Universidad Nacional Mayor de San Marcos
Universidad del Perú. Decana de América
Facultad de Ingeniería de Sistemas e Informática
Escuela Profesional de Ingeniería de Sistemas

Implementación de una metodología de gestión de riesgos para la seguridad de la información en una compañía de seguros

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de Ingeniero de Sistemas

AUTOR

Simeón Canadeo PERALTA VILLANUEVA

ASESOR

Jorge Santiago PANTOJA COLLANTES

Lima, Perú

2021

Referencia bibliográfica

Peralta, S. (2021). *Implementación de una metodología de gestión de riesgos para la seguridad de la información en una compañía de seguros*. [Trabajo de suficiencia profesional de pregrado, Universidad Nacional Mayor de San Marcos, Facultad deIngeniería de Sistemas e Informática, Escuela Profesional de Ingeniería de Sistemas]. Repositorio institucional Cybertesis UNMSM.

Metadatos complementarios autor/ asesor

Datos de autor	
Nombres y apellidos	**Simeón Canadeo Peralta Villanueva** .
Tipo de documento de identidad	DNI
Número de documento de identidad	**47274203**
URL de ORCID	https://orcid.org/0000-0001-8320-8664
Datos de asesor	
Nombres y apellidos	**Jorge Pantoja Collantes**
Tipo de documento de identidad	DNI
Número de documento de identidad	**06254022**
URL de ORCID	https://orcid.org/0000-0002-7172-1206
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	César Augusto ANGULO CALDERÓN
Tipo de documento	D.N.I
Número de documento de identidad	32907109.
Miembro del jurado 1	
Nombres y apellidos	Mario Agustín Huapaya Chumpitaz
Tipo de documento	Obligatorio. Elegir un solo tipo de documento: DNI, Carné de extranjería emitido en Perú, Pasaporte, Cédula de identidad
Número de documento de identidad	49307203
Datos de investigación	
Línea de investigación	C.0.3.3. Desarrollo de modelos y aplicación delas tecnologías de información y comunicaciones.

Grupo de investigación	KAPANAM
Agencia de financiamiento	Financiamiento propio .
Ubicación geográfica de la investigación	Distrito de Lurigancho – Chosica 11° 58' 36.7" S 76° 56' 25.6" W -11.976857 -76.940432
Año o rango de años en que se realizó la investigación	Año 2021
URL de disciplinas OCDE	Ingeniería de sistemas y comunicaciones https://purl.org/pe-repo/ocde/ford#2.02.04

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
Escuela Profesional de Ingeniería de Sistemas

Acta Virtual de Sustentación
del Trabajo de Suficiencia Profesional

Siendo las 19.10 horas del día 22 de julio del año 2021, se reunieron virtualmente los docentes designados como Miembros de Jurado del Trabajo de Suficiencia Profesional, presidido por el Lic. Angulo Calderón Cesar Augusto (Presidente), Mg. Huapaya Chumpitaz Mario Agustín (Miembro) y el Lic. Pantoja Collantes Jorge Santiago (Miembro Asesor), usando la plataforma Meet (https://meet.google.com/thz-zgfs-jwq), para la sustentación virtual del Trabajo de Suficiencia Profesional intitulado: ***"IMPLEMENTACIÓN DE UNA METODOLOGÍA DE GESTIÓN DE RIESGOS PARA LA SEGURIDAD DE LA INFORMACIÓN EN UNA COMPAÑÍA DE SEGUROS",*** *por el Bachiller* ***Peralta Villanueva Simeón Canadeo****; para obtener el Título Profesional de Ingeniero de Sistemas.*

Acto seguido de la exposición del Trabajo de Suficiencia Profesional, el Presidente invitó al Bachiller a dar las respuestas a las preguntas establecidas por los miembros del Jurado.

El Bachiller en el curso de sus intervenciones demostró pleno dominio del tema, al responder con acierto y fluidez a las observaciones y preguntas formuladas por los señores miembros del Jurado.

Finalmente habiéndose efectuado la calificación correspondiente por los miembros del Jurado, el Bachiller obtuvo la nota de ***17 DIECISIETE.***

A continuación, el Presidente de Jurados el Lic. Angulo Calderón Cesar Augusto, declara al Bachiller ***Ingeniero de Sistemas.***

Siendo las 20.00 horas, se levantó la sesión.

Presidente
Lic. Angulo Calderón Cesar Augusto

UNMSM
Firmado digitalmente por PANTOJA COLLANTES Jorge Santiago FAU 20148092282 hard
Motivo: Soy el autor del documento
Fecha: 22.07.2021 20:06:19 -05:00

Miembro
Mg. Huapaya Chumpitaz Mario Agustín

Miembro Asesor
Lic. Pantoja Collantes Jorge Santiago

FICHA CATALOGRÁFICA

Implementación de una metodología de gestión de riesgos para la seguridad de la información en una compañía de seguros

Autor: Simeón Canadeo Peralta Villanueva
Asesor: Jorge Pantoja Collantes
LIMA – PERÚ, 2021

Título profesional: Ingeniero de Sistemas.
Línea de Investigación: Seguridad de la información / Riesgos de seguridad de la información.

Pregrado: Escuela Profesional de Ingeniería de Sistemas – Facultad de Ingeniería de Sistemas e Informática. Universidad Nacional Mayor de San Marcos.

Formato 28 x 20 cm Páginas vi, 43

Dedicatoria

Dedicado el presente trabajo a mis padres y hermanos por su incondicional apoyo durante toda mi vida personal y profesional.

Agradecimiento

Agradezco principalmente a mis padres y hermanos que siempre me impulsaron a conseguir mis objetivos.

Agradezco también a mi asesor Jorge Pantoja Collantes, por sus valiosas asesorías en la realización del presente trabajo.

Por último, quiero agradecer a la compañía RIMAC SEGUROS por brindarme la oportunidad de fortalecer mi desarrollo profesional.

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Implementación de una metodología de gestión de riesgos para la seguridad de la información en una compañía de seguros

Autor: PERALTA VILLANUEVA, Simeón Canadeo
Asesor: PANTOJA COLLANTES, Jorge
Título: Trabajo de Suficiencia Profesional para optar por el Título Profesional de Ingeniero de Sistemas
Fecha: Junio del 2021

RESUMEN

El trabajo de suficiencia profesional describe la implementación de la metodología de gestión de riesgos para la seguridad de la información en una compañía de seguros en el año 2020.

La implementación de la metodología se desarrolló en cinco etapas, en la primera se realizó el diagnóstico de la situación actual de la gestión de riesgos de seguridad de la información en la compañía, identificando aquellos factores internos y externos que deben ser considerados en la elaboración de la metodología. Durante la primera y segunda etapa de la implementación se realizaron varias reuniones con cada interesado en la metodología teniendo el objetivo de que cada uno esté conforme con lo que se establecía. Luego de la validación con todos los interesados, en la tercera etapa, se procedió a publicar la metodología, la cual fue aprobada por el comité de Gestión Integral de Riesgos de la compañía.

En las etapas cuatro ycincose realizó la evaluación de riesgos para luegopresentar los resultados a cada propietario delos procesos seleccionados mediante un acta de entrega final detallando cada riesgo identificado con los planes de tratamiento.

Palabras Clave: Riesgos, Tratamiento, Impacto, Riesgos, Seguridad de la Información.

NATIONAL UNIVERSITY OF SAN MARCOS
FACULTY OF SYSTEMS ENGINEERING AND INFORMATIC
PROFESSIONAL SCHOOL OF SYSTEMS ENGINEERING

Implementation o fan informationsecurityriskmanagementmethodology in aninsurancecompany

Autor: PERALTA VILLANUEVA, Simeón Canadeo
Asesor: PANTOJA COLLANTES, Jorge
Título: Trabajo de Suficiencia Profesional para optar por el Título Profesional de Ingeniero de Sistemas
Fecha: Junio del 2021

ABSTRACT

Theprofessionalsufficiencywork describes theimplementationoftheinformationsecurityriskmanagementmethodology in aninsurancecompany in theyear 2020.

Theimplementationofthemethodologywasdeveloped in fivestages, in thefirstone a diagnosis ofthecurrentsituationofinformationsecurityriskmanagement in thecompanywasmade, identifyingthoseinternal and externalfactorsthatshould be considered in thedevelopmentofthemethodology. Duringthefirst and secondstagesoftheimplementation, severalmeetingswereheldwitheachstakeholder in themethodologywiththeobjectiveofensuringthateachonewassatisfiedwithwhatwasestablished. After validationwithallstakeholders, in thethirdstage, themethodologywaspublished and approvedbythecompany'sIntegratedRisk Management Committee.

In stagesfour and five, theriskassessmentwascarriedout and thentheresultswerepresentedtoeachowneroftheselectedprocessesbymeansof a final deliveryreportdetailingeachriskidentifiedwiththetreatmentplans..

