultado.

Figura 6: Proceso metodología Octave

Fuente: Suroso, J.S., Fakhrozi, M.A

B. MAGERIT (Methodology for Information Systems Risk Analysis and Management)

Es una metodología de gestión de riesgos originario de España, específicamente por el Consejo de Administración Electrónica. Esta metodología es simple y rápida de aplicar, además de proporcionar buenos resultados sobre el estado del riesgo asumido. También se puede utilizar como base para el apoyo al tomar decisiones para mejorar.

Esta metodología se puede aplicar desde dos enfoques diferentes: cualitativo o cuantitativo. El primero busca saber qué hay en términos booleanos. Además, el modo cualitativo también incluye cuánto hay.

MAGERIT se basa en los siguientes conceptos:

- **Activos:** cualquier cosa que sea útil o valiosa para una empresa, que puede ser material o intangible.

- **Dependencias:** Además de los activos, también debemos identificar las dependencias entre ellos. Es decir, las formas en que el impacto y el riesgo pueden propagarse de un activo a otro.
- **Amenazas:** Las amenazas deben identificarse para cada activo en cada dimensión y evaluarse de acuerdo con su frecuencia y la degradación provocada en el activo si se materializan.
- **Salvaguadas:** Como es el caso de las amenazas, MAGERIT proporciona una gran lista de salvaguadas predefinidas asociadas con activos y amenazas. De esta manera, se podría utilizar una lista de verificación para determinar cuáles se aplican y su vencimiento.

Figura 7: Componentes de la evaluación de riesgos Magerit

Fuente: Fernández, A., García, D.F

C. EBIOS

EBIOS, es una metodología que se utiliza para identificar los riesgos a los que se enfrenta un sistema de información y para proponer una política de seguridad adaptada a las necesidades de seguridad de la empresa. Fue creado por el DCSSI (dirección general de seguridad del sistema de información) del Ministerio de Defensa francés. La metodología EBIOS está acompañada por un software gratuito que ayuda a simplificar la aplicación de la metodología y a crear documentos de síntesis automáticamente. Es una metodología de 5 pasos a mencionar:

- La primera fase trata del establecimiento del contexto: la relación entre el contexto empresarial y el SI (contribución a los objetivos comerciales, límites, descomposición)
- En la segunda fase, los requisitos de seguridad se determinan en función de los eventos de seguridad temidos.
- En la tercera fase, se realiza un estudio del riesgo para identificar y analizar los escenarios de amenazas.
- En la cuarta fase, la información de los pasos anteriores se utiliza para identificar riesgos y describir los objetivos de seguridad necesarios y suficientes relacionados con estos riesgos.
- En la fase final, se determinan los controles de seguridad necesarios y cualquier riesgo residual se hace explícito.

Figura 8: Fases del método EBIOS

Fuente: Romero Mariño Brunil

D. CORAS

Es una metodología basada en modelos para realizar análisis de riesgos de seguridad. Utiliza un enfoque cualitativo para abordar los riesgos de seguridad de la información. Este método proporciona un lenguaje personalizado para el modelado de amenazas y riesgos. La metodología se basa en UML, un lenguaje que utiliza diagramas para ilustrar las relaciones y las dependencias entre los usuarios y el entorno en el que trabajan. En el método CORAS, un análisis de riesgo de seguridad se realiza en ocho pasos.

El método describe 8 pasos consecutivos, como se muestra en la figura 9.

1. El primer paso es principalmente preparatorio: identifica el objetivo de la evaluación y la profundidad del análisis.

2. El segundo paso consiste en una reunión con el cliente: alcanzar un entendimiento común de los objetivos generales y la planificación, así como el objetivo, el enfoque y el alcance de la evaluación.
3. El tercer paso define aún más el objetivo de la evaluación y sus activos más valiosos. Se acuerdan algunos escenarios de amenazas de alto nivel, vulnerabilidades y riesgos que deberían investigarse más a fondo. Los objetivos refinados y la descripción detallada del objetivo se documentan utilizando el lenguaje CORAS.
4. El cuarto paso es el último paso antes del análisis de riesgo real y se centra en obtener los criterios de evaluación de riesgo que se utilizarán más adelante. Este paso también verifica que el cliente apruebe la descripción detallada del objetivo y su contexto, incluidas las suposiciones y condiciones previas.
5. El quinto paso utiliza el lenguaje CORAS como base para un taller multidisciplinario de lluvia de ideas. El propósito de este taller es identificar tantos riesgos como sea posible (es decir, identificación de riesgos).
6. El sexto paso tiene como objetivo estimar los niveles de riesgo (es decir, el análisis de riesgo). Esto también se hace durante una sesión de lluvia de ideas multidisciplinaria donde se determinan las probabilidades y las consecuencias de cada riesgo previamente identificado.
7. En el séptimo paso, los criterios de evaluación de riesgo definidos previamente se utilizan para considerar que cada riesgo es aceptable o requiere tratamiento (es decir, evaluación de riesgo)

8. En el octavo paso, se identifican, evalúan y comparan los posibles tratamientos y mitigaciones.

Figura 9: Fases del método CORAS

Fuente: Molina Miranda María F.

E. MEHARI

MEHARI es una metodología de código abierto y libre, de evaluación y gestión de riesgos asociada con la información y sus tratamientos.

Mehari fue diseñado originalmente para ayudar a los Jefes de Seguridad de la Información (CISO) en sus tareas de gestión de seguridad del sistema de información. Mehari tiene como objetivo proporcionar un conjunto de herramientas específicamente diseñadas para la gestión de la seguridad, que comprende un conjunto de acciones administrativas, cada una de las cuales tiene un objetivo específico.

Mehari también da una guía en la evaluación de seguridad. Los pasos para realizar la evaluación de riesgos utilizando Mehari son los siguientes:

- Identificación de una situación de riesgo.
- Evaluación de la exposición natural.
- Evaluación de factores disuasivos y preventivos.
- Evaluación de factores protectores, paliativos y recuperativos.
- Evaluación de la potencialidad.
- Evaluación del impacto intrínseco.
- Evaluación de impacto y reducción de impacto.
- Evaluación global de riesgos.
- Decisión sobre si o no el riesgo es aceptable

4.1.2.3 Criterios de la Metodología Comparativa

En esta sección se muestran los criterios que se utilizaron para comparar las diferentes metodologías sobre gestión de riesgos. La comparación se realizó aplicando una escala de puntajes. Para cada criterio según su relevancia, se asigna un punto en una escala que va de 0 a 5 que se denomina peso. El número máximo de puntos para cada criterio se otorga solo cuando el criterio se cumple completamente. En el caso de cumplimiento parcial, los puntos se otorgan en proporción al grado de cumplimiento de las condiciones del criterio.

Los criterios se muestran en el **Anexo B-1: Criterios de selección del benchmarking de metodologías**, donde se lista los criterios de selección para las diferentes metodologías.

4.1.2.4 Análisis comparativo

Luego de seleccionar los criterios de selección en base a un puntaje determinado, se hace un análisis comparativo de las cinco metodologías (Octave, Magerit, Ebios, Coras y Mehari).

La **Tabla 12** presenta los resultados de la evaluación de las metodologías utilizando los criterios de comparación definidos en el **Anexo B-1: Criterios de selección del benchmarking de metodologías**.

Nº	Criterios de comparación	Peso (Puntaje)	OCTAVE	MAGERIT	EBIOS	CORAS	MEHARI
1	Costo	5	5	5	5	2	2
2	Documentación en ingles	2	2	2	2	2	2
3	Estándar nacional	2	0	0	0	0	0
4	Estándar internacional	4	0	0	0	0	0
5	Grupo objetivo	5	1	5	5	3	5
6	Complejidad	5	5	3	3	1	3
7	Popularidad	2	0	2	2	0	2
8	Flexibilidad	3	3	3	3	3	2
9	Método de identificación de riesgos	2	1	1	2	1	1
10	La base para el cálculo del riesgo	2	2	2	2	2	2
11	Monitoreo de riesgos	2	0	2	2	0	0
12	Adaptabilidad	4	2	2	2	4	2
13	Herramienta Software	5	0	5	5	2	2
14	Análisis de la metodología	5	2	5	2	2	5
15	Actualización	2	2	2	2	2	2
	Total:	50	25	39	37	24	30

Tabla 12: Comparativa de metodologías de gestión de riesgos

Fuente: Elaboración propia

4.1.2.5 Resultados

El benchmarking indica que la mayoría de las metodologías son eficientes en la identificación y análisis de riesgos. Sin embargo, la metodología que obtuvo mayor puntaje fue “**MAGERIT**”. Esto se debe principalmente al hecho de que es una metodología que tiene una herramienta de desarrollo llamada PILAR y que le saca ventaja en comparación con las demás metodologías. También es importante destacar que este método esté disponible de forma gratuita, lo que ayuda a reducir los costos de la administración de la seguridad.

4.1.3 Estándares para la gestión de seguridad de la información

4.1.3.1 Información general

Dado que la seguridad de la información tiene un papel muy importante en el apoyo a las actividades de la organización, necesitamos un estándar o punto de referencia que regule el gobierno sobre la seguridad de la información. Existen varios estándares para el Gobierno de TI que llevan a la seguridad de la información, como PRINCE2, OPM3, CMMI, P-CMM, PMMM, ISO27001, BS7799, SP 800-30 NIST, PCIDSS, COSO, SOA, ITIL y COBIT. Sin embargo, algunos de estos estándares no están bien adoptados por las organizaciones por diversas razones. Por ello, en este documento analizaremos los 3 estándares de SGSI más conocidos y ampliamente utilizados para la seguridad de la información los cuales son: ISO27001, BS 7799 y SP 800-39 NIST.

Después de comparar estos estándares, se eligió el más adecuado para su posterior implementación en una empresa del sector comercial.

4.1.3.2 Estándares

A. ISO/IEC 27001

ISO, fundada el 23 de febrero de 1947, promulga estándares industriales y comerciales de propiedad mundial, tiene su sede en Ginebra, Suiza. Cuenta con 163 miembros nacionales de un total de 203 países en el mundo [figura 10]. La norma internacional ISO 27001 especifica los requisitos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI documentado dentro de una organización.

Diseñado para garantizar la selección de controles de seguridad adecuados y proporcionados para proteger los activos de información. Este estándar generalmente se aplica a todo tipo de organizaciones, ya sean privadas o públicas. El estándar introduce un modelo cíclico conocido como el modelo " Plan-Do-Check-Act" (PDCA), que tiene como objetivo establecer, implementar, monitorear y mejorar la efectividad del SGSI de una organización.

Figura 10: Mapa de miembros ISO

Fuente: IchwanPalongengi

B. BS 7799

BS 7799 fue un estándar publicado originalmente por el British Standard Institution (BSI) Group en 1995. Fue redactado por el Departamento de Comercio e Industria (DTI) del Gobierno del Reino Unido y constaba de varias partes. La primera parte, que contiene las mejores prácticas para el SGSI fue revisada en 1998, que finalmente fue adoptada por la ISO como ISO 17799, "Tecnología de la información - Código de práctica para la gestión de la seguridad de la información". La segunda parte de BS 7799 fue publicada

por primera vez por BSI en 1999, conocida como BS 7799 Parte 2, titulada "Sistemas de Gestión de Seguridad de la Información - Especificación con orientación para su uso", BS 7799-2 se centró en cómo implementar SGSI, refiriéndose a la seguridad de la información. La estructura de gestión y los controles se identificaron en BS 7799-2, que luego se convirtió en ISO 27001. La versión 2002 de BS 7799-2 introdujo el Plan-Do-Check-Act (PDCA) (modelo de control de calidad de Deming) [figura 11], alineándolo con estándares de calidad como ISO 9000. BS 7799 Parte 2 fue adoptada por ISO como ISO 27001 en noviembre de 2005.

Esto se ha modelado para garantizar la selección de comandos de seguridad exactos y apropiados para proteger las unidades de información. Hoy en día, esta norma suele ser adecuada para todas las industrias públicas o privadas. El modelo de ida y vuelta, "Plan-Do-Check-Act" generado por este estándar, se enfoca en estabilizar, ejecutar, controlar y actualizar incesantemente el rendimiento de los Estándares del Sistema de Gestión de Seguridad de la Información (SGSI) de una organización.

Figura 11: Modelo PDCA en BS 7799

Fuente: British Standard Institution

C. SP 800-39 NIST

La publicación especial NIST 800-39 es el documento principal en la serie de estándares y pautas de seguridad de la información desarrollados por NIST en respuesta a FISMA.

El propósito de la Publicación especial 800-39 es proporcionar una guía para un programa integrado de toda la organización para gestionar el riesgo de seguridad de la información para las operaciones de la organización (es decir, misión, funciones, imagen y reputación), activos de la organización, individuos, otras organizaciones y La Nación resultante de la operación y uso de los sistemas de información federales.

La Publicación especial 800-39 proporciona un enfoque estructurado, pero flexible para la gestión del riesgo que tiene una base intencionalmente amplia, con los detalles específicos de evaluación, respuesta y supervisión del riesgo de forma continua proporcionados por otras normas y pautas de seguridad NIST de apoyo. La guía proporcionada por este estándar no pretende reemplazar o subsumir otras actividades, programas, procesos o enfoques relacionados con el riesgo que las organizaciones han implementado o tienen la intención de implementar para abordar las áreas de gestión de riesgos cubiertas por otras leyes, directivas, políticas, iniciativas programáticas, o misión / requisitos del negocio.

Figura 12: Proceso de gestión de riesgos en SP 800-39

Fuente: NIST 800-39

4.1.3.3 Criterios de selección del Estándar Comparativo

En esta sección se muestran los criterios que se utilizaron para comparar los diferentes estándares sobre seguridad de información. Los criterios son los mismos aplicados a las metodologías de gestión de riesgos de información; se eligieron 9 criterios. Los criterios se muestran en el **Anexo B-2: Criterios de selección del benchmarking de estándares**,

donde se lista los criterios de selección para los estándares de gestión de riesgos mencionados anteriormente.

4.1.3.4 Análisis comparativo

Luego de seleccionar los criterios en base a un puntaje determinado, se hace un análisis comparativo de los tres estándares (ISO 27001, BS 7799, SP 800-39 NIST).

La **Tabla 13** presenta los resultados de la evaluación de los estándares utilizando los criterios de selección definidos en el **Anexo B-2: Criterios de selección del benchmarking de estándares**.

Nº	Criterios de comparación	Peso (Puntaje)	ISO/IEC 27001	BS 7799	SP 800-39 NIST
1	Costo	5	3	0	5
2	Documentación en inglés	2	2	2	2
3	Sector objetivo	5	5	5	5
4	Complejidad	5	5	5	5
5	Uso geográfico	5	5	2	2
6	Actualización del estándar	3	3	3	3
7	Tratamiento de riesgos	5	5	5	5
8	Monitoreo de riesgos	5	5	5	5
9	Número de controles	5	5	5	1
	Total:	40	38	32	33

Tabla 13: Comparativa de estándares de gestión de seguridad de la información

Fuente: Elaboración propia

4.1.3.5 Resultados

El benchmarking indica que la mayoría de los estándares son eficientes para el tratamiento y monitoreo de riesgos. Sin embargo, el estándar que obtuvo mayor puntaje fue la “ISO/IEC 27001”. Esto se debe principalmente al hecho de que los estándares ISO son los más conocidos y usados internacionalmente, además de que ISO cuenta con organizaciones miembros en todo el mundo.

También es importante destacar que la ISO/IEC 27001 se basó en la BS 7799-2 para todo el tema de gestión de riesgos y controles para la seguridad de la información, por lo que actualmente a pesar de que se sigue actualizando se ha usado mayormente como un complemento de este estándar ISO. SP 800-39 a pesar de ser un estándar gratuito y que cuenta con procesos detallados de tratamiento y monitoreo de riesgos, no propone controles para reducir los riesgos de seguridad de la información, esto lo hace ineficiente a comparación de los otros estándares. Por lo tanto, podemos afirmar que el estándar más completo, de fácil uso es la ISO/IEC 27001 ya que nos proporciona un panorama completo del proceso de tratamiento y monitoreo de riesgos de seguridad de la información.

4.2 DISEÑO DEL MODELO DE REFERENCIA

4.2.1 Descripción

La presente sección tiene como objetivo diseñar el modelo de gestión de riesgos de seguridad de TI para una PYME del sector comercial que depende de proveedores críticos, el cual está dividido en 3 fases; cada una con diferentes procesos que se explicará más adelante.

4.2.2 Modelo de referencia

El modelo propuesto se desarrolló en base a artículos de investigación de modelos implementados con las diferentes metodologías y aplicaciones de los diferentes estándares como la ISO 27001, ISO 22301 e ISO 19011 en distintas organizaciones. La finalidad del modelo es reducir el nivel de impacto ocasionado por los riesgos que afectan los activos y procesos de TI de las Pymes que dependen de proveedores críticos.

4.2.2.1 Estructura

El modelo propuesto está dividido de la siguiente manera:

4.2.2.1.1 ENTRADAS

Está referido a la información que se obtiene mediante la recolección de datos como: entrevistas, cuestionarios, observación directa, etc. Las entradas del modelo son los siguientes:

- **Documentación relevante:** Alude al contexto y entendimiento de la organización (misión, visión, organigrama, etc.) así como tener conocimiento de los objetivos trazados por la misma. Se necesita identificar el plan estratégico de TI, sus proveedores, las actividades y recursos requeridos.
- **Procesos críticos:** Son aquellos procesos que la empresa califica como críticos y que son indispensables para que el negocio pueda funcionar, caso contrario la empresa tendría un impacto negativo causando pérdidas económicas o daños en la reputación de la misma.
- **Proveedores críticos:** Se refiere a proveedores que están asociados a procesos, servicios o productos críticos. Esta entrada contempla la información general del proveedor y del servicio que brinda. Como información general puede ser razón social, giro del negocio. Es necesario saber los acuerdos de nivel de servicio (SLA's) establecidos con el cliente.
- **Políticas:** Son los principios, reglas o lineamientos que propone la empresa para que estas se cumplan. Como ejemplo se pueden mencionar las siguientes:
  - Política de calidad
  - Política de seguridad de información
  - Políticas de gestión de riesgo
- **Cumplimiento normativo:** Está relacionado a las normas regulatorias establecidas por el gobierno o una entidad internacional, la cual debe ser acatada por todas las organizaciones que se acogen a dichas normas. Para el proyecto se tiene contemplado la norma 29733 denominada: “**Ley de protección de datos personales**” que tiene una serie de artículos que deben ser cumplidos.
- **Informes de auditoría:** Se refiere a los informes de auditorías previos que tuvo la empresa. Si es que la empresa tuvo auditoria de sistemas se toma en cuenta esas observaciones (ausencia de determinados controles, hay política, pero no se evidencia cumplimiento, hay

control, pero no se evidencia que se haga seguimiento, etc.) para el proceso de implementación del modelo. Es lo que se requiere (si es que lo hubiera) para diseñar el modelo de gestión de riesgos.

4.2.2.1.2 PROCESO DE IMPLEMENTACIÓN

La información que se obtiene de las entradas es procesada a través de la aplicación de la metodología MAGERIT, así como también del estándar ISO 27001:2013, lo cual genera 3 grandes fases que serán explicadas a continuación.

4.2.2.1.2.1 FASES DEL MODELO

El modelo propuesto sigue las pautas de aplicación de la metodología MAGERIT; asimismo, en el diseño se incluyó un punto de la norma ISO 27001:2013 el cual es: 6.1.3: Tratamiento de riesgos de seguridad de información

A. FASE 1: EVALUACIÓN DEL RIESGO

Esta fase incluye los siguientes procesos:

A.1. Análisis del contexto

Este proceso consiste en determinar el análisis situacional de la organización respecto a la gestión de seguridad de la información. Seguridad propia de la empresa y también asociado a los proveedores críticos. Este proceso está definido por los siguientes elementos:

- P1: Identificar políticas de seguridad de la organización
- P2: Seguimiento de la organización a los proveedores críticos
- P3: Identificar procesos asociados a proveedores críticos

A.2 Análisis del riesgo

En esta sección se realiza el “análisis del riesgo”, para lo cual se aplica el proceso de la metodología Magerit. Esto consta de lo siguiente:

1. Identificación de activos críticos de TI

Identificar los activos de TI asociados a proveedores críticos con la mayor relevancia y valor para la organización, y qué detrimento o costo causaría su degradación. Para ello, se hace la valoración de los activos según lo que indica Magerit.

2. Identificar amenazas

Establecer las amenazas a las que estén expuestos los activos críticos de TI identificados en el

proceso anterior, esto según MAGERIT es “**crear perfil de amenaza**”. El capítulo 5 del "Catálogo de Elementos" de Magerit presenta una relación de amenazas típicas

3. Identificar controles existentes

Este proceso consiste en determinar los controles o salvaguardas que existen y que pueden mitigar las amenazas identificadas y su efectividad.

Las salvaguardas o contra medidas son aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se conjuran simplemente organizándose adecuadamente, otras requieren elementos técnicos (programas o equipos), otras seguridades físicas y, por último, está la política de personal.

Magerit en su capítulo 6 del "Catálogo de Elementos" presenta una relación de salvaguardas adecuadas para cada tipo de activos.

A.3 Valoración del riesgo

Este proceso se realiza a través de la estimación del impacto y el riesgo

4. Estimar impacto y riesgo

4.1 Impacto

Lo peor que puede pasar. Es la medida del daño sobre el activo debido a la materialización de la amenaza.

4.2 Riesgo

Es lo que probablemente pase (Impacto ponderado con la tasa de ocurrencia de la amenaza). El riesgo se mide en las mismas unidades que el valor.

El riesgo se calcula como

$$\text{riesgo} = \text{impacto} \times \text{probabilidad (frecuencia)}$$

Es un valor real, mayor que cero.

A.4 Criterios de validación

Luego de haber desarrollado los tres procesos anteriores, se consolida el proceso: Criterios de validación, los cuales están relacionados a los procesos descritos anteriormente. Los criterios elegidos son:

- C1: Seguridad de la información de la empresa
- C2: Seguridad de la información relacionado a proveedores críticos
- C3: Procesos asociados a proveedores críticos de TI

- C4: Activos críticos de TI asociados a proveedores críticos
- C5: Amenazas asociadas a los activos de TI
- C6: Impacto y riesgo

B. FASE 2: TRATAMIENTO DEL RIESGO

Esta fase se divide en los siguientes procesos:

B.1 Modificar el riesgo

Este proceso se refiere a: Modificar el riesgo. Aquí se incluye la aplicación del punto 6.1.3: Tratamiento de riesgos de seguridad de información de la ISO 27001:2013 que refuerza el tratamiento de riesgos de seguridad de TI.

Punto 6.1.3: Tratamiento de riesgos de seguridad de información:

La norma ISO 27001 contiene entre sus cláusulas la sexta denominada planificación, entre ellas se encuentra la cláusula 6.1.3 denominada: Tratamiento de riesgos de la seguridad de la información.

La organización debe establecer e implementar un proceso de tratamiento de riesgos de la seguridad de la información, para ello se siguen los siguientes pasos:

- **Determinar acciones de tratamiento.** Seleccionar la información apropiada de opciones de tratamiento de riesgos de seguridad, teniendo en cuenta los resultados de la evaluación de riesgos realizada anteriormente.

Las acciones de tratamiento que se pueden tomar son: Mitigar, evitar, transferir y aceptar

- **Establecer controles.** Determinar todos los controles necesarios para implementar las opciones de tratamiento de riesgo de seguridad de la información
- **Contrastar controles.** Comparar los controles determinados en el paso anterior con los controles del Anexo A de la ISO 27001 y verificar que no se hayan omitido los controles necesarios

B.2. Criterios de validación

Los criterios identificados de la fase 2 se realizan en base al proceso anterior, estos se muestran a continuación:

- C7: Planes de tratamiento
- C8: Establecimiento de controles

Asimismo, después de la implementación de los controles se realiza un análisis de los resultados obtenidos.

C. FASE 3: SEGUIMIENTO Y CONTROL

Esta fase comprende todo el proceso de monitoreo de las recomendaciones establecidas luego de la implementación del modelo.

C.1 Monitoreo

Aquí se realiza el seguimiento continuo de las recomendaciones propuestas para que puedan ser cumplidas por la organización. Este proceso se realiza a través de dos subprocesos:

▪ Seguimiento continuo

Teniendo en consideración de que es muy difícil que los riesgos identificados dejen de suponer una amenaza para la organización, es imprescindible establecer los indicadores de seguimiento y control sobre las medidas que se establecen para la gestión de riesgos.

El seguimiento continuo y la revisión periódica del proceso de la gestión del riesgo y sus resultados debería ser una parte planificada del proceso de la gestión del riesgo, con responsabilidades claramente definidas.

▪ Auditorias

Las auditorias son una parte importante del proceso del seguimiento y control. Estos garantizan que las recomendaciones sean cumplidas por la organización. Por lo general se recomienda que las auditorias se hagan una vez cada año como parte de la mejora continua que indica el estándar ISO 22301.

Para realizar las auditorias, se apoya en el estándar ISO 19011. Este proceso será explicado más adelante en el proceso de implementación.

C.2 Criterios de validación

Los criterios identificados en esta fase se realizan en base al proceso anterior, estos se muestran a continuación:

- C9: Monitoreo y control
- C10: Auditorias

4.2.2.1.2.2 HERRAMIENTAS DEL MODELO

Luego de las fases del modelo, estas se relacionan con las siguientes herramientas:

- Criterios de validación
- Nivel de madurez de la gestión de riesgos
- Elementos clave de la gestión de riesgos

Como resultado de la relación de estas herramientas se desarrolla la “**matriz de evaluación**” que será la base para la construcción de la **herramienta de evaluación** que permitirá establecer el nivel de madurez de la organización respecto al gobierno de gestión de riesgos y seguridad de TI.

4.2.2.1.3 SALIDAS

Es el resultado luego del proceso de implementación, estas son:

- **Controles:** Son mecanismo que aseguran el cumplimiento de las políticas o planes de seguridad establecidos, pueden ser físicos o electrónicos.
- **Planes de seguridad de la información:** Son los planes de acción que involucran estrategias de seguridad, estructura organizacional, normas y procedimientos.
- **Métricas (KRI):** Son indicadores de gestión de riesgos que nos permiten cuantificar la situación de la organización luego de la implementación del modelo.

4.2.2.1.4 HERRAMIENTAS DE SOPORTE

Son las herramientas que sustentan el modelo. Estos se mencionan a continuación:

- Estándar ISO 19011
- Estándar ISO 22301 (Gestión de la continuidad del negocio)
- Estándar ISO 31000 (Gestión del riesgo)
- Circulares SBS
  - Circular N° G-139 "Gestión de la continuidad del negocio"
  - Circular N° G-140 "Gestión de la seguridad de la información"
- Ley “29733” – Ley de protección de datos personales

Figura 13: Modelo de gestión de riesgos de seguridad de TI.

Fuente: Elaboración propia

4.2.2.2 Criterios de validación

En base al **objetivo uno** que comprende el benchmarking de metodologías de gestión de riesgos y también de estándares de seguridad de información, se ha logrado definir las fases del **modelo de referencia**. Para el cumplimiento óptimo de cada fase del modelo se desarrollan criterios específicos denominados “**criterios de validación**” los cuales se encuentran relacionados a cada una de estas fases.

En la siguiente imagen se puede observar las fases y la relación con los criterios definidos para cada una de estas.

Figura 14: Criterios de validación del modelo

Fuente: Elaboración propia

4.2.2.3 Elementos clave de la gestión de riesgos

Existen 4 elementos los cuales son fundamentales para una adecuada gestión del riesgo. Para el proyecto se tomaron en cuenta 3 de ellos; estos son:

1. Procesos

El proceso de gestión de riesgos se refiere a la aplicación sistemática de políticas, procedimientos y prácticas que se llevan a cabo en la organización para mantener la gestión de riesgos implementada y funcionando.

Como parte del proceso podemos encontrar la identificación, evaluación, tratamiento y seguimiento de la gestión de riesgos, teniendo que estar integrada en los procesos de la organización para agregar y proteger el valor.

2. Personas

Esta referido a la relación interna de la organización con la gestión de riesgos. Es decir, el conocimiento que posee la organización sobre sus riesgos y entrenamiento que se realiza sobre estas temáticas y su cultura en materia de riesgos.

La cultura de gestión de riesgos abarca la conciencia general, las actitudes y el comportamiento de los colaboradores de una organización hacia el riesgo y cómo el riesgo se gestiona dentro de la organización. Es un indicador de qué tan ampliamente se han adoptado políticas y prácticas de gestión de riesgos en la organización.

3. Tecnología

Herramientas o soluciones tecnológicas que posee la organización para apoyar el proceso de gestión de riesgos.

A medida que ha pasado el tiempo y la gestión de riesgos se ha vuelto más relevante y robusta, se torna de real importancia la vinculación que exista entre los sistemas de información que apoyan la operación y la tecnología implementadas para soportar la gestión de riesgos, de manera de aprovechar estas tecnologías para entregar la información de riesgos en tiempo real, con información oportuna y reportable, acceso transversal y en general una optimización del proceso de gestión de riesgos para la toma de decisiones.

Dichos componentes han sido seleccionados en base al estudio realizado por la consultora mundial “Deloitte” que realizó un estudio del nivel de madurez de la gestión de riesgos en el país de Chile, el cual denominó: “**Primer estudio del nivel de madurez de la Gestión de Riesgos**”.

Figura 15: Elementos clave de la gestión de riesgos

Fuente: Consultora Deloitte

4.2.2.4 Nivel de madurez

El nivel de madurez nos permitirá saber en qué situación se encuentra la organización respecto al gobierno de gestión de riesgos y seguridad de TI relacionado a sus proveedores críticos y que tan alineado está a los objetivos del negocio; de acuerdo a ello hacer una evaluación para determinar los controles necesarios para pasar a un siguiente nivel.

Existen numerosas metodologías para realizar estimaciones del nivel de madurez de la gestión integral de riesgos, cuyo propósito final es aportar una visión sobre el estatus del desarrollo actual de sus componentes y exhortar a la búsqueda de la mejora continua de la gestión de riesgos como elemento fundamental de la sostenibilidad, buen gobierno corporativo y de la planeación estratégica de las empresas.

Como marco de referencia para la medición de la madurez de gestión de riesgos de las organizaciones, se definieron los siguientes cinco niveles:

1. Inicial o no desarrollado

No existe un enfoque estructurado para identificar y gestionar los riesgos. Las prácticas de gestión de riesgos son básicas y no son aplicadas de manera consistente, y existe un bajo nivel de entendimiento y conciencia sobre las mismas. Hay oportunidades de mejora críticas

2. Formalizado

Las políticas y procesos están siendo establecidos. Las prácticas de gestión de riesgos están en proceso de desarrollo, no son aplicadas de manera consistente, pero existe un buen entendimiento y conciencia sobre las mismas por unos pocos individuos en la organización. Hay oportunidades de mejora significativas.

3. Establecido

La gestión de riesgos ha sido implementada dentro de los procesos rutinarios de la organización. Las prácticas de gestión de riesgos están establecidas, se aplican de manera consistente con mejores niveles de entendimiento y conciencia sobre las mismas por la gerencia y por los empleados. Hay oportunidades de mejora en ciertos aspectos.

4. Implementado e Interiorizado

Existe un enfoque proactivo frente a la gestión de riesgos en todos los niveles de la organización. Las prácticas de gestión de riesgos están en un nivel avanzado, se aplican de manera consistente y están incorporadas en los procesos con altos niveles de entendimiento y conciencia por parte de la gerencia y los empleados. Hay oportunidades de mejora en unos pocos aspectos puntuales.

