ESCUELA DE POSTGRADO Y ESTUDIOS CONTINUOS

PROPUESTA DE OPTIMIZACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN UNA ENTIDAD FINANCIERA.

Tesis para optar el grado de **MAESTRO** en:

INGENIERÍA DE SISTEMAS CON MENCIÓN EN GERENCIA DE SISTEMAS DE INFORMACIÓN.

Autor:

Bach. Chimoy Asto, Guillermo Enrique

Asesor:

Dr. Alberto Carlos Mendoza de los Santos

Trujillo – Perú

2020

Resumen

La presente investigación se realizó para hallar de qué manera se debe optimizar el Sistema de Gestión de Seguridad de la información para disminuir los riesgos de la seguridad de la información en una entidad financiera regional del Perú siendo una investigación con un enfoque cuantitativo – descriptiva, además de tener un diseño de investigación no experimental, longitudinal teniendo principalmente como población a los trabajadores de los departamentos y directivos de las 15 agencias que forman parte de la entidad financiera a investigar de los cuales se toman como muestra exclusivamente a 2 representante por cada departamento y 5 directivos de agencia de las 15 sedes de la entidad financiera la recolección de datos para el estudio se realizó mediante fichas de registros, con lo que se pudo obtener como principales resultados que la mejora en la cual se hizo énfasis fue seleccionar los controles y objetivos de control, que forman parte del el Sistema de Gestión de Seguridad de la Información con la versión de la norma ISO 27001:2014, correspondientes a las cláusulas de Seguridad Organizacional, Gestión de activos, Seguridad en los recursos humanos, Seguridad física, Gestión de comunicaciones, Control de accesos además de identificar que los riesgos potenciales de seguridad de la información se encuentra con un 71.20% en el nivel más alto y que las brechas existentes de Seguridad de la Información evalúan la efectividad de los controles en la que solo el 50% de ellos son moderados y el 42% débiles.

Palabras Claves: Gestión de seguridad de la información y Riesgos de Seguridad

Abstract

This research was conducted to find out how the Information Security Management System should be optimized to reduce information security risks in a regional financial institution in Peru. This research has a quantitative-descriptive approach, as well as a non-experimental research design, The main results of the longitudinal study were the selection of controls and control objectives, which are part of the Information Security Management System with the version of ISO 27001: 2014, corresponding to the clauses of Organizational Security, Asset Management, Security in human resources, Physical Security, Communications Management, Access Control in addition to identifying that the potential risks of information security is with a 71. 20% at the highest level and that the existing gaps in Information Security evaluate the effectiveness of controls in which only 50% of them are moderate and 42% weak.

Keywords: Information Security Management and Security Risks

Dedicatoria

A mis Padres y hermana por todas sus enseñanzas y apoyo a lo largo de mi vida, de manera especial a mi Madre por su entrega y amor que me han permitido perseverar y dar lo mejor de mí.

A mi Esposa Rosa, mi fiel compañera, amiga y el amor de mi vida, quien siempre me ha apoyado en mis decisiones personales y profesionales, eres una gran bendición para mí.

A Guillermo y Enrique, mis adorados hijos, una inmensa bendición de Dios para mi vida.

Agradecimiento

A Dios que me conforta y apoya con sus bendiciones en todo momento.

Al Dr. Alberto Mendoza de los Santos por su apoyo en el desarrollo de la presente investigación.

Tabla de Contenidos

ÍNDICE DE TABLAS

Índice de figuras

I. INTRODUCCION

I.1. Realidad problemática

La información es el activo más importante para una institución, y mucho más para las entidades financieras en las cuales no solo se maneja la información administrativa sino también la de los clientes, el valor de esta traspasa las palabras, los números o imágenes, el concepto y las ideas son formas intangibles de la información, consideradas después del recurso humano como datos de suma importancia, estos recurso en su mayoría son adquiridos con el apoyo de los accionistas, clientes, trabajadores, reguladores y se generan también al realizar ciertas actividades como lo son las transacciones de ahorros, créditos, gestiones administrativas entre otras. (NTP-ISO/EIC 27002,2017).