Key words: Risks, Treatment, Impact, Risks, Information Security.

Índice

Índice de figuras

Índice de tablas

Introducción

En los últimos años el incremento de las amenazas cibernéticas ha afectado en gran medida a todas las organizaciones a nivel mundial, por lo que organizaciones como International OrganizationforStandardization (ISO), NationalInstituteofStandards and Technology (NIST), Cloud Security Alliance (CSA) entre otros han plasmado en documentos, informes o matrices las buenas prácticas que permitan a las organizaciones proteger su información de estas amenazas.

Las buenas prácticas que permiten proteger la información en las compañías son implementadas a través de un Sistema de Gestión de Seguridad de la Información (SGSI), teniendo como base la gestión de riesgos, lo que permite identificar escenarios que impactarán negativamente a la compañía.

El proceso de Gestión de Riesgos de Seguridad de la Información permite identificar los activos de información y las amenazas a las cuales se encuentran expuestas. Esto permite evaluar los escenarios que impactan negativamente a la compañía, sus posibles consecuencias y de esta forma se realicen las acciones más adecuadas de tratamiento de los riesgos que se identifiquen.

El presente trabajo de suficiencia profesional se encuentra estructurada en cinco capítulos que se describen a continuación.

En el CAPÍTULO I se realiza la descripción en forma cronológica de los roles y las funciones realizadas como suficiencia profesional.

En el CAPÍTULO II se realiza la descripción de la compañía, su visión, su misión. Además de indicar su estructura organizacional y productos que brinda.

En el CAPÍTULO III se describe en el trabajo realizado en la Implementación de la Metodología de Gestión de Riesgos para la Seguridad de la Información en la compañía de seguros en el 2020.

El CAPÍTULO IV describe el aporte realizado en la implementación de la metodología, además de indicar las mejoras que se deben realizar.

En el CAPÍTULO V se describen las conclusiones y también las recomendaciones.

Capítulo I – Trayectoria profesional

A continuación, se detalla cronológicamente la trayectoria profesional del autor del presente trabajo de suficiencia profesional:

Experiencia profesional	
Analista Training de Seguridad TI Experis – Rímac Seguros y Reaseguros. - Gestión de identidades en las plataformas tecnológicas de la compañía. - Atención de requerimientos de gestión de acceso en coordinación con el equipo de Mesa de Ayuda. - Presentación de informes de gestión, evidenciando el cumplimiento de los controles establecidos para el Sistema de Gestión de Seguridad de la Información.	01.09.2016 – 30.05.2018
Asistente de Administración de Accesos Rímac Seguros y Reaseguros. - Gestión de identidades en las plataformas tecnológicas de la compañía. - Implementación de las herramientas de seguridad tecnología ATP, DLP en Office365 y DLP Symantec. - Gestión de la implementación del proyecto Administración de Usuarios Privilegiados (PAM). - Automatización procedimiento de gestión de accesos mediante el desarrollo de scripts en PowerShell y tareas programadas en Windows. - Gestión del componente IAM de las plataformas Cloud de la compañía (Azure y AWS)	01.06.2018 – 31.10.2019
Analista de Riesgos de Seguridad de la Información Rímac Seguros y Reaseguros. - Implementación de una metodología para la gestión de riesgos de seguridad de la información. - Evaluación de riesgos de seguridad de la información en los proyectos, procesos y tecnologías emergentes de la compañía. - Seguimiento de los planes de tratamiento. - Desarrollo de políticas y procedimientos relacionados a seguridad de la información. - Implementación del programa de cultura en Seguridad de la Información en la compañía.	01.11.2019 – hasta la fecha

Tabla 1. Experiencia profesional.
Fuente: Elaboración Propia

Formación profesional	
Educación Superior – Grado obtenido Bachiller (01–Dic–2017) Ingeniería de Sistemas Universidad Nacional Mayor de San Marcos	Mar. 2011 – Dic. 2016

Tabla 2. Formación profesional.
Fuente: Elaboración Propia

Idiomas	
Inglés – Fase básico parcial Centro de Idiomas de la UNMSM	Ene. 2016 – May. 2016

Tabla 3. Formación en idiomas.
Fuente: Elaboración Propia

Cursos	
"Power BI" Netzun Plus	Feb. 2021
"Tecnología que transforma en la Era Digital" Laboratoria	Sep. 2020
"Fundamentos de Transformación Digital" En Estado beta	Jun. 2020
"CertifiedInformationSystems Security Professional (CISSP)" New Horizon	Mar. 2020 – May. 2020
"Implementador Líder ISO 27001" Certificación ERCA	Dic. 2019 – Ene. 2020
"Gestión de Riesgos Operacionales – ISO 31000" Cibertec	Feb. 2019 – Mar. 2019
"Gestión de Seguridad de la Información y Continuidad de Negocio – ISO 27001, 27002, 27005, 22301" Cibertec	Oct. 2018 – Dic. 2018
"Excel nivel básico, intermedio y avanzado" Netzun Plus	Ene. 2018
Nivel Avanzado en "Profesional en Ethical Hacking" Wit Plus Perú	Mar. 2017
"Interpretación de la Norma ISO 27001:2013" ARGOS ConsultingGroup	Dic. 2016
"Programación con java WEB (Spring, Hibernate, PrimeFaces JSF)"	Mar. 2016 – May. 2016

Centro de extensión universitaria – UNMSM	

Tabla 4. Cursos y especializaciones.
Fuente: Elaboración Propia

Seminarios	
"AdvancedInvestigations& Open SourceIntelligenceTechniques Training" EKOPARTY Security Conference 2020	Sep. 2020

Tabla 5. Seminarios. Fuente.
Elaboración Propia

Otros conocimientos	
Lenguajes de programación	Visual Basic 6.0, PHP, Python, C++, HTML, PLSql, Kotlin, Android Studio.
Sistemas Operativos	Windows (Allversions), Linux.
Manejadores de Bases de Datos	Access, MySQL, Oracle.
Diseño	Corel Draw, Corel Photo, Adobe Flash, Dreamweaver, Illustrator, PhotoShop, Modelado 3D.
Otros	Microsoft Office, MS Project, Modelado de procesos (BPM), BSoft, Storytelling, TransmediaStorytelling, Presentaciones efectivas.

Tabla 6. Conocimientos adicionales.
Fuente: Elaboración Propia

Capítulo II – Contexto en el que se desarrolló la experiencia

Empresa – Actividad que realiza

Rimac Seguros y Reaseguros es una compañía peruana fundada en 1992 a partir de la fusión de dos aseguradoras de ese entonces. En la actualidad solo tiene operaciones en Perú, ofreciendo seguros personales, seguros de vida, seguros para el hogar, seguros de jubilación, seguros para automóviles, SOAT, EPS, SCTR, entre otros.

La compañía es parte del grupo BRECA, un conglomerado empresarial originado en el Perú que cuenta con más de 130 años de existencia, que tiene operaciones en Perú y otros países de Latinoamérica. (RIMAC, 2021)

A continuación, los datos generales de la compañía:

- Razón social: RIMAC SEGUROS Y REASEGUROS SAC
- Domicilio legal: Las Begonias N° 475.
- RUC: 20100041953
- Teléfono: (01) 411 1111
- Rubro: Banca y Seguros

El marco regulatorio que se aplica a la compañía, en referencia a la seguridad de la información es:

- Resolución SBS N° 504 – 2021. Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad.
- Ley N° 29733. Protección de datos personales.
- Resolución SBS N° 272 – 2017 Reglamento de Gobierno Corporativo y Gestión Integral de Riesgos.
- Superintendencia del Mercado de Valores (SMV). Código de buen gobierno corporativo para las sociedades peruanas.

Visión

"Protegemos tu mundo, impulsamos tu bienestar".

Misión

Innovando para seguir creciendo y consolidarnos como la compañía de seguros que más peruanos prefieren, liderando la transformación digital del sector que nos posiciona como una empresa más ágil, simple y conectada con sus clientes.

Organización de la empresa

A continuación, se muestra la estructura organizacional de la alta gerencia de la compañía actualizada en el año 2021

Figura 1. Estructura organizacional de la compañía

Nota. El gráfico representa la estructura organizacional de la alta gerencia de la compañía actualizada al año 2021. El área de Seguridad de la Información es parte de la Gerencia de Tecnología.

Fuente: Elaboración Propia.

En la figura 2 se muestra la estructura organizacional del área de seguridad de la información.

Área, cargo y funciones desempeñadas

El autor de este trabajo de suficiencia profesional se desempeña como Analista de Riesgos de Seguridad de la Información en el área GRC, este constituyó el equipo encargado de la implementación de la Metodología de Gestión de Riesgos para la Seguridad de la Información.

Figura 2. Estructura organizacional del área de Seguridad de la Información

Nota. El departamento responsable de la implementación de la metodología de Riesgos de seguridad de la Información y de la que el autor del presente trabajo de suficiencia profesional pertenece es el departamento de Gobierno, Riesgos y Cumplimiento.