5. Optimizado

Se está llevando a cabo mejora continua y la gama completa de actividades del programa de gestión de riesgos se están ejecutando. Las prácticas de gestión de riesgos son innovadoras y vanguardistas en la industria, se aplican de manera consistente, están integradas transversalmente en la organización y son fácilmente replicables en nuevas áreas de la misma. Hay muy altos niveles de entendimiento y conciencia sobre las prácticas de gestión de riesgos por parte de la gerencia y los empleados.

Estos niveles fueron realizados en base al estudio realizado por la consultora mundial de riesgos “**Marsh Risk Consulting**” que realizó un estudio de la gestión de riesgos en Latinoamérica, el cual denominó: “**Navegando la incertidumbre: III Benchmark de gestión de riesgos en Latinoamérica**”.

Figura 16: Nivel de madurez de gestión de riesgos y seguridad de TI

Fuente: Marsh Risk Consulting

Finalmente, los niveles de madurez con respecto a la gestión de riesgos y seguridad de TI se muestran a continuación:

Puntaje	Nivel
1 <= Puntaje < 2	Inicial o no desarrollado
2 <= Puntaje < 3	Formalizado
3 <= Puntaje < 4	Establecido
4 <= Puntaje < 5	Implementado e interiorizado
5	Optimizado

Tabla 14: Nivel de madurez de la gestión de Riesgos y seguridad de TI

Fuente: Marsh Risk Consulting

Dada la evaluación se determinará en qué nivel o grado se encuentra la empresa del sector comercial para luego tomar decisiones que permitan reducir el impacto causado por los riesgos que afectan a los procesos de TI.

4.2.2.5 Matriz de evaluación

En base a los criterios de validación, los elementos claves del riesgo y los niveles de madurez de la gestión del riesgo, se desarrolló una matriz el cual relacionó estos 3 elementos. Dicha matriz se realizó con los siguientes objetivos:

- Desarrollar la herramienta de evaluación (assessment)
- Evaluar los criterios de validación a través de expertos

A continuación, se describe los criterios de validación cada una con su respectiva matriz y para cada fase del modelo.

1. Fase 1: Evaluación del Riesgo

1.1. C1: Seguridad de la información de la empresa

Fuente: ISO 27001, Deloitte, Marsh Risk Consulting

Criterio	Nivel	Personas	Procesos	Tecnología
Seguridad de la información de la empresa	Inicial o no desarrollado	La empresa no cuenta con políticas o si los tiene son mínimos; motivos por los cuales tiene poca conciencia sobre la seguridad de información.	La organización casi no tiene internalizada una política de gestión de riesgos que aseguren la confidencialidad, integridad y disponibilidad de la información para disminuir los riesgos asociados a los activos, procesos y servicios de TI.	La empresa cuenta con muy pocas herramientas para gestionar de manera adecuada las amenazas asociadas a la seguridad de información.
	Formalizado	Se establecen políticas de seguridad de información siguiendo los objetivos de la organización.	La empresa tiene definido políticas de gestión de riesgos de seguridad de TI que aseguren disminuir el impacto ocasionado por las amenazas a los activos, procesos y servicios de TI.	La empresa cuenta con algunas herramientas para mitigar las amenazas de seguridad de información y por ende no desarrolla una adecuada gestión de las mismas.
	Establecido	Se divulgan las políticas, controles y demás lineamientos de seguridad de información en toda la organización para que todos tengan conciencia sobre la misma.	La política de gestión de riesgos establece claramente los lineamientos, roles y responsabilidades y declaración del apetito al riesgo. Esto asegura una gestión eficaz de la seguridad de información.	La organización cuenta con herramientas propias y adquiridas como por ejemplo la ISO 27001 para tratar las amenazas asociadas a la seguridad de información.
	Implementado e interiorizado	Se hacen revisiones periódicas a las políticas de seguridad de información a través de herramientas de auditoría de sistemas de información.	Se hacen revisiones periódicas a la política de gestión de riesgos a través de procesos sistemáticos para asegurar el cumplimiento y validación de estas y así asegurar una adecuada seguridad de información.	La organización tiene roles y responsabilidades definidos para hacer uso de las diferentes herramientas con que cuenta para mitigar las amenazas asociadas a la seguridad de información.
	Optimizado	La organización apoya y contribuye al mejoramiento continuo de la seguridad de información incluyendo a todas las áreas de la organización.	Se utiliza un indicador de cumplimiento para establecer si las políticas de gestión de riesgos establecidas por la organización	Se hacen revisiones y controles periódicos a todas las herramientas (propias y adquiridas) con que cuenta la

			están siendo llevadas conforme fueron establecidas.	organización contribuyendo a la mejora continua.

Tabla 15: Criterio: Seguridad de la información de la empresa

Fuente: Elaboración propia

1.2. C2: Seguridad de la información asociado a proveedores críticos

Fuente: Deloitte, Marsh Risk Consulting

Criterio	Nivel	Personas	Procesos	Tecnología
Seguridad de la información asociado a proveedores críticos	Inicial o no desarrollado	La organización no se encuentra preparada para gestionar los riesgos de seguridad de información, por lo que no le da la debida importancia a los riesgos de seguridad de TI asociados al proveedor crítico.	La organización no cuenta con políticas o procedimientos para supervisar la entrega de servicios de parte del proveedor crítico que aseguren la información de la empresa.	La organización no cuenta con herramientas de apoyo para realizar un adecuado seguimiento al proveedor critico respecto a la seguridad de información que este maneja sobre la empresa.
	Formalizado	La organización se comunica con el proveedor solo cuando existen problemas respecto al servicio o producto que este le brinda.	La organización define políticas para hacer un adecuado seguimiento a las políticas de seguridad de información respecto de los servicios o productos que el proveedor crítico ofrece.	La organización cuenta con herramientas propias para el apoyo a la supervisión del proveedor crítico, respecto al servicio brindado.
	Establecido	La organización tiene constante comunicación con el proveedor crítico, por lo que conoce los servicios, procesos o productos que este le brinda.	Se desarrollan informes de seguimiento para verificar que los proveedores cumplan con los SLA's establecidos en el contrato y	La organización cuenta con herramientas propias los cuales son revisados de manera periódica por la organización.

			evitar cualquier eventualidad que cause daños o perjuicios a la empresa.	
	Implementado e interiorizado	Todas las áreas de la organización tienen conciencia sobre la seguridad de la información, por lo que conocen perfectamente a todos los proveedores y el servicio que este le brinda.	La organización solicita constantemente las políticas o auditorías de seguridad de TI a los proveedores críticos para verificar que los servicios o productos tengan una alta disponibilidad.	La organización tiene herramientas propias y adquiridas que apoyan el seguimiento y supervisión de los productos y servicios que el proveedor crítico brinda.
	Optimizado	La organización supervisa continuamente al proveedor a través de un área especializada que establece políticas y controles de cómo hacerlo y así disminuir el riesgo ocasionado ante cualquier eventualidad.	La empresa verifica las pruebas de seguridad de TI que realiza el proveedor para validar las políticas que éste tiene respecto a la seguridad de información.	Se mantiene en constante mejora las diferentes herramientas con que cuenta la organización, estableciendo el mejoramiento continuo de las mismas.

Tabla 16: Criterio: Seguridad de la información asociado a proveedores críticos

Fuente: Elaboración propia

1.3. C3: Procesos asociados a proveedores críticos de TI

Fuente: Deloitte, Marsh Risk Consulting, CMMI

Criterio	Nivel	Personas	Procesos	Tecnología
Procesos asociados a proveedores	Inicial o no desarrollado	La empresa no tiene un conocimiento adecuado de sus procesos y proveedores críticos de TI.	Los procesos y proveedores críticos de TI no se encuentran identificados ni documentados.	No existen sistemas donde se registren procesos y proveedores de TI.
	Formalizado	La empresa empieza a tomar conciencia e identifica algunos procesos y proveedores	La identificación de procesos y proveedores críticos de TI se encuentra en desarrollo.	Se empieza a registrar los procesos y proveedores críticos de TI en algún sistema o bases de datos.

		críticos de TI con un adecuado nivel de entendimiento.		
	Establecido	La empresa tiene identificado a los procesos y proveedores críticos TI con un buen nivel de entendimiento.	La identificación de procesos y proveedores críticos de TI se encuentra implementada.	Los procesos o proveedores críticos de TI se encuentran registrados en algún sistema, pero sin clasificar o categorizar.
	Implementado e interiorizado	La empresa tiene identificado, registrado y/o documentado los procesos y proveedores críticos de TI con un alto nivel de entendimiento.	La identificación de procesos y proveedores críticos de TI se encuentra documentada e interiorizada.	Los procesos y proveedores críticos de TI se encuentran registrados y clasificados en un sistema de información listo para su rápida explotación.
	Optimizado	La empresa mantiene documentado, interiorizado y actualizado el conocimiento de los procesos y proveedores críticos de TI, así estos sean dinámicos en el tiempo.	La identificación de procesos y proveedores críticos de TI se encuentra documentada, interiorizada y en mejora continua.	Se mantiene en constante mejora el sistema que aloja el registro de procesos y proveedores críticos de TI para su rápida explotación y así apoyar al análisis.

Tabla 17: Criterio: Procesos asociados a proveedores críticos de TI

Fuente: Elaboración propia

1.4. C4: Activos críticos de TI asociado a proveedores críticos

Fuente: Deloitte, Marsh Risk Consulting, CMMI, Magerit v3.0

Criterio	Nivel	Personas	Procesos	Tecnología
Activos críticos	Inicial o no desarrollado	La empresa no tiene un conocimiento adecuado de los activos de TI que gestionan sus proveedores críticos.	La identificación de los activos de TI que gestionan los proveedores críticos no se encuentra desarrollada ni documentada.	No existen sistemas donde se registren los activos de TI identificados.

	Formalizado	Algunos individuos de la organización entienden la importancia de tener los activos de TI correctamente identificados y clasificados y empiezan a realizar estas tareas.	El proceso de identificación de los activos de TI se encuentra en desarrollo.	Se empieza a registrar los activos de TI identificados en algún sistema o base de datos.
	Establecido	Los empleados y la gerencia tienen identificados sus activos de TI a conciencia.	La identificación de los activos de TI se ha implementado de manera consciente.	Los activos de TI se encuentran registrados en algún sistema, pero sin clasificar o categorizar.
	Implementado e interiorizado	Los empleados y la gerencia tienen correctamente identificados y clasificados los activos de TI.	La identificación de los activos de TI se encuentra implementada, documentada e interiorizada.	Los activos de TI se encuentran registrados y clasificados en un sistema de información listo para su rápida explotación.
	Optimizado	La alta gerencia mantiene a los activos de TI correctamente identificados, clasificados, actualizados y divulgados en toda la organización.	La identificación de los activos de TI se encuentra implementada, documentada, interiorizada y en mejora continua.	Se mantiene en constante mejora el sistema que aloja el registro de activos de TI identificados y así apoyar a la gestión de riesgos respecto a estos.

Tabla 18: Criterio: Activos críticos de TI asociado a proveedores críticos

Fuente: Elaboración propia

1.5. C5: Amenazas asociadas a los activos de TI

Fuente: Deloitte, Marsh Risk Consulting, CMMI, Magerit v3.0

Criterio	Nivel	Personas	Procesos	Tecnología
Amenazas asociadas	Inicial o no desarrollado	La organización tiene prácticas pobres o nulas para la identificación de amenazas que pueden afectar a los activos de TI.	El proceso de identificación de las amenazas que afectan a los activos de TI no	No existen sistemas donde se registren las amenazas que afectan a los activos de TI.

			se encuentra desarrollada ni mucho menos documentada.	
	Formalizado	Algunos individuos de la organización están tomando conciencia sobre las amenazas que pueden afectar a los activos de TI y empiezan a identificarlas.	El proceso de identificación de amenazas que afectan a los activos de TI se encuentra en proceso de desarrollo.	Se empieza a registrar las amenazas en algún sistema o base de datos.
	Establecido	La organización tiene un buen conocimiento sobre las amenazas que afectan a los activos de TI, clasificándolas por tipología.	La identificación de las amenazas se ha implementado de manera consciente en la organización.	Las amenazas identificadas se encuentran registradas en algún sistema, pero sin clasificar o categorizar.
	Implementado e interiorizado	La organización tiene correctamente identificadas, clasificadas y valoradas a las amenazas que afectan a sus activos de TI.	La identificación de las amenazas que afectan a los activos de TI se encuentra implementada, documentada e interiorizada.	Las amenazas identificadas se encuentran registradas y clasificadas en un sistema de información listo para su rápida explotación.
	Optimizado	La organización mantiene las amenazas que afectan a sus activos de TI identificadas, clasificadas, valoradas y divulgadas. Esta información es actualizada periódicamente.	La identificación de los activos de TI se encuentra implementada, documentada, interiorizada y en mejora continua.	Se mantiene en constante mejora el sistema donde se registran las amenazas para apoyar al análisis y facilitar una toma de decisiones.

Tabla 19: Criterio: Amenazas asociadas a los activos de TI

Fuente: Elaboración propia

1.6. C6: Impacto y riesgo

Fuente: Deloitte, Marsh Risk Consulting, CMMI, Magerit v3.0

Criterio	Nivel	Personas	Procesos	Tecnología
Impacto y riesgo	Inicial o no desarrollado	La empresa tiene prácticas pobres sobre la determinación del riesgo potencial derivado de la materialización de amenazas en los activos de TI.	La determinación del riesgo potencial que afecta a los activos de TI no se encuentra desarrollada ni documentada.	No existen sistemas donde se registren y calculen los riesgos potenciales que afectan a los activos de TI.
	Formalizado	Algunos individuos en la organización toman conciencia y empiezan a desarrollar el cálculo de los riesgos potenciales.	El proceso de cálculo o determinación del riesgo potencial se encuentra en proceso de desarrollo.	Se empieza a registrar los riesgos potenciales en algún sistema o base de datos existente.
	Establecido	La organización tiene un buen conocimiento sobre el cálculo del impacto y probabilidad de los riesgos sobre los activos de TI.	La determinación del riesgo potencial de ha implementado de manera consciente en la organización.	Los riesgos potenciales se encuentran registrados en algún sistema, pero sin un cálculo adecuado del impacto y la probabilidad, ya que se carece de herramientas para el cálculo del riesgo potencial.
	Implementado e interiorizado	La organización tiene un alto nivel de conocimiento sobre los riesgos potenciales que afectan a sus activos de TI.	La determinación del riesgo potencial se encuentra implementada, documentada e interiorizada.	Los riesgos potenciales se encuentran correctamente registrados, calculados y clasificados en un sistema de información listo para su explotación, además de contar con herramientas para el cálculo del impacto y probabilidad.

	Optimizado	La organización mantiene el cálculo de los riesgos potenciales interiorizado y este se realiza periódicamente.	La determinación del riesgo potencial se encuentra implementada, documentada, interiorizada y en mejora continua.	Se mantiene en constante mejora el sistema donde se registra y calcula los riesgos potenciales para apoyar al análisis y toma de decisiones.

Tabla 20: Criterio: Impacto y riesgo

Fuente: Elaboración propia

2. Fase 2: Tratamiento del riesgo

2.1. C7: Planes de tratamiento

Fuente: ISO 31000, Nivel de madurez CMMI, DELOITTE

Criterio	Nivel	Personas	Procesos	Tecnología
Planes de tratamiento	Inicial o no desarrollado	La organización implementa pocas opciones de tratamiento para abordar los riesgos de seguridad de TI.	La organización cuenta con una política de gestión de riesgos, pero casi no lo implementa para realizar planes de tratamiento de riesgos de seguridad de TI.	No se cuenta con herramientas para realizar un adecuado plan de tratamiento sobre los riesgos de seguridad de TI.
	Formalizado	La organización cuenta con un área especializada en gestión de riesgos de TI, el cual desarrolla políticas y procedimientos para realizar planes de tratamiento para los riesgos de seguridad de TI.	La organización tiene definido políticas y procedimientos de gestión de riesgos que ayudan a desarrollar un eficaz plan de tratamiento.	Se cuenta con algunas herramientas tecnológicas propias para dar apoyo a la gestión de riesgos y afrontar un adecuado plan de tratamiento de riesgos de seguridad de TI.

	Establecido	Se divulgan las políticas y procedimientos sobre los planes de tratamiento de riesgos de seguridad de TI en toda la organización.	Se cuenta con una política de gestión de riesgos el cual establece claramente los lineamientos, roles y declaración del apetito del riesgo que conlleva a mejorar los planes de tratamiento.	La organización actualiza y da soporte a las herramientas tecnológicas que apoyan el proceso de gestión de riesgos de seguridad de información.
	Implementado e interiorizado	La organización realiza pruebas de manera sistemática a los planes de tratamiento, para determinar si estas funcionan correctamente.	Se utiliza un indicador de cumplimiento para establecer si los planes de tratamiento establecidos por la organización están siendo llevados de la mejor manera.	La organización desarrolla y optimiza herramientas tecnológicas propias que sirven para una mejor gestión de los riesgos de seguridad de TI.
	Optimizado	La organización difunde y aprende continuamente sobre los resultados arrojados luego de los planes de tratamiento de riesgos de seguridad de TI.	El plan de tratamiento identifica con claridad el orden de prioridad en que se debe implementar los controles para tratar los riesgos de seguridad de TI.	Las herramientas tecnológicas son innovadoras y vanguardistas, con ello se logra realizar un adecuado plan de tratamiento sobre los riesgos de seguridad de TI.

Tabla 21: Criterio: Planes de tratamiento

Fuente: Elaboración propia

2.2. C8: Establecimiento de controles

Fuente: ISO 31000, ISO 27001, DELOITTE

Criterio	Nivel	Personas	Procesos	Tecnología
Establecimiento de controles	Inicial o no desarrollado	La organización cuenta con mínimos conocimientos para realizar una propuesta de controles para los riesgos de seguridad de TI.	Las políticas y procedimientos de gestión de riesgos para establecer controles se encuentran en proceso de elaboración.	Las herramientas de apoyo con que cuenta la organización para realizar una propuesta de controles se encuentran en proceso de elaboración.

	Formalizado	La organización sigue una política y procedimientos para proponer controles sobre gestión de riesgos de seguridad de TI.	El proceso de gestión de riesgos de seguridad de TI tiene opciones para realizar los controles, pero no se encuentran alineados a los objetivos del negocio.	La organización cuenta con algunas herramientas propias para realizar los controles de gestión de riesgos de seguridad de TI.
	Establecido	La organización define opciones de tratamiento de riesgos los cuales son: - Mitigar - Evitar - Transferir - Aceptar	Se establecen controles que definen el orden en el que se debe llevar a cabo el tratamiento de riesgos de seguridad de TI.	Las herramientas con que cuenta la organización son deficientes porque no modifican el riesgo, por lo que se debe desarrollar o adquirir otras herramientas de apoyo para una mejor gestión del riesgo.
	Implementado e interiorizado	La selección de las opciones de tratamiento del riesgo se realiza de acuerdo con los objetivos de la organización, los criterios del riesgo y los recursos disponibles.	Los controles para el tratamiento de los riesgos implican un proceso iterativo de: formular y seleccionar opciones de tratamiento, planificar e implementar el tratamiento y evaluar la eficacia de ese tratamiento.	Se dispone de herramientas propias y adquiridas como el estándar ISO:31000, ISO:270001, ISO:27002, etc. para realizar una propuesta de controles eficaz sobre los riesgos de seguridad de TI.
	Optimizado	Al seleccionar las opciones de tratamiento del riesgo, la organización considera los valores, las percepciones, involucra potencialmente a las partes interesadas y los medios más apropiados para comunicarse con ellas y consultarlas.	La propuesta de controles para el proceso de gestión de riesgos se encuentra documentada siguiendo políticas y procedimientos establecidos por la organización. Los controles se mantienen y se reevalúan.	La organización aplica de manera eficiente los controles de seguridad obtenidos del Anexo A de la ISO 27001, y también de la ISO 31000 para mitigar el riesgo.

Tabla 22: Criterio: Establecimiento de controles

Fuente: Elaboración propia

3. Fase 3: Seguimiento y control

3.1. C9: Monitoreo y control

Fuente: ISO 31000, ISO 27001, DELOITTE

Criterio	Nivel	Personas	Procesos	Tecnología
Monitoreo y control	Inicial o no desarrollado	La organización tiene muy poco conocimiento sobre el proceso de seguimiento y control acerca de los riesgos de seguridad de TI.	La organización no cuenta con una política de gestión de riesgos; en caso lo tuviera estos se encuentran a un nivel muy bajo.	La organización no cuenta con herramientas tecnológicas para el seguimiento y control de los riesgos de seguridad de TI.
	Formalizado	La alta gerencia usa como herramienta de seguimiento y control las auditorías, los cuales son realizados de forma escasa.	La organización cuenta con una política de gestión de riesgos que se encuentra documentada y apoya al monitoreo y control.	La organización cuenta con algunas herramientas de seguimiento y control los cuales fueron desarrollados en la organización (aplicaciones, Excel, etc.)
	Establecido	La organización establece registros de auditoría de las actividades más relevantes para tener un eficaz seguimiento y control de los riesgos identificados.	La organización ha establecido planes, políticas y controles los cuales han sido aprobados y se realizan de manera continua que apoya al monitoreo y control.	La organización cuenta con herramientas propias y adquiridas como la ISO 19011 para el seguimiento y control de los riesgos de seguridad de TI.
	Implementado e interiorizado	La organización revisa los resultados de las actividades de seguimiento y formula acciones correctivas que fueran necesarias luego de la evaluación.	La organización tiene diferentes formas de identificar riesgos como el estratégico o alto nivel; los cuales están aprobados y difundidos en toda la empresa y facilitan al proceso de seguimiento y control.	Las herramientas tecnológicas para el monitoreo y control incorporan características como: visualización, configuración, reportes y cuadro de mando.
	Optimizado	La organización realiza un seguimiento y control en todas las etapas de la gestión de riesgos. Esta incluye planificar, recopilar y	La organización revisa las políticas y a su vez aplica técnicas de mejora continua para el apoyo del seguimiento y control.	La organización apoya y contribuye al mejoramiento continuo de las herramientas de

		analizar información, registrar resultados y proporcionar retroalimentación.		apoyo para el seguimiento y control

Tabla 23: Criterio: Monitoreo y control

Fuente: Elaboración propia

3.2. C10: Auditorías

Fuente: ISO 19011, Circular SBS G-139, DELOITTE

Criterio	Nivel	Personas	Procesos	Tecnología
Auditorías	Inicial o no desarrollado	La organización tiene conocimiento que su proveedor crítico realiza auditorias de manera incipiente.	Las políticas mencionadas no existen o están en proceso de elaboración.	La empresa no audita o no participan de las pruebas respecto a los productos o servicios o productos que el proveedor le ofrece. Si lo hacen es de forma incipiente.
	Formalizado	La empresa informa que su proveedor establece programas de auditoria que contribuye a la determinación de la eficacia del sistema de gestión del auditado.	El proveedor cuenta con algunas políticas mencionadas los cuales son auditados de manera incipiente por el mismo.	La empresa asigna a responsables de seguridad de información para que puedan participar de las pruebas respecto al servicio o producto que le ofrece al proveedor.
	Establecido	La organización verifica que la alta dirección del proveedor se asegura de que los objetivos del programa de auditoria se han establecido y que se asigne a las personas indicadas para gestionarlo.	El proveedor cuenta con casi todas las políticas los cuales son auditados de manera continua siguiendo un programa de auditoria liderados por un equipo especialista en la materia.	La organización además de tener responsables, desarrolla planes de auditoria para llevar a cabo las pruebas de seguridad de información y continuidad de negocios al proveedor.

	Implementado e interiorizado	El proveedor crítico da seguimiento al programa de auditoría considerando: ▪ Evaluar la conformidad del programa de auditoría ▪ Evaluar desempeño de los miembros del equipo auditor ▪ Evaluar la capacidad de los equipos auditores	El proveedor crítico cuenta con todas las políticas mencionadas las cuales se establecen, mantienen y son documentados luego de un programa de auditoría interna que se realiza continuamente.	Para la supervisión de las pruebas de seguridad y continuidad de negocios se siguen los principios de auditoría los cuales son: Integridad, imparcialidad, confidencialidad, juicio, independiente, basado en la evidencia.
	Optimizado	El proveedor crítico revisa el programa de auditoría para evaluar si se ha alcanzado los objetivos establecidos (revisión y mejora).	El proveedor crítico cuenta con todas las políticas las cuales son auditadas interna y externamente siguiendo planes de auditoría basados en la información contenida en el programa de auditoría y en la documentación proporcionada por el proveedor.	El proveedor apoya y contribuye al mejoramiento continuo de auditoría priorizando las pruebas de seguridad de información y continuidad de negocios. Los cuales son auditados de manera interna (proveedor) y externa (empresa).

Tabla 24: Criterio: Auditoría

Fuente: Elaboración propia

4.2.2.6 Herramienta de evaluación

La herramienta de evaluación es una encuesta desarrollada en base a la matriz de evaluación. Esta encuesta consta de 30 preguntas referidas al gobierno de gestión de riesgos, gobierno de seguridad de información y gobierno de continuidad de negocios.

Cada pregunta consta de 5 respuestas las cuales tienen un puntaje máximo de 5 de acuerdo a la respuesta que seleccione el especialista encuestado. Luego de ello, los puntajes son llevados a una matriz en Excel donde se hacen cálculos para determinar el nivel de madurez de la organización respecto al gobierno de la gestión de riesgos y seguridad de TI.

4.2.2.6.1 Assessment

La evaluación refleja el nivel de actual de la organización respecto a la gestión de riesgos y seguridad de TI relacionado a sus proveedores críticos, es decir, relaciona los tres elementos (criterios de validación, nivel de madurez y elementos clave de la gestión de riesgos) mencionados a través de una matriz que permita realizar la evaluación.

Esta evaluación, mediante los puntajes obtenidos permite mostrar una representación gráfica de cómo es la situación actual de la organización, así como también permite interpretar e identificar dichos resultados para establecer un plan de acción para mejorar el nivel de madurez de la organización. Esta evaluación en algunos casos es de carácter confidencial, es decir, debido a la sensibilidad de la información que manejan las organizaciones de este sector, es necesario un acuerdo de confidencialidad entre la organización y los encargados del proyecto.

Para la evaluación, es importante que la organización cuente con un equipo de trabajo que tenga conocimientos en seguridad de la información; a ellos los denominaremos evaluadores. Estos deben contar con al menos uno de los siguientes perfiles en la organización para que puedan realizar la evaluación:

- Especialista en seguridad de la información.
- Oficial de Seguridad de Información.
- Analista de Seguridad de Información.
- Analista de Gestión de riesgos

Luego de la definición del equipo de evaluadores, la empresa esta apta para aplicar el modelo de gestión de riesgos; esto se realizará a través de la herramienta que se desarrolló en base a la matriz de evaluación. La idea es que la organización aplique el modelo de referencia contemplando todas las fases del modelo, esto significa la evaluación final.

Código	Pregunta	Respuesta	Puntaje
P1	¿La empresa tiene identificados a sus procesos y proveedores críticos de TI? ¿Se encuentran documentados o registrados? ¿La empresa entiende los procesos y conoce los productos o servicios que brindan estos proveedores?	R2	2
P2	¿Se encuentra establecido en la organización algún procedimiento para la identificación de procesos y proveedores críticos? ¿El procedimiento se encuentra documentado, divulgado dentro de la organización y en mejora continua?	R1	1
P3	¿La empresa cuenta con herramientas o sistemas donde se tenga un registro de los procesos y proveedores críticos de TI categorizados o clasificados? ¿Estos sistemas se prestan a la rápida obtención de la información, apoyando al análisis y toma de decisiones?	R1	1
P4	¿La empresa tiene identificados y clasificados los activos de TI que gestionan sus proveedores críticos?	R2	2
P5	¿Se encuentra establecido el procedimiento de identificación y registro de activos de TI? ¿Este procedimiento se encuentra documentado, divulgado y en mejora continua?	R2	2
P6	¿La empresa cuenta con herramientas o sistemas donde se tenga un registro de los activos de TI de la organización, clasificados o categorizados? ¿Estos sistemas se prestan a la rápida obtención de la información, apoyando al análisis y toma de decisiones?	R1	1
P7	¿La empresa tiene identificadas, clasificadas y valoradas las amenazas que afectan a sus activos de TI?	R2	2
P8	¿Se encuentra establecido algún procedimiento de identificación de amenazas que afectan a los activos de TI? ¿Este procedimiento se encuentra documentado, divulgado y en mejora continua?	R1	1
P9	¿La empresa cuenta con herramientas o sistemas donde se tenga un registro de las amenazas que afectan a los activos de TI clasificadas o categorizadas? ¿Estos sistemas se prestan a la rápida obtención de la información, apoyando al análisis y toma de decisiones?	R1	1
P10	¿La empresa cuenta con políticas o procedimientos de seguridad de la información? ¿En caso de ser afirmativo, cuáles son los puntos más importantes?	R1	1
P11	¿La organización tiene definida una política o procedimiento de gestión de riesgos que apoye a una adecuada gestión de la seguridad de información asociado a los activos, procesos y servicio de TI?	R1	1
P12	¿La organización cuenta con herramientas tecnológicas para gestionar de manera eficiente las amenazas asociadas a la seguridad de información?	R1	1

Tabla 25: Herramienta de evaluación

Fuente: Elaboración propia

Código respuesta	Puntaje
R1	1
R2	2
R3	3
R4	4
R5	5

Tabla 26: Herramienta de evaluación (Puntajes por pregunta)

Fuente: Elaboración propia

Luego de la aplicación de la herramienta, la organización es capaz de interpretar los resultados de cada score en base a la Tabla 26 desarrollada anteriormente, esto permite concluir en qué nivel de madurez se encuentra la misma en lo que respecta al gobierno de gestión de riesgos y seguridad de TI. En base a este resultado, se proponen controles para pasar a un siguiente nivel de madurez y la organización este mejor preparada para afrontar los riesgos que afectan a los procesos de TI.

CAPITULO 5   RESULTADO DEL PROYECTO

El capítulo cinco consta del detalle de los resultados del proyecto de investigación a través de la validación y el plan de continuidad del modelo. Se realiza la validación y pruebas del mismo a través de un caso de estudio en una PYME del sector comercial y a través de la evaluación de juicios de expertos, para finalizar con el análisis de los resultados de la implementación del modelo. Por último, se desarrolla un Plan de continuidad que asegure que el modelo sea escalable y por ende se mantenga en el tiempo pudiendo ser aplicado de manera continua por cualquier Pyme.

5.1 VALIDACIÓN DEL MODELO

La validación del modelo se realizó de dos formas: a través de un juicio de expertos y un caso de estudio real. En el juicio de expertos, se procederá a evaluar respecto a la matriz de los criterios de validación del modelo. Con esto se espera verificar que el modelo cumpla con las características establecidas en la motivación del trabajo y obtener oportunidades de mejora.

La segunda será una evaluación aplicando todas las fases del modelo en una PYME del sector comercial. Esta tendrá como resultados indicadores que permitirán medir la efectividad del modelo para resolver la necesidad identificada.