Las empresas al pasar del tiempo se han preocupado más por modernizar los sistemas informáticos más no por darle prioridad a la seguridad de la información que contienen estos, el progreso tecnológico y la evolución del internet a dado lugar a que personas sin autorización accedan a información y se dediquen a realizar ataques informáticos con la finalidad de cometer actos ilícitos que pueden llegar a perjudicar a la empresa. (Recovery Labs, 2019)

Por ello es que es de suma importancia perfeccionar los sistemas de información y manipulación de documentación física, en donde se incluyan criterios de seguridad para resguardar y evitar exponerla, estos controles se refieren a un conjunto de normas, procedimientos y mecanismos que garantizarán la confidencialidad, integridad y disponibilidad de los datos para las personas de la organización. (ISOtOOLS Excellence, 2014)

Esta gestión de seguridad debe dar solución de manera proactivos y oportuna, para ser considerada efectivo ligado siempre a los objetivos de la organización, por lo que a la actualidad la Superintendencia de Banca y Seguros (SBS) intenta regular a las Instituciones Financieras con informes de gestión de riesgos tal como lo establece Basilea II. (Conexionesan, 2019).

En el Perú, se han presentado cientos de ataques de ciber crimen a diario generando grandes pérdidas y esto debido a que solo se invierte el 15% del presupuesto en la gestión de seguridad de información y control de riesgos, siendo los principales blancos de ataques los bancos más pequeños por ser los más desprotegidos. (Gestión, 2017)

En el entorno en que desenvuelve la entidad financiera regional del Perú, materia del presente estudio, se observa que los entes reguladores (Superintendencia de Banca, Seguros y AFPs, el Banco Central de Reserva del Perú, la Superintendencia del Mercado de Valores y SUNAT), proveedores de servicios (RENIEC, Equifax, Telefónica, Rimac Seguros, Hermes) y bancos (BCP, Interbank, BBVA y Scotiabank) cuentan con Sistemas de Gestión de Seguridad de la Información alineados a la ISO27001.

Este Sistema de Gestión de Seguridad de la Información tiene un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la organización para lograr los objetivos comerciales, esta se basa en una evaluación de riesgos y los niveles de aceptación de riesgos de la organización diseñados para tratar y administrar los riesgos de manera efectiva. (ISO/EIC 27000:2018).

La adoptar este Sistema de Gestión de Seguridad de la Información es una decisión estratégica de la organización. El diseño y la implementación del SGSI dependen de sus necesidades y objetivos, así como de sus requisitos de seguridad, procesos utilizados, el tamaño y estructura de la organización, el cual mantendrá mantiene la confidencialidad, integridad y disponibilidad de la información mediante un proceso de gestión de riesgos y da la confianza a las partes interesadas de que los riesgos son manejados adecuadamente (ISO27001, cláusula 0.1 Generalidades).

Las incidencias que afecten a la información comprometiendo su confidencialidad, integridad y/o disponibilidad puede ser causado por caídas en el soporte informático, desastres naturales, siniestros, sustracción o mal uso de la información, ataques informáticos, ingeniería social y otras que pueden originar colateralmente impactos en la reputación, daños económicos y de incumplimiento regulatorio por parte de la entidad financiera.

La entidad financiera a investigar forma su sistema a partir de inventariar los activos de información que son soportados por los sistemas informáticos dejando, fuera de su alcance, los activos no informáticos como son los documentos físicos, por esta razón, se hace necesario optimizar el Sistema de Gestión de Información alineándolo a la ISO 27001 para elevar su grado de madurez, proteger los activos de información no-informáticos y gestionar de mejor manera los riesgos que amenazan la información.

I.2. Pregunta de investigación

¿De qué manera se debe optimizar el Sistema de Gestión de Seguridad de la información en una entidad financiera regional del Perú?

I.3. Objetivos de la Investigación

A. Objetivo General

Generar una propuesta de Optimización del Sistema de Gestión de Seguridad de la Información en una entidad financiera regional del Perú.

B. Objetivos Específicos

1. Analizar el sistema de gestión de seguridad de activos.
2. Identificar los riesgos potenciales de seguridad de la información en la entidad financiera.
3. Determinar las mejoras del Sistema de Gestión de Seguridad de la Información en una entidad financiera regional del Perú.

I.4. Justificación de la investigación

Esta investigación basa su justificación en el aspecto valorativo, ya que la entidad financiera a investigar podrá identificar los riesgos y errores que se comenten en el sistema de seguridad de la información, por lo que se podrá tomar como referencia para dar solución a estos y establecer las estrategias que disminuyan el impacto y posibilidad de ocurrencias, otorgando confianza a las partes interesadas: accionistas, entes reguladores, clientes, proveedores y la comunidad en general, que los riesgos son administra adecuadamente por la organización.