Fuente: Elaboración Propia

Experiencia profesional realizada en la organización

Funciones realizadas:

- Implementación de una metodología para la gestión de riesgos.
- Evaluación de riesgos en los procesos de la compañía. Revisión de los procesos críticos de la compañía identificados en el análisis de impacto (BIA) y en base a criterios de seguridad (impacto en confidencialidad, integridad y disponibilidad).
- Evaluación de riesgos en los proyectos de la compañía. En base a los proyectos e iniciativas que defina la compañía y su respectiva calificación basada en los criterios de seguridad
- Evaluación de riesgos de seguridad de la información en tecnología emergentes que se implementen en la compañía. Cambios significativos, aplicaciones, entre otros; que por su impacto pueda afectar el negocio.
- Seguimiento de controles y planes de tratamiento.
- Desarrollo de políticas, procedimientos y manuales de seguridad.
- Implementación del programa de cultura en seguridad en la compañía.

- Seguimiento de los planes de acción a las observaciones de auditoría interna y externa.

Capítulo III – Actividades desarrolladas

Situación problemática

Definición del problema

En el año 2020 el área GRC de la compañía detectó que la metodología actual para la gestión de riesgos de seguridad de la información no reflejaba la realidad actual de la compañía, encontrándose incompleta debido a que no consideraba la evaluación de riesgos de los procesos de negocio. Esto provocaría que, ante una auditoría interna o externa, se declare una observación para la cual se deben asignar recursos que desarrollen un plan de subsanación de la observación y en caso no se subsane satisfactoriamente se tendría como consecuencia una sanción por incumplimiento regulatorio.

En el Artículo 8 del Reglamento para la Gestión de la Seguridad de la Información N° 504 – 2021 promulgado por la SBS en febrero del año 2021, se indica que unas de las funciones que se debe cumplir en Seguridad de la Información y Ciberseguridad es:

> "Artículo 8. La función de Seguridad de Información y Ciberseguridad la de evaluar los riesgos y proponer medidas de mitigación"(SBS, 2021)

Además, desde el año 2019 la compañía se encuentra en una transformación hacia la cultura ágil, lo que provocaba que la metodología actual de ese entonces para la gestión de riesgos de seguridad de la información genera reprocesos y retrasos en los proyectos de la compañía.

Elproblema

Ausencia de una metodología para la gestión de riesgos, que contemple la evaluación de los procesos de negocio (priorizando procesos críticos), la evaluación de los proyectos, evaluación de iniciativas y evaluación de cambios significativos. Además, esta metodología está alineada a la cultura ágil de la compañía.

Solución

Obj

etivo

Objetivo

general

Implementación de una metodología integral para la gestión de riesgos de seguridad de la información en la compañía.

Objetivos específicos

- Desarrollo de una metodología para la gestión de riesgos.
- Aprobación y publicación de la metodología para la gestión de riesgos.
- Evaluación de riesgos en los procesos de negocio, aplicando la metodología aprobada y publicada.

Alcance

El presente trabajo de suficiencia profesional describe el proceso realizado para el desarrollo de la metodología de gestión de riesgos y su aplicación en los procesos de la compañía. Los procesos para evaluar son definidos mediante la técnica de Business ImpactAnalysis (BIA).

Etapas

En la figura 3 se describen las etapas de la implementación de la metodología de gestión de riesgos para la seguridad de la información.

Figura 3. Etapas de la implementación de la metodología.

Nota. El gráfico indica las cinco etapas para la implementación de la metodología de gestión de riesgos de seguridad de la información.

Fuente: Elaboración Propia

Diagnóstico

Los factores relevantes previos al inicio de la implementación de la metodología integral para la Gestión de Riesgos de Seguridad de la Información.

- Desde el año 2019 la compañía inició una transformación en la estructura organizativa estableciendo una metodología estructural de tribus orientadas a la agilidad.
- En la auditoría externa realizada por la Superintendencia de Banca y Seguros (SBS) en el año 2019, se observó una deficiencia en la Gestión de Riesgos de Seguridad de la Información, la cual fue revalidada por la auditoría interna del año 2020.

Título de la Observación	Hallazgo
SBS-2019-011 Debilidades en la gestión de seguridad de la información	El base a la Circular SBS N° G-140-2009, se realizó la evaluación identificando la siguiente deficiencia: a) Ausencia de una periodicidad definida para la evaluación de riesgos de seguridad de la información, situación que no permitiría la identificación y tratamiento oportuno de dichos riesgos.
SEG-008-2020. Deficiencias menores en el diseño de la normativa interna y falta de aprobaciones finales por los responsables del proceso.	El base a la Circular SBS N° G-140-2009, se realizó la evaluación identificando la siguiente deficiencia: a) Ausencia de una periodicidad definida para la evaluación de riesgos de seguridad de la información, situación que no permitiría la identificación y tratamiento oportuno de dichos riesgos.

Tabla 7. Hallazgos identificados en las auditorías realizadas en los años 2019 y 2020.

Fuente: Elaboración Propia

Se tuvieron reuniones con la Gerencia de Seguridad de la información donde se presentó la iniciativa de implementar la metodología para la gestión de riesgos.

En el diagnóstico se identificó lo siguiente:

- El área de seguridad de la información no realizaba evaluación de riesgos de seguridad de la información en los procesos del negocio.
- La metodología actual no se encontraba publicada y aprobada.
- La metodología actual generaba retrasos en los proyectos durante el proceso de evaluación de riesgos, esto debía a que no se encontraba alineado a la cultura de agilidad de la compañía.

Elaboración del documento. La metodología

La metodología implementada para la Gestión de Riesgos de Seguridad de la Información se estructuró en cuatro etapas, estas se muestran en la Figura 4.

Se definió que la metodología debe ser aplicada en la:

- Evaluación de procesos: La revisión de los procesos críticos de la compañía identificados en el análisis de impacto (BIA) y en base a criterios de seguridad (impacto en confidencialidad, integridad y disponibilidad). Los procesos por evaluarse se clasificarán y seleccionarán al inicio de cada año y se aprobarán en el comité de seguridad.
- Evaluación de proyectos: En base a los proyectos e iniciativas que defina la compañía y su respectiva calificación basada en los criterios de seguridad.
- Evaluación emergente: Cambios significativos en la infraestructura tecnológica que pueda afectar a la organización.

Figura 4. Metodología de Gestión de Riesgos para la Seguridad de la Información

Nota. En el gráfico se muestran las cuatro etapas de la metodología de Gestión de Riesgos para la Seguridad de la Información.

Fuente: Elaboración Propia.

Etapa 1: Identificación de riesgos

En esta etapa se desarrollan las siguientes actividades:

- Entendimiento del contexto interno y externo y alcance de evaluación.
- Identificación de activos, amenazas, controles existentes, vulnerabilidades y consecuencias.

Las herramientas que facilitarán el desarrollo de estas actividades incluyen: Entrevistas, talleres, cuestionarios, revisión de documentos e informes internos o externos, según aplique.

El resultado de esta etapa corresponde a una lista de escenarios de riesgos de Seguridad de la Información con sus consecuencias relacionadas a activos y procesos de negocio.

Etapa 2: Análisis del riesgo

En esta etapa se desarrollan las siguientes actividades:

- Evaluación del impacto a la organización que pudieran resultar los incidentes de la seguridad.
- Evaluación de la probabilidad de ocurrencia de escenarios.

- Determinación del nivel de riesgo para los escenarios de incidentes relevantes.

Las herramientas que facilitarán el desarrollo de estas actividades incluyen:

- Escalas de Impacto: Muy Bajo (1), Bajo (2), Moderado (3), Alto (4), Muy Alto (5)
- Escalas de Probabilidad: Muy Baja (1), Baja (2), Moderada (3), Alta (4), Muy Alta (5)
- Matriz con niveles de Impacto y Probabilidad, descrita a continuación.

Figura 5. Matriz de impacto vs probabilidad

		Probabilidad				
		Muy baja	Baja	Moderada	Alta	Muy Alta
Impacto	Muy alto	5	10	15	20	25
	Alto	4	8	12	16	20
	Moderado	3	6	9	12	15
	Bajo	2	4	6	8	10
	Muy Bajo	1	2	3	4	5

Nota. En el gráfico se muestra la matriz de impacto vs probabilidad la cual permite identificar el nivel de riesgo.

Fuente: Elaboración Propia

Los valores numéricos indicados en la matriz se obtienen al multiplicar el nivel de impacto y nivel de probabilidad lo que permite asignar el nivel de riesgo. El nivel se realiza considerando la siguiente distribución indicada en la Tabla 2.

El resultado de esta etapa corresponde a una lista de riesgos con su nivel asignado. Los riesgos serán registrados de manera centralizada asignándole una categoría que permita establecer un perfil de riesgos de seguridad de la información.