5.1.1 Juicio de expertos

El presente apartado se centra en la utilización del juicio de expertos como parte del proceso para la validación del modelo. Esta técnica debe realizarse de manera adecuada, ya que muchas veces constituye el único indicador de la validez de contenido respecto a un modelo de referencia. Actualmente el juicio de expertos es una práctica generalizada que requiere interpretar y aplicar sus resultados de manera acertada, eficiente y con toda la rigurosidad metodológica y estadística, para permitir que la evaluación basada en la información obtenida de la prueba pueda ser utilizada con los propósitos para la cual fue diseñada.

La validez del modelo generalmente se evalúa a través de un panel o un juicio de expertos, y en muy raras ocasiones la evaluación está basada en datos empíricos. En concordancia con esto, Utkin (2005) plantea que el juicio de expertos en muchas áreas es una parte importante de la información cuando las observaciones experimentales están limitadas.

El juicio de expertos se define como una opinión informada de personas con trayectoria en el tema, que son reconocidas por otros como expertos calificados en éste, y que pueden dar información, evidencia, juicios y valoraciones.

Para este punto es necesario tener en cuenta los criterios de validación respecto al modelo para su respectiva evaluación. Para ello, se debe considerar la formación académica de los expertos y su experiencia. El proceso de validación de juicio de expertos consta de la selección de jueces según criterios establecidos tales como años de experiencia, conocimientos, entre otros. Seguidamente, se elaboró una carta de presentación contenida por una breve descripción del modelo y la encuesta de valorización.

5.1.1.1 Perfil de los expertos

Los expertos que evaluarán el modelo de referencia deberán cumplir ciertos criterios a nivel de conocimientos y experiencia profesional como se detalla a continuación:

- **Formación académica:** Los expertos deberán contar con estudios superiores culminados.
- **Experiencia Profesional:** Los expertos deberán contar con experiencia en lo que se refiere a temas de seguridad de información y gestión de riesgos o cargos directivos concerniente a gestión de riesgos en diferentes empresas del medio.

5.1.1.2 Proceso de validación

Para realizar la validación por los expertos, se siguió un proceso que nos permitirá hacer dicha validación de manera óptima. Este proceso es el que se muestra en la figura 17. Los pasos son los siguientes:

- Proceso de selección de expertos
- Instrumento de evaluación
- Ejecución de la evaluación
- Análisis de resultados

Figura 17: Proceso de Juicio de Expertos

Fuente: Elaboración propia.

1. Selección de expertos

Para la validación se trabajó con profesionales especialistas en seguridad de información y amplia experiencia en el tema. Ello con el objetivo de garantizar que los criterios definidos aseguren el cumplimiento óptimo de cada fase y por ende cumpla con las necesidades del sector comercial al momento de su validación. Los expertos seleccionados para la evaluación se muestran a continuación en la siguiente Tabla 27:

Nº	Experto	Cargo actual	Conocimientos
1	Félix Ccoicca Sarmiento	Jefe de Riesgos y Cumplimiento TI - Interbank	▪ Gestión de Programa de Continuidad de Negocios ▪ Gestión de Riesgos TI ▪ Gobierno TI ▪ Gestión de Programa de Recuperación de Desastres
2	Willian Carrasco E.	Subgerente de Auditoría de Riesgos de Ciberseguridad - BCP	▪ Gobierno TI ▪ Gestión de Programa de Continuidad de Negocios
3	Rómulo Lomparte	Gerente general de ITG Consulting	▪ Information Security Manager (CISM) ▪ Risk and Information Systems Control (CRISC) ▪ COBIT 5 Foundation ▪ Gobierno TI ▪ Information Systems Auditor (CISA)
4	Marco Antonio Vía Escalante	Auditor Senior TI	▪ Cyber and IT Security Foundation ▪ Scrum Master ▪ ITIL Foundation v3
5	Christian Quispe Quispe	Especialista en Seguridad de la Información - Culqi	▪ Information Security Manager (CISM) ▪ COBIT 5 Foundation

			▪ Cisco Certified Network Associate Cyber Ops (CCNA Cyber Ops) ▪ Ethical Hacker - C EH

Tabla 27: Expertos para evaluación de criterios

Fuente: Elaboración propia

2. Instrumento de evaluación

El instrumento de evaluación fue una encuesta de valorización y juicio de expertos que está basada en un estudio realizado en Colombia sobre la validez de contenido y juicio de expertos (Escobar-Pérez, 2008). La encuesta es evaluada en base a cuatro categorías las cuales son:

- **Suficiencia:** Indicador que mide si los criterios de validación corresponden realmente a cada fase del modelo.
- **Claridad:** Indicador que mide si los criterios de validación definidos cuentan con la semántica y sintaxis adecuada.
- **Coherencia:** Indicador que mide la coherencia entre los criterios de validación y tienen relación directa con el modelo.
- **Relevancia:** Indicador que mide si todos los criterios de validación se consideran relativamente importantes para la medición del modelo

Estas categorías tienen una calificación en base a la matriz de criterios de validación (Matriz de evaluación). La calificación tiene 4 valores:

- 1: No cumple
- 2: Bajo nivel
- 3: Moderado nivel
- 4: Alto nivel

Cada calificación corresponde a cada categoría, donde el experto evaluará según su criterio luego de la revisión del modelo y la relación con los criterios de validación. Esto se desarrollará de manera confidencial. A continuación, se muestra la herramienta de evaluación (Tabla 28) que será evaluado por los expertos en seguridad de la información.

Categoría	Calificación	Indicador
Suficiencia	1. No cumple	Los criterios seleccionados no son suficientes para medir el modelo de referencia.
	2. Bajo nivel	Los criterios miden algún aspecto del modelo de referencia, pero no son suficientes.
	3. Moderado nivel	Se deben incrementar algunos criterios para poder evaluar todo el modelo de referencia.
	4. Alto nivel	Los criterios son lo suficientes y consistentes para medir el modelo de referencia.
Claridad	1. No cumple	Los criterios no están claros.
	2. Bajo nivel	Los criterios requieren varias modificaciones en el uso de las palabras de acuerdo con su significado o por la ordenación de las mismas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del criterio.
	4. Alto nivel	Los criterios son claros, tienen semántica y sintaxis adecuada.
Coherencia	1. No cumple	Los criterios no tienen relación lógica con el modelo de referencia.
	2. Bajo nivel	Los criterios tienen alguna relación lógica con el modelo de referencia.
	3. Moderado nivel	Los criterios tienen una relación moderada con el modelo de referencia que se está midiendo.
	4. Alto nivel	Los criterios se encuentran completamente relacionados con el modelo de referencia.
Relevancia	1. No cumple	Existen criterios que pueden ser eliminados sin que se vea afectado el modelo de referencia.
	2. Bajo nivel	Algunos criterios tienen relevancia, pero pueden ser reemplazados por otros perteneciente al modelo de referencia.
	3. Moderado nivel	Los criterios son relativamente importantes.
	4. Alto nivel	Los criterios son muy relevantes y deben ser incluidos para medir el modelo de referencia.

Tabla 28: Instrumento de evaluación

Fuente: Elaboración propia

3. Ejecución de la evaluación

La herramienta de evaluación fue desarrollada por los expertos, los cuales demoraron en responder un promedio de dos semanas. Las respuestas llegaron mediante emails o documentos en físico.

En la calificación por los expertos se obtuvo los siguientes resultados: Para más detalle revisar el “Anexo C – Resultados de la encuesta Juicio de expertos”.

Experto 1: Sr. Félix Ccoicca Sarmiento

Dominio	Criterio	Suficiencia	Claridad	Coherencia	Relevancia
1. Evaluación del riesgo	Procesos asociados a proveedores críticos de TI	3	3	3	4
	Activos de TI asociados a proveedores críticos	3	3	3	4
	Amenazas asociadas a los activos de TI	4	3	4	4
	Amenazas asociadas a la seguridad de información de la empresa	4	3	4	4
	Amenazas asociadas a la seguridad de información relacionado a proveedores críticos	4	3	4	4
	Impacto y riesgo	4	3	3	4
2. Tratamiento del riesgo	Establecimiento de controles	4	3	4	4
	Establecimiento de controles	4	3	4	4
3. Seguimiento y control	Monitoreo y control	4	3	4	4
	Auditorias	4	3	4	4

Tabla 29: Calificación experto 1

Fuente: Elaboración propia

Experto 2: Sr William Carrasco E.

Dominio	Criterio	Suficiencia	Claridad	Coherencia	Relevancia
1. Evaluación del riesgo	Procesos asociados a proveedores críticos de TI	4	4	4	4

	Activos de TI asociados a proveedores críticos	4	4	4	4
	Amenazas asociadas a los activos de TI	4	4	4	4
	Amenazas asociadas a la seguridad de información de la empresa	4	4	4	4
	Amenazas asociadas a la seguridad de información relacionado a proveedores críticos	4	4	4	4
	Impacto y riesgo	4	4	4	4
2. Tratamiento del riesgo	Establecimiento de controles	4	4	4	4
	Planes de tratamiento	4	4	4	4
3. Seguimiento y control	Monitoreo y control	4	4	4	4
	Auditorías	4	4	4	4

Tabla 30: Calificación experto 2

Fuente: Elaboración propia

Experto 3: Rómulo Lomparte

Dominio	Criterio	Suficiencia	Claridad	Coherencia	Relevancia
1. Evaluación del riesgo	Procesos asociados a proveedores críticos de TI	4	4	4	4
	Activos de TI asociados a proveedores críticos	4	4	4	4
	Amenazas asociadas a los activos de TI	4	4	4	4
	Amenazas asociadas a la seguridad de información de la empresa	4	4	3	4
	Amenazas asociadas a la seguridad de información relacionado a proveedores críticos	4	4	4	4
	Impacto y riesgo	4	4	4	4
2. Tratamiento del riesgo	Establecimiento de controles	4	4	4	3
	Planes de tratamiento	4	4	4	4
	Monitoreo y control	4	4	4	4

3. Seguimiento y control	Auditorias	4	4	4	4

Tabla 31: Calificación experto 3

Fuente: Elaboración propia

Experto 4: Marco Antonio Vía Escalante

Dominio	Criterio	Suficiencia	Claridad	Coherencia	Relevancia
1. Evaluación del riesgo	Procesos asociados a proveedores críticos de TI	3	4	3	3
	Activos de TI asociados a proveedores críticos	3	3	4	4
	Amenazas asociadas a los activos de TI	2	3	3	4
	Amenazas asociadas a la seguridad de información de la empresa	4	3	4	4
	Amenazas asociadas a la seguridad de información relacionado a proveedores críticos	2	3	3	4
	Impacto y riesgo	3	4	3	3
2. Tratamiento del riesgo	Establecimiento de controles	4	3	4	4
	Planes de tratamiento	3	3	3	3
3. Seguimiento y control	Monitoreo y control	2	3	3	2
	Auditorias	3	3	3	3

Tabla 32: Calificación experto 4

Fuente: Elaboración propia

Experto 5: Christian Quispe Quispe

Dominio	Criterio	Suficiencia	Claridad	Coherencia	Relevancia
1. Evaluación del riesgo	Procesos asociados a proveedores críticos de TI	3	2	4	4
	Activos de TI asociados a proveedores críticos	3	2	4	4
	Amenazas asociadas a los activos de TI	3	2	4	4

	Amenazas asociadas a la seguridad de información de la empresa	3	2	4	4
	Amenazas asociadas a la seguridad de información relacionado a proveedores críticos	3	2	4	4
	Impacto y riesgo	3	2	4	4
2. Tratamiento del riesgo	Establecimiento de controles	3	2	4	4
	Planes de tratamiento	3	2	4	4
3. Seguimiento y control	Monitoreo y control	3	2	4	4
	Auditorias	3	2	4	4

Tabla 33: Calificación experto 5

Fuente: Elaboración propia

4. Análisis de resultados

Luego de los resultados se hace la interpretación de las calificaciones; esta se hace por categorías y por fases del modelo para cada categoría. En donde se puede apreciar que la categoría con mayor puntaje es el de Relevancia (3.86), lo que significa que los expertos consideran que los criterios son muy relevantes y deben ser incluidos y la categoría con el menor puntaje es el de Claridad (3.24), lo que significa que los expertos sugieren una modificación muy específica de algunos de los términos del criterio.

Figura 18: Resultado por Categoría

Fuente: Elaboración propia

Finalmente, se realiza el análisis por fases para cada categoría; donde se puede observar que la fase con el puntaje más bajo es el de **“Tratamiento de riesgos”** y la fase con el puntaje más alto es la **“Evaluación del riesgo”**.

Figura 19: Resultado por Fases del modelo

Fuente: Elaboración propia

5.1.2 Aplicación del modelo en un caso de estudio

En esta sección se realiza la implementación del Proyecto “**Modelo de gestión de riesgos de seguridad de TI para PYMES del sector comercial que dependen de proveedores críticos**” en la empresa de estudio denominada **Kukyflor**.

La validación inicia con la aplicación del nivel de madurez al proceso de gestión de riesgos de seguridad de TI de la organización, siendo este transversal a todo el modelo ya que abarca las tres fases del mismo.

Con el objetivo de medir el nivel de madurez de la organización respecto al gobierno de gestión de riesgos y seguridad de TI, se aplica la herramienta assessment; la cual luego de la evaluación indicará el nivel actual y se propondrá controles de gobierno para pasar a un siguiente nivel de madurez.

Por otra parte, la validación del modelo se hace también a través del nivel de riesgo (activos de TI) para lo cual se hace uso de la metodología MAGERIT, para ello se sigue el proceso de implementación del modelo para gestionar los riesgos que afectan a los activos de TI. En esta parte se trabaja con los activos críticos de TI que tiene la organización y que dependen de proveedores críticos ya que es la parte fundamental que se debe proteger de las amenazas externas.

Luego de verificar los resultados de estas evaluaciones, se propone los controles para mitigar los riesgos más críticos a los cuales están expuestos los activos de TI identificados, además de proponer mejoras para los procedimientos y políticas relacionadas a la gestión del riesgo de la seguridad de la información. Finalmente, se obtiene el riesgo residual y se medirá los resultados obtenidos mediante indicadores.

Para ambos casos, tanto en la aplicación de la herramienta assessment y la aplicación de la metodología se medirá los resultados mediante indicadores de éxito, los cuales indicarán en qué medida la organización ha mejorado respecto a la gestión de riesgos de seguridad de TI.

Para obtener el nivel de madurez inicial (AS-IS) de la organización se aplicó la encuesta (herramienta de evaluación) basada en la matriz de evaluación que consta de 30 preguntas, las cuales tienen un determinado puntaje dependiendo de la respuesta obtenida durante su aplicación.

En lo que respecta al tiempo establecido para hacer el levantamiento de información por parte del evaluador, se estableció un tiempo aproximado de evaluación de 1 semana con 5 días laborales destinando el tiempo de una hora diaria, en donde luego de cada dos semanas se lleva a cabo una reunión para realizar el seguimiento respectivo del proceso de levantamiento de información.

5.1.2.1.1 Evaluación AS-IS

Los resultados de la encuesta y visitas en sitio fueron validados y corroborados en una matriz para luego tener un resultado final respecto a cada fase del modelo, el cual promediando estos puntajes nos indica el nivel de madurez inicial en el que se encuentra la organización en lo que respecta al gobierno de gestión de riesgos y seguridad de TI.

Asimismo, en el gráfico radial (Figura 21) se muestra el puntaje por criterios, donde se puede observar que el puntaje más bajo es 1.0 y el puntaje más alto es 1.67.

Figura 21: Puntaje por criterios AS-IS

Fuente: Elaboración propia

Finalmente, al promediar los puntajes por criterio de validación correspondiente a las 3 fases del modelo, se obtuvo como puntaje: 1.11, el cual según indica el “**capítulo 4.2.2.4 - Nivel de madurez**” se puede decir que la organización está en un nivel: “**Inicial o no desarrollado**”.

Puntaje	Nivel
1.11	Inicial o no desarrollado

Tabla 34: Evaluación AS-IS del nivel de madurez

Fuente: Elaboración propia

5.1.2.1.2 Evaluación TO-BE

Para incrementar el nivel de madurez de la organización y pasar a un siguiente nivel, se propuso controles de gobierno (Gobierno de: Gestión de riesgos, Seguridad de Información y Continuidad del negocio). Estos controles se basaron en los estándares ISO 31000, ISO 27001, ISO 22301 y las Circulares SBS: N° G-139, N° G-140.

A continuación (Tabla: 35 – 36 - 37) se muestran algunos de los controles propuestos.

Objetivo	Hallazgo	Nivel de riesgo	Sustento	Controles
1. Gestión del riesgo	La empresa carece de un procedimiento adecuado para evaluar los riesgos de los activos de TI	A	Magerit v3.0 ISO 31000: 2018	Desarrollar y documentar un procedimiento para la identificación, análisis y valoración de los riesgos asociados a los activos de TI
	La empresa carece de un procedimiento adecuado para el tratamiento de riesgos de los activos de TI	A	Magerit v3.0 ISO 31000: 2018	Desarrollar y documentar un procedimiento para seleccionar opciones de tratamiento, proponer controles y planes para reducir los riesgos asociados a los activos de TI
	Se carece de una política que apoye a una adecuada gestión de riesgos de los activos y procesos de TI de la organización	MA	Magerit v3.0 ISO 27001: 2013 Anexo: A.5.1.1	Diseñar y desarrollar una política con los lineamientos a cumplir para una adecuada gestión de riesgos de TI, la cual deberá ser aprobada, publicada y comunicada a los empleados y partes externas pertinentes por la alta dirección
		MA	ISO 27001: 2013 Anexo: A.5.1.2	Se deben revisar la política de gestión de riesgos de TI a intervalos planificados, o si se producen cambios significativos, para asegurar su conveniencia, suficiencia, y eficacia continua
	Se carece de una cultura organizacional en gestión de riesgos de TI	MA	ISO 27001: 2013 Anexo: A.7.2.2	Entrenamiento y charlas de concientización a todos los empleados de la organización, y en donde sea pertinente a los contratistas, sobre la importancia de la gestión de riesgos de los activos de TI
	La organización no tiene mucho conocimiento de los procesos, productos y servicios que les brindan los proveedores críticos de TI	M	ISO 27001: 2013 Anexo: A.8.1.1	Realizar y mantener un inventario de los productos y servicios que brindan los proveedores críticos de TI

Tabla 35: Controles para Gestión del riesgo

Fuente: Elaboración propia

Objetivo	Hallazgo	Nivel	Sustento	Controles
2. Gestión de Seguridad de Información	Se carece de una política de seguridad de la información que regule o norme las actividades de la organización.	MA	Circular N° 140 SBS - Gestión de la seguridad de la información	Definir una política de seguridad de información aprobada por la alta gerencia. Además, esta se debe comunicar a todos los empleados y a las partes externas pertinentes
			Estándar: ISO 27001 Anexo: A.5.1.2	Se deben revisar las políticas de seguridad de la información a intervalos planificados para asegurar su conveniencia, suficiencia, y eficacia continuas.
	La organización no tiene conciencia sobre la seguridad de la información. Ello se ve reflejado en algunos SLA'S que tienen con los proveedores críticos.	MA	Circular N° 140 SBS -Gestión de la seguridad de la información	Desarrollar actividades de concientización y entrenamiento en seguridad de información.
	Inexistencia de "política de protección de datos personales" que permita asegurar la privacidad y protección de la información de identificación personal	MA	Estándar: ISO 27001 Anexo: A.18.1.4	Se debe asegurar la privacidad y protección de la información de identificación personal, como se exige en la legislación y regulaciones pertinentes, donde corresponda.
	Inexistencia de inventario de activos de TI, lo cual imposibilita su identificación y dependencia entre estos	A	Circular N° 140 SBS -Gestión de la seguridad de la información	Realizar y mantener un inventario de activos asociados a la tecnología de información y asignar responsabilidades respecto a la protección de estos activos.
	El proceso de identificación de activos de TI se encuentra en desarrollo, lo cual hace que las amenazas puedan degradarlo en gran medida.	A	Estándar: ISO 27001 Anexo: A.8.1.3	Identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con la información y las instalaciones de procesamiento de información.
	Inexistencia de seguridad física y ambiental; lo cual facilita que una amenaza degrade con mayor facilidad los activos de TI de la organización	MA	Estándar: ISO 27001 Anexo: A.11.1.1	Se deben definir y utilizar perímetros de seguridad para proteger las áreas que contienen ya sea información sensible o crítica y las instalaciones de procesamiento de información.

Tabla 36: Controles para Gestión de Seguridad de información

Fuente: Elaboración propia

Objetivo	Hallazgo	Nivel	Sustento	Controles
3. Continuidad del negocio	La organización no tiene conciencia sobre la continuidad de negocios que garantice la resiliencia de esta ante cualquier amenaza a los activos de TI.	MA	Estándar: ISO 22301 Acápito: 7.4	La organización debe determinar la necesidad de comunicación interna y externa relevante para la gestión de un Plan de continuidad de negocios.
			Circular N° 139 SBS - Gestión de la Continuidad de negocios	La organización debe identificar los principales procesos, productos, servicios y proveedores, así como las actividades y recursos requeridos; evaluar los riesgos que podrían causar una interrupción de dichas actividades, y el impacto que podría tener dicha interrupción.
	Se carece de una política de continuidad de negocios que permita que la organización pueda recuperarse en el menor tiempo posible ante cualquier amenaza que puede afectar a los activos de TI asociado a proveedores críticos.	MA	Estándar: ISO 22301 Acápito: 5	Establecer una política para el sistema de gestión de la continuidad del negocio y que sea compatible con la dirección estratégica de la organización.
			Estándar: ISO 22301 Acápito: 5.3	La política de continuidad de negocio debe ser revisado para determinar su idoneidad continua a intervalos definidos y cuando se producen cambios significativos.

Tabla 37: Controles para la continuidad del negocio

Fuente: Elaboración propia

Luego que la empresa validó, aprobó y seleccionó los controles que puede implementar, se realizó una simulación del estado futuro de la empresa en base a la encuesta realizada al inicio de la evaluación obteniéndose nuevos resultados o nivel de madurez final (TO-BE). Los resultados se pueden observar en el siguiente diagrama radial, donde ahora el menor puntaje es de 1.33 y el mayor de 3.00.

Figura 22: Puntaje por criterios TO-BE
Fuente: Elaboración propia

Al promediar los nuevos puntajes por criterio correspondientes a las fases del modelo, obtenemos como nuevo resultado: **2.07**, lo cual indica que el nivel de madurez de la empresa de estudio pasó a ser **“Formalizado”**.

Puntaje	Nivel
2,07	Formalizado

Tabla 38: Evaluación TO-BE del nivel de madurez
Fuente: Elaboración propia

5.1.2.1.3 Indicadores de éxito del nivel de madurez

Para medir el éxito de esta evaluación se propusieron los siguientes indicadores:

Indicador de éxito	Puntaje AS-IS	Puntaje TO-BE	Resultado
% de incremento del nivel de madurez en la fase de evaluación del riesgo	1,33	2,39	79,17%
% de incremento del nivel de madurez en la fase de tratamiento del riesgo	1,00	2,33	133,33%
% de incremento del nivel de madurez en la fase de seguimiento y control	1,00	1,50	50,00%
% de incremento del nivel de madurez de la empresa en base al modelo	1,11	2,07	86,49%

Tabla 39: Indicadores de éxito del nivel de madurez

Fuente: Elaboración propia

Como se puede observar, luego de aplicar las recomendaciones y controles propuestos en la empresa de estudio Kukyflor, esta mejoró en un 86.49% en lo que respecta al gobierno de la gestión de riesgos y la seguridad de TI, temas transversales a todas las fases del modelo.

5.1.2.2 Nivel de riesgo (activos de TI)

Luego de finalizado la evaluación y sabiendo en qué nivel de madurez respecto al gobierno de gestión de riesgos y seguridad de TI se encuentra la organización, el siguiente paso es la aplicación del modelo a los activos de TI. Este proceso consiste en implementar las fases 1 y 2 del modelo de gestión de riesgos, para luego desarrollar el plan de tratamiento y proponer los controles que harán que el nivel de riesgo disminuya.

Para llevar a cabo este proceso, en primer lugar, es fundamental contar con un equipo que apoye constantemente en el desarrollo del proyecto, además de contar con un especialista en la organización con uno de los siguientes perfiles:

- Jefe de TI
- Analista de gestión de riesgos
- Especialista de seguridad de la información.

5.1.2.2.1 Evaluación del riesgo

Para medir el estado inicial de los riesgos en los activos de TI de la empresa de estudio (Kukyflor), debemos seguir los pasos de la fase de evaluación del riesgo del modelo, descrita en el punto 4.2.2.1.2.1 (A. Fase 1: “Evaluación del riesgo”).

En esta primera parte se aplicó la metodología Magerit, lo cual indica lo siguiente:

- Identificar los activos críticos de TI que dependen de proveedores críticos; para ello se realizó la valoración del activo.
- Identificar las amenazas significativas sobre aquellos activos de TI identificados. Se realizó la valoración de la amenaza en términos de probabilidad y degradación
- Identificar los controles existentes de la organización y la efectividad de su implementación
- Estimar el impacto y el riesgo

Se calculó el valor de los riesgos de los activos críticos de TI mediante el método cuantitativo de Magerit y se clasificaron según su nivel de criticidad tal como se puede observar en el siguiente mapa de calor:

Riesgo		Probabilidad				
		0,01	0,1	1	10	100
Impacto	$8 \leq I \leq 10$	A	MA	MA	MA	MA
	$5 \leq I < 8$	M	A	A	MA	MA
	$3 \leq I < 5$	B	M	M	A	A
	$2 \leq I < 3$	MB	B	B	M	M
	$0 < I < 2$	MB	MB	MB	B	B

Figura 23: Mapa de calor del nivel de riesgo

Fuente: Elaboración propia

El cálculo del riesgo potencial o inherente asociado a las amenazas que afectan a los activos de TI se muestra en la siguiente Tabla 40.

ID Activo	Nombre Activo Crítico	ID Amenaza	Nombre amenaza	Impacto	Probabilidad	Riesgo
A-HARD-001	Servidor Web	[A.1]	Difusión de software malicioso	4,14	0,1	0,41
		[A.2]	Manipulación de la configuración	6,44	1	6,44
		[E.1]	Uso del servidor de forma indebida	0,92	1	0,92
		[E.2]	Denegación del servicio	9,20	1	9,20
A-HARD-002	Servidor de base de datos	[A.3]	Ciberataques	4,61	0,1	0,46
		[A.4]	Acceso de personal no autorizado	4,80	1	4,80
		[A.5]	Alteración de la información	2,70	1	2,70
		[A.6]	Manipulación de los registros de actividad	5,85	100	585,00
		[E.3]	Errores de configuración	0,70	1	0,70
		[E.4]	Fuga de información	2,25	1	2,25
A-HARD-005	Servidor de aplicaciones	[A.1]	Difusión de software malicioso	3,41	0,1	0,34
		[A.4]	Acceso de personal no autorizado	3,41	1	3,41
		[E.5]	Falla del sistema /daño disco duro	3,96	1	3,96
		[E.6]	Manejo inadecuado de la información	1,91	1	1,91
		[E.7]	Caída del sistema por agotamiento de recursos	7,92	1	7,92

Tabla 40: Lista de riesgos potenciales de Kukyflor

Fuente: Elaboración propia

5.1.2.2.2 Tratamiento del riesgo

Luego de haber desarrollado el proceso anteriormente mencionado. Para establecer del plan de tratamiento, primero es necesario seleccionar la acción de tratamiento, para lo cual la empresa de estudio optó por mitigar los riesgos altos y muy altos asociados a los activos críticos de TI. Para ello, se propuso los siguientes controles basados en la metodología Magerit y el estándar ISO:27001, los cuales como se mencionó líneas arriba ayudarán a mitigar los riesgos de seguridad de TI y por consiguiente disminuir el nivel de riesgo.

ID Activo	Nombre Activo Crítico	ID Amenaza	Nombre amenaza	Impacto	Probabilidad	Riesgo	Controles propuestos	Sustento
A-HARD-001	Servidor Web	[A.2]	Manipulación de la configuración	6.4	1	6.4	- Revisar los derechos de acceso de los usuarios periódicamente - Se deben retirar los derechos de acceso de todos los empleados y usuarios externos a la información y al servidor, una vez que termine su relación laboral, contrato o acuerdo o se ajuste según el cambio	ISO 27001: 2013
		[E.2]	Denegación del servicio	9.2	1	9.2	- Solicitar al proveedor el mantenimiento y actualización periódica de los últimos parches de seguridad del sistema - Monitoreo de recursos de forma periódica	Magerit v3.0
A-HARD-002	Servidor de base de datos	[A.6]	Manipulación de los registros de actividad	5.9	100	585.0	- Se deben generar, mantener y revisar con regularidad los registros de eventos de las actividades del usuario, excepciones, faltas y errores - Emitir informes de las actividades del operador y del administrador del servidor, los registros se deben proteger y revisar con regularidad	ISO 27001: 2013
A-HARD-005	Servidor de aplicaciones	[E.7]	Caída del sistema por agotamiento de recursos	7.9	1	7.9	- Mantenimiento preventivo del servidor - Monitoreo de recursos de forma periódica	Magerit v3.0
A-HARD-010	Routers	[N.1]	Terremoto	8.4	0.1	0.8	- El equipo se debe ubicar y proteger para reducir los riesgos de peligros ambientales o desastres naturales - Proteger el cableado de energía y de telecomunicaciones que transporta datos o brinda soporte a servicios de información	ISO 27001: 2013

Tabla 41: Controles propuestos para los activos críticos de TI

Fuente: Elaboración propia

Una vez propuestos los controles, pasamos a la etapa de simulación de la implementación del plan de tratamiento del riesgo, donde se calculó el riesgo residual asociado a los activos críticos de TI en base a la efectividad de los controles.

Nombre amenaza	Valor del Activo	Degradación	Impacto	Eficacia controles sobre Impacto	Impacto residual	Probabilidad (Frecuencia)	Eficacia controles sobre Probabilidad	Probabilidad residual	Riesgo residual
Manipulación de la configuración	9.20	70%	6.44	65%	2.25	1	45%	0.55	1.24
Denegación del servicio	9.20	100%	9.20	50%	4.60	1	40%	0.60	2.76
Manipulación de los registros de actividad	9.00	65%	5.85	60%	2.34	100	50%	50.00	117.00
Caída del sistema por agotamiento de recursos	8.80	90%	7.92	55%	3.56	1	45%	0.55	1.96
Terremoto	8.40	100%	8.40	45%	4.62	0.1	0%	0.10	0.46
Suplantación de identidad	8.80	67%	5.90	60%	2.36	0.1	40%	0.06	0.14

Tabla 42: Lista de riesgo residual de Kukyflor

Fuente: Elaboración propia

Como se puede observar en la Tabla 42, el nivel de riesgo alcanzó un nivel aceptable luego de aplicados los controles propuestos.

Finalmente, haciendo una comparativa del riesgo inherente y riesgo residual, se nota una disminución del nivel de riesgo que afectan a los activos críticos de TI.