Además, se justifica de manera teórica al optimizar el Sistema de Gestión de Seguridad de la Información (SGSI) alineándola a la norma ISO/EIC 27001:2013 (NTP-ISO/EIC 27001:2014) que permitirá establecer políticas y procedimientos, que podrá ser usada como referencia y texto informativo para futuros investigadores de proyectos de mejora que se apliquen para entidades financieras o rubros aledaños al de la investigación.

Académicamente, la aplicación de los conocimientos en sistemas de información adquiridos durante el proyecto de investigación apoyará a mejorar las deficiencias en el sistema de Gestión de Seguridad de la Información (SGSI) estableciendo las políticas necesarias y optimizando los procesos.

I.5. Alcance de la Investigación

Esta investigación propone optimizar el Sistema actual de Gestión de Seguridad de la Información para incluir los activos de información no informáticos, cuantificar los riesgos a los que están expuesto e identificar los riesgos existentes con el objetivo de una mejor gestión del riesgo para la entidad financiera.

Para el desarrollo del presente trabajo, se va a rediseñar el Sistema de Gestión de Seguridad de la Información alineándolo con la norma ISO/EIC 27001:2013 (NTP-ISO/EIC 27001:2014).

II. MARCO TEÓRICO

II.1. Antecedentes

Molano (2017) En su investigación Estrategia para implementar un sistema de gestión de la Seguridad de la información basada en la norma ISO 27001 en el Área de TI para la empresa market mix, con el objetivo de identificar los riesgo y la vulnerabilidad que amenazan a la empresa para obtener un diagnóstico del estado actual de la empresa e implementar a las recomendaciones necesarias, se obtuvo como resultados que se debe implementar un comité que supervise el buen funcionamiento del sistema, además de implementar capacitaciones constantes y pruebas con el proveedor de servicios de internet para garantizar que no existirán

fallas en el operador, además de mejorar la seguridad del ingreso al área de servidores ya que no se registraba de manera correcta el personal que tenía acceso.

García y Huamani (2019) en su investigación titulada Modelo de gestión de riesgos de seguridad de la información para pymes en el Perú, la cual tiene como objetivo Implementar un modelo de gestión de riesgos de seguridad de la información para una empresa de productos de arcilla cerámica, basado en la metodología OCTAVE-S y la norma ISO/IEC 27005, utilizo la metodología PMBOK, con la intensión de definir los documentos de gestión y poder realizar la comparación en la que obtuvo que la implementación del modelo permite genera conocimientos de cuáles son los riesgos de seguridad de la información, además de reducirlos y monitorear el control de la información tangible e intangibles, de tal manera que se puedan tomar las mejores decisiones reduciendo gastos.

Cruz y Fukusaki (2017) con su investigación Diseño e implementación de un sistema de gestión de seguridad de la información para proteger los activos de información de la Clínica MEDCAM Perú SAC. tuvo el objetivo de diseñar e implementar un Sistema de Gestión de Seguridad de la Información (SGSI) para proteger los activos de información que influyen en el cumplimiento de los objetivos de la empresa, se utilizó el diseño del SGSI y el PDCA (Plan-Do-Check-Act), sugerida por la norma ISO/IEC 27001, teniendo como resultados minimizar los riegos de amenazas y vulnerabilidad de la información, además de lograr la confidencialidad disponibilidad e integridad de la información, teniendo como beneficio principal asegurar los activos de información, cumplimiento los objetivos de la empresa; así como, que cada SGSI debe estar acorde con el tamaño y madurez de los procesos de la empresa.

Guamán (2015) En su investigación Diseño de un sistema de gestión de seguridad de la información para instituciones militares, tuvo como objetivo incorporar estándares internacionales ajustados al campo militar con nuevas tecnologías de la información contribuyendo a la modernización, se tomó como metodología la norma ISO 27001:2005 junto a la metodología para la evaluación de riesgos, obteniendo como resultados que la implementación del diseño de gestión de seguridad de la información disminuyo de manera significativa, reevaluando los activos de la información y reconociendo las responsabilidades de seguridad de la información.