Clasificación	Rango	Descripción
Crítico	16 – 25	Riesgo con impacto extremadamente severo sobre los activos. Lo que conlleva a una pérdida altamente costosa o afectar totalmente las operaciones
Alto	10 – 15	Riesgo con impacto alto sobre los activos. Existe una interrupción de una parte de las operaciones.
Medio	5 – 9	Riesgo moderado sobre los activos. Hay una posibilidad de que las operaciones se vean afectados
Bajo	0 – 4	Riesgo mínimo o insignificante sobre los activos de información. No afecta las operaciones ni la productividad.

Tabla 8. Clasificación del nivel de riesgo identificado
Fuente: Elaboración Propia

Etapa 3: Evaluación del riesgo

En esta etapa se compara el resultado del análisis de riesgos con el criterio de nivel de riesgo aceptable. La atención a los riesgos con nivel crítico y alto deben priorizarse, sobre los de nivel moderado. Para los riesgos con nivel bajo podría no realizarse una acción adicional. Sin embargo, debe considerarse que la agregación de riesgos de nivel bajo puede generar un riesgo con un nivel mayor.

El resultado de esta etapa corresponde a un listado de escenarios de riesgos priorizados de acuerdo con los criterios de valoración.

Etapa 4: Tratamiento del riesgo

En esta etapa se definen las acciones frente a los riesgos identificados. Estas acciones pueden estar orientadas a mitigar, evitar, transferir o aceptar el riesgo.

Los enfoques de tratamiento no son mutuamente excluyentes, pudiendo adoptarse una combinación de estos frente a los riesgos:

- Mitigar el riesgo involucra implementar nuevos controles o mejorar los existentes, con el objetivo de reducir el nivel de impacto o la probabilidad de ocurrencia.

- Evitar el riesgo conlleva a no realizar la actividad o la condición que genera el riesgo.
- Transferir el riesgo involucra compartir el riesgo con otra entidad con el objetivo de gestionar con eficacia el riesgo.
- Aceptar el riesgo involucra la decisión de convivir con el riesgo y su nivel actual. En caso el nivel de riesgo sea de Crítico, Alto o Moderado, la aceptación debe formalizarse mediante una carta de aceptación del riesgo.

El resultado de esta etapa corresponde a los planes de tratamiento de riesgos.

Etapa 5: Comunicación y monitoreo

Las actividades de comunicación y monitoreo son transversales a todas las etapas descritas en la metodología. Las actividades de comunicación y monitoreo involucran:

- Presentación de informes y obtener aprobación del Owner responsable del proceso/proyecto.
- Socialización de los riesgos a la Vicepresidencia responsable.
- Coordinación de la ejecución de los Comités de Seguridad.
- Participación en Comité Integral de Riesgos, llevando los aspectos más relevantes de la gestión de riesgos.
- Monitoreo y revisión de riesgos
- Seguimiento de planes de tratamiento y niveles de riesgos.

Para el registro de las actividades de las etapas de identificación, análisis, evaluación y tratamiento de riesgos se utilizará como herramienta la Matriz de Evaluación de Riesgos de Seguridad de la Información (Ver Anexo A).

Verificación, aprobación y publicación de la metodología

El documento fue revisado por analistas de seguridad, arquitectos y validado por la Jefatura del área de GRC, así como la Gerencia de Seguridad de la Información.

La metodología se publicó en el repositorio de control documentario de la compañía y fue aprobada por el comité de Gestión Integral de Riesgo y la Vicepresidencia de Tecnología (Ver Anexo B).

Evaluación de riesgos en los procesos críticos del negocio

Se identificó y seleccionó los procesos con mayor impacto en la compañía. La selección tuvo como base la técnica Business ImpactAnalysis (BIA) con el Recovery Time Objective (RTO) menor a 24 horas, se definió dentro del alcance a 9 procesos en los cuales se realizó la evaluación de riesgos de seguridad de la información aplicando la metodología desarrollada. Los procesos seleccionados se detallan en la Tabla 9.

La evaluación se inició con la presentación inicial a cada Owner de proceso, donde se indicó el objetivo, alcance, las etapas y la importancia de la evaluación de riesgos, siendo unos de los objetivos generar valor a cada proceso evaluado.

Las etapas y la participación que el Owner tendrá durante la evaluación de riesgos de seguridad de la información se muestran en el Anexo C.

Proceso	RTO (En horas)
Central de Emergencias	0,5
Central de Consultas	1
Inversiones – Mesa de Negociación	4
Tesorería – Control de Caja	24
Cartas de garantía	24
Siniestros vehiculares	24
SOAT	24
Suscripción de Cauciones	24
Estrategia y Gestión de Cobranzas	24

Tabla 9. Procesos seleccionados para la evaluación de riesgos.
Fuente: Elaboración Propia.

Resultados de la evaluación

Los resultados de la evaluación fueron comunicados a cada propietario del proceso mediante correo electrónico (Ver Anexo D) adjuntando:

- Matriz de Inventarios de Activos.
- Matriz de Riesgos de Seguridad.
- Documentos de Seguridad.
- Acta de Cierre de la evaluación.

Como resultado final de la evaluación realizada en todos los procesos, se presentó a la Gerencia de Seguridad de la Información el número de riesgos identificados y el nivel de riesgos valorado en cada proceso. Estos resultados se detallan en la Tabla 10.

Proceso	Número y nivel de riesgo
Central de Emergencias	(6) Crítico (3) Alto
Central de Consultas	(7) Crítico (2) Alto
Inversiones – Mesa de Negociación	(3) Moderado (1) Bajo
Tesorería – Control de Caja	(2) Moderado
Cartas de garantía	(3) Alto (2) Moderado
Siniestros vehiculares	(1) Alto (1) Moderado
SOAT	(2) Moderado
Suscripción de Cauciones	(1) Crítico (1) Moderado
Estrategia y Gestión de Cobranzas	(1) Crítico (3) Alto (1) Moderado

Tabla 10. Resultados de la evaluación de riesgos de seguridad de la información.
Fuente: Elaboración Propia.

Fundamentos utilizados

En el estudio publicado por Filho, Rego y Claro (2021)se indicó que las compañías tienenla necesidad y dependencia de las tecnologías de información, esto para lograr una mejor oferta de valor para sus clientes.

> "…La digitalización impulsa una competitividad global, mediante una respuesta rápida y masiva…. Pero no se debe dejar de lado que este proceso está acompañado de muchos riesgos de entre los cuales los ciber riesgoscontribuyen uno de los principales…"*(Filho, Rego, & Claro, 2021)*

Pero esta dependencia no es resultado de un estudio reciente, porque ya fue expuesta en un artículo publicado en el año 2015 por Fazlida y Said donde indicaron que "existe una gran dependencia de las empresas hacia las tecnologías lo que las expones a riesgos de seguridad" (Fazlida & Said, 2015)

Los ciber riesgos son amenazas presentes en la adopción de tecnologías y que puedenmodificar el logro de los objetivossi se llegaran a materializar, provocandopérdidaseconómicas, sanciones regulatorias, gastos legales, pérdida de la reputación entro otros efectos negativos. Por ello las compañías deben contar con un departamento que se encargue de implementarlo que algunos autores como Ramalingam, Arun y Anbazhgan (2018) definen el Gobierno, Riesgo y Cumplimiento (GRC) de Seguridad de la Información.

> "…la gobernanza de seguridad debe incorporar elementos de estrategia, cumplimiento, responsabilidades y las buenas prácticas…además de ser parte del gobierno corporativo"*(Fazlida & Said, 2015)*

Así como los estudios mencionados en párrafos anteriores existen muchos otros donde se resalta la importancia de las tecnologíaspara las compañías y los peligros a los que se encuentran expuestos, por lo que la necesidad de implementar la seguridad de la información y la gestión de riesgos debe ser prioridad para las compañías.

Modelo de gestión de riesgos de seguridad de la información (GRSI)

Según Ramalingam, Arun y Anbazhgan (2018) “la seguridad debe enfocarse en tres dimensiones: Gobierno, Gestión de Riesgos y Cumplimiento (GRC). Aunque la implementación de cada una de estas dimensiones suele ser un desafío debido a los siguientes problemas …” (Ramalingam, Arun, & Anbazhagan, 2018).

- “Las técnicas de medición cualitativas se basan en información subjetiva…”
- “Las métricas cuantitativas utilizadas por plataformas comerciales no reflejan la realidad de la compañía…”
- “Debido a que los riesgos emergentes no son considerados por muchos directorios, las estrategias empresariales y los planes operativos no están alineados…”

Según Mohamend S (2011) existen muchas metodologías internacionales (ISO, NISY, Margerit) para la gestión de riesgos y todas tienen el mismo objetivo de identificar, priorizar, estimar y definir un plan de mitigación de los riesgos.