Activo	Amenaza	Valor Riesgo	Valor Riesgo Residual
Servidor Web	Manipulación de la configuración	6.44	1.24
	Denegación del servicio	9.20	2.76
Servidor de base de datos	Manipulación de los registros de actividad	585	117
Servidor de aplicaciones	Caída del sistema por agotamiento de recursos	7.92	1.96
Router	Terremoto	0.84	0.46
Sistema de ventas	Suplantación de identidad	0.59	0.14
	Caída del sistema por agotamiento de recursos	7.04	1.55
	Ausencia de soporte técnico	5.28	1.19

Tabla 43: Comparativa: Riesgo inherente vs Riesgo residual

Fuente: Elaboración propia

5.1.2.2.3 Indicador de éxito del nivel de riesgo

Para medir el éxito de la mejora del nivel de riesgo en los activos de TI de la empresa de estudio, se propuso el siguiente indicador:

Indicador de éxito	Riesgo inherente	Riesgo residual	Resultado
% de disminución del nivel de riesgo en los activos de TI	50,34	10,34	79,46%

Tabla 44: Indicador de éxito del nivel de riesgo Kukyflor

Fuente: Elaboración propia

Como se puede observar, luego de la simulación de la implementación del plan de tratamiento, el nivel del riesgo en los activos de TI mejoró en un 79.46%, lo cual demuestra cuantitativamente la efectividad del modelo propuesto para resolver la necesidad identificada.

5.2 PLAN DE CONTINUIDAD DEL PROYECTO

La presente sección se enfoca en el plan de continuidad, la cual es desarrollada en la etapa de ejecución del Proyecto **MODELO DE GESTIÓN DE RIESGOS DE SEGURIDAD DE TI PARA PYMES DEL SECTOR COMERCIAL QUE DEPENDEN DE PROVEEDORES CRÍTICOS**. Para ello se establecen lineamientos que permiten que el modelo se mantenga vigente en el tiempo, por lo que debe estar alineado a la mejora continua. Con esto, se asegura la continuidad y actualización del modelo.

Para el plan de continuidad del proyecto se abarcan los siguientes puntos:

- Etapas del modelo de Referencia
- Estrategia de continuidad del modelo
- Implementación del modelo
- Actualización del modelo

5.2.1 ETAPAS DEL MODELO DE REFERENCIA

El proceso de gestión de riesgos debe ser repetitivo pues los sistemas de información rara vez son inmutables; más bien se encuentran sometidos a evolución continua tanto propia (nuevos activos) como del entorno (nuevas amenazas), lo que exige una revisión periódica en la que se aprende de la experiencia y se adapta al nuevo contexto.

La propuesta del modelo de gestión de riesgos de seguridad de TI formaliza cuatro etapas cíclicas:

5.2.1.1 Plan (planear)

En esta etapa se desarrolla la planificación de la implementación del modelo de gestión de riesgos de seguridad de TI. Para ello se realiza los siguientes procesos:

- Cronograma de Implementación del modelo
- Reunión con los interesados
- Formación de equipos de trabajo

5.2.1.2 Do (Hacer)

En esta etapa la empresa realiza la aplicación del modelo de gestión de riesgos de seguridad de TI, para ello se hace una recolección de información a través de entrevistas, encuestas y observaciones en sitio; a través del cual se identificarán las entradas que nos servirán para la aplicación de los 2 niveles de riesgos propuestos: Nivel de madurez y Nivel de riesgo (Activos de TI).

Para el nivel de madurez, se aplicará la herramienta assessment para identificar el nivel de madurez actual en el que se encuentra la organización respecto a la gestión de riesgos y seguridad de TI relacionado a sus proveedores críticos. Luego de la evaluación inicial se realiza una propuesta de controles con el objetivo de pasar a un siguiente nivel de madurez. Finalmente se realiza una comparativa en base al nivel de madurez inicial y final observándose un incremento en el mismo.

Por otro lado, se desarrollará las fases del modelo de gestión de riesgos de seguridad de TI, para lo cual se sigue lo que indica la metodología MAGERIT, donde el componente principal son los activos de TI de la empresa y que están asociados a proveedores críticos. Luego de la evaluación, el modelo muestra el riesgo inherente de la organización. Para reducir el riesgo a un nivel residual se hace una propuesta de planes y controles que permitirá mitigar dichos riesgos identificados inicialmente a través de un plan de remediación. A partir de los planes y controles propuestos se generan indicadores que permiten validar el tratamiento del riesgo.

Para ambas aplicaciones (nivel de madurez y nivel de riesgo de los activos de TI) la empresa se encargará de priorizar la implementación de los planes y controles propuestos según sus capacidades en el corto, mediano y largo plazo.

5.2.1.3 Check (Verificar)

El modelo de gestión de riesgos de seguridad de TI para PYMES del sector comercial que dependen de proveedores críticos es cíclico e iterativo por lo que se recomienda ser tratado anualmente.

El proceso de verificación consiste en asegurarse que los planes y controles propuestos en la aplicación del modelo sean implementados por la organización; para ello se debe hacer una revisión periódica a través de una auditoría de cumplimiento.

Asimismo, en esta etapa se recomienda realizar actividades de “seguimiento y control” que aseguren en lo posible el cumplimiento del establecimiento de los planes y controles propuestos luego de la aplicación del modelo.

Existen estándares para la realización de auditorías, por ejemplo: el estándar ISO 19011 (Gestión de la auditoría de Sistemas de información) para asegurar el cumplimiento de la implementación de los controles. Lo que se va a realizar es auditar el cumplimiento de la implementación de los controles propuestos. Finalizado la auditoría se realiza un informe el cual indica el nivel de madurez que tiene la organización producto del cumplimiento de los controles propuestos.

5.2.1.4 Act (actuar)

Producto del informe de “seguimiento y control” y las auditorías realizadas en la fase anterior se obtienen acciones correctivas, cuya implementación debe planificarse en un plan de remediación de observaciones de acciones correctivas que debe ser realizado por la organización en un lapso de tiempo determinado.

Una acción correctiva, es cualquier política o lineamiento que se encuentra dentro de los controles propuestos y que la empresa luego del informe de “seguimiento y control” o auditoría no ha logrado cumplir. Para la siguiente auditoría esas acciones debieron ser levantadas, y por ende sale un nuevo informe que indica que la organización está en un nivel de madurez superior al anterior.

Figura 24: Ciclo PDCA

Fuente: Shona D. Morgan, Alice C. Stewart

5.2.2 Estrategia de continuidad del modelo

La estrategia de continuidad del modelo que asegura la vigencia del mismo en el tiempo, se define en los siguientes procesos:

5.2.2.1 Seguimiento y control

Este proceso consiste en que un especialista de seguridad de información realice revisiones al estado de la implementación del modelo (“Modelo de gestión de riesgos de seguridad de TI para Pymes del sector comercial que dependen de proveedores críticos”) de manera periódica a fin de verificar el cumplimiento de las recomendaciones propuestas. Se recomienda hacerlo cada 3 meses a fin de estar más en contacto con los interesados del proyecto y absolver cualquier inquietud que este tenga.

Asimismo, el especialista en seguridad puede realizar un seguimiento a toda la organización mediante diferentes maneras como:

- Observaciones
- Entrevistas

- Reuniones con el especialista de TI

Con este proceso, se puede asegurar el cumplimiento de las recomendaciones, por ende, la organización se encuentre mejor preparada para el siguiente proceso que son las auditorias que pueden ser internas (auditoria de primera parte) o externas (auditoria de tercera parte). Para nuestro caso se desarrollará la auditoria externa.

Al finalizar el proceso de seguimiento y control, el especialista de seguridad realiza un informe que será remitido a la alta gerencia de la organización, el cual deberá tomar acciones para hacer cumplir las recomendaciones. Estas acciones son las siguientes:

- La alta gerencia comunicara a todas las áreas de la organización la importancia de realizar las recomendaciones propuestas.
- Se formará un comité de personas responsables lideradas por el Gerente general a fin de hacer cumplir las recomendaciones establecidas
- Se realizará charlas de concientización respecto a los riesgos y seguridad de información. Estas charlas pueden darse de manera continua. A medida que se implementen las recomendaciones estas pueden disminuir.

5.2.2.2 Auditorias de cumplimiento

Las auditorias aseguran el cumplimiento de los planes y controles propuestos y la organización evolucione con el modelo de referencia. De esta manera se asegura la aplicabilidad y el cumplimiento del modelo en la organización.

En realidad, es incierto saber si la empresa ha implementado algunos o todas las recomendaciones sugeridas, por ello es que se tiene que validar con una auditoría para verificar hasta qué punto se ha cumplido la implementación de estos. Las auditorias terminan en un informe de auditoría, la cual deberán ser subsanadas para la auditoria posterior. Para ello la organización debe desarrollar un plan de remediación y observación la cual debe ser validada e implementada luego de la auditoria.

Producto de las auditorias, la organización estará en la capacidad de pasar a un siguiente nivel de madurez mejorando sus procesos de gestión de riesgos. Esto permitirá que la misma sea resiliente a las amenazas que pueden afectar la continuidad de sus operaciones y tenga menos impacto económico y daños en la reputación.

La auditoría no solo se realiza para verificar que los controles se están cumpliendo, en la auditoría también se deberá revisar que todo esté debidamente documentado y validado. Este es un proceso muy importante, ya que asegura el cumplimiento de la implementación de los controles propuestos. Para ello, se apoya de algunos criterios del estándar **ISO 19011: Directrices para la Auditoría de los Sistemas de Gestión**.

Esta norma proporciona orientación sobre sistemas de gestión de auditoría, incluidos los principios de auditoría, la gestión de un programa de auditoría y la realización de auditorías del sistema de gestión, así como orientación sobre la evaluación de la competencia de las personas involucradas en el proceso de auditoría, incluida la persona que gestiona la auditoría, auditores y equipos de auditoría.

5.2.2.2.1 Cláusula 6 - ISO 19011

Para el apoyo en la auditoría se hace uso de la cláusula 6 del estándar ISO 19011, denominado **“Realización de una auditoría”**. Esta cláusula define las guías para organizar y realizar una auditoría conforme al programa establecido por esta norma. Se describe a continuación el acápite:

Cláusula 6.2: Inicio de la auditoría

6.2.1 Generalidades

Cuando se inicia una auditoría, la responsabilidad de llevar a cabo la auditoría corresponde al líder del equipo auditor designado hasta que la auditoría finaliza.

Para iniciar una auditoría, deberían considerarse los pasos de la Figura 25; sin embargo, la secuencia puede diferir dependiendo del auditado, de los procesos y de las circunstancias específicas de la auditoría.

6.2.2 Establecimiento del contacto inicial con el auditado

El contacto inicial con el auditado para la realización de la auditoría puede ser informal o formal y debería realizarse por el líder del equipo auditor. Los propósitos del contacto inicial son los siguientes:

- *establecer comunicaciones con los representantes del auditado;*
- *confirmar la autoridad para llevar a cabo la auditoría;*

- *proporcionar información sobre los objetivos de la auditoría, el alcance, los métodos y la composición del equipo auditor, incluyendo los expertos técnicos;*
- *solicitar acceso a los documentos y registros pertinentes con propósitos de planificación;*
- *determinar los requisitos legales y contractuales aplicables y otros requisitos pertinentes para las actividades y productos del auditado;*
- *confirmar lo acordado con el auditado respecto al grado de difusión y al tratamiento de la información confidencial;*
- *hacer los preparativos para la auditoría incluyendo la programación de las fechas;*
- *determinar los requisitos específicos de la ubicación en cuanto al acceso seguridad, salud y protección u otros requisitos especiales;*
- *acordar la asistencia de observadores y la necesidad de guías para el equipo auditor;*
- *determinar cualquier área de interés o preocupación para el auditado en relación con la auditoría específica.*

6.2.3 Determinación de la viabilidad de la auditoría

Debería determinarse la viabilidad de la auditoría para proporcionar la confianza razonable en que los objetivos de la auditoría pueden alcanzarse.

La determinación de la viabilidad debería tener en cuenta factores tales como la disponibilidad de lo siguiente:

- *la información suficiente y apropiada para planificar y llevar a cabo la auditoría;*
- *la cooperación adecuada del auditado;*
- *el tiempo y los recursos adecuados para llevar a cabo la auditoría.*

Cuando la auditoría no es viable, debería proponerse al cliente de la auditoría una alternativa, de acuerdo con el auditado.

6.3 Preparación de las actividades de auditoría

6.3.1 Realización de la revisión de la documentación en la preparación de la auditoría

Debería revisarse la documentación pertinente del sistema de gestión del auditado para:

- *reunir información para preparar las actividades de auditoría y los documentos de trabajo aplicables, por ejemplo, sobre procesos, funciones;*

- *establecer una visión general del grado de la documentación del sistema para detectar posibles carencias;*

6.3.2 Preparación del plan de auditoría

6.3.2.1 El líder del equipo auditor debería preparar un plan de auditoría basado en la información contenida en el programa de auditoría y en la documentación proporcionada por el auditado. El plan de auditoría debería considerar el efecto de las actividades de auditoría en los procesos del auditado y proporcionar la base para el acuerdo entre el cliente de la auditoría, el equipo auditor y el auditado en lo relativo a la realización de la auditoría. El plan debería facilitar la programación en el tiempo y la coordinación eficientes de las actividades de auditoría a fin de alcanzar los objetivos.

6.3.2.2 El grado de detalle y el contenido del plan de auditoría pueden diferir, por ejemplo, entre la auditoría inicial y las posteriores, así como entre las auditorías internas y externas. El plan de auditoría debería ser lo suficientemente flexible para permitir los cambios que pueden hacerse necesarios a medida que las actividades de auditoría se vayan llevando a cabo.

6.3.3 Asignación de las tareas al equipo auditor

El líder del equipo auditor, consultando con el equipo auditor, debería asignar a cada miembro del equipo la responsabilidad para auditar procesos, actividades, funciones o lugares específicos. Tales asignaciones deberían tener en cuenta la independencia y la competencia de los auditores y el uso eficaz de los recursos, así como las diferentes funciones y responsabilidades de los auditores, los auditores en formación y los expertos técnicos.

6.3.4 Preparación de los documentos de trabajo

Los miembros del equipo auditor deberían recopilar y revisar la información pertinente a las tareas de auditoría asignadas y preparar los documentos de trabajo, según sea necesario, para referencia y registro de evidencias de la auditoría. Tales documentos de trabajo pueden incluir lo siguiente:

- *listas de verificación;*
- *planes de muestreo de auditoría;*
- *formularios para registrar la información, tales como evidencias de apoyo, hallazgos de la auditoría y*

- registros de las reuniones.

6.4 Realización de las actividades de auditoría

6.4.1 Generalidades

Normalmente las actividades de auditoría se realizan en una secuencia definida como se indica en la Figura 25. Esta secuencia puede variar para adaptarse a las circunstancias de auditorías específicas.

6.4.2 Realización de la reunión de apertura

El propósito de la reunión de apertura es:

- *confirmar el acuerdo de todas las partes (por ejemplo, auditado, equipo auditor) sobre el plan de auditoría,*
- *presentar al equipo auditor, y*
- *asegurarse de que se pueden realizar todas las actividades de auditoría planificadas.*

6.4.3 Realización de la revisión de la documentación durante la auditoría

La documentación pertinente del auditado debería revisarse para:

- *determinar la conformidad del sistema con los criterios de auditoría, con base en la documentación disponible;*
- *reunir información para apoyar las actividades de auditoría.*

6.4.4 Comunicación durante la auditoría

Durante la auditoría, puede ser necesario llegar a acuerdos formales para la comunicación dentro del equipo auditor, así como con el auditado, el cliente de la auditoría y potencialmente con organismos externos (por ejemplo, autoridades reglamentarias), especialmente cuando los requisitos legales exijan la comunicación obligatoria de los no cumplimientos.

El equipo auditor debería reunirse periódicamente para intercambiar información, evaluar el progreso de la auditoría y reasignar las tareas entre los miembros del equipo auditor, según sea necesario.

6.4.5 Asignación de funciones y responsabilidades de los guías y los observadores

Los guías y los observadores (por ejemplo, una autoridad reglamentaria u otras partes interesadas) pueden acompañar al equipo auditor. No deberían influir ni interferir en la realización de la auditoría. Si esto no se puede asegurar, el líder del equipo auditor debería tener el derecho de negarse a que los observadores tomen parte en ciertas actividades de auditoría.

Para los observadores, cualquier obligación en relación con la salud y la protección, la seguridad y la confidencialidad deberían gestionarse entre el cliente de la auditoría y el auditado.

Los guías, designados por el auditado, deberían asistir al equipo auditor y actuar cuando lo solicite el líder del equipo auditor. Sus responsabilidades deberían incluir lo siguiente:

- *ayudar a los auditores a identificar a las personas que participarán en las entrevistas y a confirmar los horarios;*
- *acordar el acceso a ubicaciones específicas del auditado;*
- *asegurarse de que las reglas concernientes a los procedimientos relacionados con la protección y la seguridad de las ubicaciones, son conocidas y respetadas por los miembros del equipo auditor y los observadores.*

6.4.6 Recopilación y verificación de la información

Durante la auditoría, debería recopilarse mediante un muestreo apropiado y verificarse la información pertinente a los objetivos, el alcance y los criterios de la misma, incluyendo la información relativa a las interrelaciones entre funciones, actividades y procesos. Sólo la información que es verificable debería aceptarse como evidencia de la auditoría. Debería registrarse la evidencia que conduce a hallazgos de la auditoría. Si, durante la recopilación de evidencias, el equipo auditor es consciente de cualquier circunstancia de riesgo nuevo o que ha cambiado, el equipo debería tratarlo en consecuencia.

6.4.7 Generación de hallazgos de la auditoría

La evidencia de la auditoría debería evaluarse frente a los criterios de auditoría para determinar los hallazgos de la auditoría. Los hallazgos de la auditoría pueden indicar conformidad o no conformidad con los criterios de auditoría. Cuando lo especifique el plan de auditoría, los hallazgos de una auditoría individual deberían incluir la conformidad y las buenas prácticas junto con la evidencia que los apoya, las oportunidades de mejora y cualquier recomendación para el auditado.

Deberían registrarse las no conformidades y la evidencia de la auditoría que las apoya. Las no conformidades pueden clasificarse. Deberían revisarse con el auditado para reconocer que la evidencia de la auditoría es exacta y que las no conformidades se han comprendido. Se debería realizar todo el esfuerzo posible para resolver cualquier opinión divergente relativa a las evidencias o a los hallazgos de la auditoría, y deberían registrarse los puntos para los que no haya acuerdo.

6.4.8 Preparación de las conclusiones de la auditoría

El equipo auditor debería reunirse antes de la reunión de cierre para:

- *revisar los hallazgos de la auditoría y cualquier otra información apropiada recopilada durante la auditoría frente a los objetivos de la misma;*
- *acordar las conclusiones de la auditoría, teniendo en cuenta la incertidumbre inherente al proceso de auditoría;*
- *preparar recomendaciones, si estuviera especificado en el plan de auditoría;*
- *comentar el seguimiento de la auditoría, cuando sea aplicable.*

6.4.9 Realización de la reunión de cierre

La reunión de cierre, facilitada por el líder del equipo auditor, debería realizarse para presentar los hallazgos y las conclusiones de la auditoría. Entre los participantes en la reunión de cierre debería incluirse a los representantes de la dirección del auditado y, cuando sea apropiado, a aquellos responsables de las funciones o procesos que se han auditado, y también puede incluirse al cliente de la auditoría y otras partes.

Si es aplicable, el líder del equipo auditor debería prevenir al auditado de las situaciones encontradas durante la auditoría que pueden disminuir la confianza en las conclusiones de la auditoría. Si está definido en el sistema de gestión o por acuerdo con el cliente de la auditoría, los participantes deberían acordar el periodo de tiempo para un plan de acción que trate los hallazgos de la auditoría.

El grado de detalle debería ser coherente con la familiaridad del auditado con el proceso de auditoría. Para algunas situaciones de auditoría, la reunión puede ser formal y las actas, incluyendo los registros de asistencia, deberían conservarse. En otras situaciones, por ejemplo, en auditorías internas, la reunión de cierre es menos formal y puede consistir sólo en comunicar los hallazgos de la auditoría y las conclusiones de la misma.

6.5 Preparación y distribución del informe de auditoría

6.5.1 Preparación del informe de auditoría

El líder del equipo auditor debería informar de los resultados de la auditoría de acuerdo con los procedimientos del programa de auditoría.

El informe de auditoría debería proporcionar un registro completo, preciso, conciso y claro de la auditoría, y debería incluir o hacer referencia a lo siguiente:

- *los objetivos de la auditoría;*
- *el alcance de la auditoría, particularmente la identificación de las unidades de la organización y de las unidades funcionales o los procesos auditados;*
- *la identificación del cliente de la auditoría;*
- *la identificación del equipo auditor y de los participantes del auditado en la auditoría;*
- *las fechas y ubicaciones donde se realizaron las actividades de auditoría;*
- *los criterios de auditoría;*
- *los hallazgos de la auditoría y las evidencias relacionadas;*
- *las conclusiones de la auditoría;*
- *una declaración del grado en el que se han cumplido los criterios de la auditoría;*

6.5.2 Distribución del informe de auditoría

El informe de auditoría debería emitirse en el periodo de tiempo acordado. Si se retrasa, las razones deberían comunicarse al auditado y a la persona responsable de la gestión del programa de auditoría.

El informe de auditoría debería estar fechado, revisado y aprobado, cuando sea apropiado, de acuerdo con los procedimientos del programa de auditoría.

A continuación, el informe de la auditoría debería distribuirse a los receptores, tal y como se define en los procedimientos de auditoría o en el plan de auditoría.

6.6 Finalización de la auditoría

La auditoría finaliza cuando se hayan realizado todas las actividades de auditoría planificadas, o si se ha acordado de otro modo con el cliente de la auditoría (por ejemplo, podría haber una situación inesperada que impida que la auditoría se finalice de acuerdo con el plan).

Los documentos pertenecientes a la auditoría deberían conservarse o destruirse de común acuerdo entre las partes participantes y de acuerdo con los procedimientos del programa de auditoría y los requisitos aplicables.

Salvo que se requiera por ley, el equipo auditor y la persona que gestiona el programa de auditoría no deberían revelar el contenido de los documentos, otra información obtenida durante la auditoría ni el informe de auditoría a ninguna otra parte, sin la aprobación explícita del cliente de la auditoría y, cuando sea apropiado, la del auditado. Si se requiere revelar el contenido de un documento de la auditoría, el cliente de la auditoría y el auditado deberían ser informados tan pronto como sea posible.

6.7 Realización de las actividades de seguimiento de una auditoría

Las conclusiones de la auditoría pueden, dependiendo de los objetivos de la auditoría, indicar la necesidad de correcciones, o de acciones correctivas, preventivas o de mejora. Tales acciones generalmente son decididas y emprendidas por el auditado en un intervalo de tiempo acordado. Cuando sea apropiado, el auditado debería mantener informada a la persona responsable de la gestión del programa de auditoría y al equipo auditor sobre el estado de estas acciones.

Debería verificarse si se completaron las acciones y su eficacia. Esta verificación puede ser parte de una auditoría posterior.

Figura 25: Actividades típicas de auditoría

Fuente: ISO 19011 - Directrices para la auditoría de los sistemas de gestión

El informe de auditoría presenta el nivel de madurez de la organización en gestión de riesgos de seguridad de TI orientados a proveedores críticos. Generalmente las empresas no implementan todas las recomendaciones sugeridas, de hecho, la principal restricción es la económica, razón por la cual salen algunas acciones correctivas las cuales deberán ser corregidas para la siguiente auditoría.

Es importante mencionar que se debe aplicar el modelo de manera periódica, recomendable luego de cada auditoria (cada año), esto hará posible la aparición de nuevas recomendaciones que la organización deberá implementar en el siguiente año.

5.2.3 Implementación del modelo

5.2.3.1 Planificación de implementación

Esta referido al plan de trabajo que se debe seguir para la aplicación del modelo. Este consta de los siguientes pasos:

1. Obtener información

Se inicia con el proceso de recabar información de la organización. Se hace hincapié de los criterios más importantes que nos servirán para la implementación del modelo. Esto es información de: procesos de negocios, activos de TI, políticas de seguridad, gestión de riesgos y plan de continuidad, etc. Toda esta información se recoleta mediante lo siguiente:

- Solicitud documentos (políticas, planes, normas, etc.)
- Entrevistas
- Encuestas
- Reuniones

2. Planificación

Etapa que consiste en hacer una planificación detallada de la aplicación del modelo. Consiste en preparar a la organización para llevar a cabo la implementación. Esto se hace a través de las siguientes actividades:

- Reuniones con la alta gerencia y los empleados de la organización acerca de la Implementación del modelo
- Reuniones con los proveedores críticos de TI con los que cuenta la organización e informar acerca de la implementación
- Capacitación de los empleados de la organización a fin de que puedan apoyar en todo momento durante la implementación del modelo
- Preparar los formatos necesarios para que sean aplicados durante la implementación
- Selección del equipo de trabajo encargado de la implementación del modelo

3. Ejecución

Es la etapa durante el cual se desarrolla la aplicación del modelo. La aplicación del mismo dura un mes, durante el cual se llevan a cabo distintas tareas y se trabaja en conjunto con los responsables de la organización formalizando reuniones cada cierto tiempo para realizar una correcta implementación.

Una vez finalizado la aplicación del modelo se proponen planes y controles para que puedan ser implementados por la organización en un determinado periodo de tiempo y en consecuencia esta pueda mitigar los riesgos identificados y se encuentre mejor preparado para afrontar posibles eventos de pérdida adecuadamente.

Luego de la ejecución del modelo salen los resultados finales los cuales serán analizados por los jefes de proyecto y serán reflejados en un informe final.

4. Informe

En esta etapa se realiza un informe general producto de la aplicación del modelo. Es el resultado del análisis de: indicadores de gestión de riesgo, nivel de madurez respecto al gobierno de gestión de riesgos y seguridad de TI y el nivel de riesgos respecto a los activos de TI que dependen de proveedores críticos. Asimismo, se presentan los planes y controles propuestos los cuales se sustentan en diferentes estándares ISO, la metodología en estudio (MAGERIT) y las Circulares de la Superintendencia de Banca y Seguros (SBS).

Estos planes y controles deberán ser implementados en la organización a través de un plan de implementación de controles que será desarrollada por la misma y verificada cada cierto tiempo a través de un seguimiento y control y auditorias de cumplimiento.

5. Presentación

Finalmente, luego del informe final se hace la presentación del mismo a la alta gerencia que estará en la facultad de implementar los planes y controles propuestos a corto, mediano o largo plazo. Esto dependerá de la viabilidad económica de la empresa por lo que es su decisión hacer la implementación de todos los controles propuestos o en su defecto hacerlo gradualmente. Todo ello se ve reflejado en el Plan de implementación que deberá ser desarrollado por la organización.

La presentación deberá realizarse de manera formal y usando un lenguaje acorde a la alta gerencia, de manera que ellos puedan entender fácilmente todo el informe y en su defecto puedan tomar la mejor decisión para implementar de una manera adecuada todos los controles propuestos y de esta forma lograr los objetivos propuestos por la organización.

Figura 26: Cronograma de actividades implementación del modelo

Fuente: Elaboración propia

5.2.3.2 Aplicación del modelo

Son los pasos que se debe seguir para la implementación del modelo de referencia. Para este punto se hace uso del documento Implementación del modelo, la cual se encuentra en el documento denominado: “MGRSTI - Guía Aplicación Modelo v.2.0.”

Figura 27: Pasos a seguir para la implementación del modelo

Fuente: Elaboración propia

5.2.3.3 Monitoreo

Luego de la aplicación del modelo se deben cumplir los planes y controles propuestos, para ello se realiza las siguientes actividades:

- **Seguimiento y control**

Consiste en verificar el estado de la implementación de los planes y controles propuestos en la etapa de la aplicación del modelo. Con esto se asegura que la organización se encuentre mejor preparada para una auditoría. Para más detalle revisar el punto “**5.2.2.1: Seguimiento y control**”.

- **Auditorías de cumplimiento**

Esta referido a las auditorías externas que se realiza para garantizar el cumplimiento de los planes y controles propuestos. Se recomienda hacerlo cada año. Para más detalle revisar el punto “**5.2.2.2: Auditorías de cumplimiento**”.

5.2.3.4 Plan de remediación y acciones correctivas

El resultado final de la auditoria es el informe de auditoría, donde se establece las acciones correctivas que deberán ser subsanadas por la organización. Para la implementación de dichas acciones se realiza un Plan de remediación en el cual se detalla cómo se procederá a su cumplimiento. Esto es realizado por la organización en conjunto con el especialista de TI y el analista de seguridad. Ello asegura una adecuada ejecución del cumplimiento de dichas acciones correctivas y por ende un incremento en el nivel de madurez de la organización en respecto a la gestión de riesgos y seguridad de TI.

5.2.4 Actualización del modelo

El modelo de gestión de riesgos de seguridad de TI está conformado por estos componentes: estándares, normativas, metodología. Con el paso del tiempo cualquiera de estos puede surgir cambios o actualizaciones por lo que el modelo debe estar en la capacidad de adaptarse a estos cambios. Para ello, se debe hacer un análisis de estos, como también evaluar el impacto de dichos cambios en el modelo para ver si es posible su implementación.

Para esta parte, se definen los siguientes criterios:

- 1. Lineamientos para la actualización del modelo**

Se debe seguir determinados lineamientos que harán posible que el modelo este apto para afrontar los posibles cambios o actualizaciones de cualquier componente del mismo, estos son:

- Se recomienda que el modelo sea revisado por lo menos una vez al año, para alinear este con los cambios menores que se han dado hasta la fecha.
- El modelo debe ser revisado por lo menos cada 3 años, o cuando exista un cambio significativo referido a normas, metodologías o estándares que a su vez deben ser evaluados dependiendo del impacto que causa.
- Se debe hacer una revisión continua de los componentes del modelo, ya que estos pueden cambiar o actualizarse en cualquier momento
- La organización debe mejorar de manera continua la conveniencia, suficiencia y efectividad del modelo de referencia. Esto es parte del plan de continuidad del modelo de referencia.

2. Actualizaciones

2.1 Estándares y Leyes

En el modelo presentado en el proyecto **“Modelo de gestión de riesgos de seguridad de ti para PYMES del sector comercial que dependen de proveedores críticos”** se han utilizado las normas ISO/IEC:27001, ISO/IEC:22301, ISO/IEC:19011, Circulares SBS y la Ley de protección de datos personales. Si se diera el caso de que alguna de ellas se actualice o cambien algunas directrices, lo que se debería de identificar es qué cambios se han contemplado y si estos tienen un gran impacto en el modelo desarrollado para su posterior inclusión en el modelo de referencia.

2.2 Magerit

El componente principal del modelo es la metodología MAGERIT, el cual es una herramienta muy usada para la gestión de riesgos. La versión actual de la metodología es la versión 3.0, el cual está vigente desde el año 2012. Para la gestión de riesgos de TI la metodología define los siguientes procesos:

- Identificar los activos con la mayor relevancia y valor para la organización, y qué detrimento o costo causaría su degradación.
- Establecer amenazas a las que estén expuestos los activos identificados y valorarlos en términos de probabilidad de ocurrencia y degradación que causan sobre el valor del activo afectado.

- Determinar las salvaguardas o los controles existentes y valorar la eficacia de su implementación
- Estimar el impacto, es decir, el daño al activo debido a la materialización de una amenaza
- Evaluar el riesgo, utilizando la fórmula de impacto ponderada con la tasa de ocurrencia de la amenaza.
- Establecer salvaguardas o controles para mitigar, aceptar, eliminar o transferir riesgos que tienen un alto impacto.

Si en caso la metodología sufre un cambio o una actualización, el modelo debería ser capaz de adaptarse a dicho cambio. Cualquier cambio de la metodología debe ser analizado y evaluado para revisar el impacto que tiene sobre el modelo y actualizar este a una nueva versión de acuerdo a los resultados de la evaluación.