Moncada e Israel (2018) diseñaron un modelo que permite gestionar la seguridad de la Información para la Cooperativa de Ahorro y Crédito ABC, en base a la norma ISO 27001:2013, teniendo en cuenta la evolución y los problemas internos de este tipo de instituciones financieras, que poseen la necesidad de darle dirección a los procesos hacia una efectiva gestión de riesgos, así como, la adecuación a los requerimientos regulatorios vigentes, permitiendo que se preserve la disponibilidad, confidencialidad e integridad de la información, obteniendo como resultados que se mejore de manera significativa la gestión de los activos en un 22% superando el análisis inicial, con un enfoque más rentable que le puede dar frente a cualquier riesgo de los recursos, determinado así los planes de seguridad pertinentes.

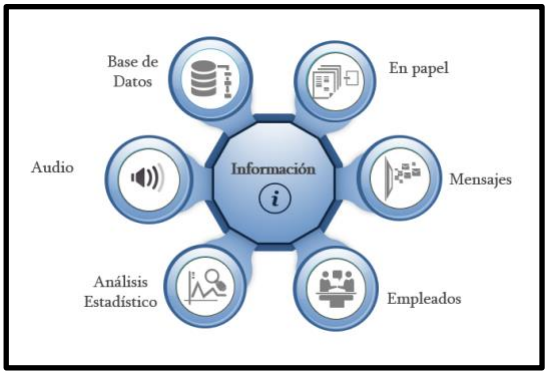
Niño (2018) realizó la investigación modelo de un sistema de gestión de seguridad de información – sgsi, para fortalecer la confidencialidad, integridad, disponibilidad y monitorear los activos de información para el instituto nacional de estadística e informática – INEI filial Lambayeque, con el objetivo de proteger los activos de información, siguiendo el modelo PDCA y la metodología de Magerit VS 3, con la intención de identificar el nivel de riesgos activos en la información, obteniendo como resultados que la seguridad de la información es un apoyo para la dirección de las organizaciones manteniendo un control en los sistemas y transparencia de los procesos, además que la metodología aplicada demostró que existían problemas con el uso de los recursos, colaboradores y la información con la que se opera, con respecto al análisis de riesgos se encontró que el nivel de madurez de la seguridad de la información era muy bajo.

II.2. Bases teóricas

A. Gestión de seguridad de la Información

El sistema de información es la unión de servicios, aplicativos y activos tecnológicos que contienen información y otros componentes externos a la tecnología que administran la información. El activo informático es todo elemento que se contiene para obtener beneficios estratégicos, esta puede ser contenida de manera física, escrita, imágenes, audios, base de datos, de manera electrónica o de otra naturaleza. (Vergara, 2009)

Figura 1 - Información y sus contenedores



Elaboración propia

Un Sistema de Gestión de Seguridad de la Información es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información en una organización para conseguir los objetivos del negocio. Se basa en una evaluación del riesgo y de los niveles de aceptación del riesgo de la organización diseñados para tratar y gestionar los riesgos de manera eficaz, analizar los requisitos para la protección de los activos de información y aplicar controles adecuados para garantizar la protección de estos activos de información. (ISO 27000, cláusula 4.2.1).

Las tres propiedades que busca salvaguardar el Sistema de Gestión de Seguridad de la Información son:

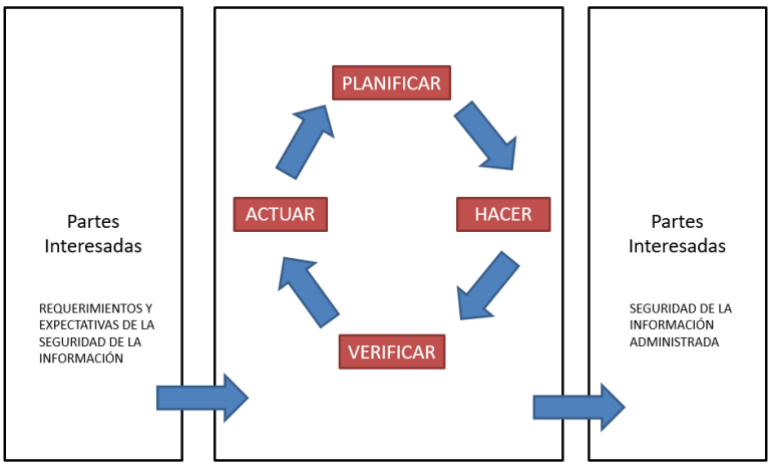
Confidencialidad: Propiedad que determina que la información no esté disponible, ni sea divulgada a personas o procesos no autorizados. Si se llegara a perder este principio se optará y considerara como un robo.