También existen varios modelos de “evaluación de riesgos que permiten cuantificar la seguridad de los cuales cinco fueron presentados en un artículo el 2016, estos modelos toman en cuenta la cantidad de pérdidas y vulnerabilidades existentes…” (Jouini & Rabai, 2016)

- “SecAgreement: Basado en los servicio y probabilidad de fallas, considerando costos de incumplimiento…”
- “The Mean Failure (MFC): Toma en cuenta la media de la pérdida de todos los involucrados…”
- “The Mean FailureCostExternal (MFCext) and The Mean FailureCostInternal (MFCint): Considera la identificación de las amenazas existentes…”
- “The MFC Extensionmodel (MFCE): Considera la amenaza, intención y consecuencia…”
- “Multi – dimensional Mean FailureCostModel (M^2FC): Propone que la evaluación debe ser realizada desde varias perspectivas definiendo una de ellas la principal…”

Uno de los mayores problemas en la gestión de riesgos es cuantificar el impacto, la probabilidad y hasta la efectividad de los planes de tratamiento por lo que el trabajo realizado por Zarreh, Wan, Lee, Saygin y Janahi (2019) aporta mucho valor a la gestión de riesgos.

> "el método FailureMode and EffectiveAnalysis (FMEA) toma en cuenta el número de criticidad de la ciberseguridad para identificar si un riesgo es crítico y debe ser aplicar un plan de tratamiento". *(Zarreh, Wan, Lee, Saygin, & Janahi, 2019)*

El número de criticidad de la ciberseguridad al que se refieren los autores depende de dos elementos (1) La gravedad del riesgo y (2) La probabilidad que el riesgo se materialice, y lo plasmaron en valores numéricos de las Tablas 11 y 12

Gravedad	Efecto	Descripción
10	Catástrofe	Daño irreversible a la empresa en su operación o reputación.
9	Extremo	La operación se ve afectada negativamente y tiene un tiempo de recuperación de más de 5 días.
8	Muy alta	La operación se ve afectada negativamente y tiene un tiempo de recuperación de 3 a 5 días.
7	Alto	La operación se ve afectada negativamente y tiene un tiempo de recuperación de 1 a 5 días.
6	Moderado	La operación se ve afectada negativamente y tiene un tiempo de recuperación de 1 día.
5	Bajo	La operación se ve interrumpida por violaciones graves en los procesos.
4	Muy Bajo	La operación se ve interrumpida por violaciones importantes en los procesos
3	Menor	La operación se ve interrumpida por violaciones menores en los procesos.
2	Muy Pequeño	Violación menos de los procedimientos.
1	Ninguno	Ningún efecto.

Tabla 11. Tabla de gravedad.
Fuente: (Zarreh, Wan, Lee, Saygin, & Janahi, 2019)

Ocurrencia	Descripción
10	Es probable que ocurra en el 90% – 100% de las experiencias.
9	Es probable que ocurra en el 80% – 90% de las experiencias.
8	Es probable que ocurra en el 70% – 80% de las experiencias.
7	Es probable que ocurra en el 60% – 70% de las experiencias.
6	Es probable que ocurra en el 50% – 60% de las experiencias.
5	Es probable que ocurra en el 40% – 50% de las experiencias.
4	Es probable que ocurra en el 30% – 40% de las experiencias.
3	Es probable que ocurra en el 20% – 30% de las experiencias.
2	Es probable que ocurra en el 10% – 20% de las experiencias.
1	Es probable que ocurra en el 0% – 10% de las experiencias.

Tabla 12. Tabla de gravedad.
Fuente: (Zarreh, Wan, Lee, Saygin, & Janahi, 2019)

Otro artículo publicado en el 2018 aporta gran valor estableciendo como medir si un control implementado ha cumplido con el objetivo, este artículo realizado por Ramalingam, Arun y Anbazhgan (2018)quecombina "técnicas de investigación cualitativa y cuantitativaque identifican las principales métricas que deben tener la gestión de riesgos para evaluar la eficacia y eficiencia de los controles…" (Ramalingam, Arun, & Anbazhagan, 2018)

El proceso del modelo

Mohamend S (2011) indicó la importancia que tiene realizar un proceso cíclico en la gestión de riesgos proponiendo el modelo DMAIC (Define, Measure, Analyze, Improve, Control), cada una de estas etapas aborda su propio objetivo, entrada y salida.

- "Define: Esta etapa comienza o da continuación al proceso con un nuevo ciclo, realizando las actividades de entender el contexto identificando los activos, amenazas, vulnerabilidades y controles existentes…"
- "Measure: Considera como entrada los obtenido en la etapa Define y añade la evaluación del estado actual de los activos, amenazas, vulnerabilidades y controles…"

- “Analyze: Se realiza una comparación del estado actual y el estado requerido obteniendo de esta fase el análisis de brechas…”
- “Improve: El objetivo de esta etapa es definir un plan de acción para lograr el estado requerido según el análisis de brechas…”
- “Control: Se realiza la supervisión del plan y documentar las actividades que se realicen…”

En el 2019 fue publicado el artículo de Zarreh, Wan, Lee, Saygin, Lee y Janahi en el que nos indica que “el marco de ciberseguridad es para reducir el riesgo de ciberseguridad…creado por el NationalInstituleofStandars and Technology (NIST) de los EEUU define las etapas identificar, proteger, detectar, responder y recuperar…” (Zarreh, Wan, Lee, Saygin, & Janahi, 2019)

- “Identificar para entender a la compañía y realizar la gestión de riesgos en sistemas, personas, activos, datos y capacidades…”
- “Proteger implementando controles de seguridad para garantizar la entrega de productos y servicios…”
- “Detectar implementando controles que identifican eventos…”
- “Responder tomando medidas ante incidentes…”
- “Recuperar manteniendo planes de resiliencia…”

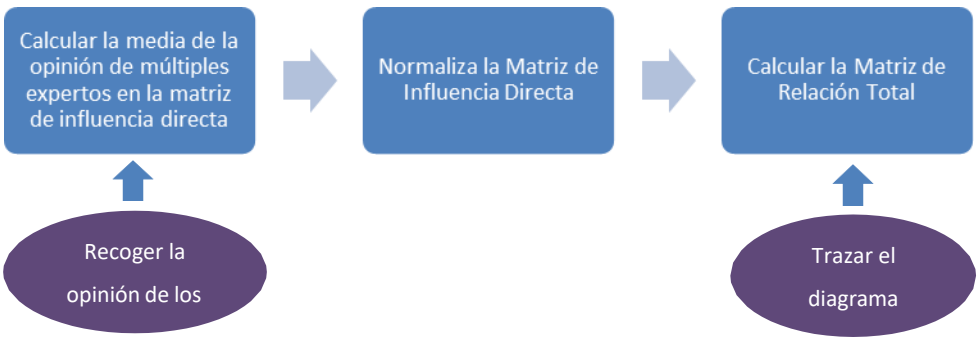
En los dos modelos presentados en los anteriores párrafos la primera etapa (“Define” e “Identificar”) tiene objetivos de entender en contexto e identificar los activos por lo que se aplicaría el modelo STOPE (Strategy, Technology, Organization, People andEnvironment) expuesto por Mohamend S. (2011), el cual permite definir cuáles son los activos de información a considerar. En el desarrollo de la metodología expuesta en el presente trabajo se consideró los dominios del modelo STOPE para definir las categorías de activos de información las cuales se detallan en la Tabla 13.

En las últimas etapas (“Improve – Control” y “Recuperar”) de los modelos presentados en anteriores párrafos se debe de considerar los expuesto por Ramalingam, Arun y Anbazhgan (2018) para medir la efectividad del control de seguridad que se proponga en el plan de tratamiento del riesgo, aplicando el método de Decision – Making Trial and EvaluationLaboratory (DEMATEL) expuesto de manera gráfica en la Figura 6.

Categoría	Definición
Datos e información	Es considerado como el activo principal, En esta categoría ingresan los procesos relevantes para la organización e información en cualquier medio de soporte (físico y/o digital)
Hardware	Esta categoría consta de todos los elementos físicos que soportan los procesos y la información.
Software	En esta categoría consta de todos los programas adquiridos y/o desarrollados que contribuyen al procesamiento de información
Red	En esta categoría consta de todos los dispositivos de telecomunicaciones utilizados para interconectar varios computadoras o elementos físicamente remotos de un sistema de información
Personal	En esta categoría consiste en todos los grupos de personas involucradas en el sistema de información.
Infraestructura	Esta categoría comprende todos los lugares que contienen el alcance o parte del alcance y los medios físicos necesarios para que funcione el sistema de información
Organización	Esta categoría describe el marco organizacional, que consiste en todas las estructuras de personal asignadas a un área y los procedimientos de control.