Plan de continuidad del modelo de Gestión de riesgos de seguridad de TI

Figura 28: Plan de continuidad del modelo de gestión de riesgos de seguridad de TI

Fuente: Elaboración propia

5.3 COSTOS Y PRESUPUESTOS

5.3.1 Propósito

El propósito de este plan de gestión de costos es definir la metodología mediante la cual se administrarán los costos asociados con el Proyecto. Esto es necesario para asegurar la finalización exitosa del proyecto dentro de las restricciones presupuestarias asignadas. Hay varios componentes de costos asociados con este proyecto, así como muchas métricas, consideraciones de variación de costos e informes que se detallan en este plan. Para completar este proyecto con éxito, todos los miembros clave del proyecto y las partes interesadas deben cumplir y trabajar dentro de este plan de administración de costos y el plan general del proyecto que respalda.

5.3.2 Alcance

El plan de gestión de costos para el proyecto incluye componentes de costos internos y externos. La propuesta debe aplicar a lo largo del ciclo de vida del proyecto. Estos componentes incluyen:

A. Internal

- Project Management/project team resources
- Recruiting and hiring for additional staffing
- Capital equipment
- Software and licensing

B. External

- Support costs
- Insurance

5.3.3 Costos internos y externos

5.3.3.1 Internal Support

Esta sección define las funciones y responsabilidades de los participantes del proyecto internos en relación con la administración de los costos del proyecto.

A. Costo de investigación y desarrollo del modelo

Gastos			Tipo de cambio		3.25
		Cantidad	Precio Unitario	Tiempo (Hora/mes)	Precio Total (S/.)
Desarrollo de la solución					
Adquisición de documentación					
	Metodología Magerit	1	-		-
	Estándar ISO 27001	1	\$ 117.80		S/ 382.85
	Estándar ISO 31000	1	\$ 87.85		S/ 285.51
	Estándar ISO 22301	1	\$ 117.80		S/ 382.85
	Estándar ISO 19011	1	\$ 157.73		S/ 512.62
	Ley 29733	1	-		-
	Circular SBS G-139	1	-		-
	Circular SBS G-140	1	-		-
	Subtotal				S/ 1,563.84
Equipos					
	Laptop	1	S/ -		S/ -
	PC escritorio	1	S/ -		S/ -
	Subtotal				S/ -
Licencias y software					
	Microsoft Office 365	2	\$ 120.00		S/ 780.00
	Photoshop	1	S/ 409.92		S/ 409.92
	Google Drive	1	-		-
	Windows 10	2	S/ 900.00		S/ 1,800.00
	Subtotal				S/ 2,989.92
Personal de investigación					
	Jefe de proyecto 1	1	S/ 30.00	240	S/ 7,200.00
	Jefe de proyecto 2	1	S/ 30.00	240	S/ 7,200.00
	Recurso de investigación	8	S/ 15.60	20	S/ 2,496.00
	Subtotal				S/ 16,896.00
Costo total del desarrollo					S/ 21,449.76

Tabla 45: Costo de Investigación y desarrollo del modelo

Fuente: Elaboración propia

B. Costos de implementación del modelo

Gastos				Tipo de cambio	3.25
			Cantidad	Precio Unitario	Precio Total (S/.)
Implementación de la solución					
Equipos					
	PC escritorio		2	S/ 1,890.00	S/ 3,780.00
	Subtotal				S/ 3,780.00
Licencias y software					
	Microsoft Office 365		2	\$ 120.00	S/ 780.00
	Windows 10		2	S/ 900.00	S/ 1,800.00
	Subtotal				S/ 2,580.00
Personal de implementación					
	Jefe de proyecto		1	S/ 30.00	42 S/ 1,260.00
	Especialista de TI		1	S/ 20.00	84 S/ 1,680.00
	Analista de seguridad		1	S/ 20.00	84 S/ 1,680.00
	Subtotal				S/ 4,620.00
Costo total de la implementación					S/ 10,980.00

Tabla 46: Costo de Implementación del modelo

Fuente: Elaboración propia

5.3.3.2 External support

El contratista proporciona el apoyo relacionado con el servicio tercerizado que apoya en el proyecto. Es responsable de proporcionar una estimación inicial del costo de su servicio que incluya todos los costos asociados con el proyecto. Además, el contratista deberá proporcionar un plan que incluya todos los paquetes de trabajo y sus costos asociados. Para nuestro caso, se necesita los siguientes recursos los cuales apoyan a la mejora continua del modelo. Estos tendrán un costo por hora como se muestra en el siguiente cuadro:

Gasto anual				Tipo de cambio	3.25
		Cantidad	Precio Unitario	Tiempo (Hora/mes)	Precio Total (S/.)
Seguimiento y control					
	Especialista de seguridad	1	S/ 25.00	120	S/ 3,000.00
Auditorías					
	Auditor senior	1	S/ 50.00	80	S/ 4,000.00
Costo total de soporte externo					S/ 7,000.00

Tabla 47: Costo de soporte externo del modelo

Fuente: Elaboración propia

5.3.4 Flujo de caja

Tasa de descuento	12%					
Periodos	0	1	2	3	4	5
Ahorros estimados		10,179.00	17,813.25	25,447.50	25,447.50	25,447.50
Inversiones Inv-desarrollo	21,449.76					
Gastos						
Implementacion	10,980.00					
Implementación de controles (Especialista de TI y analista de seguridad)		-	-	-	-	-
Seguimiento y control (Especialista de seguridad)		3,000.00	3,000.00	3,000.00	3,000.00	3,000.00
Auditorías (Auditor senior)		4,000.00	4,000.00	4,000.00	4,000.00	4,000.00
Flujo de caja	-32,429.76	3,179.00	10,813.25	18,447.50	18,447.50	18,447.50
VAN	14,350.79					
TIR	25.10%					
B/C	1.44					

Figura 29: Flujo de Caja

Fuente: Elaboración propia

Se tomó la tasa de descuento o tasa de interés a partir del informe del BCP sobre el conglomerado logístico AIH donde la tasa ronda entre 11% y 13%, promediando así 12%. La importancia de este análisis radica en que la inversión estará retornando a partir del año 1, manteniéndose constante a partir del año 3, siendo este mismo año el periodo donde retornará totalmente la inversión. El VAN tiene un valor positivo, por lo tanto, podemos demostrar así la viabilidad económica de la propuesta. El TIR (Tasa de interna de retorno) de 25.10% nos indica la rentabilidad del proyecto, debido a que este porcentaje es mayor a la tasa de descuento. La relación Beneficio Costo (B/C) es mayor a 1, en consecuencia, el proyecto debe ser considerado por la gerencia de la empresa. Interpretado de otra forma, por cada S/ 1.00 invertido se obtiene un beneficio de S/ 1.44.

CAPITULO 6   GESTIÓN DEL PROYECTO

El capítulo seis consta del detalle de la gestión del proyecto haciendo uso de la metodología PMBOK, detallando los planes de gestión, matrices, entre otros documentos necesarios para el desarrollo el proyecto.

6.1. GESTIÓN DEL PROYECTO

6.1.1 Gestión del tiempo

A continuación, se detallan los cronogramas elaborados a inicio de ciclo y que fueron actualizados conforme al avance del proyecto:

El cronograma elaborado para el desarrollo del proyecto se muestra en el plan de trabajo denominado: MGRSTI- Plan de Trabajo v.3.0.

PLAN DE TRABAJO - PT								
MGRSTIPC								
JEFES DE PROYECTO		Vladimir Flores Huamani			CÓDIGO	u201316714		
PREPARADO		Manuel Chavez Junior			CÓDIGO	u201114131		
REVISADO		Vladimir Flores / Manuel Chavez			FECHA	18/03/2019		
SEMANA	DESCRIPCIÓN DE LAS ACTIVIDADES	Porcentaje de Avance (%)	ENTREGABLES	Horas Hombre por Actividad	Horas Hombre Semanal	Horas Reales	Horas Hombre Semanal	
1	Elaboración de Project Charter	100%	Project Charter	3	4	3	4	
1	Definición del problema	100%	Project Charter	2	2	2	2	
1	Definición alcance del Proyecto	100%	Project Charter	3	4	3	4	
1	Cap 4. Investigación Marco Teórico	100%		3	4	5	4	
1	Realización de Plan de Trabajo	100%	Plan de trabajo	2	2	2	2	
1	Cap 2. Plan. Alineamiento del proyecto con los Outcomes	100%	Documento de Outcomes ABET	4	4	5	4	
1	Reunión con profesor gerente	100%		1	2	2.5	2	
1	Reunión con profesor cliente	100%	Acta de reunión	1	2	1.5	2	
2	Revisión y actualización del Project Charter	100%	Project Charter	3	4	3	4	
2	Elaboración del capítulo 1 de la memoria	100%	Memoria del proyecto	3	4	3	4	
2	Revisión y actualización del Cap 2. Plan	100%	Documento de Outcomes ABET	2	2	2	2	
2	Realización de Plan de Trabajo	100%	Plan de trabajo	2	2	2	2	
2	Cap 4. Investigación Marco Teórico	100%		3	4	5	4	
2	Cap 3. Elaboración del Estado del Arte	100%		4	5	6	5	
2	Reunión con profesor gerente	100%		1	2	2.5	2	
2	Reunión con profesor cliente	100%	Acta de reunión	1	2	1.5	2	
3	Validación del proyecto con el comité	100%	Objetivos y Resultados	0.5	0.5	0.5	0.5	
3	Elaboración del Objetivo 1	100%		3	4	3	4	
3	Revisión del capítulo 1 de la memoria	100%		2	2	2	2	

Figura 30: Plan de trabajo del proyecto

Fuente: Elaboración propia

6.1.2 Gestión de los Recursos Humanos

La gestión de los recursos humanos se llevó acorde a lo planificado. Durante el desarrollo del proyecto se manejaron los siguientes roles:

- **Comité de Proyectos:** Es rol dado al grupo liderado por las autoridades de la Escuela de Ingeniería de Sistemas y Computación de la UPC que se encarga de revisar y validar la calidad del proyecto brindado a través de las distintas fases del proyecto, definiendo el alcance de los objetivos planteados.
- **Profesor Gerente:** Es el rol encargado de brindar asesoría a los jefes de proyecto sobre el desarrollo del proyecto. Interviene de manera directa para la adecuada gestión del proyecto y ofrece recomendaciones según vaya avanzando el proyecto. Encargado de la revisión de indicadores con el fin de dar un monitoreo adecuado y tomar acciones correctivas y/o preventivas en caso sea necesario.
- **Gerente IT-Research & Games:** Rol correspondiente al gerente profesor de la empresa virtual IT-Research & Games, encargado de establecer y cumplir los objetivos principales de la empresa IT-Research & Games; con respecto a la participación en el proyecto, el gerente profesor realizará las siguientes funciones:
  - Presentar oportunidades de mejora para el cumplimiento de objetivos de la empresa IT-Research & Games en base a los proyectos propuestos.
  - Realizar un seguimiento del proyecto con el fin de evaluar si se cumple con lo estipulado de acuerdo al cronograma establecido.
  - Brindar comentarios y observaciones de los entregables realizados para su mejora y levantamiento antes de la presentación de estos al cliente y comité.
- **Profesor Cliente:** El cliente tiene como responsabilidad dar seguimiento al avance del proyecto y guiar a los jefes en el desarrollo del mismo. El cliente debe ayudar a que el proyecto esté bien encaminado y tenga el proceso correcto para su buen desarrollo.
- **Coautor:** Es el principal asesor en cuanto al desarrollo de la investigación del proyecto, con profundos conocimientos sobre investigación y sobre el tema desarrollado. Es una persona calificada con altos conocimientos en la tesis que tiene asignada.
- **Jefe de Proyecto:** Es el rol que define los objetivos del proyecto, el alcance y los revisa con el profesor Gerente y Profesor Cliente, con el fin de mantenerse todos de acuerdo e

incorporar su retroalimentación. Además, es el encargado de sustentar el proyecto ante el comité de proyectos.

- **Recurso de IT Service:** Es el analista de calidad de la empresa IT Services que brindará servicios de aseguramiento de calidad a través del desarrollo del proyecto.

6.1.3 Gestión de las Comunicaciones

El Plan de Comunicaciones tiene como objetivo definir los lineamientos para la comunicación interna y externa respecto a todos los interesados del proyecto. El plan de comunicaciones se cumplió en un 100% respecto a lo planificado:

- **Guía para reuniones**

Todas las reuniones deben seguir las siguientes pautas:

- En caso de tener un nuevo miembro en cada reunión, se hará la respectiva presentación de éste ante los asistentes.
- Se manejará una agenda para cada reunión de acuerdo a los temas de interés a tratarse, así como también las tareas pendientes de reuniones anteriores. Para este caso, se debe tener en cuenta el entregable a realizar según el diccionario EDT.
- Cada punto de la agenda contará con un nivel de prioridad a ser tratado.
- Se cuenta con un horario específico para cada reunión, sin embargo, será necesario confirmar/recordar la reunión vía correo electrónico un día antes como máximo.
- En caso se deba postergar una reunión, se deberá justificar y además acordar el nuevo día de esta.
- Al finalizar cada reunión se deberá recopilar lo tratado, resaltando los acuerdos para posteriormente elaborar el acta de reunión.
- Todas las actas de reunión deberán ser firmadas por el jefe de proyecto, asistente de proyecto y gerente general o cliente, respectivamente.

- **Guía para correo electrónico**

Todas las remisiones de correos electrónicos deben seguir las siguientes pautas:

- Cada correo electrónico debe ser redactado de una manera formal.

- Todo correo electrónico al cliente debe ser copiado a todo el equipo de proyecto; en especial a gerente, jefe, asistente de proyecto.
- Los correos electrónicos entre el gerente de la empresa y el cliente, deberá ser enviado por el jefe de proyecto para establecer un estándar en la conexión.
- En caso de envíos de solicitud de servicios a empresas externas, se debe copiar al correo de la empresa.

6.1.4 Gestión de los Riesgos

A continuación, se muestran los riesgos que se tenían mapeados al inicio de la planificación:

Descripción del riesgo	Probabilidad	Impacto
Actividades y entregables fuera del tiempo planificado en el cronograma	30% Baja	4 Alta
Cambio en el alcance del proyecto	30% Baja	4 Alta
Problemas por discrepancias en el desarrollo del proyecto por parte de los profesores cliente y gerente	30% Baja	4 Alta
Empresa de estudio poca o nada colaborativa para el levantamiento de información	50% Media	4 Alta
Rechazo del modelo de gestión de riesgos por parte de la empresa de estudio	30% Baja	4 Alta

Tabla 48: Matriz de riesgos del proyecto

Fuente: Elaboración propia

6.1.5 Lecciones Aprendidas

A continuación, se señalan los puntos a mejorar y tener en cuenta para futuros proyectos:

1. Al iniciar el proyecto se define un plan de trabajo, por lo que se debe de seguir los tiempos establecidos en este plan para que durante el proyecto no se presenten retrasos o se necesite realizar un mayor esfuerzo para poder lograr el objetivo deseado. Si se sigue los tiempos establecidos, el proyecto se desarrollará correctamente y sin apuros.
2. Plantear las reuniones desde un inicio para que el profesor cliente gestione su tiempo con anticipación y poder estar presente en la reunión sin ningún problema.
3. Definir un horario específico para contactar al personal responsable de brindar información de la organización.

4. Plantear tareas específicas de cambios para cada jefe de proyecto, según el área que más domine.
5. Coordinar con anticipación las reuniones con los recursos de apoyo para un correcto desarrollo del proyecto. Asimismo, definir las fechas que deberán entregar la información requerida.
6. Seleccionar más personas que se puedan considerar en el equipo de trabajo por si alguna de ellas decidiera retirarse de la empresa.

CONCLUSIONES

A continuación, se mencionan las conclusiones del proyecto:

- Como resultado del trabajo de investigación y análisis, se determinó que el modelo de gestión de riesgos de seguridad de TI debería orientarse a los activos y procesos de TI que dependen de proveedores críticos, ya que se evidenció que gran parte de los incidentes de seguridad están relacionados a proveedores.
- La metodología Magerit es la más adecuada para mejorar el nivel de riesgo de los activos y procesos de TI en las pymes, debido a que es una metodología cuantitativa, de baja complejidad y tiene un bajo costo de implementación.
- Tomando en cuenta la necesidad de las pymes, la realidad y normatividad peruana se consideró diseñar un modelo de gestión de riesgos de seguridad de TI que abarque estos temas y sea escalable en el tiempo, algo que en la actualidad no existe.
- Durante la aplicación del modelo en el caso de estudio se concluyó que el modelo es efectivo, ya que permitió aumentar el nivel de madurez respecto a la gestión de riesgos y seguridad de TI en un 86.49% y disminuir el nivel de riesgo de los activos de TI en un 79.46% (ambos relacionados a proveedores críticos).
- Pensando en la mejora continua, se concluyó que el plan de continuidad debe considerar una guía de implementación basado en el modelo PDCA (Plan-Do-Check-Act) y de procedimientos que permitan la actualización del modelo tomando en cuenta actualizaciones de metodología, normativas y estándares empleados.

RECOMENDACIONES

Las recomendaciones que se definieron luego de la elaboración del proyecto son:

- Se recomienda trabajar en conjunto con un especialista de seguridad de TI durante todas las fases del modelo, esto para asegurar que cada fase esté alineada y por ende gestionar adecuadamente los riesgos identificados.
- El modelo debe ser aplicado de manera periódica. Se recomienda hacerlo 1 vez al año. Esto debido a que los sistemas de información se encuentran sometidos a evolución continua tanto propia (nuevos activos) como del entorno (nuevas amenazas).
- El modelo debe ser revisado por lo menos cada 3 años, o cuando exista un cambio significativo referido a normas, metodologías o estándares que a su vez deben ser evaluados dependiendo del impacto que estos ocasionen.
- La organización debe realizar auditorías de manera periódica a fin de asegurar el cumplimiento de los planes y controles propuestos luego de la aplicación del modelo.
- Se recomienda que la organización cumpla las recomendaciones o controles propuestos luego de la aplicación del modelo; esto a fin de asegurar la disminución de los riesgos a las que puedan ser afectados.
- A partir de la investigación realizada, se pueden hacer estudios para que el modelo pueda ampliarse hacia la gestión de riesgos de seguridad de los sistemas de información, y además para que este sea aplicable a otros sectores empresariales.

GLOSARIO

- **Pyme:** Unidad económica constituida por una persona natural o jurídica, bajo cualquier forma de organización o gestión empresarial contemplada en la legislación vigente, que tiene como objeto desarrollar actividades de extracción, transformación, producción, comercialización de bienes o prestación de servicios. (Cendoc ESAN, 2005)
- **Stakeholder:** Hace referencia sobre todo a las organizaciones o personas que toman parte en las decisiones de una compañía y que están afectadas por sus actividades. (Economía Simple, 2019)
- **Activo:** Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos. (MAGERIT, 2012)
- **Riesgo:** Se denomina riesgo a la medida del daño probable sobre un sistema. (MAGERIT, 2012)
- **Amenaza:** Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización. (MAGERIT, 2012)
- **Confidencialidad:** Propiedad de prevenir que se divulgue la información a personas o sistemas no autorizados. (SGSI, 2015)
- **Integridad:** Propiedad que busca proteger que se modifiquen los datos libres de forma no autorizada. (SGSI, 2015)
- **Disponibilidad:** Característica, cualidad o condición de la información que se encuentra a disposición de quien tiene que acceder a esta, bien sean personas, procesos o aplicaciones. (SGSI, 2015)

- **Vulnerabilidad:** toda debilidad que puede ser aprovechada por una amenaza, o más detalladamente a las debilidades de los activos o de sus medidas de protección que facilitan el éxito de una amenaza potencial. (MAGERIT, 2012)
- **Estado del arte:** Investigación documental que permite el estudio del conocimiento acumulado (escrito en textos) dentro de un área específica. Esto implica revisar artículos, revistas, libros, bases de datos, tesis y extraer la información más relevante en un único documento. (ATRIA Innovation, 2016)
- **Paper:** Es un trabajo científico destinado a la publicación en revistas académicas y que hace referencia a una actividad de indagación teórica o teórica-empírica realizada con antelación.
- **Auditoria interna:** Es un sistema de control interno de la empresa y consiste en el conjunto de medidas, políticas y procedimientos establecidos en una organización concreta para proteger su activo, minimizar riesgos, incrementar la eficacia de los procesos operativos y optimizar y rentabilizar, en definitiva, el negocio. (Emprende Pyme, 2019)
- **Auditoria externa:** Consiste en un análisis y control exhaustivos por parte de un auditor, el cual es totalmente ajeno a la actividad de la empresa, con el objetivo de emitir una opinión imparcial e independiente sobre el sistema de operación de la empresa y su control interno. (Emprende Pyme, 2019)

SIGLARIO

ISO: International Organization for Standardization.

IEC: International Electrotechnical Commission

PMBOK: Project Management Body of Knowledge

TI: Tecnologías de Información.

IE: Indicador de éxito.

OE: Objetivo específico.

OG: Objetivo general

MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

OCTAVE: Operationally Critical Threat, Asset and Vulnerability Evaluation

ABET: Accreditation Board for Engineering and Technology

WOS: Web of Science

BCMS: Business Continuity Management System - Sistema de Gestión de Continuidad del Negocio

SBS: Superintendencia de Banca y Seguros del Perú

CMMI: Capability Maturity Model Integration

BIBLIOGRAFÍA

- A. Santos-Olmo, L. E.-M. (2016). Methodology for Dynamic Analysis and Risk Management on ISO27001. *IEEE Latin America Transactions* , 2897-2911.
- Agrawal, V. (2017). A Comparative Study on Information Security Risk. *Journal of Computers*, 57-67.
- Agrawal, Vivek. (2017). A Comparative Study on Information Security Risk. *Journal of Computers*, 57-67.
- ATRIA Innovation. (2016, noviembre 20). Retrieved from ATRIA Innovation: <http://atriainnovation.com/que-es-el-estado-del-arte/>
- Author (s): Montenegro, C. M. (2016). Information security risk in SMEs: A hybrid model compatible with IFRS: Evaluation in two Ecuadorian SMEs of automotive sector. *International Conference on Information Communication and Management*, 115-121.
- Camara de Comercio, C. (2016, 09). *Camara de Comercio*. Retrieved from Camara de Comercio: https://www.camaralima.org.pe/RepositorioAPS/0/0/par/EDICION741/ED_DIGITAL741.pdf
- Cendoc ESAN. (2005, 09). Retrieved from Cendoc ESAN: <http://cendoc.esan.edu.pe/fulltext/e-journals/PAD/7/arbulu.pdf>
- COBIT 5, C. (2012). *COBIT 5 - Un Marco de Negocio para el gobierno y la gestion de la empresa*.
- Comercio. (2017, 12 29). *Diario El Comercio*. Retrieved from Diario El Comercio: <https://elcomercio.pe/economia/20-grandes-empresas-realizan-auditoria-digital-noticia-485188-noticia/>
- Comercio, D. E. (2018, 08 28). *El Comercio Perú*. Retrieved from Diario el Comercio: <https://elcomercio.pe/economia/peru/sector-comercio-expandira-3-2-2018-estima-ccl-noticia-nndc-551366>
- Economía Simple*. (2019, 06). Retrieved from Economía Simple: <https://www.economiasimple.net/glosario/stakeholders>
- Emprende Pyme*. (2019). Retrieved from Emprende Pyme: <https://www.emprendepyme.net/auditoria-interna.html>
- Gestión. (2018, 04 11). *Gestión*. Retrieved from Gestión: <https://gestion.pe/economia/empresas/6-empresas-sufren-perdidas-catastroficas-datos-logran-sobrevivir-231238>
- Gestion, D. (2015, 04 24). *Gestion Perú*. Retrieved from Gestion Perú: <https://gestion.pe/tu-dinero/diez-respuestas-ley-proteccion-datos-personales-152808>
- Gestión, D. (2017, 10 30). Retrieved from <https://gestion.pe/tecnologia/54-empresas-procesos-respuesta-incidentes-ciberneticos-221651>
- INEI. (2015). *Directorio central de empresas y establecimientos*. Lima.
- INEI. (2018). *Indicador de la Actividad Productiva departamental*. Lima.
- INEI Peru, I. (2015). *Instituto Naciona de Estadística e Informatica*. Retrieved from https://www.inei.gob.pe/media/MenuRecursivo/publicaciones_digitales/Est/Lib1398/parte04.pdf
- ISO 19011, N. I. (2012). *Directrices para la auditoría de los sistemas de gestión*.
- ISO 22301, O. (2012). *ISO 22301:2012(en)*. Retrieved from ISO 22301:2012(en): <https://www.iso.org/obp/ui/#iso:std:iso:22301:ed-1:v2:en>
- ISO 27001. (2015, 05). *ISO 27001: ¿Qué significa la Seguridad de la Información?* Retrieved from ISO 27001: ¿Qué significa la Seguridad de la Información?: <https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/>

- ISO 27001, O. (2013, 10). *ISO/IEC 27001:2013*. Retrieved from ISO/IEC 27001:2013: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en>
- ISO 31000, G. d. (2018). *ISO ORG*. Retrieved from ISO ORG: <https://www.iso.org/iso-31000-risk-management.html>
- Jarot S. Suroso, M. A. (2018). Assessment Of Information System Risk Management with Octave. *ScienceDirect*.
- Jarot S., Muhammad A. (2018). Assessment Of Information System Risk Management with Octave. *Science Direct*.
- LEY 29733, L. N. (2011). *Ley de protección de datos personales*. Lima.
- MAGERIT, C. d. (2012). *MAGERIT V3.0 Metodología de Análisis y Gestión de riesgos de los sistemas de información*. Ministerio de Hacienda y Administraciones Públicas: Madrid - España.
- MTPE. (2006). *Ministerio de Trabajo y promocion del Empleo*. Retrieved from MTPE: https://www.trabajo.gob.pe/archivos/file/estadisticas/peel/beo/BEO2006-III_7.pdf
- PWC. (2017). *The Global State of Information Security Survey: PwC*. Retrieved from The Global State of Information Security Survey 2018: PwC: <https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html>
- Roel Wieringa, W. P. (2013). *Current Established Risk Assessment Methodologies and Tools*.
- Rubén Arroyo and Sang Guun Yoo, R. G. (2017). Title of paper: Experience in Applying the Analysis and Risk Management Methodology called MAGERIT to Identify Threats and Vulnerabilities in an Agro-industrial Company. *International Journal of Applied Engineering Research*, 6741-6750.
- Salimeh Dashti, P. G. (2017). Information Security Risk Management. *Lecture Notes in Business Information Processing*, 19 - 33.
- SGSI. (2015, mayo 21). Retrieved from Blog especializado en Sistemas de Gestión: <https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/>
- Silva, F. M. (2012). Comparative Study of Information Security Risk. 1 - 11.

ANEXOS

ANEXO A – WASC

WASC Jefe de Proyecto 1

1. Comunicación escrita

Esta competencia se define como la capacidad para construir mensajes con contenido relevante, argumentos sólidos y claramente conectados adecuados a diversos propósitos y audiencia; todo lo anterior respecto al proyecto realizado.

El presente proyecto: “Modelo de gestión de riesgos de seguridad de TI para Pymes del sector comercial que dependen de proveedores críticos”, ha logrado cumplir esta competencia a través de la elaboración de diferentes entregables los cuales describen que el proyecto se esté llevando correctamente y fueron revisados por diferentes interesados del proyecto (Comité de proyectos, Gerente de Proyecto, Cliente de Proyecto, Co-autor, responsables de la organización, etc.) los cuales supervisaron que el proyecto se esté llevando correctamente de acuerdo al Plan de trabajo presentado al inicio del ciclo 2018-2.

Todos los entregables desarrollados a lo largo del proyecto tienen una relación directa con el problema o necesidad identificado, los cuales contienen textos con una estructura clara y con ideas suficientes para que pueda ser fácilmente entendible por todos los interesados en revisar dicho documento. Estos entregables fueron de gran apoyo para el correcto desarrollo del proyecto y se realizaron para validar el cumplimiento de cada objetivo específico que tiene el proyecto.

Para el desarrollo del proyecto se hizo una investigación de diferentes fuentes confiables tales como: artículos, revistas, informes, etc. Todas ellas actualizadas y con una antigüedad máxima de 4 años, las cuales fueron revisadas y aprobadas por el asesor de paper en las diferentes reuniones que se tuvieron a lo largo del proyecto.

Asimismo, el contenido de cada entregable cuenta con información actualizada y relevante la cual fue extraída de diferentes fuentes confiables por lo que se aseguraron argumentos sólidos y claramente conectados. También se utilizó un léxico variado, preciso, académico y especializado para que pueda ser fácilmente entendible por los diferentes interesados del proyecto y puedan realizar la implementación del modelo en la organización perteneciente al sector comercial.

A continuación, se presenta la evidencia necesaria para validar el cumplimiento de esta competencia:

- Documentos de gestión de proyecto (PMBOK)
- Benchmarking de metodologías de gestión de riesgos
- Benchmarking de estándares de gestión de seguridad de la información
- Modelo de Gestión de Riesgos de Seguridad de TI para PYMES del sector comercial que depende de proveedores críticos
- Criterios de validación del modelo
- Herramienta assessment
- Evaluación de criterios de validación (juicio de expertos)
- Plan de continuidad
- Memoria del proyecto
- Poster del proyecto

2. Comunicación oral

Esta referido a la capacidad para transmitir oralmente el desarrollo del proyecto mediante mensajes de manera eficaz dirigidos a diversas audiencias, usando diferentes herramientas que faciliten su comprensión y el logro del propósito.

El presente proyecto: “Modelo de gestión de riesgos de seguridad de TI para Pymes del sector comercial que dependen de proveedores críticos” ha logrado cumplir esta competencia mediante diferentes reuniones y exposiciones que se tuvieron con los interesados del proyecto. Las reuniones que se tuvieron a lo largo del proyecto fueron con: Gerente del proyecto, cliente del proyecto, asesor de paper, comité de proyectos, representantes de la empresa donde se hizo la validación del modelo a través de un caso de estudio como el gerente general y el gerente de TI. Asimismo, durante el desarrollo del proyecto se realizaron en varias oportunidades exposiciones presenciales con todos los interesados del proyecto. Para la alta gerencia de la Pyme del sector comercial seleccionada se usó la comunicación oral para expresarle la idea del proyecto y la posterior validación del modelo. Para la validación del modelo en la organización, se realizaron presentaciones formales ante la alta gerencia de la organización para mostrar los resultados finales de la validación y dar a conocer las recomendaciones que deben cumplir para una adecuada gestión de los riesgos.

Para realizar una buena sustentación se siguió una serie de recomendaciones que nos ayudaron a realizar presentaciones que además de dejar una buena impresión al comité y a los representantes de la empresa, nos permitió vencer en el tiempo las dificultades más comunes. Estas recomendaciones corresponden a: lenguaje corporal, herramientas de soporte, organización del mensaje, entonación, etc. Todas estas recomendaciones ayudaron para transmitir un mensaje eficaz y comprensivo para los interesados del proyecto.

También, durante las reuniones o exposiciones con los interesados del proyecto, se usó palabras o expresiones académicas relacionadas al proyecto. En algunos casos palabras especializadas que aporten a la comprensión del mensaje, pero siempre haciendo una breve explicación para que el público pueda entender y esté en todo momento conectado a la presentación del desarrollo del proyecto.