Disponibilidad: Propiedad que asegura que los usuarios autorizados tienen acceso a la información cuando la requieran. Cuando se refiere a los sistemas de información, se deben tener controles que protejan los canales de comunicación, todo dependerá de lo que se quiera proteger y el nivel del servicio dado.

Integridad: La propiedad de proteger la exactitud y completitud de los activos, para que de esta manera se evite modificaciones, eliminación o edición de datos de suma importancia, considerándolo un contenido inalterado a menos que sea por un personal autorizado.

La norma ISO 27001, como la mayoría de normas ISO, adopta el modelo de proceso “Planificar, hacer, verificar y actuar” conocido como PDCA (Plan-Do-Check-Act), por sus siglas en inglés o “rueda de Deming” que se aplica a la estructura de todos los procesos en un sistema de gestión. El SGSI toma como entrada los requerimientos y expectativas de las partes interesadas, y cómo se producen, con las acciones y procesos necesarios, los resultados de seguridad de la información que cumpla con los requisitos y expectativa.

Figura 2 - Modelo Deming aplicado a la ISO 27001



Fuente: ISO27001

Deming (2008) señala que su modelo se centra principalmente en la gestión de calidad, la cual persigue el objetivo de hacer mejoras para el desempeño de los procesos, para evitar defectos y conseguir resultados para la organización.

Las fases para este método son:

- Planificar, se establece el SGSI que es la etapa donde se generan los objetivos, se identifican procesos y se marcan las políticas de la empresa para lograr los resultados.
- Hacer, se implementan los cambios que se planificaron con la intensión de mejorar los procesos.
- Verificar, monitoriar y revisar el SGSI en esta etapa se regulará los periodos de tiempo que verifiquen y midan que se esté llevando a cabo la efectividad de los procesos.
- Actuar, ya una vez verificado y realizado las mediciones correspondientes, se determinará si los resultados no son los esperados, se procederá a desarrollar correcciones y modificaciones necesarias.

Norma ISO /IEC 27001

Según Kosutic (2014), es una norma internacional en la que se explica los lineamientos de seguridad para la información, que se implementarán en la gestión de la seguridad, para cualquier tipo de empresa, para de esta forma protegerla de robos, daños o modificaciones, se recomienda su uso ya que disminuye riesgos, mejora procesos y aumenta la competitividad empresarial salvaguardando la integridad, confiabilidad y disponibilidad de la información de los clientes.

La ISO Survey of Management System Standar Certifications (ISO MSSC) encuesta anualmente sobre las certificaciones a sus estándares de sistemas de gestión. El top 10 de países por empresas certificadas en ISO27001 está encabezado por países de Asia y Europa principalmente, solamente Estados Unidos figura por el continente americano, lo que demuestra la ventaja que este país nos lleva en la gestión de la seguridad de la Información. El cuadro 03 muestra el top 10 de países con empresas certificadas en ISO27001.

Tabla 1 - *Top 10 países con empresas certificadas en ISO 27001*

Puesto	País	Certificaciones
1	China	7,199
2	Japón	5,093
3	Reino Unido	2,444
4	India	2,161
5	Alemania	1,057
6	Italia	1,041
7	USA	911
8	Taiwán	827
9	Países Bajos	788
10	España	726

Fuente: Iso.org/iso/survey/iso_27001_iso_survey2018.xls

Perú se encuentra en el quinto puesto, en el ranking de países latinoamericanos, de empresas certificadas en Seguridad de la Información, la brecha entre nosotros y México es muy notoria.

Tabla 2 - *Países latinoamericanos con empresas certificadas en ISO 27001*

Puesto	País	Certificaciones
1	México	218
2	Colombia	146
3	Brasil	110
4	Chile	54
5	Perú	49
6	Argentina	48
7	Uruguay	13
8	Costa Rica	6
9	Ecuador	6
10	Bolivia	5

Fuente: Iso.org/iso/survey/iso_27001_iso_survey2018.xls

B. Riesgos en las seguridades de la información

Amenaza

Una amenaza es una causa potencial de un incidente no deseado que puede resultar en daño en la organización. Los activos de información están expuestos a varios tipos de amenazas que pueden ser físicas o lógicas que al producir un incidente origine impactos materiales o inmateriales que afecten a los activos de información en su integridad, disponibilidad y/o confidencialidad.