Tabla 13. Categorías de activos de información.
Fuente: Elaboración Propia

Figura 6. Decision – Making Trial and EvaluationLaboratory (DEMATEL)



Fuente: (Ramalingam, Arun, & Anbazhagan, 2018)

En el proceso de implementación de la metodología se usaron las indicaciones de los autores citados anteriormente y las prácticas indicadas en las normas internacionales NTP – ISO / IEC 27001:2014. Sistema de Gestión de Seguridad de la Informacióny NTP ISO 27005:2018. Gestión de Riesgos de Seguridad de la Información.

3.2.4.3.NTP – ISO / IEC 27001:2014.

> "La NTP tiene como objetivo definir los requisitos para establecer, implementar, mantener y mejorar continuamente un SGSI que permita preservar la integridad, confidencialidad y disponibilidad de la información…"(ISO 27001, 2014)

La norma se encuentra estructurada en 10 capítulos que describen qué es lo que se debe realizar para la implementación y mantenimiento de un SGSI, los capítulos son:

- Capítulo 4: Contexto de la organización
- Capítulo 5: Liderazgo
- Capítulo 6: Planificación
- Capítulo 7: Soporte
- Capítulo 8: Operación
- Capítulo 9: Evaluación del desempeño
- Capítulo 10: Mejoras

El sistema de gestión de seguridad de la información (SGSI) debe tener un enfoque en los riesgos que impacte negativamente a la organización, en el *Capítulo 6 – Planificación* y en el *Capítulo 8 – Operación* la norma lo aborda.

> "6.1.1 Acciones para el tratamiento de riesgos. En la planificación del SGSI, la organización debe considerar el contexto interno, contexto externo y las necesidades de las partes interesadas…" (ISO 27001, 2014)

La norma indica explícitamente que la organización debe contar procesos para la identificación, valoración y tratamiento de riesgos de seguridad.

Para la valoración de riesgos de seguridad de la información la norma establece:

> "En la valoración del riesgo de seguridad de la información se debe definir un proceso que establezca y mantenga criterios de riesgo de seguridad de la información asegurando que las valoraciones repetitivas cuenten con resultados consistentes, válidos y comparables…" (ISO 27001, 2014)

Para el tratamiento de riesgos de seguridad de la información la norma establece:

> "El tratamiento de riesgos de seguridad de la información debe definir un proceso que establezca opciones de tratamiento de riesgos apropiadas, tomando en cuenta los resultados de la valoración de riesgos y así determinar todos los controles necesarios, además de obtener la aprobación de los propietarios de los riesgos…"(ISO 27001, 2014)

La norma también presenta 114 controles para: las políticas de seguridad, los recursos humanos, los activos, los accesos, la criptografía, la seguridad física, las comunicaciones, las aplicaciones, los incidentes y el cumplimiento.

NTP ISO 27005:2018. Gestión de Riesgos de Seguridad de la Información

> "Esta NTP proporciona requisitos para la gestión del riesgo de seguridad en una organización, donde la está debe definir su enfoque según su contexto y sus necesidades" (ISO 27005, 2018)

La norma se encuentra estructurada en 12 capítulos, y a partir del capítulo 6 se inicia con la descripción del proceso de gestión del riesgo de seguridad de la información.

- Capítulo 6. Descripción del proceso de gestión de riesgos de seguridad.
- Capítulo 7. Establecimiento del contexto.
- Capítulo 8. Evaluación de riesgo de seguridad.
- Capítulo 9. Tratamiento del riesgo de seguridad.
- Capítulo 10. Aceptación del riesgo de seguridad.
- Capítulo 11. Comunicación y consulta del riesgo de seguridad.

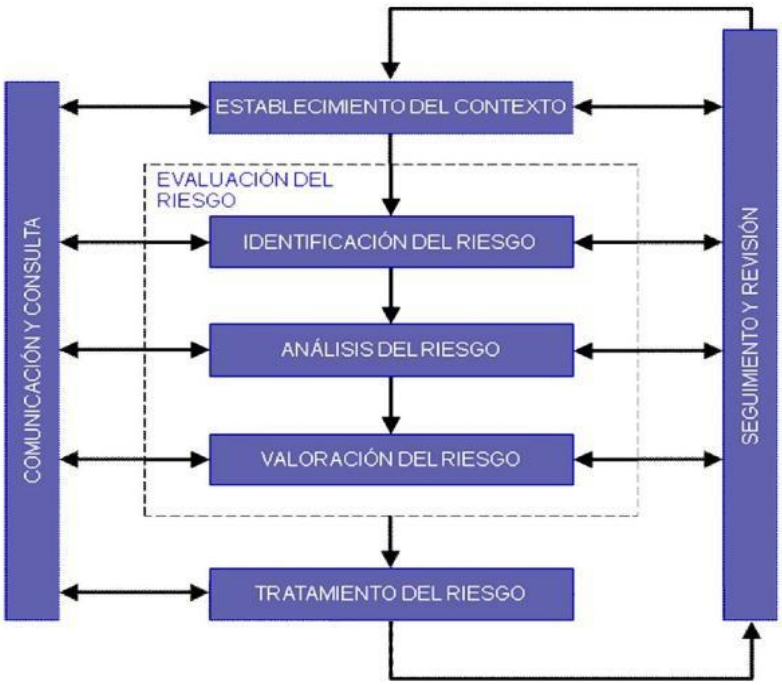
- Capítulo 12. Seguimiento y revisión del riesgo de seguridad.

En la Figura 6 veremos la representación gráfica del proceso de gestión de riesgos que se describe en el capítulo 6 de la norma.

Para un proceso adecuado de gestión de riesgos se deben definir criterios de valoración del riesgo e impacto del riesgo. La norma describe las consideraciones que debe tener para cada uno.

- Para los criterios de valoración del riesgo se debe tener en cuenta la criticidad de los activos de información implicados, la importancia operacional y las expectativas de las partes interesadas. Además de las consecuencias negativas para la organización.
- Para los criterios de impacto del riesgo se debe tener en cuenta el nivel de clasificación del activo involucrado, las pérdidas financieras, alteración de las operacionales, sanciones por incumplimiento regulatorio y la pérdida reputacional

Figura 7. Proceso de gestión del riesgo de Seguridad de la Información.



Nota. La figura presenta las acciones que se deben realizar en el proceso de gestión de riesgos de seguridad de la información.

Fuente*:* (ISO 27005, 2018)

Luego de la definición de los criterios de evaluación del riesgo e impacto se debe iniciar con la identificación de activos, amenazas, controles existentes, vulnerabilidades, consecuencias con el objetivo de determinar el nivel del riesgo. En el capítulo 8 de la norma se describen las consideraciones que se debe tener para la identificación de cada uno de estos elementos.

Los elementos de entrada y salida para la identificación de activos, vulnerabilidades, controles, amenazas y consecuencias que describe la norma son:

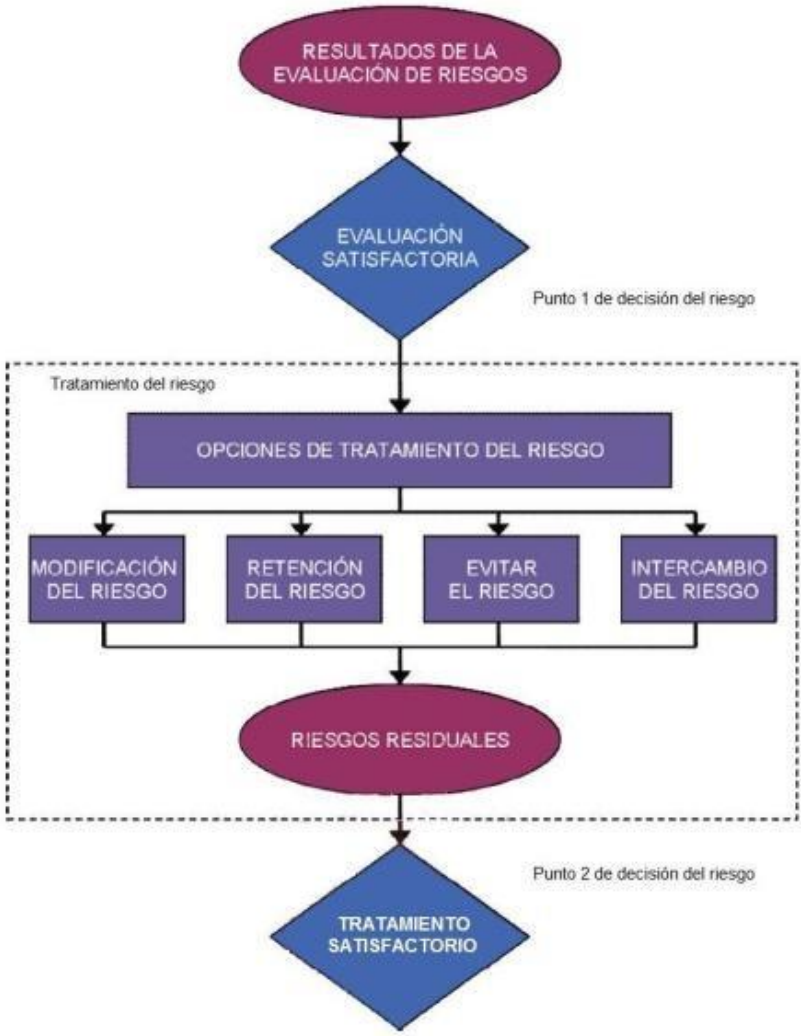
- Para los activos.
  Entrada: Alcance y lista de activos con sus propietarios, ubicación y función.
  Salida: Lista de activos priorizados que entrarán al proceso de gestión de riesgos.
- Para las vulnerabilidades.
  Entrada: Vulnerabilidades identificadas en la revisión de incidentes.
  Salida: Lista de vulnerabilidades, su tipo y fuente.
- Para los controles existentes.
  Entrada: Documentación de los controles y planes actuales.
  Salida: Lista de todos los controles existentes y su plan de acción.
- Para las amenazas.
  Entrada: Lista de amenazas conocidas, activos y controles existentes.
  Salida: Lista de vulnerabilidades relacionadas a los activos y controles.
- Para las consecuencias.
  Entrada: Lista de activos, procesos de negocio, amenazas y vulnerabilidades.
  Salida: Lista de posibles consecuencias relacionadas a los activos y procesos.