Finalmente, para reforzar la presentación y sea del agrado del público se hizo uso de diferentes recursos y medios de soporte como: Gráficos estadísticos, cuadros comparativos, diagramas, etc. Todas estas herramientas aportan a la comprensión del mensaje e hicieron que los interesados del proyecto puedan estar atentos a las presentaciones realizadas.

A continuación, se presentan las evidencias necesarias para validar el cumplimiento de esta competencia:

- Actas de reunión con profesor gerente, profesor cliente, con los representantes de la empresa perteneciente al sector comercial.
- Pre - sus tenciones y sustentaciones parcial y final.

3. Ciudadanía

Está enfocado en la capacidad para valorar la convivencia humana en sociedades plurales, reflexionando acerca de las dimensiones morales de las propias acciones y decisiones, asumiendo la responsabilidad por las consecuencias en el marco del respeto de los derechos y deberes ciudadanos.

La competencia de Ciudadanía contiene un conjunto de conocimientos, habilidades y actitudes que todos los estudiantes de la carrera de Ingeniería de Sistemas de Información deben poseer y poner en práctica para la construcción de una sociedad pacífica, democrática e incluyente. Gracias

a esta competencia es posible comprender el valor de los derechos humanos y actuar de manera constructiva dentro de nuestra sociedad.

El presente proyecto ha logrado cumplir esa competencia, gracias a la identificación de la necesidad descrita en el documento del Project Charter. En él se puede evidenciar el impacto que se tiene frente a la sociedad y frente a la organización donde se implementará el modelo; asimismo, también se muestra cual sería la posible solución a implementar. En dicho documento se evalúa diferentes eventos catastróficos (terremotos, ciberataques, huelgas, robos, etc.) que afectan a la sociedad, específicamente a las Pymes del sector comercial causando pérdidas económicas y daños en su reputación.

Para poder encontrar la solución más adaptable a las empresas pymes, las cuales según diferentes investigaciones cuentan con poco presupuesto para los temas de seguridad de la información, se realizó un análisis comparativo entre diversas metodologías de gestión de riesgos y estándares de gestión de seguridad de información para identificar el más idóneo. El resultado final de la comparativa fue la elección de la metodología y el estándar para realizar el diseño del modelo de gestión de riesgos de seguridad de TI. Esto fue revisado y aprobado por el profesor cliente a través del acta de aprobación del proyecto del objetivo 1 y del objetivo 2.

Asimismo, la validación del modelo se realizó en una empresa perteneciente al sector comercial donde se intercambió opiniones con personas de diferente contexto social, político y económico. Desde el responsable del área de soporte, hasta el gerente general. Todos ellos apoyaron al desarrollo del proyecto, la cual se validó en la respectiva empresa comercial. Durante el desarrollo del proyecto se contó con el apoyo de diferentes interesados, pero también se buscaron diferentes puntos de vista de los entregables realizados, para lo cual se realizaron consultas con diferentes expertos dentro y fuera de la universidad. Un ejemplo de esto es la evaluación realizada por los expertos de seguridad a profesionales que laboran en bancos y corredores de seguros; esto se realizó a fin de evaluar los criterios de validación del modelo de referencia.

Para el desarrollo del proyecto se tuvo que realizar reuniones y exposiciones con diferentes interesados de este, prácticamente fue una convivencia durante todo un año que duró el mismo. En todo ese tiempo se presentaron situaciones de disconformidad y desacuerdo (reclamos, opiniones discordantes, etc.), las cuales fueron resueltas oportunamente luego de una conversación con cada uno de los interesados del proyecto. Todo ello en un marco de respeto de los derechos y deberes hacia los interesados.

A continuación, se presenta la evidencia necesaria para validar el cumplimiento de esta competencia:

- Project Charter
- Actas de reunión
- Criterios Validación del modelo

4. Manejo de la información

Esta competencia se define como la capacidad de identificar la información necesaria, así como de buscarla, seleccionarla, evaluarla y usarla éticamente, con la finalidad de resolver un problema o necesidad. Todos los criterios descritos anteriormente deben ser puestos en práctica por todos los estudiantes de la carrera de Ingeniería de Sistemas de Información para identificar cualquier tipo de información cuando la necesite o sea requerida y poder convertirla en conocimiento útil para solucionar problemas o generar nuevas ideas dentro de su vida académica o cotidiana.

El presente proyecto: “Modelo de gestión de riesgos de seguridad de TI para Pymes del sector comercial que dependen de proveedores críticos”, ha logrado cumplir esta competencia mediante la identificación de una necesidad que tienen las Pymes, la cual es reducir el nivel de impacto ocasionado por los riesgos que afectan a sus procesos y activos de TI asociados a proveedores críticos. Riesgos como: desastres naturales, ciberataques, fraudes electrónicos, etc. que de alguna u otra manera hacen que la organización deje de operar causando grandes pérdidas económicas y daños en su reputación.

Para proponer una solución a la necesidad identificada se tuvo que seleccionar y evaluar diferentes fuentes de información (artículos, informes, noticias, reportes, tesis, etc.) confiables referidos al tema de investigación y que cuentan con un máximo de 4 años de antigüedad, además de usar las últimas versiones de los estándares, metodologías y modelos de referencia, para así capturar y analizar la información más reciente y poder realizar la propuesta de solución. Se utilizaron diferentes recursos de investigación como: Web of Science (WOS), IEEE Explore, Scopus, Science Direct, etc. Todos los artículos utilizados en este trabajo están indexados en revistas especializadas y validadas.

La información requerida fue organizada y sintetizada empleando diferentes citas directas e indirectas de manera pertinente. En algunos casos fue necesario parafrasear el texto, en otros se hizo un resumen de éste, y también se utilizaron citas; todos los anteriores respetando su contexto

original. Durante el desarrollo del estado del arte se elaboraron conclusiones por objetivo y una conclusión general que engloba todo el trabajo de investigación de todos los artículos revisados. En cada entregable elaborado se encuentra una sección bibliográfica donde se encuentra la información de todas las fuentes utilizadas, así como también citas y parafraseo en todos los textos del documento según corresponda. Todo lo mencionado bajo las normas APA, siendo este el estándar para la universidad.

Se hizo una evaluación, análisis y una comparativa con la información recolectada, teniendo como resultado una síntesis de todo lo investigado, logrando alcanzar por completo un objetivo específico del proyecto. Esto se evidenció en los entregables siguientes: Benchmarking de metodologías de gestión de riesgos y Benchmarking de Estándares de gestión de seguridad de información, los cuales fueron la base para el diseño del modelo de gestión de riesgos de seguridad de TI.

Finalmente, a lo largo del proyecto se cumplió el aspecto normativo del sistema de referencia, sea para las citas o referencias. Demostrando así que se respetó las consideraciones éticas del uso de la información. Ello se puede evidenciar en todos los entregables redactados en todo el proyecto, las cuales fueron de gran apoyo para el correcto desarrollo de este.

A continuación, se presenta la evidencia necesaria para validar el cumplimiento de esta competencia:

- Project Charter
- Memoria del proyecto
- Benchmarking de metodologías de gestión de riesgos
- Benchmarking de estándares de gestión de seguridad de la información

5. Pensamiento innovador

Esta competencia se define como la capacidad para detectar necesidades y oportunidades para generar proyectos o propuestas innovadoras, viables y rentables. Planifica y toma decisiones eficientes orientadas al objetivo del proyecto.

El presente proyecto: “Modelo de gestión de riesgos de seguridad de TI para Pymes del sector comercial que dependen de proveedores críticos”, ha logrado cumplir esta competencia mediante la identificación de la problemática o necesidad que tienen las Pymes de reducir el nivel de

impacto que afectan a los procesos y activos de TI que dependen de proveedores críticos. Esta necesidad se ve reflejado en los entregables como: El Project charter, la Memoria, Análisis comparativo. Además, se ha encontrado una oportunidad de aplicar el modelo en este sector donde según las investigaciones realizadas, en el Perú no existe un modelo de gestión de riesgos aplicados a las Pymes que dependen de proveedores críticos. Razón por la cual es una gran oportunidad de hacer este trabajo de investigación.

Debido a que se observó que la metodología MAGERIT con la ayuda del estándar ISO 27001 hacen una gran combinación, se decidió unir ambos, incluyendo en el modelo el estándar mencionado. Esto se hizo añadiendo procesos necesarios que sí contemplaba la ISO/IEC 27001. De esta manera se puede identificar los riesgos y proponer los controles para mitigarlos de una manera muy eficaz. También al modelo propuesto se agregó herramientas de soporte como: ISO 19011, ISO 22301, Circulares SBS y la Ley de Protección de datos personales. Todo ello conlleva a que la propuesta sea novedosa y funcional ya que como se mencionó líneas arriba, en el Perú no existe un modelo de gestión de riesgos que estén enfocadas a las Pymes que dependen de proveedores críticos.

Los planes de acción donde se establecen procesos y tareas claves alineadas a resolver el problema eficientemente fueron: El seguimiento y control, las auditorias y la actualización del modelo. Estos planes aseguran que las organizaciones cumplan las recomendaciones o controles propuestas producto de la validación del modelo. Se recomienda que lo cumplan en un tiempo prudencial (1 año). De esta manera las Pymes podrán reducir el nivel de impacto generado por los riesgos que las afectan y recuperarse en el menor tiempo posible reestableciendo sus operaciones rápidamente.

Para demostrar que el proyecto es rentable y viable, se realizó el impacto económico donde se aprecia un aproximado del costo del proyecto, y cuál sería el retorno de inversión de este; demostrando que en solo en 1 año como máximo la empresa puede empezar a recuperar lo invertido si gestionara los recursos mencionados; y máximo en 3 años se recupera la inversión total realizada. Esto nos hace ver que el proyecto es viable y puede implementarse sin ningún inconveniente en la Pyme del sector comercial.

A continuación, se presenta la evidencia necesaria para validar el cumplimiento de esta competencia:

- Project Charter

- Memoria del proyecto
- Benchmarking de metodologías de gestión de riesgos
- Benchmarking de estándares de gestión de seguridad de la información
- Plan de Costos de Proyecto

6. Pensamiento crítico

Esta competencia se define como la capacidad para explorar de manera exhaustiva problemas, ideas o eventos para formular conclusiones u opiniones sólidamente justificadas. Es decir, la habilidad de pensar de una manera clara, razonada, reflexiva, informada por evidencia y dirigida a decidir qué creer o hacer.

El presente proyecto: “Modelo de gestión de riesgos de seguridad de TI para Pymes del sector comercial que dependen de proveedores críticos”, ha logrado cumplir esta competencia mediante la identificación de las causas que originan la necesidad identificada para el desarrollo del proyecto, el cual es: Reducir el nivel de impacto ocasionado por los riesgos que afecta a los activos y procesos de TI en las Pymes que dependen de proveedores críticos. Estas causas son:

- Falta de seguimiento del cumplimiento de los controles de seguridad que se deben realizar a los proveedores.
- No existe implementación de controles adecuados debido a que no cuentan con un área de gestión de riesgos o tienen deficiencias en la gestión de las mismas.
- Deficiencia de auditorías de la empresa a los proveedores que permita asegurar el cumplimiento de los Acuerdos de nivel de servicio (SLAs) establecidos por los proveedores.
- Falta de controles adecuados hacia los proveedores con acceso a los activos de información de la empresa.

Para la solución del problema o necesidad identificado, se tuvo que evaluar la información que fue recopilada de diferentes fuentes confiables. Ello conllevó a un análisis y síntesis coherente para llegar a un resultado final el cual apoye a la solución de la necesidad. Esto se vio reflejado en diferentes entregables como: El Benchmarking de gestión de riesgos, Benchmarking de estándares de gestión de seguridad de información, Criterios de validación, Herramienta assessment, diseño del modelo de gestión de riesgos de TI.

Asimismo, se identificó y analizó la necesidad de acuerdo a un estudio del análisis de contexto de los riesgos que afectan a las Pymes. Este contexto abarcó a los eventos que ocurren en el país y que traen consecuencias negativas a las Pymes que depende de proveedores críticos. Eventos como: desastres naturales, ataques cibernéticos, fraudes electrónicos, huelgas, etc. Por todo lo anterior mencionado es que se pensó en una solución en base el análisis realizado.

Hay un problema de seguridad de información. Nuestra propuesta es un modelo que busca proponer estrategias, controles y recomendaciones para reducir los riesgos que afectan a los activos y procesos de TI que dependen de proveedores críticos en las pymes. El modelo se desarrolló en base a una metodología y estándares de gestión de riesgos y seguridad de la información, lo cual, según nuestra investigación, actualmente no existe en el mercado. Esto, sumado a la necesidad identificada, demuestra la viabilidad de nuestra solución.

Finalmente, mediante las investigaciones realizadas a través de fuentes confiables se concluyó que no hay ningún Modelo de gestión de riesgos aplicados a las Pymes del sector comercial que dependen de proveedores críticos que se ajuste a las necesidades de estas. También se puede concluir que las pymes en general no se encuentran preparadas para afrontar riesgos que afecten a la continuidad de sus operaciones, ya que estas no cuentan con un adecuado proceso de gestión de riesgos y carecen de una cultura organizacional sobre seguridad de la información. Para ello, nos basamos en investigaciones de artículos científicos y estadísticas de fuentes confiables.

A continuación, se presenta la evidencia necesaria para validar el cumplimiento de esta competencia:

- Project Charter
- Memoria del proyecto
- Benchmarking de metodologías de gestión de riesgos
- Benchmarking de estándares de gestión de seguridad de la información

7. Razonamiento cuantitativo

Esta competencia está referida a la capacidad para interpretar, representar, comunicar y utilizar información cuantitativa diversa en situaciones de contexto real. Incluye calcular, razonar, emitir juicios y tomar decisiones con base en esta información cuantitativa.

El presente proyecto: “Modelo de gestión de riesgos de seguridad de TI para Pymes del sector comercial que dependen de proveedores críticos”, ha logrado cumplir esta competencia mediante la interpretación de los resultados obtenidos producto de la comparativa de metodologías de gestión de riesgos, validación del modelo y los costos y presupuestos de este. Estos resultados fueron valores cuantitativos, los cuales en algunos casos se vieron reflejados en indicadores de éxito y otros en cuadros estadísticos. Para cada una de ellas, durante la presentación se hizo una descripción detallada estableciendo relaciones e infiriendo contenidos a partir de la información cuantitativa diversa a fin de que el público objetivo pueda comprender muy fácilmente.

Para la solución del problema o necesidad identificado, se apoyó de diferentes datos estadísticos de contexto real tales como los eventos que ocurren en la sociedad y que afectan a las Pymes de manera general. Se obtuvieron diferentes estadísticas como: porcentaje de pérdida que sufren las Pymes luego de un desastre, cantidad de Pymes que no están preparadas para afrontar situaciones diversas, estadística de metodologías de gestión de riesgos, etc. Todos estos hechos fueron matematizados en situaciones de contexto real. Asimismo, luego de la validación se hizo una representación matemática mediante cuadros estadísticos. Este desarrollo se hizo luego de la evaluación de los criterios de validación que se hizo a los expertos del tema, los cuales evaluaron cada criterio en base a un determinado puntaje, para finalmente mostrar en un cuadro estadístico los resultados de la evaluación.

Durante la validación del modelo se efectuaron cálculos matemáticos. Primero, para hallar el nivel de madurez de la organización respecto a la gestión de riesgos y seguridad de TI. Esto se hizo a través de una herramienta Excel. Segundo, para la aplicación de la metodología se hicieron cálculos para gestionar el riesgo. Cálculos para hallar: impacto, riesgo inherente y riesgo residual luego de la aplicación de las salvaguardas o controles. Como se indicó líneas arriba también se hizo cálculos matemáticos para los cuadros estadísticos producto de la evaluación de expertos. Finalmente, para realizar el retorno de inversión del proyecto, se realizó un flujo de caja para evaluar la inversión del proyecto, el cual se puede evidenciar en el punto **5.3 “Costos y presupuestos”** incluido en el capítulo **5 “Resultado del proyecto”**.

Se desarrolló la propuesta de solución del problema o necesidad. Esto mediante la aplicación de métodos matemáticos tanto para realizar el benchmarking de metodologías de gestión de riesgos de TI, el nivel de madurez de la organización, la validación de los expertos y también para hallar el riesgo inherente y residual aplicado en el caso de estudio. Para finalmente establecer

conclusiones precisas coherentes y relevantes. Esto se vio reflejado en los entregables como: Herramienta assessment, Evaluación de expertos y la Matriz de riesgos.

Por último, luego del análisis y desarrollo del proyecto, los resultados del razonamiento fueron explicados y argumentados de forma ordenada y coherente, mediante evidencias cuantitativas o relaciones matemáticas, esto haciendo uso adecuado del lenguaje matemático. Esto se evidenció con los entregables como: Benchmarking de metodologías, Criterios de validación, Matriz de riesgos, Análisis de costo y presupuesto.

A continuación, se presentan las evidencias necesarias para validar el cumplimiento de esta competencia:

- Benchmarking de metodologías de gestión de riesgos
- Benchmarking de estándares de gestión de seguridad de la información
- Plan de Costos de Proyecto
- Lista riesgos
- Criterios de validación del modelo
- Plan de Costos de Proyecto

WASC Jefe de Proyecto 2

1. Comunicación escrita

La comunicación escrita se define como la capacidad para construir mensajes con contenido relevante, argumentos sólidos y claramente conectados adecuados a diversos propósitos y audiencia. La comunicación por medio del lenguaje escrito es con fines informativos, persuasivos y expresivos. Por ello, este tipo de comunicación depende del dominio de las convenciones del lenguaje escrito, facilidad con estructuras culturalmente aceptadas para la presentación y el argumento, conocimiento de la audiencia y otros factores específicos de la situación.

Durante el desarrollo del proyecto, se cumplió esta competencia mediante los entregables, los cuales han sido presentados a diferentes profesionales tales como el profesor gerente, el asesor cliente y el asesor de paper o co-autor, quienes son los encargados de revisar cada uno de estos documentos, ya sea en contexto, redacción, estructura clara, léxico variado y académico, y suficiencia de ejemplos y gramática. Asimismo, las presentaciones y revisiones de avances se realizaron con el profesor gerente, con el cual siempre se llevó un registro por cada uno de los

avances u objetivos cumplidos. Podría recomendar también revisiones, haciendo uso de los repositorios de archivos online, tales como Google Drive, Sharepoint, entre otros. Herramientas que facilitan el compartir archivos, permiten la edición online y la adición de comentarios por parte del revisor. A continuación, se presenta la evidencia del cumplimiento de este objetivo:

- Documentos de gestión de proyecto (PMBOK)
- Análisis de metodologías y estándares de gestión de riesgos y seguridad de la información (Benchmarking)
- Modelo de gestión de riesgos de seguridad de TI
- Herramienta de evaluación del nivel de madurez del gobierno de gestión de riesgos y seguridad de TI
- Evaluación del nivel de madurez de la empresa de estudio
- Evaluación del nivel de riesgo de los activos de TI que dependen de proveedores críticos en la empresa de estudio
- Plan de continuidad

En ese sentido, podemos concluir que la competencia WASC de comunicación escrita se cumplió durante todo el desarrollo del proyecto asegurando la calidad de cada uno de los documentos y entregables, mediante revisiones constantes. Solo puedo recomendar que, para facilitar el seguimiento y revisión de estos mismos, se podría utilizar alguna herramienta como el Jira, con la finalidad de facilitar estas tareas la necesidad de reuniones presenciales.

2. Comunicación oral

La comunicación oral se define como la capacidad para transmitir oralmente mensajes de manera eficaz dirigidos a diversas audiencias, usando diferentes herramientas que faciliten su comprensión y el logro del propósito. La comunicación se logra a través del lenguaje hablado con fines informativos, persuasivos y expresivos. Además del habla, la comunicación oral puede emplear ayudas visuales, lenguaje corporal, entonación y otros elementos no verbales para apoyar la transmisión del significado y la conexión con la audiencia. Por ello, cumplir con esta competencia plantea cierta dificultad para estudiantes como nosotros. Para nuestro caso en particular, significó explicar y hacer comprender a audiencia no especializada, sobre temas de gestión de riesgos y seguridad de TI.

Durante el transcurso del proyecto se desarrolló esta competencia gracias a las reuniones semanales realizadas con el profesor gerente, el asesor cliente y el co-autor para la revisión de

avances o validaciones necesarias. En estas reuniones se explicaban los distintos avances y entregables del proyecto, además de debatir posibles mejoras para estos mismos. Asimismo, se realizó reuniones con el gerente general de la empresa de estudio Kukyflor para presentar nuestro proyecto y los beneficios que obtendría luego de su implementación. Además, se realizaron reuniones periódicas con el personal de la empresa para el levantamiento de información y posterior trabajo de implementación. Adicionalmente, se realizó pre-sustentaciones frente al profesor gerente y asesor cliente para obtener feedback sobre la estructura de la presentación, la jerarquía y conexión de ideas, postura, fluidez, pronunciación y palabras usadas, a fin de ir mejor preparados a la sustentación con el comité del cual también se obtuvo observaciones importantes. Por ello, podría recomendar a otros estudiantes realizar siempre reuniones de pre-sustentaciones frente a sus asesores, sea esta presencial u online mediante videollamada, ya que nos percatamos que, esto fue lo que más no ayudó a desarrollar esta competencia. La evidencia principal del cumplimiento de esta competencia se puede observar en:

- Las actas de reunión con el profesor gerente, asesor cliente, co-autor y personal de la empresa de estudio.
- Pre-sustentaciones y sustentaciones

Se puede concluir que esta competencia WASC de comunicación oral sigue en constante desarrollo, ya que siempre se obtienen nuevas observaciones a partir de las reuniones con los distintos profesionales y asesores. Se pudo observar que las más grandes mejoras en las presentaciones se obtuvieron a partir de las reuniones de pre-sustentación y la misma sustentación ante el comité, las cuales considero son de suma importancia para el desarrollo de esta competencia.

3. Ciudadanía

La competencia de ciudadanía se refiere a la capacidad para valorar la convivencia humana en sociedades plurales, reflexionando acerca de las dimensiones morales, de las propias acciones y decisiones, asumiendo la responsabilidad por las consecuencias en el marco del respeto de los derechos y deberes ciudadanos. Por ello, fue muy importante identificar la necesidad de las pymes en el contexto de riesgos de TI, además de mantener en estricta reserva la información confidencial recopilada de la empresa de estudio.

Durante el desarrollo del proyecto, se logró el cumplimiento de esta competencia mediante la identificación de la necesidad en el documento de Project Charter, donde se evidenció el posible

impacto en las empresas frente a la sociedad por una mala gestión de riesgos de seguridad de TI. Por ello, se analizó la situación actual de las pymes a nivel nacional e internacional para poder plantear una solución adaptable a este tipo de empresas, las cuales cuentan con poca capacidad económica para implementación de estrategias de seguridad de TI y además tienen una cultura incipiente sobre este tipo de temas. En ese sentido, se realizó un análisis de las principales metodologías y estándares de gestión de riesgos y seguridad de la información que, mediante diálogos con el asesor cliente, se seleccionó las más idóneas para desarrollar un modelo de baja complejidad y costo adaptable a la necesidad de las pymes. Además, es importante resaltar que la validación del modelo en la empresa de estudio se dio gracias al diálogo que se llevó a cabo con el gerente general de la empresa Kukyflor, donde se explicó detalladamente y siempre con respeto los beneficios de la implementación del modelo y el cómo disminuirían los riesgos y el descontento de los clientes como consecuencia de ello. Por otro lado, se mantuvo en estricta reserva la información proporcionada por la empresa de estudio para la validación del modelo de gestión de riesgos de seguridad de TI. El cumplimiento de esta competencia se puede evidenciar en lo siguiente:

- Project Charter
- Memoria del proyecto
- Benchmarking

En conclusión, esta competencia WASC se cumplió gracias a la identificación de la necesidad o problemática en las pymes y la sociedad, en el contexto de la gestión de riesgos de TI, donde siempre se consideró la situación de este tipo de empresas para el planteamiento de la solución. Asimismo, por principios de moral y ética, se mantuvo en estricta reserva la información proporcionada por la empresa Kukyflor para la validación de la solución.

4. Manejo de la información

Esta competencia se refiere a la capacidad de identificar la información necesaria, así como de buscarla, seleccionarla, evaluarla y usarla éticamente, con la finalidad de resolver un problema. Por ello, durante el proyecto fue necesario partir de una necesidad o problema, para luego dirigir la investigación en seleccionar y evaluar los componentes necesarios para la elaboración de la solución, siempre respetando la propiedad intelectual y derechos de autor.

Durante el desarrollo del proyecto, el cumplimiento de esta competencia se ve evidenciada en el Project Charter, donde se identificó la necesidad de las pymes la cual está ligada a los procesos y

activos de TI que dependen de proveedores críticos y de donde partió toda la investigación. Se realizó la búsqueda de conceptos claves a partir de fuentes confiables y especializadas, que servirían como base para entender todo el tema abordado y poder continuar con la investigación de las metodologías y estándares, para luego comparar y seleccionar las que se adapten mejor a la situación de las pymes y finalmente, proponer la solución. Esta investigación, ayudó también a la elaboración del estado del arte, y la memoria del proyecto, donde se citaron y referenciaron debidamente los aportes de otros autores con la finalidad de respetar la propiedad intelectual y los derechos de autor. Después de organizar, sintetizar y utilizar la información necesaria, se obtuvo como resultado el modelo propuesto que satisface la necesidad de las pymes objeto de estudio. En la documentación del proyecto se respetó el estilo APA de referencias, recomendado por la facultad de ingeniería de la UPC. Se presenta la evidencia del cumplimiento de la competencia:

- Project Charter
- Memoria proyecto

Se puede concluir que, la identificación de la necesidad fue fundamental para iniciar toda la investigación. La búsqueda de conceptos, la comparativa, análisis y selección de metodologías y estándares se realizó a partir de fuentes confiables y especializadas, citadas debidamente en el formato APA en la documentación. De esto se obtuvo como resultado el modelo de gestión de riesgos de seguridad de TI que busca satisfacer la necesidad de las pymes.

5. Pensamiento innovador

Esta competencia se refiere a la capacidad para detectar necesidades y oportunidades para generar proyectos o propuestas innovadoras, viables y rentables. Se planifica y toma decisiones eficientes orientadas al objetivo del proyecto. Por ello, para el desarrollo del proyecto, supuso un reto la construcción de una solución innovadora que pueda satisfacer la necesidad de las pymes de disminuir el impacto de sus riesgos de TI asociados a proveedores críticos.

Durante el desarrollo del proyecto se logró cumplir con esta competencia, gracias a la identificación de la necesidad en el documento de Project Charter. Esta necesidad se refería al impacto generado por una mala gestión de los procesos y activos de TI que dependían de proveedores críticos en las pymes. Se llegó a esta conclusión luego de investigar, sintetizar y analizar la información de diferentes fuentes confiables como páginas reconocidas de noticias mundiales, informes de consultoras, artículos, tesis, entre otros. Proponer una solución innovadora que satisfaga esta necesidad en las pymes presentó un gran reto, ya que fue necesario

investigar y comparar distintas metodologías y estándares de gestión de riesgos y seguridad de la información para luego seleccionar las más idóneas y que mejor se complementarían con ayuda de la herramienta denominada Benchmarking. El resultado de esta investigación fue el modelo de gestión de riesgos de seguridad de TI orientado a proveedores críticos, el cual detalla un procedimiento a seguir y tiene como resultado planes de tratamiento o planes de acción para mejorar la gestión y disminuir el riesgo en las pymes. Por otro lado, en el desarrollo de la documentación del proyecto se presentó también el plan de costos, donde se aprecia el costo aproximado de la implementación y se demuestra la viabilidad económica de la propuesta; además, se puede apreciar como la pyme obtendría beneficios a partir del siguiente año a la implementación y recuperar toda la inversión en el año tres. Para el desarrollo del proyecto fue importante el uso de herramientas que manejen datos cuantitativos para la toma de decisiones, lo cual podría recomendar a otros estudiantes y profesionales para futuros proyectos. Los documentos que validaron el cumplimiento de esta competencia son los siguientes:

- Project Charter
- Benchmarking
- Modelo de gestión de riesgos de seguridad de TI
- Plan de costos del proyecto

En conclusión, para el cumplimiento de esta competencia fue muy importante recabar, sintetizar, analizar y seleccionar la información necesaria tanto para identificar la problemática o necesidad como para desarrollar la propuesta innovadora, la cual tendría como resultado un plan de acción priorizado para satisfacer la necesidad de las pymes, y siendo de igual importancia demostrar la viabilidad económica de esta propuesta.

6. Pensamiento crítico

Esta competencia se refiere a la capacidad para explorar de manera exhaustiva problemas, ideas o eventos para formular conclusiones u opiniones sólidamente justificadas. Por ello, para evidenciar esta competencia en el presente proyecto fue necesaria la motivación para buscar la verdad y poder identificar el problema o necesidad de las pymes a partir del análisis de la información recopilada tomando en consideración el contexto de este tipo de empresas.

Durante el desarrollo del proyecto se cumplió con esta competencia, gracias a la identificación de la necesidad de las pymes en materia de gestión de riesgos y seguridad de TI. En ese sentido, considerando este contexto, se analizó y sintetizó información de diferentes fuentes, tales como

páginas web de noticias, papers, informes de consultoras, tesis, entre otras. Luego de un proceso de evaluación y cuestionamiento de esta información se identificó la necesidad de este tipo de empresas, la cual se refiere a disminuir el impacto de los riesgos que afectan a los procesos y activos de TI que dependen de proveedores críticos. Las causas que originan esta necesidad son variadas; sin embargo, entre las principales tenemos:

- La falta de seguimiento al cumplimiento de los controles de seguridad en los proveedores.
- No existe una implementación de controles adecuados debido a que la mayoría de las pymes no cuentan con un área especializada de gestión de riesgos o tienen deficiencias en la gestión de las mismas.
- La falta de auditorías que permita asegurar el cumplimiento de los acuerdos de nivel de servicio (SLAs) establecidos por los proveedores.
- Falta de controles adecuados para los proveedores con acceso a los activos de información de las empresas.

En general, las pymes dedican la mayor parte de sus recursos y presupuesto a los procesos relacionados a la actividad principal de la organización, es decir la que genera la mayor cantidad de ingresos, descuidando así la gestión de riesgos y más aún la seguridad de TI y, por consiguiente, la mayoría de estas empresas no cuentan con una adecuada cultura organizacional relacionada a estos temas. Según un informe de PWC (PricewaterhouseCoopers), la globalización de las TI y el constante cambio que sufren estas, genera cada vez más incidentes de seguridad que afecta directamente a las empresas y a la calidad del servicio que ofrecen a sus clientes. Además, se afirma que, de estos incidentes de seguridad, el 20% están relacionados con contratistas o proveedores. Asimismo, según un estudio realizado por A. Santos-Olmo (2016), el 73% de las pymes de Gran Bretaña cuentan con un nivel incipiente en gestión de riesgos y de estas pymes se encontró que la mayoría carecen de políticas de seguridad y sistemas de evaluación de riesgos, siendo un caso aún más preocupante en Latinoamérica donde la cifra superaría el 80%. Por otro lado, la cultura en gestión de riesgos y seguridad de la información en este tipo de organizaciones es otro factor para tomar en cuenta. De un estudio realizado por Montenegro y Moncayo (2016) a 307 pymes, se obtuvo que solo en el 9% de ellas puede considerarse que existe una cultura organizacional sobre la seguridad de la información. Por consiguiente, después de un análisis exhaustivo, se concluyó que es necesario un modelo de referencia que esté compuesto por una metodología y un estándar de gestión de riesgos y seguridad de la información, que se complementen y a su vez, se adapten a la realidad de las pymes. El resultado del procedimiento

planteado por el modelo debería satisfacer la necesidad de disminuir el nivel de riesgo en los procesos y activos de TI que dependen de proveedores críticos. El cumplimiento de esta competencia de evidencia en los siguientes entregables:

- Project Charter
- Benchmarking
- Modelo de gestión de riesgos de seguridad de TI

En síntesis, el cumplimiento de esta competencia se evidencia en la identificación de la necesidad en las pymes, la cual se planteó y explicó en base a la información recopilada y analizada de manera exhaustiva en el contexto de la gestión de riesgos y seguridad de TI. A partir de esta evaluación, se pudo concluir que, es necesaria una solución que satisfaga esta necesidad latente y que se adapte a la realidad de las pymes, es por ello, que se propuso el modelo de gestión de riesgos de seguridad de TI como resultado de nuestro proyecto.