Tabla 3 - *Clasificación de amenazas según el origen*

Daño Físico	Eventos Naturales	Radiación
Fuego Agua Contaminación Destrucción de equipos o medios Polvo, corrosión	Fenómeno climático Fenómenos sísmicos Fenómenos volcánicos Fenómeno meteorológico Inundación	R. electromagnética R. térmica R. termo magnética
Pérdida de servicios esenciales	**Fallas Técnicas**	**Acciones no autorizadas**
Falla de aire acondicionado Falla de suministro de energía Falla de equipos de telecomunicaciones Falla de suministro de agua	Falla de equipo Mal funcionamiento de equipo Mal funcionamiento de software Saturación de sistema de información	Uso no autorizado de equipo Copia fraudulenta de software Uso de software falsificado o copiado Corrupción de datos Procesamiento ilegal de datos
Compromiso de funciones	**Hacker**	**Delito Informático**
Erros de uso Abuso de derechos Falsificación de derechos Negación de acciones Brecha de disponibilidad de personal	Hacking Ingeniería Social Intrusión a los Sistemas	Escucha secreta Divulgación ilegal de información Alteración no autorizada de datos Destrucción de información Espionaje remoto
Terrorismo	**Espionaje Industrial**	**Interno**
Guerra de información Ataque de sistema Bomba terrorismo	Ventaja de Defensa Ventaja Política Explotación económica Robo de información Intrusión en privacidad personal	Asalto a empleado Chantaje Fraude y ribo Soborno de información

Fuente: ISO27005 anexo C

Vulnerabilidades

Las vulnerabilidades son todas las debilidades de un activo de información o de un control que puede ser explotada por una o más amenazas, estas incluyen Hardware, Software, Red, etc. (INACAL, 2017).

Riesgos

ISO 27001 define riesgo es la amenaza potencial a que explote una vulnerabilidad en un activo de información y por lo tanto causando un daño a la organización. El nivel de riesgo se calcula en función de la probabilidad de ocurrencia y la severidad del impacto si se materializa el riesgo. Una vez identificadas las amenazas y vulnerabilidades relacionadas con los activos de información, se procede a definir y describir el riesgo de seguridad de la información. Para la descripción del riesgo se tienen en cuenta los siguientes elementos:

- La descripción del activo de información.
- La amenaza que afecta al activo de información.
- La vulnerabilidad que expone una debilidad de un activo.
- La severidad o impacto que ocasiona

Controles

Los controles son los medios de gestión del riesgo, incluidas las políticas, procedimientos, directrices, prácticas y estructuras organizativas. Los controles según la ISO27000 se clasifican en:

- Control preventivo: Tiene como objetivo desalentar o evitar la aparición de problemas.
- Control de detección: Busca e identifica anomalías.
- Control correctivo: Evita la repetición de las anomalías.

Identificación de amenazas y vulnerabilidades

Realizado el inventario de los activos de información se debe identificar las amenazas a las que se encuentran expuestos y las vulnerabilidades que pueden ser aprovechadas para causar un impacto negativo sobre los activos de información afectando a su confidencialidad, integridad y/o confidencialidad. Esta actividad se realiza por cada activo de información empezando por los de mayor valor para posteriormente cuantificar los riesgos existentes. (INACAL, 2018)

Para calcular el nivel de riesgo que afectan a los activos de información, la organización establece una metodología de valoración de acuerdo a su apetito al riesgo. El cálculo se realiza en función de:

- Frecuencia (probabilidad): Es el número de veces que puede materializarse el riesgo, considerando la frecuencia de las amenazas y vulnerabilidades.
- Severidad: Es una estimación de la magnitud de la consecuencia si se materializa el riesgo, expresada en términos de severidad de la perdida de la confidencialidad, integridad y disponibilidad del activo.