El nivel de riesgo será determinado por las consecuencias y probabilidad de ocurrencia del riesgo, las consideraciones que se debe tener según la norma son

> "La determinación del nivel de riesgos se realiza mediante la asignación de valores de probabilidad e impacto. Adicionalmente, este puede considerar costo beneficio, las preocupaciones de las partes interesadas, y otras variables" (ISO 27005, 2018)

Cuanto se determine el nivel de riesgo existen cuatro opciones para el tratamiento de riesgo: modificación, retención, evitar y compartir el riesgo. Estas opciones son presentadas de manera gráfica en la Figura 7 que es presentada en el capítulo 9 de la norma.

Figura 8. La actividad de tratamiento del riesgo.



Nota. La figura presenta las opciones de tratamiento de riesgos de seguridad de la información.

Fuente*:* (ISO 27005, 2018)

Evaluación

Evaluación económica – Técnica

Las áreas de la compañía que participaron en la implementación de la metodología de gestión de riesgos para seguridad de la información se muestran en la Tabla 11.

Área	
GRC	- Desarrollo y revisión del documento. - Evaluación de riesgos en los procesos de la compañía.
Área de Cumplimiento y Riesgo Operacional	- Revisión y aprobación del documento.
Vicepresidencia de Tecnología	- Revisión y aprobación del documento.

Tabla 14. Áreas y roles que participaron en la implementación de la metodología.
Fuente: Elaboración Propia

Como primera evaluación económica, en la Tabla 15 se detallan los recursos de personal necesarios para el desarrollo y aprobación del documento.

Personal requerido	HH por mes	Costo por HH	# de personas	Costo Mensual
Analista de Seguridad Desarrollo de la Metodología	30	S/. 40	1	S/. 1200
Jefe de GRC Revisión de la Metodología	3	S/ 60	1	S/ 180
Analista de Cumplimiento / Riesgos Operacional Revisión de la Metodología	1	S/. 40	2	S/. 80
Vicepresidente de Tecnología Aprobación de la Metodología	1	S/.250	1	S/. 250

Tabla 15. Personal necesario para el desarrollo y aprobación del documento.
Fuente: Elaboración Propia

Como segunda evaluación económica, en la Tabla 16 se detallan los recursos de personal necesarios para la implementación de la metodología y evaluación de riesgos en los procesos de la compañía. Además, en la Tabla 14 se detallan otros gastos relacionados.

Personal requerido	HH por mes	Costo por HH	# de personas	Costo Mensual
Analista de Seguridad	80	S/. 40	3	S/. 7200

Tabla 16. Personal para la implementación y evaluación de riesgos.
Fuente: Elaboración Propia

Otros costos	Costo Mensual
Luz	S/. 30
Uso de Internet	S/. 30

Tabla 17. Otros costos.
Fuente: Elaboración Propia

Capítulo IV – Reflexión crítica de la experiencia

Aporte / lecciones aprendidas

La participación del autor permitió la implementación de una metodología de gestión de riesgos para la seguridad de la información donde se describen todos los posibles escenarios para la evaluación de riesgos. También permitió la adecuación de la metodología a la cultura de agilidad que tiene la compañía y a las buenas prácticas de las normas internacionales.

La metodología implementada para la gestión de riesgos mejoraría con el desarrollo de lo siguiente:

1. La determinación del nivel de riesgo cambie de un enfoque cualitativo actual a un enfoque cuantitativo. Te tomo como referencia lo expuesto por (Zarreh, Wan, Lee, Saygin, & Janahi, 2019)

   En la metodología se definió que el nivel de impacto sea medida con una escala cualitativa de cinco niveles: Muy Bajo (1), Bajo (2), Moderado (3), Alto (4), Muy Alto (5). Se deben mejorar los criterios de la escala dando un enfoque cuantitativo de pérdidas económicas. El ejemplo para la mejora se muestra en la Tabla 15.

Nivel	Descripción	Valor del Nivel de Impacto Valor de la pérdida expresado en Dólares Americanos ($)
1	Muy Bajo	De 0 a 50 000
2	Bajo	De 50 001 a 100 000
3	Moderado	De 100 000 a 200 000
4	Alto	De 200 000 a 500 000
5	Muy Alto	De 500 000 a más

Tabla 18. Matriz de escala del nivel de impacto.
Fuente: Elaboración Propia

En la metodología se definió que el nivel de probabilidad sea medida con una escala cualitativa de cinco niveles: Muy Bajo (1), Bajo (2), Moderado (3), Alto (4), Muy Alto (5). Se deben mejorar los criterios de la escala dando un enfoque

cuantitativo en el número de ocurrencias en las que el riesgo se materializa al año. El ejemplo para la mejora se muestra en la Tabla 16.

Nivel	Descripción	Probabilidad por Ocurrencias. Valor expresado por cantidad de ocurrencias en el año
1	Muy Bajo	De 0 a 1
2	Bajo	De 2 a 3
3	Moderado	De 4 a 6
4	Alto	De 7 a 9
5	Muy Alto	De 10 a más

Tabla 19. Matriz de escala del nivel de probabilidad.
Fuente: Elaboración Propia

2. Para determinar los procesos más críticos de la compañía se debe aplicar los siguientes criterios u otros que se considere necesario.
    - Procesos que soportan a procesos críticos.
    - Procesos que manipulan información confidencial de la compañía.
    - Business ImpactAnalysis (BIA), con el Recovery Time Objective (RTO)
3. La metodología debe complementar con un adecuado Procesos de Clasificación de la Información el permitiría definir e identificar información sensible para la compañía.
4. La metodología debe contemplar un plan para la revisión de los riesgos residuales.

Capítulo V – Conclusiones y recomendaciones

Conclusiones

Durante las primeras tres etapas de la implementación de la metodología se requirió la participación de un analista de riesgos de seguridad de la información, también las aprobaciones de las jefaturas y del comité de Gestión Integral de Riesgos.

En las etapas cuatro y cinco de la implementación se realizó la evaluación de riesgos de en los procesos más sensibles de la compañía, requiriendo la participación de tres analistas de seguridad los cuales se encargaron de la identificación de riesgos, evaluación de los riesgos identificados y determinar los planes de tratamiento aplicando los criterios que fueron definidos en la metodología.

La realización de las actividades planificadas permitió el cumplimiento de los objetivos, logrando:

- La implementación de la Metodología de Gestión de Riesgos para la Seguridad de la Información.
- Identificar y definir procesos críticos de la compañía que se evaluarán con la metodología implementada. Estos procesos fueron obtenidos mediante análisis BIA, priorizando aquellos procesos con un RTO menor a 24 horas.
- Evaluar los riesgos de seguridad en los procesos críticos de la compañía que al finalizar se presentan los resultados de cadapropietario del proceso. Además de la presentación global a la gerencia de Seguridad de la Información.

Recomendaciones

- Implementar las mejoras que se indican en la sección 4.1
- Es necesario que el Comité General de Riesgos tenga información plena del nivel de riesgo identificado en los procesos críticos de la compañía.
- Se debe revisar y actualizar la metodología por lo menos una vez al año o cada vez que lo amerite.

Fuentes de información

Fazlida, M., & Said, J. (2015). Information Security: Risk, Governance and Implementation Setback. *Procedia Economics and Finance*, 6.

Filho, N. G., Rego, N., & Claro, J. (2021). Supply chain flows and stocks as entry points for cyber-risks. *Procedia Computer Science*, 8.

ISO 27001. (2014). NTP - ISO / IEC 27001:2014.

ISO 27005. (2018). NTP - ISO / IEC 27005:2018.