7. Razonamiento cuantitativo

Esta competencia se refiere a la capacidad para interpretar, representar, comunicar y utilizar información cuantitativa diversa en situaciones de contexto real. Incluye calcular, razonar, emitir juicios y tomar decisiones con base en esta información cuantitativa. Por ello, para evidenciar el cumplimiento de esta competencia, se demostrará como los datos cuantitativos fueron importantes para el análisis y toma de decisiones durante el desarrollo de los entregables del proyecto.

Esta competencia se evidencia en varias etapas del proyecto. Recordemos que, en base a la necesidad identificada al inicio del proyecto, se propuso la elaboración de un modelo de gestión de riesgos de seguridad de TI. Para la construcción del modelo de referencia fue necesario realizar una comparativa entre metodologías y estándares de gestión de riesgos y seguridad de la información seleccionados cuidadosamente y que puedan adaptarse a la realidad de las pymes. Esta comparativa se realizó mediante la herramienta denominada Benchmarking, la cual está compuesta por criterios comunes a cada uno de los elementos a comparar y con una respectiva escala de puntajes asociada a cada uno de estos criterios. Luego de colocar puntajes por cada criterio comparativo y mediante una simple suma de estos puntajes, esta herramienta permitió seleccionar la mejor metodología y estándar para la construcción del modelo de gestión de riesgos de seguridad de TI. En adición, para la etapa de validación del modelo en un caso de estudio, se usaron métodos cuantitativos para realizar cálculos, emitir juicios y demostrar la efectividad del modelo mediante indicadores de éxito. En ese sentido, se diseñó una herramienta de evaluación

en base a puntajes asignados a preguntas para la empresa de estudio que, mediante un cálculo cuantitativo se obtiene como resultado niveles de madurez para cada uno de los componentes del modelo, además de un nivel general, esto con la finalidad de medir el estado de actual de la empresa en lo que respecta al gobierno de gestión de riesgos y seguridad de TI, y proponer opciones de mejora o recomendaciones. Por otro lado, se realizó una simulación de la implementación del procedimiento del modelo, donde en las diferentes fases de este, se aplicó el método cuantitativo de la metodología Magerit para valorizar los activos y amenazas, y calcular el impacto, riesgo inherente y riesgo residual de los activos de TI, esto con la finalidad de proponer controles o recomendaciones para la empresa de estudio y medir la efectividad de estos controles. Además, para cada uno de estos procedimientos que fueron parte de la etapa de validación en la empresa de estudio, se propusieron métricas de éxito para medir la efectividad del modelo en lo que respecta al nivel de madurez del gobierno de gestión de riesgos y seguridad de TI, y al nivel de riesgo de los activos de TI que dependen de proveedores críticos. Adicionalmente, en el plan de costos del proyecto se usaron cálculos matemáticos para obtener el costo aproximado del proyecto, los ahorros o beneficios que se obtendrían luego de su implementación y la viabilidad económica de la propuesta. Los entregables que evidencian el cumplimiento de esta competencia son los siguientes:

- Benchmarking
- Herramienta de evaluación
- Hoja de trabajo de la simulación de la implementación del modelo
- Plan de costos del proyecto

En conclusión, se evidenció el cumplimiento de esta competencia mediante el uso de métodos y cálculos cuantitativos en la etapa de análisis y selección de metodologías y estándares para el diseño del modelo, en la etapa de validación del modelo y en la elaboración del plan de costos del proyecto, ya que fueron muy importantes para facilitar el análisis, emitir juicios y tomar decisiones sobre los planes de acción o medir el éxito de la implementación.

ANEXO B – BENCHMARKING

Anexo B-1: Criterios de selección del benchmarking de metodologías

Nº	Criterio	Descripción	Puntaje
1	Costo de la metodología (5 puntos)	Costo de la documentación, licencias y otros cargos necesarios para adquirir el derecho a utilizar la herramienta. No incluye software que respalde lo mencionado anteriormente si está disponible por una tarifa o costo adicional de implementación de la solución. El costo tiene un impacto significativo en la disponibilidad de soluciones para empresas y organizaciones que tienen un presupuesto menor o administran activos de menor valor.	• 5 puntos si es una solución gratuita; • 2 puntos si la herramienta esta no más de 1000 euros; • 0 puntos si la herramienta es superior a 1000 euros.
2	Documentación en inglés (2 puntos)	Disponibilidad de documentación estándar en inglés. El inglés es ampliamente reconocido como el idioma principal de comunicación en el sector de TI. Otros idiomas, aunque se usan en muchos países, pueden considerarse idiomas nacionales.	• Documentación disponible (2 puntos); • Documentación no disponible (0 puntos).
3	Estándar nacional (2 puntos)	¿Es la metodología un estándar en al menos un país? La estandarización de metodologías a nivel nacional, por un lado, puede implicar el requisito de la aplicación de un método en un país determinado. Por otro lado, el hecho de que una determinada metodología se reconozca como estándar demuestra	• Sí (2 puntos); • No (0 puntos)

		tanto la calidad como el reconocimiento de la metodología determinada.	
4	Estándar internacional (4 puntos)	¿Es la metodología un estándar internacional? Por un lado, la estandarización de metodologías a nivel internacional puede indicar el requisito de utilizar un método autorizado por la ley. Por otro lado, el hecho de que una determinada metodología se reconozca como estándar demuestra tanto la calidad como el reconocimiento de una metodología determinada.	• Sí (4 puntos); • No (0 puntos).
5	Grupo objetivo (5 puntos)	Destinatario de la metodología debido al tipo de actividad, tamaño, área de operación, etc. Cuanto más universal sea la metodología, mayor será el grupo objetivo que lo use.	• Sin limitación (5 puntos); • Limitación del tamaño o tipo de entidad (3 puntos); • Limitación del tamaño y tipo de entidad (1 punto).
6	Complejidad de uso (5 puntos)	El nivel de dificultad relacionado con la implementación y el mantenimiento de la metodología. Se asocia con la experiencia requerida. Un alto nivel de complejidad de la metodología restringe a los usuarios a un grupo de especialistas, en muchos casos, impidiendo su uso por parte de los gerentes en todos los niveles de la empresa	• Fácil + fácil (5 puntos); • Fácil + normal (3 puntos); • Normal + difícil (1 puntos).

7	Popularidad (2 puntos)	Popularidad de la metodología en el mundo. La popularidad en el mercado internacional es una prueba de la universalidad de las soluciones y una prueba de su alta calidad como producto.	• Grandes, internacionales (2 puntos); • Pequeño, local (0 puntos).
8	Flexibilidad (3 puntos)	La capacidad de la metodología para adaptarse a una empresa específica (evaluación personalizada de los eventos). El mismo evento puede tener diferentes significados en función de la vista en perspectiva, las características específicas del mercado, la empresa (ubicación, un equipo de personas, etc.).	• Grande (3 puntos) • Promedio (2 puntos) • Pequeño (1 puntos).
9	Método de identificación de riesgos (2 puntos).	Sistema de identificación de riesgos (auditoría, listas de verificación, etc.) utilizado en el método / metodología.	• Directo (2 puntos) • Indirecto (1 punto) • Ninguno (0 puntos)
10	La base para el cálculo del riesgo (2 puntos)	Método para determinar el valor de riesgo (equitación, matriz, otro) y los valores de los componentes utilizados para calcularlo.	• Basado en los valores cualitativos (2 puntos) • Basado en los valores cuantitativos (0 puntos)
11	Monitoreo de riesgos (2 puntos)	Si la metodología permite el monitoreo de riesgos. La detección de un evento reconocido, como un elemento de riesgo debe ser registrado. Se evalúa el método de manejo de tales eventos	• Si tiene (2 puntos) • No tiene (0 puntos)
12	Adaptabilidad (4 puntos)	La capacidad de metodología para adaptarse a las condiciones ambientales	• Automático (4 puntos) • Manual (2 puntos);

		cambiantes, la capacidad de uso en condiciones no estándar.	• Ninguno (0 puntos)
13	Herramienta Software (5 puntos)	Si la metodología cuenta con un software personalizado que lo respalde.	• Free Tool (5 puntos) • Paid Tool (2 puntos) • No tiene (0 puntos)
14	Análisis de la metodología (5 puntos)	Enfoques disponibles para evaluar los componentes de un riesgo. Estos enfoques se pueden categorizar como: Cualitativo y Cuantitativo	• Cuantitativo (5 punto) • Cualitativo (2 puntos)
15	Actualización de la metodología (2 puntos)	Si la metodología está actualizada con los últimos cambios	• Actualizado (2 punto) • Descontinuado (0 puntos)

Tabla B-1: Criterios de selección metodologías

Fuente: Elaboración propia

Anexo B-2: Criterios de selección del benchmarking de estándares

Nº	Criterio	Descripción	Puntaje
1	Costo del uso del estándar (5 puntos)	Costo de la documentación, licencias y otros cargos necesarios para adquirir el derecho a utilizar el estándar. No incluye software que respalde lo mencionado anteriormente si está disponible por una tarifa o costo adicional de implementación de la solución. El costo tiene un impacto significativo en la disponibilidad de soluciones para empresas y organizaciones que tienen un presupuesto menor o administran activos de menor valor.	• La documentación es gratuita (5 puntos); • Documentación cuesta no más de 150 dólares (3 puntos) • La documentación tiene un costo superior a 150 dólares (0 puntos)
2	Documentación en inglés (2 puntos)	Disponibilidad de documentación estándar en inglés. El inglés es ampliamente reconocido como el idioma principal de comunicación en el sector de TI. Otros idiomas, aunque se usan en muchos países, pueden considerarse idiomas nacionales.	• Documentación disponible (2 puntos); • Documentación no disponible (0 puntos).
3	Sector objetivo (5 puntos)	El tipo o sector más apropiado de organizaciones a los que el producto apunta para su implementación.	• Pequeña / Mediana / Grande / Gubernamental (Todos los sectores) (5 puntos); • Pequeña / Mediana (3 puntos); • Grande / Gubernamental (1 punto).

4	Complejidad de uso (5 puntos)	El nivel de dificultad relacionado con la implementación y el mantenimiento del estándar. Se asocia con la experiencia requerida. Un alto nivel de complejidad en el estándar restringe a los usuarios a un grupo de especialistas, en muchos casos, impidiendo su uso por parte de los gerentes en todos los niveles de la empresa.	• Baja (5 puntos); • Media (3 puntos); • Alta (1 puntos).
5	Uso geográfico (5 puntos)	Que un estándar sea usado a nivel internacional o en el mayor número de zonas geográficas es una prueba de la alta calidad de sus soluciones.	• Internacional (5 puntos); • Continente / local (2 puntos).
6	Actualización del estándar (3 puntos)	Si el estándar está actualizado con los últimos cambios.	• Actualizado (3 puntos) • Descontinuado (0 puntos)
7	Tratamiento de Riesgos (5 puntos)	Si el estándar cuenta con estrategias de tratamiento de riesgos. Se identifica estrategias o controles para aceptar, evadir, transferir o mitigar el riesgo.	• Si tiene (5 puntos) • No tiene (0 puntos)
8	Monitoreo de riesgos (5 puntos)	Si la metodología permite el monitoreo de riesgos. La detección de un evento reconocido, como un elemento de riesgo debe ser registrado. Se evalúa el método de manejo de tales eventos	• Si tiene (5 puntos) • No tiene (0 puntos)
9	Número de controles (5 puntos)	La cantidad de controles que propone el estándar son importantes ya que permite a las organizaciones tener un mayor número	• Más de 100 controles (5 puntos); • Entre 50 y 100 controles

		de opciones para mantener la seguridad de la información.	• (3 puntos) • Menos de 50 controles (1 puntos).

Tabla B-2: Criterios de selección estándar de gestión de seguridad de información

Fuente: Elaboración propia

ANEXO C - RESULTADOS DE LA ENCUESTA JUICIO DE EXPERTOS

1. Experto 1

Universidad Peruana de Ciencias Aplicadas		
ENCUESTA DE VALORIZACIÓN (JUICIO DE EXPERTOS)		
Estimado experto, usted ha sido seleccionado para validar el "Modelo de gestión de riesgos de seguridad de TI para PYMES del sector comercial que dependen de proveedores críticos". La validación es de gran relevancia para medir la eficiencia del modelo y que los resultados obtenidos a partir de estos sean utilizados eficientemente. Agradecemos su valiosa colaboración al completar la encuesta referida en este documento.		
Nombre y apellidos del experto:	<u>Felix Ccoicca Sarmiento</u>	
Cargo actual:	<u>Jefe de Riesgos y Cumplimiento TI - Interbank</u>	
Fecha:	<u>24 - Abril - 2018</u>	
Firma:		
 Objetivo del proyecto:		
Implementar un Modelo de Gestión de Riesgos de Seguridad de TI en una Pyme del Sector Comercial que dependa de proveedores críticos		

Calificación

Marque la opción según la matriz de indicadores mostradas anteriormente

Fase	Criterio	Suficiencia	Claridad	Coherencia	Relevancia
1. Evaluación del riesgo	Procesos asociados a proveedores críticos de TI	3	3	3	4
	Activos de TI asociados a proveedores críticos	3	3	3	4
	Amenazas asociadas a los activos de TI	4	3	4	4
	Amenazas asociadas a la seguridad de información de la empresa	4	3	4	4
	Amenazas asociadas a la seguridad de información relacionado a proveedores críticos	4	3	4	4
	Impacto y riesgo	4	3	3	4
2. Tratamiento del riesgo	Establecimiento de controles	4	3	4	4
	Planes de tratamiento	4	3	4	4
3. Seguimiento y control	Monitoreo y control	4	3	4	4
	Auditorías	4	3	4	4

2. Experto 2

Universidad Peruana de Ciencias Aplicadas

ENCUESTA DE VALORIZACIÓN (JUICIO DE EXPERTOS)

Estimado experto, usted ha sido seleccionado para validar el "Modelo de gestión de riesgos de seguridad de TI para PYMES del sector comercial que dependen de proveedores críticos". La validación es de gran relevancia para medir la eficiencia del modelo y que los resultados obtenidos a partir de estos sean utilizados eficientemente. Agradecemos su valiosa colaboración al completar la encuesta referida en este documento.

Nombre y apellidos del experto: Willian Antonio Carrasco Exebio

Cargo actual: Subgerente de Auditoría de Riesgos de Ciberseguridad

Fecha: 23/04/2019

Firma:

Objetivo del proyecto:

Implementar un Modelo de Gestión de Riesgos de Seguridad de TI en una Pyme del Sector Comercial que dependa de proveedores críticos

Calificación

Marque la opción según la matriz de indicadores mostradas anteriormente

Fase	Criterio	Suficiencia	Claridad	Coherencia	Relevancia
1. Evaluación del riesgo	Procesos asociados a proveedores críticos de TI	4	4	4	4
	Activos de TI asociados a proveedores críticos	4	4	4	4
	Amenazas asociadas a los activos de TI	4	4	4	4
	Amenazas asociadas a la seguridad de información de la empresa	4	4	4	4
	Amenazas asociadas a la seguridad de información relacionado a proveedores críticos	4	4	4	4
	Impacto y riesgo	4	4	4	4
2. Tratamiento del riesgo	Establecimiento de controles	4	4	4	4
	Planes de tratamiento	4	4	4	4
3. Seguimiento y control	Monitoreo y control	4	4	4	4
	Auditorias	4	4	4	4

Observaciones

Universidad Peruana de Ciencias Aplicadas

Observaciones para el modelo

CONSIDERO QUE EL MODELO Y ESTANDAR SELECCIONADO SON ADECUADOS Y PERMITIRÁN IDENTIFICAR LOS RIESGOS ASOCIADOS Y EFECTUAR SU TRATAMIENTO.

3. Experto 3

ENCUESTA DE VALORIZACIÓN (JUICIO DE EXPERTOS)

Estimado experto, usted ha sido seleccionado para validar el “**Modelo de gestión de riesgos de seguridad de TI para PYMES del sector comercial que dependen de proveedores críticos**”. La validación es de gran relevancia para medir la eficiencia del modelo y que los resultados obtenidos a partir de estos sean utilizados eficientemente. Agradecemos su valiosa colaboración al completar la encuesta referida en este documento.

Nombre y apellidos del experto: Rómulo Longarte Alvarado
Cargo actual: Gerente General de ITB Consulting
Fecha: 24/04/2019
Firma: [Firma manuscrita]

Objetivo del proyecto:

Implementar un Modelo de Gestión de Riesgos de Seguridad de TI en una Pyme del Sector Comercial que dependa de proveedores críticos

Calificación

Marque la opción según la matriz de indicadores mostradas anteriormente

Fase	Criterio	Suficiencia	Claridad	Coherencia	Relevancia
1. Evaluación del riesgo	Procesos asociados a proveedores críticos de TI	4	4	4	4
	Activos de TI asociados a proveedores críticos	4	4	4	4
	Amenazas asociadas a los activos de TI	4	4	4	4
	Amenazas asociadas a la seguridad de información de la empresa	4	4	3	4
	Amenazas asociadas a la seguridad de información relacionado a proveedores críticos	4	4	4	4
	Impacto y riesgo	4	4	4	4
2. Tratamiento del riesgo	Establecimiento de controles	4	4	4	3
	Planes de tratamiento	4	4	4	4
3. Seguimiento y control	Monitoreo y control	4	4	4	4
	Auditorias	4	4	4	4

Observaciones

Observaciones para el modelo

La cantidad de preguntas podría disminuir a el porcentaje que resulta la encuesta.
La posibilidad de remota que posible.

4. Experto 4

ENCUESTA DE VALORIZACIÓN (JUICIO DE EXPERTOS)

Estimado experto, usted ha sido seleccionado para validar el "Modelo de gestión de riesgos de seguridad de TI para PYMES del sector comercial que dependen de proveedores críticos". La validación es de gran relevancia para medir la eficiencia del modelo y que los resultados obtenidos a partir de estos sean utilizados eficientemente. Agradecemos su valiosa colaboración al completar la encuesta referida en este documento.

Nombre y apellidos del experto: Marco Antonio Via Escalante

Cargo actual: Auditor Senior de TI

Fecha: 02/05/2019

Firma:

Objetivo del proyecto:

Implementar un Modelo de Gestión de Riesgos de Seguridad de TI en una Pyme del Sector Comercial que dependa de proveedores críticos

Calificación

Fase	Criterio	Suficiencia	Claridad	Coherencia	Relevancia
1. Evaluación del riesgo	Procesos asociados a proveedores críticos de TI	Moderado	Alto	Moderado	Moderado
	Activos de TI asociados a proveedores críticos	Moderado	Moderado	Alto	Alto
	Amenazas asociadas a los activos de TI	Bajo	Moderado	Moderado	Alto
	Amenazas asociadas a la seguridad de información de la empresa	Alto	Moderado	Alto	Alto
	Amenazas asociadas a la seguridad de información relacionado a proveedores críticos	Bajo	Moderado	Moderado	Alto
	Impacto y riesgo	Moderado	Alto	Moderado	Moderado
Tratamiento del riesgo	Establecimiento de controles	Alto	Moderado	Alto	Alto
	Planes de tratamiento	Moderado	Moderado	Moderado	Moderado
Seguimiento y control	Monitoreo y control	Bajo	Moderado	Moderado	Bajo
	Auditorías	Moderado	Moderado	Moderado	Moderado

Observaciones

Universidad Peruana de Ciencias Aplicadas Observaciones para el modelo Considero que durante la evaluación de los procesos y activos gestionados por proveedores externos se deben contemplar herramientas que complementen al modelo de seguridad de grado; ~~Un~~ Un Security Operation Center que monitoree los servicios o procesos críticos de las empresas y que existan cláusulas específicas que garanticen la transparencia ~~y~~ integridad de la información utilizada por los proveedores.	

5. Experto 5

ENCUESTA DE VALORIZACIÓN (JUICIO DE EXPERTOS)

Estimado experto, usted ha sido seleccionado para validar el “**Modelo de gestión de riesgos de seguridad de TI para PYMES del sector comercial que dependen de proveedores críticos**”. La validación es de gran relevancia para medir la eficiencia del modelo y que los resultados obtenidos a partir de estos sean utilizados eficientemente. Agradecemos su valiosa colaboración al completar la encuesta referida en este documento.

Nombre y apellidos del experto: Christian Quispe Quispe
 Cargo actual: Oficial de Seguridad de la Información
 Fecha: 04/05/2019
 Firma: [Firma manuscrita]

Objetivo del proyecto:

Implementar un Modelo de Gestión de Riesgos de Seguridad de TI en una Pyme del Sector Comercial que dependa de proveedores críticos

Calificación

Marque la opción según la matriz de indicadores mostradas anteriormente

Fase	Criterio	Suficiencia	Claridad	Coherencia	Relevancia
1. Evaluación del riesgo	Procesos asociados a proveedores críticos de TI	3	2	4	4
	Activos de TI asociados a proveedores críticos	3	2	4	4
	Amenazas asociadas a los activos de TI	3	2	4	4
	Amenazas asociadas a la seguridad de información de la empresa	3	2	4	4
	Amenazas asociadas a la seguridad de información relacionado a proveedores críticos	3	2	4	4
	Impacto y riesgo	3	2	4	4
2. Tratamiento del riesgo	Establecimiento de controles	3	2	4	4
	Planes de tratamiento	3	2	4	4
3. Seguimiento y control	Monitoreo y control	3	2	4	4
	Auditorías	3	2	4	4

[Firma manuscrita]
 04/05/2019

2/3

Observaciones

Observaciones para el modelo

En base a la información enviada revise el modelo presentado por los alumnos y, si bien a alto nivel lo considero correcto por el alineamiento a estándares y prácticas recomendadas por la industria, sugiero las siguientes oportunidades de mejora:

- 1- El modelo debe tener en cuenta desde el inicio las limitantes propias del sector en análisis (PYMES), por ejemplo: limitaciones en conocimiento especializado, asignación de recursos, jerarquías y roles, etc.
- 2- Teniendo en cuenta la relevancia de cada criterio, no se ha profundizado en los mismos, quedando muy abierta la interpretación de los mismos.
- 3- Se sugiere mejorar el modo de recolección basado en encuestas: Por ejemplo, encuesta de alto nivel para el rol más elevado de la PYME y encuesta específica para los roles operativos.
- 4- Utilizar un lenguaje sencillo de entender en las encuestas teniendo en cuenta el punto 1.
- 5- Incorporar los criterios y/o estándares para dar claridad a cómo obtener el objetivo específico "Plan de Continuidad" especialmente si por ello se refieren a un plan de continuidad de negocio.

04/05/2019

ANEXO D - CUESTIONARIO ASSESSMENT

- 1. ¿La empresa tiene identificados sus procesos y proveedores críticos de TI? ¿Se encuentran documentados o registrados? ¿La empresa entiende los procesos y conoce los productos o servicios que brindan estos proveedores?**

R1: La empresa no tiene un conocimiento adecuado de sus procesos y proveedores críticos de TI

R2: La empresa tiene identificado algunos procesos y proveedores críticos de TI con un incipiente nivel de entendimiento

R3: La empresa tiene identificados sus procesos y proveedores críticos TI con un buen nivel de entendimiento

R4: La empresa tiene identificados, registrados y/o documentados sus procesos y proveedores críticos de TI con un alto nivel de entendimiento

R5: La empresa mantiene documentado, interiorizado y actualizado el registro de sus procesos y proveedores críticos de TI, así estos sean muy cambiantes en el tiempo

- 2. ¿Se encuentra establecido en la organización algún procedimiento para la identificación de procesos y proveedores críticos de TI? ¿El procedimiento se encuentra documentado, divulgado dentro de la organización y en mejora continua?**

R1: Los procesos y proveedores críticos de TI no se encuentran identificados ni documentados o se identificaron de manera incipiente

R2: El procedimiento de identificación de procesos y proveedores críticos de TI se encuentra en desarrollo

R3: El procedimiento de identificación de procesos y proveedores críticos de TI se encuentra implementado

R4: La identificación de procesos y proveedores críticos de TI se encuentra documentado y divulgada en toda la organización

R5: La identificación de procesos y proveedores críticos de TI se encuentra documentada, interiorizada y en mejora continua

3. ¿La empresa cuenta con herramientas o sistemas donde se tenga un registro de los procesos y proveedores críticos de TI categorizados o clasificados? ¿Estos sistemas se prestan a la rápida obtención de la información, apoyando al análisis y toma de decisiones?

R1: No existen sistemas donde se registren los procesos y proveedores de TI o si se tienen, se registran en muy raras ocasiones

R2: Se registran los procesos y proveedores críticos de TI en algún sistema o base de datos

R3: Los procesos o proveedores críticos de TI se encuentran registrados en algún sistema, pero sin clasificar o categorizar

R4: Los procesos y proveedores críticos de TI se encuentran registrados y clasificados en un sistema de información listo para su rápida explotación

R5: Se mantiene en constante mejora el sistema que aloja el registro de procesos y proveedores críticos de TI para su rápida explotación y así apoyar al análisis de gestión de riesgos

4. ¿La empresa tiene identificados y clasificados los activos de TI que gestionan sus proveedores críticos?

R1: La empresa no tiene un conocimiento adecuado de los activos de TI que gestionan sus proveedores críticos

R2: Algunos empleados entienden la importancia de tener los activos de TI correctamente identificados y clasificados, por ello empiezan a realizar tareas sencillas de identificación

R3: Los empleados y la gerencia tienen identificados sus activos de TI a conciencia

R4: Los empleados y la gerencia tienen identificados y clasificados los activos de TI

R5: La empresa mantiene a los activos de TI identificados, clasificados, actualizados y divulgados en toda la organización

5. ¿Se encuentra establecido el procedimiento de identificación y registro de activos de TI? ¿Este procedimiento se encuentra documentado, divulgado y en mejora continua?

R1: El procedimiento de identificación de activos de TI no se encuentra desarrollado ni documentado

R2: El procedimiento de identificación de activos de TI se encuentra en desarrollo

R3: El procedimiento de identificación de activos de TI se ha implementado de manera consciente

R4: El procedimiento de identificación de activos de TI se encuentra implementada, documentada y divulgada en toda la organización

R5: El procedimiento de identificación de los activos de TI se encuentra implementada, documentada, divulgada y en mejora continua

6. ¿La organización cuenta con herramientas o sistemas donde se tenga un registro de los activos de TI, además se encuentran clasificados o categorizados? ¿Estos sistemas se prestan a la rápida obtención de la información, apoyando al análisis y toma de decisiones?

R1: No existen sistemas donde se registren los activos de TI de la organización o si se tienen, se registran en muy raras ocasiones

R2: Se registran los activos de TI en algún sistema o base de datos que tiene la organización

R3: Los activos de TI se encuentran registrados en algún sistema, pero sin clasificar o categorizar

R4: Los activos de TI se encuentran registrados y clasificados en un sistema de información listo para su rápida explotación

R5: Se mantiene en constante mejora el sistema que aloja el registro de activos de TI para su rápida explotación y así apoyar al análisis y toma de decisiones

7. ¿La empresa tiene identificadas, clasificadas y valoradas las amenazas que afectan a sus activos de TI?

R1: La empresa tiene prácticas iniciales o nulas para la identificación de amenazas que pueden afectar a sus activos de TI

R2: Algunas personas de la organización están tomando conciencia sobre las amenazas que pueden afectar a los activos de TI y empiezan a identificarlas

R3: La empresa tiene un buen conocimiento sobre las amenazas que afectan a los activos de TI, las identifican y clasifican por tipología

R4: La empresa tiene correctamente identificadas, clasificadas y valoradas a las amenazas que afectan a sus activos de TI

R5: La empresa mantiene las amenazas que afectan a sus activos de TI identificadas, clasificadas, valoradas y divulgadas en toda la organización. Esta información es actualizada periódicamente

8. ¿Se encuentra establecido algún procedimiento de identificación de amenazas que afectan a los activos de TI? ¿Este procedimiento se encuentra documentado, divulgado y en mejora continua?

R1: El procedimiento de identificación de las amenazas que afectan a los activos de TI no se encuentra desarrollada ni documentada

R2: El procedimiento de identificación de amenazas que afectan a los activos de TI se encuentra en proceso de desarrollo

R3: El procedimiento de identificación de las amenazas se ha implementado de manera consciente en la organización

R4: El procedimiento de identificación de las amenazas que afectan a los activos de TI se encuentra implementada, documentada y divulgada en toda la organización

R5: El procedimiento de identificación de amenazas que afectan a los activos de TI se encuentra implementada, documentada, divulgada y en mejora continua

9. ¿La empresa cuenta con herramientas o sistemas donde se tenga un registro de las amenazas que afectan a los activos de TI, además estas se encuentran clasificadas o categorizadas? ¿Estos sistemas se prestan a la rápida obtención de la información, apoyando al análisis y toma de decisiones?

R1: No existen sistemas donde se registren las amenazas que afectan a los activos de TI o si se tienen, se registran muy raras veces

R2: Se registran las amenazas en algún sistema o base de datos

R3: Las amenazas se encuentran registradas en algún sistema, pero sin clasificar o categorizar

R4: Las amenazas se encuentran registradas y clasificadas en un sistema de información listo para su rápida explotación

R5: Se mantiene en constante mejora el sistema donde se registran las amenazas para apoyar al análisis y toma de decisiones

10. ¿La empresa cuenta con políticas o procedimientos de seguridad de la información?

R1: La empresa no cuenta con políticas o si los tiene son mínimos; motivo por los cuales tiene poca conciencia sobre la seguridad de información.

R2: Se establecen políticas de seguridad de información siguiendo los objetivos de la organización

R3: Las políticas o procedimientos se divulgan en toda la organización para que esta se encuentre preparada ante cualquier eventualidad

R4: Se hacen revisiones periódicas a las políticas de seguridad de información a través de auditorías de sistemas de información

R5: La organización apoya y contribuye al mejoramiento continuo de la seguridad de información incluyendo todas las áreas de la empresa.

11. ¿La organización tiene definida una política o procedimiento de gestión de riesgos que apoye a una adecuada gestión de la seguridad de información asociado a los activos, procesos y servicio de TI?

R1: La organización tiene políticas de gestión de riesgos de seguridad de TI, pero estas no aseguran la confidencialidad, integridad y disponibilidad de la información

R2: La empresa tiene definido políticas de gestión de riesgos de seguridad de TI que aseguren disminuir el impacto ocasionado por las amenazas a los activos, procesos y servicios de TI

R3: La política de gestión de riesgos establece claramente los lineamientos, roles y responsabilidades y declaración del apetito al riesgo. Esto asegura a una gestión eficaz de la seguridad de información

R4: Se hacen revisiones periódicas a la política de gestión de riesgos a través de procesos sistemáticos para asegurar el cumplimiento y validación de estas y así asegurar una adecuada seguridad de información.