Figura 3 - Matriz para la medición del riesgo

Fuente: Elaboración propia

Se determina el riesgo de acuerdo a su ubicación en la matriz, de acuerdo a la siguiente regla:

- Cuadrantes verdes: Riesgo Bajo
- Cuadrantes amarillos: Riesgo Moderado
- Cuadrantes anaranjados: Riesgo Relevante
- Cuadrantes rojos: Riesgo Alto
- Cuadrantes azules: Riesgo Crítico

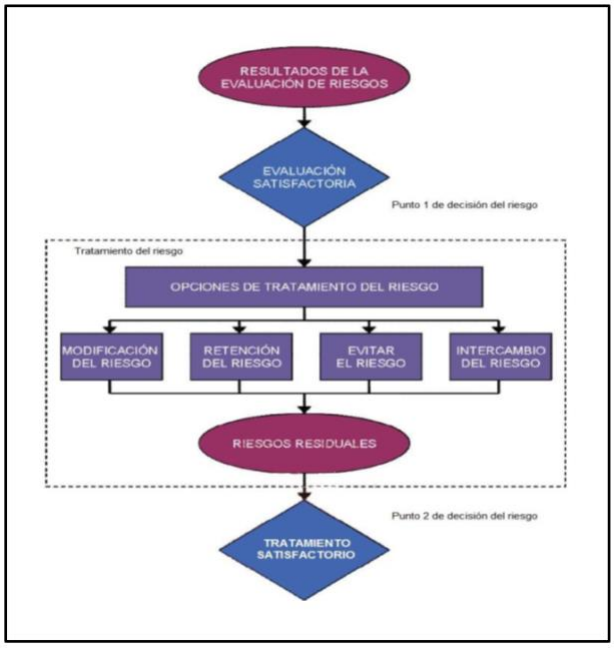
Gestión del Riesgo

Los responsables de la Gestión del Riesgo de la Información, deciden de que manera proteger los activos de información comprometidos, dándoles un tratamiento luego de este tratamiento dentro del margen establecido, este proceso debe ser interactivo proporcionando pruebas suficientes para determinar las acciones necesarias para reducir el riesgo a un nivel aceptable.

Para el tratamiento de riesgos se tiene en cuenta cuatro opciones que no son mutuamente excluyentes, a veces, podemos hacer combinación de opciones para la reducción de la probabilidad de los riesgos, la reducción de sus consecuencias y compartir o retener cualquier riesgo residual, las opciones son las siguientes:

- Retención del riesgo, la organización asume el riesgo porque se encuentra debajo del valor aceptable, se debe elegir esta alternativa, ya que solo requiere que quede un registro documentado de la decisión de aceptar el riesgo.
- Evitar el Riesgo, en este caso se considera que el riesgo es muy alto, por lo que implementar otras opciones del tratamiento del riesgo exceden los costos sin llegar a los beneficios.
- Compartir o intercambio el Riesgo, con una organización que pueda gestionar de manera mucho más eficiente el riesgo en función a su valoración.
- Mitigar o modificar el Riesgo, se decide reducir las mejoras de los controles para que reduzcan hasta un nivel aceptable.

Figura 4 - Actividad de tratamiento del riesgo

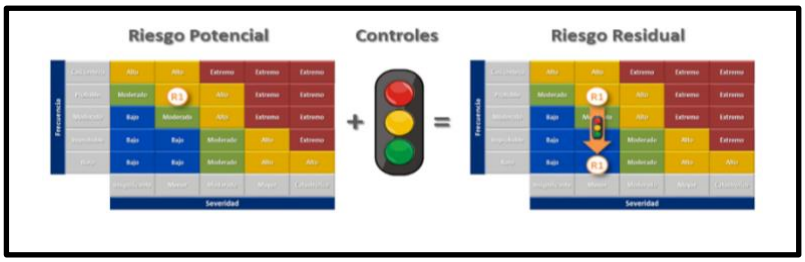


Fuente: ISO27005

Implementación de controles

Para gestionar los riesgos de manera eficiente se decide mitigar e implementar controles de seguridad para impedir que el riesgo potencial sea procesado por el control y así llegar a un nivel inferior al riesgo aceptable.

Figura 5 - Tratamiento de riesgos por controles de seguridad



Fuente: Documento metodológico de la organización

Plan de tratamiento de riesgos

El plan de tratamiento de riesgos de seguridad de la información, es un listado de planes de acción para implementar los controles necesarios para cerrar las brechas del riesgo que su opción de tratamiento es “mitigar” o “transferir”. En base a los controles propuestos a implementar se consolida la siguiente información:

- Responsable de la implementación
- Nivel de urgencia
- Recursos financieros, físicos, tecnológicos y recursos humanos

- Cronograma de actividades
- Estado de la implementación, y
- Observaciones

Medición del Sistema de Gestión de Seguridad de la Información

Para medir la efectividad del Sistema de Gestión de Seguridad de la Información y evaluar el desempeño de los controles de Seguridad se utilizará métodos que involucran una variedad de fuentes tales como cuestionarios, entrevistas personales, resultados del análisis y evaluación de riesgos, reportes de auditoría interna y/o externa, registros de logs, reportes de incidentes; y resultados de pruebas tales como pruebas de penetración, ingeniería social, herramientas de cumplimiento y auditoría.