Jouini, M., & Rabai, L. B. (2016). Comparative Study of Information Security Risk Assessment Models for Cloud Computing systems. *Procedia Computer Science*, 6.

Mohamed S. Saleh, A. A. (2011). A new comprehensive framework for enterprise information security risk management. *Applied Computing and Informatics*, 12.

Ramalingam, D., Arun, S., & Anbazhagan, N. (2018). A Novel Approach for Optimizing Governance, Risk management and Compliance for Enterprise Information security using DEMATEL and FoM. *Procedia Computer Science*, 6.

RIMAC. (2021). *RIMAC SEGUROS y REASEGUROS*. Obtenido de https://www.rimac.com/nosotros

SBS. (2021). Reglamento para la Gestión de la Seguridad de la Información N° 504 – 2021.

Zarreh, A., Wan, H., Lee, Y., Saygin, C., & Janahi, R. A. (2019). Risk Assessment for Cyber Security of Manufacturing Systems: A Game Theory Approach. *Procedia Manufacturing*, 8.

Glosario

Activo: Un activo es todo aquello que tiene valor para la compañía, cualquier recurso (información, software, infraestructura física, servicios, personas, etc.) que sustenta uno o más procesos de las áreas de negocio.

Amenaza: Una causa potencial de un incidente no deseado, el cual puede ocasionar daños a un sistema u organización.

Confidencialidad: la propiedad que la información no pone a disposición y no sea divulgada a personas, entidades o procesos no-autorizados.

Disponibilidad: la propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada.

Dueño del Riesgo: Persona o entidad que tiene la responsabilidad y autoridad para gestionar un riesgo.

Integridad: la propiedad de salvaguardar la exactitud e integridad de los activos.

Impacto: Efecto adverso a los objetivos del negocio.

Nivel de Riesgo: Magnitud de un riesgo o combinación de riesgos, expresados en términos de la combinación de las consecuencias y de su probabilidad.

Probabilidad: Posibilidad de que algún hecho se produzca.

Riesgo: Efecto de la incertidumbre sobre los objetivos.

Riesgo residual: Riesgo remanente luego de tratamiento del riesgo.

Vulnerabilidad: Una debilidad de un activo o grupo de activos que puede ser aprovechada por una amenaza.

Anexos

Anexo A: Matriz de Riesgos

En la Matriz de Riesgos se contemplan los siguientes campos:

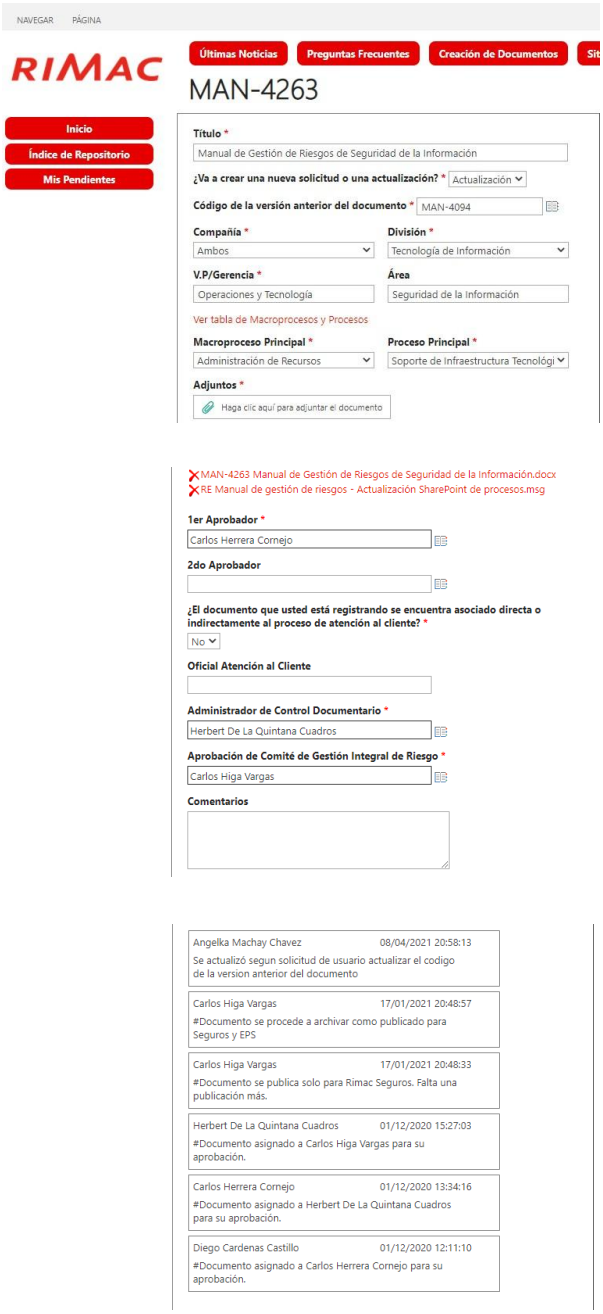
- Activos de Información.
- Situación Identificada.
- Descripción del Riesgo.
- Probabilidad.
- Impacto.
- Nivel de Riesgos.
- Control Propuesto.
- Medidas de Tratamiento.
- Tipo de Tratamiento.
- Fecha de Implementación del Tratamiento.
- Comentarios del Owner.

A continuación, se adjunta la matriz como un archivo Excel.

Matriz de Riesgos de Seguridad de la Infor

Anexo B: Aprobación de la metodología

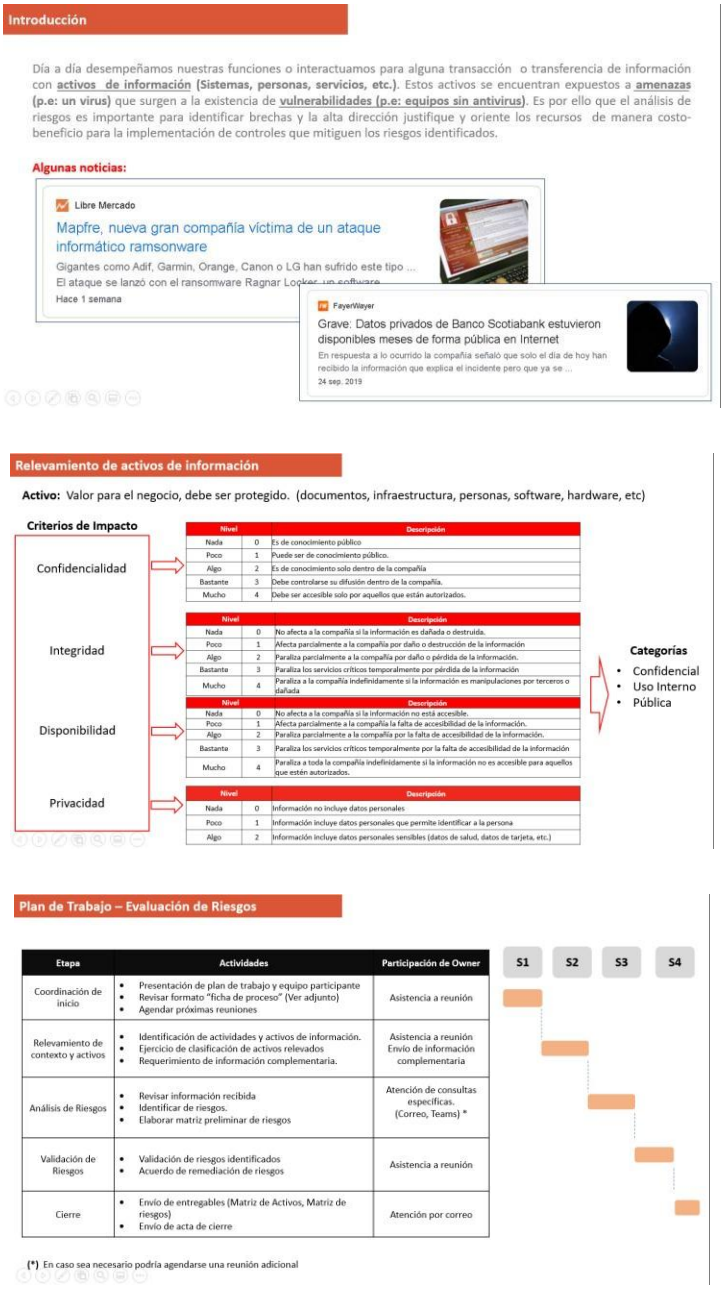
Figura 9. Aprobación y publicación de la metodología.



Fuente: Elaboración Propia

Anexo C: Presentación para el de inicio de la evaluación

Figura 10. Presentación a los propietarios delos procesos.



Fuente: Elaboración Propia

Anexo D: Envió de los resultados de la evaluación

Figura 11. Presentación de resultados de la evaluación.

Nota: Se envió por correo el resultado de la evaluación de riesgos de seguridad de la información a los propietarios de cada proceso.

Fuente: Elaboración Propia.