R5: Se utiliza un indicador de cumplimiento para establecer si las políticas de gestión de riesgos establecidas por la organización están siendo llevándose conforme fueron establecidas.

12. ¿La organización cuenta con herramientas tecnológicas para gestionar de manera eficiente las amenazas asociadas a la seguridad de información?

R1: La empresa no cuenta con herramientas para gestionar de manera adecuada las amenazas asociadas a la seguridad de información.

R2: La empresa cuenta con algunas herramientas para mitigar las amenazas de seguridad de información por lo cual la gestión de las amenazas es deficiente

R3: La organización cuenta con herramientas propias y adquiridas para tratar las amenazas asociadas a la seguridad de información

R4: La organización tiene roles y responsabilidades definidos para hacer uso de las diferentes herramientas con que cuenta para mitigar las amenazas asociadas a la seguridad de información

R5: Se hacen revisiones y controles periódicos a todas las herramientas (propias y adquiridas) con que cuenta la organización contribuyendo a la mejora continua

13. ¿La organización tiene identificados los procesos, servicios o productos que le brinda el proveedor crítico?

R1: La organización se encuentra en un nivel inicial sobre gestión de riesgos de seguridad de información, por lo que no les da la debida importancia a los riesgos de seguridad de TI asociados al proveedor crítico.

R2: La organización se comunica con el proveedor solo cuando existen problemas respecto al servicio o producto que este le brinda

R3: La organización tiene constante comunicación con el proveedor crítico, por lo que conoce los servicios, procesos o productos que este le brinda

R4: Todas las áreas de la organización están informados sobre el proveedor por lo que la organización conoce perfectamente a todos los proveedores y producto o servicio que este le brinda

R5: La organización supervisa continuamente al proveedor a través de un área especializada que establece políticas y controles de cómo hacerlo

14. ¿La empresa tiene políticas o procedimientos para verificar que el proveedor crítico garantice la seguridad de la información de los procesos, servicios o productos que maneja de la misma?

R1: La organización no cuenta con políticas o procedimientos para supervisar la entrega de productos o servicios de parte del proveedor crítico

R2: La organización define políticas para hacer un adecuado seguimiento a las políticas de seguridad de información

R3: La organización realiza informes de seguimiento para verificar que el proveedor cumpla los acuerdos de nivel de servicio (SLA's) establecido por el proveedor

R4: La organización solicita constantemente las políticas o auditorias de seguridad de TI a los proveedores críticos para verificar que los servicios o productos tengan una alta disponibilidad en la misma

R5: La empresa verifica las pruebas de seguridad de TI que realiza el proveedor para validar las políticas que este tiene respecto a la seguridad de información

15. ¿La organización cuenta con herramientas apropiadas para hacer un seguimiento respecto a los productos o servicios brindados por el proveedor?

R1: La organización no cuenta con herramientas de apoyo para realizar un adecuado seguimiento al proveedor crítico

R2: La organización cuenta con herramientas propias para el apoyo a la supervisión del proveedor crítico

R3: La organización cuenta con herramientas propias los cuales son revisados de manera periódica por la organización

R4: La organización tiene herramientas propias y adquiridas que apoyan el seguimiento y supervisión de los productos o servicios que el proveedor crítico brinda

R5: La organización mantiene en constante mejora las diferentes herramientas con las que cuenta, estableciendo al mejoramiento continuo de las mismas

16. ¿La empresa puede determinar el riesgo potencial de los activos de TI expuestos a amenazas?

R1: La empresa tiene prácticas incipientes para la determinación del riesgo potencial derivado de la materialización de amenazas en los activos de TI

R2: Algunas personas en la organización toman conciencia y empiezan a desarrollar el cálculo de los riesgos potenciales asociados a los activos de TI

R3: La empresa tiene un buen conocimiento sobre el cálculo del riesgo potencial sobre los activos de TI derivados del impacto y probabilidad de ocurrencia

R4: La empresa tiene un alto nivel de conocimiento sobre los riesgos potenciales asociados a sus activos de TI

R5: La empresa mantiene el registro y cálculo de los riesgos potenciales interiorizado y este se realiza periódicamente

17. ¿Se encuentra establecido algún procedimiento para determinar el impacto y riesgo potencial de los activos de TI? ¿Este procedimiento se encuentra documentado, divulgado y en mejora continua?

R1: El procedimiento de determinación del riesgo potencial que afecta a los activos de TI no se encuentra desarrollado ni documentado

R2: El procedimiento de cálculo o determinación del riesgo potencial se encuentra en desarrollo

R3: El procedimiento de determinación del riesgo potencial se ha implementado de manera consciente en la organización

R4: El procedimiento de determinación del riesgo potencial se encuentra implementado, documentado y divulgado en toda la organización

R5: El procedimiento de determinación del riesgo potencial se encuentra implementado, documentado, interiorizado y en mejora continua

18. ¿La organización cuenta con herramientas o sistemas donde se tenga un registro de los riesgos potenciales clasificados o categorizados? ¿Se cuenta con herramientas que apoyen al cálculo de los riesgos potenciales? ¿Estos sistemas se prestan a la rápida obtención de la información, apoyando al análisis y toma de decisiones?

R1: No existen sistemas donde se registren y calculen los riesgos potenciales que afectan a los activos de TI o si se tienen, se realizan estas tareas de manera incipiente

R2: Se calculan y/o registran los riesgos potenciales en algún sistema o base de datos

R3: Los riesgos potenciales se registran en algún sistema, pero sin un cálculo adecuado del impacto y la probabilidad ya que se carece de herramientas para el cálculo del riesgo

R4: Los riesgos potenciales se encuentran correctamente registrados, calculados y clasificados en un sistema de información listo para su rápida explotación, además de contar con herramientas para el cálculo de estos

R5: Se mantiene en constante mejora los sistemas donde se registran y calculan los riesgos potenciales para apoyar al análisis y toma de decisiones

19. ¿La organización cuenta con una estrategia para establecer controles que apoyen en el tratamiento de riesgos de seguridad de TI?

R1: La empresa cuenta con mínimos conocimientos para realizar o establecer los controles que apoyen en la gestión de riesgos de seguridad de TI

R2: La organización tiene políticas y procedimientos definidos para establecer los controles que apoyen la gestión de riesgos de seguridad de TI

R3: La empresa define opciones de tratamiento como: evitar, aceptar, transferir o mitigar el riesgo

R4: Las opciones de tratamiento de riesgos de seguridad de TI se realizan de acuerdo con los objetivos de la organización, criterios y recursos disponibles

R5: Para seleccionar las opciones de tratamiento de riesgos de seguridad de TI; la organización considera criterios como: valor, percepción y partes interesadas

20. ¿Se cuenta con políticas o procedimientos de gestión de riesgos que apoyen a establecer controles para un adecuado tratamiento de riesgos de seguridad de TI?

R1: La organización no cuenta o en su defecto; las políticas, procedimientos de gestión de riesgos para establecer controles se encuentran en proceso de elaboración.

R2: Se cuenta con políticas que apoyen a establecer controles, pero no están alineados a los objetivos del negocio

R3: Se establecen controles que definen el orden en el que se debe llevar a cabo el tratamiento de riesgos de seguridad de TI

R4: Los controles para el tratamiento de riesgos de seguridad de TI siguen un proceso iterativo el cual es: formular y seleccionar opciones de tratamiento, planificar e implementar el tratamiento, evaluar la eficacia de ese tratamiento

R5: los controles establecidos se encuentran documentados siguiendo políticas de gestión de riesgos establecidos por la organización. Los controles se mantienen y evalúan

21. ¿La organización cuenta con herramientas que apoyen a establecer controles para el tratamiento de riesgos de seguridad de TI?

R1: Las herramientas de apoyo con que cuenta la organización para realizar una propuesta de controles se encuentran en proceso de elaboración

R2: La organización cuenta con algunas herramientas propias para realizar los controles de gestión de riesgos de seguridad de TI

R3: Las herramientas con que cuenta la organización son deficientes, pues no modifican el riesgo, por lo que se debe desarrollar o adquirir otras herramientas de apoyo

R4: Se dispone de herramientas propias y adquiridas como el estándar ISO 31000, ISO 270001, ISO 27002 etc. para realizar una propuesta de controles eficaz sobre los riesgos de seguridad de TI

R5: La organización aplica de manera eficiente los controles de seguridad obtenidos del Anexo A de la ISO 27001, y también de la ISO 31000 para mitigar el riesgo.

22. ¿La organización tiene conocimiento de los planes de tratamiento que apoyen a la gestión de riesgos de seguridad de TI?

R1: La organización tiene poco conocimiento sobre los controles que se deben realizar para tratar los riesgos de seguridad de TI

R2: La organización tiene un área especializada en gestión de riesgos para desarrollar planes de tratamiento que apoyen a mitigar los riesgos de seguridad de TI

R3: Todas las áreas de la organización tienen conocimiento sobre los planes de tratamiento que se debe realizar para tratar los riesgos de seguridad de TI

R4: La empresa realiza pruebas de manera sistemática para corroborar si estas funcionan correctamente

R5: La organización difunde y aprende continuamente sobre los resultados generados a partir de los planes de tratamiento

23. ¿La organización cuenta con políticas o procedimientos para gestionar los riesgos de seguridad de TI que apoyen a determinar de manera eficaz los planes de tratamiento?

R1: La organización cuenta con una política de gestión de riesgos, pero casi no lo implementa para realizar planes de tratamiento de riesgos de seguridad de TI.

R2: La organización tiene definido políticas y procedimientos de gestión de riesgos que apoyan a los planes de tratamiento identificados

R3: Se cuenta con políticas y procedimientos de gestión de riesgos que establecen lineamientos, roles y apetito por el riesgo que apoyan en gran medida a gestionar los planes de tratamiento

R4: La organización cuenta con indicadores de cumplimiento para definir si los planes de tratamiento se están llevando correctamente.

R5: Los planes de tratamiento para gestionar los riesgos de seguridad de TI identifican de forma clara el orden de prioridad que se debe implementar los controles para tratar los riesgos de seguridad de TI

24. ¿La organización cuenta con herramientas tecnológicas para el apoyo a la gestión de riesgos que mejoren el desarrollo de los planes de tratamiento?

R1: La organización no cuenta con herramientas tecnológicas para gestionar los riesgos de seguridad de TI y por ende realizar un adecuado plan de tratamiento

R2: Se cuenta con algunas herramientas tecnológicas propias para dar apoyo a la gestión de riesgos y afrontar un adecuado plan de tratamiento de riesgos de seguridad TI

R3: La organización actualiza y da soporte a las herramientas tecnológicas que apoyan el proceso de gestión de riesgos de seguridad de información.

R4: La organización desarrolla y optimiza herramientas tecnológicas propias que sirven para una mejor gestión de los riesgos de seguridad de TI

R5: Las herramientas tecnológicas son innovadoras y vanguardistas, con ello se logra realizar un adecuado plan de tratamiento sobre los riesgos de seguridad de TI.

25. ¿Se cuenta con actividades, planes de monitoreo y control de la gestión de riesgos?

R1: La organización tiene muy poco conocimiento sobre el seguimiento y control acerca de los riesgos de seguridad de TI.

R2: La organización realiza algunas actividades de seguimiento y control que son hechas de forma escasa.

R3: Se establecen registros de auditoria o seguimiento de las actividades más importantes dentro de la organización

R4: Se revisan los resultados de las actividades de seguimiento, además de realizar acciones correctivas.

R5: Se realiza seguimiento y control en todas las etapas de la gestión de riesgos

26. ¿La organización cuenta con una política de gestión de riesgos que apoye al monitoreo y control de los riesgos de seguridad de TI?

R1: No se cuenta, o si tienen estas políticas de gestión de riesgos están a muy bajo nivel

R2: La organización cuenta con una política de gestión de riesgos que se encuentra documentada y apoya al monitoreo y control

R3: La organización ha establecido planes, políticas y controles los cuales han sido aprobados y se realizan de manera continua

R4: Se cuenta con diferentes maneras de identificar los riesgos como el estratégico y el de alto nivel los cuales están aprobadas y difundidas

R5: La organización revisa las políticas y a su vez aplica técnicas de mejora continua para el apoyo del seguimiento y control.

27. ¿Se cuenta con herramientas apropiadas para una buena gestión del riesgo que apoyen al seguimiento y control?

R1: La organización no cuenta con herramientas para el seguimiento y control

R2: Se cuenta con algunas herramientas internas que apoyen al seguimiento y control

R3: La empresa cuenta con herramientas propias y adquiridas que ayuden en el seguimiento y control de los riesgos de seguridad de TI

R4: Las herramientas que tiene la organización cuentan con especificaciones técnicas avanzadas para el seguimiento y control.

R5: La organización apoya y contribuye a la mejora continua de las herramientas de apoyo para el seguimiento y control

28. ¿El proveedor crítico realiza auditorias de gestión de riesgos, seguridad de la información y continuidad de negocios a los productos, productos o servicios que brinda a la organización?

R1: La organización tiene conocimiento que su proveedor crítico realiza auditorias de manera incipiente

R2: La empresa informa que su proveedor establece programas de auditoria que contribuye a la determinación de la eficacia del sistema de gestión del auditado.

R3: La organización verifica que la alta dirección del proveedor se asegura de que los objetivos del programa de auditoria se han establecido y que se asigne a las personas indicadas para gestionarlo.

R4: EL proveedor crítico da seguimiento al programa de auditoría considerando:

- Evaluar la conformidad del programa de auditoria
- Evaluar desempeño de los miembros del equipo auditor
- Evaluar la capacidad de los equipos auditores

R5: El proveedor crítico revisa el programa de auditoria para evaluar si se ha alcanzado los objetivos establecidos.

29. ¿Cuenta el proveedor crítico con una política de gestión de riesgos, política de seguridad de la información, política de protección de datos personales y política de continuidad del negocio?

R1: Las políticas mencionadas no existen o están en proceso de elaboración.

R2: El proveedor cuenta con algunas políticas mencionadas los cuales son auditados de manera incipiente por el mismo

R3: El proveedor cuenta con casi todas las políticas los cuales son auditados de manera continua siguiendo un programa de auditoria liderados por un equipo especialista en la materia

R4: El proveedor crítico cuenta con todas las políticas mencionadas los cuales establecen, mantienen y son documentados luego de un programa de auditoría que se realiza continuamente por el mismo.

R5: El proveedor crítico cuenta con todas las políticas los cuales son auditados interna y externamente siguiendo planes de auditoria basados en la información contenida en el programa de auditoría y en la documentación proporcionada por el proveedor

30. ¿Realiza la empresa auditorías o participa en las pruebas de seguridad de información y continuidad de negocios asociados a los productos o servicios que el proveedor crítico ofrece a la organización?

R1: La empresa no audita o no participan de las pruebas respecto a los productos o servicios o productos que el proveedor le ofrece. Si lo hacen es de forma incipiente

R2: La empresa asigna a responsables de seguridad de información para que puedan participar de las pruebas respecto al servicio o producto que le ofrece al proveedor.

R3: La organización además de tener responsables desarrolla planes de auditoria para llevar a cabo las pruebas de seguridad de información y continuidad de negocios al proveedor.

R4: Para la supervisión de las pruebas de seguridad y continuidad de negocios se siguen los principios de auditoria los cuales son: Integridad, imparcialidad, confidencialidad, juicio, independiente, basado en la evidencia.

R5: El proveedor apoya y contribuye al mejoramiento continuo de auditoría priorizando las pruebas de seguridad de información y continuidad de negocios. Los cuales son auditados de manera interna (proveedor) y externa (empresa)

ANEXO E - CARTERA DE PROYECTOS

PROYECTO 01 - Modelo de Gestión de Seguridad de la información en una empresa del sector comercial

1. Introducción

La finalidad de este documento es la de presentar la propuesta de “Implementación de un Sistema de Gestión de Seguridad de la información en una empresa del sector comercial (SGSI)”.

Actualmente, las organizaciones y sistemas están en un ambiente lleno de desafíos y transformaciones. Por lo tanto, en este entorno dinámico, las organizaciones necesitan adaptarse a los cambios ambientales y tomar decisiones acertadas, bajo el marco de un sistema de seguridad de la información.

La gestión efectiva de la seguridad de la información es un tema estratégico para las organizaciones para salvaguardar sus recursos de información. La alineación estratégica de valores es un enfoque proactivo para gestionar el conflicto de valores en la gestión de la seguridad de la información.

2. Problemática

Salvaguardar a las empresas del sector comercial de riesgos potenciales ocasionados por amenazas que afectan a los activos de información de la misma causando pérdidas económicas o daños en la reputación de la empresa.

3. Descripción de la propuesta

3.1 Nombre

Modelo de Gestión de Seguridad de la información en una empresa del sector comercial

3.2 Descripción

Con este proyecto se busca garantizar que los riesgos de la seguridad de la información en las empresas del sector comercial sean evaluados, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías. Para ello, el proceso de gestión debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

4. Tecnologías relacionadas

En esta sección se describen las principales tecnologías que construyen y/o complementan esta propuesta.

4.1 ISO 27001: Sistemas de gestión de seguridad de la información

Especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información dentro del contexto de la organización. También incluye requisitos para la evaluación y el tratamiento de riesgos de seguridad de la información adaptados a las necesidades de la organización perteneciente al sector comercial.

4.2 ISO27005: Directrices generales para la gestión de riesgos en sistema de gestión de seguridad de la información

La norma ISO 27005 contiene diferentes recomendaciones y directrices generales para la gestión de riesgo en Sistemas de Gestión de Seguridad de la Información.

Es compatible con los conceptos generales especificados en la norma ISO 27001 y se encuentra diseñada como soporte para aplicar de forma satisfactoria un SGSI basado en el enfoque de gestión de riesgo.

4.3 OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)

OCTAVE es una metodología utilizada para identificar y evaluar los riesgos de seguridad de la información. El uso de OCTAVE está destinado a ayudar a la organización en términos de:

- Desarrollar un criterio de evaluación de riesgo cualitativo que describa la tolerancia de riesgo operacional de la compañía.
- Identificar los activos que son importantes para la misión de la empresa.
- Identificar vulnerabilidades y amenazas a esos activos.

- Determinar y evaluar las posibles consecuencias para la empresa si se produce la amenaza.

5. Solución propuesta

A continuación, se describe la solución desarrollada que buscan resolver de manera total a la problemática o necesidad descrita anteriormente.

5.1 Sistema de Gestión de Seguridad de la información

5.1.1. Dimensiones de la seguridad de información

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Estas tres dimensiones constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información.

- **Confidencialidad:** la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- **Integridad:** mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- **Disponibilidad:** acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

5.1.2. Implementación

Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información según el estándar ISO 27001, se utiliza el ciclo continuo: Plan-Do-Check-Act (PDCA), conocido como el ciclo de Deming.

Figura E-1: Ciclo PDCA del Sistema de Gestión de seguridad de la información

Fuente: Pacheco, 2017.

- Plan (planificar): establecer el SGSI.
- Do (hacer): implementar y utilizar el SGSI.
- Check (verificar): monitorizar y revisar el SGSI.
- Act (actuar): mantener y mejorar el SGSI.

PROYECTO 02 - Implementación de un Plan de Continuidad de Negocios para Centros de Salud

1. Introducción

La finalidad de este documento es la de presentar la propuesta de “Implementación de un Plan de Continuidad de Negocios para centros de salud”.

Las empresas de cualquier sector, a lo largo de su trayectoria, es muy posible que se hayan encontrado con alguna situación que le haga temblar poniendo en peligro la supervivencia. Muchas empresas optan por implantar Sistemas de Gestión de Continuidad de Negocio apoyados en estándares como la ISO 22301 o alguna otra de forma rápida ante amenazas que alteren sus operaciones diarias.

Los Sistemas de Gestión de Continuidad de Negocio permiten que las empresas reestablezcan sus operaciones después de que haya ocurrido un accidente, que haya provocado la interrupción de su

negocio, pero además tratará de proteger la reputación, el cumplimiento de plazos, la satisfacción del cliente y la prevención de posibles pérdidas económicas.

2. Problemática

Reestablecer las operaciones de los centros de salud en el menor tiempo posible ante cualquier amenaza interna o externa protegiendo la reputación y economía de la misma

3. Descripción de la propuesta

3.1 Nombre

Metodología para la Implementación de un Plan de Continuidad de Negocios para Centros de Salud

3.2 Descripción

Con este proyecto se busca que las empresas del sector salud puedan priorizar las amenazas y que puedan reestablecer sus operaciones en el menor tiempo posible sin afectar a los interesados del negocio como pueden ser los usuarios finales.

Para ello, el Plan de Continuidad de Negocio deberá identificar la capacidad táctica y estratégica que tiene la empresa para proveer y hacer frente a posibles amenazas que puedan interrumpir el funcionamiento del negocio.

Un Sistema de Gestión de la Continuidad de Negocio permite mejorar el negocio, al garantizar una efectiva planificación de la Continuidad del mismo en todos los niveles.

4. Tecnologías relacionadas

En esta sección se describen las principales tecnologías que construyen y/o complementan esta propuesta.

4.1 ISO 222301: Sistema de gestión de la continuidad del negocio

Esta norma especifica los requisitos para la creación y gestión de un sistema eficaz de gestión de la continuidad del negocio (BCMS).

Esta norma internacional para la gestión de la continuidad del negocio especifica los requisitos para planificar, establecer, implementar, operar, monitorear, revisar, mantener y mejorar

continuamente un sistema de gestión documentado para proteger, reducir la probabilidad de ocurrencia, prepararse, responder y recuperarse ante incidentes o amenazas que puedan surgir.

Los requisitos especificados en esta Norma Internacional son generales y se pretende que sean aplicables a todas las organizaciones, o partes de los mismos, independientemente del tipo, tamaño y naturaleza de la organización. La extensión de la aplicación de estos requisitos depende del entorno operativo de la organización y la complejidad.

4.2 Circular SBS N° G-139: Gestión de la continuidad del negocio

En abril del 2009, la Superintendencia de Banca, Seguros y AFP (SBS), publicó la circular G-139-2009 referido a la Gestión de Continuidad del Negocio. Está enfocada principalmente para las empresas pertenecientes al sector financiero. Pero se puede tomar de referencia para el presente proyecto.

La circular G-139-2009 es de cumplimiento obligatorio para las empresas del sector financiero peruano, incluidos los bancos, cajas municipales de ahorro y crédito, financieras, compañías de seguros y administradoras de fondos de pensiones (AFP); y tiene como propósito definir los criterios mínimos para elevar el nivel de preparación de las organizaciones para poder hacer frente a eventos externos que puedan interrumpir las actividades críticas de la organización, así como contar con la capacidad para recuperar dichas actividades en el menor tiempo posible.

Basado en la norma BS 25999, esta circular establece cinco fases, como parte del sistema de gestión de continuidad del negocio:

Figura E-2: Fases de la continuidad de negocios SBS G-139

Fuente: Circular SBS G-139.

5. Solución propuesta

A continuación, se describe la solución desarrollada que buscan resolver de manera total la problemática o necesidad descrita anteriormente.

5.1 Sistema de Gestión de Continuidad de negocios

5.1.1. Lineamientos de Continuidad de negocios

La organización debe cumplir lineamientos que aseguren la continuidad de negocios. Estos lineamientos se desarrollan en base a las tecnologías anteriormente mencionadas. Las empresas deberán desarrollar como mínimo las siguientes fases como parte de la Gestión de la continuidad del negocio:

- Entendimiento de la organización
- Selección de la estrategia de continuidad
- Desarrollo e implementación de la estrategia de continuidad

- Pruebas y actualización
- Integrar la gestión de la continuidad del negocio a la cultura organizacional

5.1.2. Pasos para gestionar la Continuidad de Negocio

El proceso de Gestión de la Continuidad del Negocio incluye seis pasos:

- Paso 1: Elaboración del programa de BCM
- Paso 2: Comprensión de la organización
- Paso 3: Definición de las estrategias para la gestión de la continuidad de negocio
- Paso 4: Elaboración y ejecución de una respuesta
- Paso 5: Poner en práctica, cumpliendo los acuerdos definidos del BCM
- Paso 6: Incorporar la Continuidad de Negocio en la cultura de la organización

5.1.3. Implementación

Para la implementación del Plan de continuidad se debe hacer un caso de estudio de manera que satisfaga las necesidades de la misma, reduciendo las amenazas y por consiguiente reestableciendo sus operaciones en el menor tiempo posible.

Para una adecuada gestión del Plan de continuidad se debe seguir el ciclo PDCA o PHVA. “Planificar-Hacer-Verificar-Actuar” (PHV) para planificar, establecer, implementar, operar, monitorear, revisar, mantener y mejorar continuamente la eficacia del Plan de continuidad.

La figura E-3 ilustra cómo un Sistema de gestión de Plan de Continuidad toma como entradas las partes interesadas, los requisitos para la gestión de la continuidad y, a través de las acciones y procesos necesarios, produce resultados de continuidad (es decir, administrado de continuidad de negocio) que cumplen dichos requisitos.

Figura E-3: Modelo PDCA aplicado a los procesos del Plan de continuidad de negocios

Fuente: ISO 220301, 2012.

PROYECTO 03 - Implementación de una herramienta para la auditoria de la seguridad de la información y continuidad del negocio aplicado a empresas del sector financiero

1. Introducción

La finalidad de este documento es la de presentar la propuesta de “Implementación de una herramienta para la auditoria de la seguridad de la información y continuidad del negocio aplicado a empresas del sector financiero”.

El control de los sistemas de información de gestión de riesgos en el mundo en desarrollo es actualmente necesario para mejorar el rendimiento y proporcionar un impacto muy importante para los usuarios de los sistemas de información, especialmente para promover el enfoque

empresarial en los sistemas de información. Por lo tanto, para el propósito de la investigación, se debe realizar una auditoría del sistema de información de gestión de riesgos en una empresa del sector financiero o bancario para determinar el nivel de madurez que se ha aplicado, de acuerdo con la Metodología que utiliza la norma ISO/IEC 27001 y algún otro estándar o marco de referencia.

2. Problemática

Las empresas del sector financiero en el Perú, a pesar de contar con procedimientos y políticas bien desarrolladas en seguridad de la información y continuidad del negocio, estos muchas veces aplazan la resolución de los hallazgos de auditoría causando la aparición de nuevas amenazas y vulnerabilidades mientras la tecnología va evolucionando. Esto se demuestra en los incidentes recientes de seguridad ocurridos en la banca peruana, tales como el ataque cibernético que paralizó las transacciones en los cajeros y algunos otros servicios en muchos bancos a nivel nacional.

3. Descripción de la propuesta

3.1 Nombre

Implementación de una herramienta para la auditoría de la seguridad de la información y continuidad del negocio aplicado a empresas del sector financiero

3.2 Descripción

Con este proyecto se busca auditar el proceso de gestión de riesgos de seguridad de la información en una empresa del sector financiero para evaluar el nivel de madurez de este y proponer mejoras sin descuidar el seguimiento y control. Para ello, mediante una herramienta se evaluará todo el proceso de gestión del riesgo, se obtendrá registros de hallazgos para calcular el nivel de madurez de la empresa en materia de seguridad de la información y continuidad del negocio. Esto permitirá proponer planes de acción y recomendaciones para mejorar este nivel de madurez.

4. Tecnologías relacionadas

En esta sección se describen las principales tecnologías que construyen y/o complementan esta propuesta.

4.1 ISO 27001: Sistemas de gestión de seguridad de la información

Especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información dentro del contexto de la organización. También incluye requisitos para la evaluación y el tratamiento de riesgos de seguridad de la información adaptados a las necesidades de la organización perteneciente al sector comercial.

4.2 ISO 19011 – 2011: Directrices para la Auditoría de los Sistemas de Gestión

Esta norma proporciona orientación sobre sistemas de gestión de auditoría, incluidos los principios de auditoría, la gestión de un programa de auditoría y la realización de auditorías del sistema de gestión, así como orientación sobre la evaluación de la competencia de las personas involucradas en el proceso de auditoría, incluida la persona que gestiona la auditoría, auditores y equipos de auditoría.

Es aplicable a todas las organizaciones que necesitan realizar auditorías internas o externas de sistemas de gestión o administrar un programa de auditoría.

4.3 ISO 22301: Sistema de gestión de la continuidad del negocio

Esta norma especifica los requisitos para la creación y gestión de un sistema eficaz de gestión de la continuidad del negocio (BCMS).

Esta norma internacional para la gestión de la continuidad del negocio especifica los requisitos para planificar, establecer, implementar, operar, monitorear, revisar, mantener y mejorar continuamente un sistema de gestión documentado para proteger, reducir la probabilidad de ocurrencia, prepararse, responder y recuperarse ante incidentes o amenazas que puedan surgir.

Los requisitos especificados en esta Norma Internacional son generales y se pretende que sean aplicables a todas las organizaciones, o partes de los mismos, independientemente del tipo, tamaño y naturaleza de la organización. La extensión de la aplicación de estos requisitos depende del entorno operativo de la organización y la complejidad.

4.4 Tecnología de la herramienta de auditoría

La tecnología usada para el diseño y desarrollo de la herramienta es libre.

5. Solución propuesta

A continuación, se describe la solución desarrollada que busca resolver de manera total a la problemática o necesidad descrita anteriormente.

5.1 Herramienta de auditoría de gestión de seguridad de la información y continuidad del negocio

5.1.1. Implementación

El desarrollo de la herramienta de auditoría podría tener como base el estándar ISO 27001, ya que cuenta con el ciclo de vida PDCA, el cual hace posible analizar cosas que se pueden usar como referencia para maximizar la implementación de un SGSI. Estos son los cuatro ciclos de vida en cuestión:

- **Plan (Determinación del SGSI):** Establecer políticas, objetivos, procesos y procedimientos adecuados de un sistema de gestión de seguridad para gestionar los riesgos y resultados apropiados con políticas y objetivos generales de la organización.
- **Hacer (Aplicación y operación del SGSI):** Implementar y operar políticas, controles, procesos y procedimientos de gestión de riesgos de seguridad.
- **Verificación (Monitoreo y evaluación del SGSI):** Evaluar y, cuando corresponda, medir el desempeño del proceso en relación con la política, los objetivos de la gestión de seguridad de información y la experiencia práctica e informar los resultados a la administración para su evaluación.
- **Actuar (Mejora y mantenimiento de SGSI):** Tomar medidas correctivas y preventivas basadas en los resultados de las auditorías internas y las revisiones de la gerencia u otra información relevante, para lograr una mejora continua en la gestión de la seguridad de la información.

Para medir este ciclo de vida en la herramienta, se deberán diseñar encuestas y programar visitas a una empresa seleccionada del sector financiero con la finalidad de tomar los datos de entrada necesarios y así medir la eficacia respecto a los procedimientos de gestión de riesgos de seguridad de la información, mediante un registro de hallazgos. Con este registro, la herramienta calculará el nivel de madurez inicial, basándose en alguna metodología o estándar a elección (Cobit, CMMI, etc.) lo cual permitirá proponer mejoras o recomendaciones, considerando los controles del anexo A de la ISO 27001 y las buenas prácticas de la ISO 22301, por ejemplo. La herramienta apoyará al seguimiento de estas recomendaciones y mientras se vayan cerrando, el nivel de madurez irá aumentando siendo este uno de los indicadores más importantes de la mejora continua.

Figura E-4: Ciclo PDCA del sistema de gestión de seguridad de la información

Fuente: ISO 27001, 2013.