II.3 Marco Conceptual

A. **Activo de información:** Elemento que contiene o manipula información, a través del cual la entidad obtiene beneficios para el logro de sus objetivos estratégicos.
B. **Estimación del riesgo:** Proceso para asignar valores a la probabilidad y el impacto de un riesgo.
C. **Evaluación de riesgos:** Proceso de comparación de los resultados del análisis del riesgo con los criterios de riesgo para determinar si el riesgo y/o su magnitud son aceptables o tolerables y decidir si corresponde o no tratarlo.
D. **Gestión de riesgos:** Actividades coordinadas para dirigir y controlar el riesgo en una entidad.
E. **Identificación del riesgo**: Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.
F. **Modelo de Deming:** Es una herramienta que permite la mejora continua en base a la repetición de sus cuatro fases que son: "Planificar-Hacer-Verificar-Actuar" que es usada para mejorar los procesos de gestión.
G. **Nivel de riesgo:** Magnitud de un riesgo expresado en términos de la combinación de consecuencias y su posibilidad.
H. **Plan de tratamiento de riesg**o: Son las actividades que se ejecutan una vez tomada la decisión de tratamiento de riesgos, aquí es donde se determinan los recursos económicos, tiempo, personas a utilizar, los resultados esperados y la supervisión del avance y cumplimiento.
I. **Riesgo:** Potencialidad de que una amenaza explote una vulnerabilidad en un activo o grupo de activos y por lo tanto causará daño a la organización.
J. **Sistema de gestión de seguridad de la información:** Su objetivo es preservar la confidencialidad, integridad y disponibilidad de la información en la organización estableciendo políticas y controles en relación con los objetivos del negocio de la organización.
K. **Tratamiento de riesgos:** Proceso de selección e implementación de las medidas encaminadas a modificar los riesgos.

III. HIPÓTESIS

III.1 Declaración de hipótesis

El sistema de seguridad de la información presenta problemas en la visibilidad en los riesgos de la información en una entidad financiera regional del Perú.

III.2 Operacionalización de variable

A Variable

Sistema de Gestión de Seguridad de la Información

Tabla 4 - *Operacionalización de variables*

Variable	Tipo de variable	Operacionalización		Dimensiones	Definición conceptual	Indicador	Índice	Nivel de medición
		Definición conceptual	Definición Operacional					
Sistema de Gestión de Seguridad de la Información	Cuantitativa	Un Sistema de Gestión de Seguridad de la Información es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información en una organización para conseguir los objetivos del negocio. (ISO 27000)	Es aquel sistema que nos permite brindar la seguridad de manera eficaz y suficiente para salvaguardar los procesos, datos e información de la entidad	Confidencialidad	Propiedad que determina que la información no esté disponible ni se divulgue a las personas no autorizadas.	Cantidad de activos de información evaluados por su confidencialidad	Índice de activos de información evaluados por su confidencialidad	Unidades
				Disponibilidad	Acceso de la información al personal autorizado, con controles que protejan los canales de comunicación.	Cantidad de activos de información evaluados por su disponibilidad	Índice de activos de información evaluados por su disponibilidad	Unidades
				Integridad	Evita modificaciones, eliminación o edición, de contenido inalterable por personal no autorizado	Cantidad de activos de información evaluados por su Integridad	Índice de activos de información evaluados por su Integridad	Unidades

IV. DESCRIPCIÓN DE MÉTODOS Y ANÁLISIS

IV.1. Tipo de investigación

Esta investigación sigue un enfoque cuantitativo, ya que se analizó y proceso datos de manera estadística, lo cual nos permitió obtener información estadística, gráficos.

Además, es de tipo descriptiva, ya que se analizó un problema y se desarrolló una opción de solución para el mismo, teniendo en cuenta las teorías tratadas en la presente investigación.

IV.2. Diseño de Investigación

La investigación tiene un diseño no experimental, longitudinal ya que se evaluó las decisiones tomadas con anterioridad por la gerencial y se analizó los cambios que se deben implementar posteriormente sobre los riesgos de seguridad de la información.

IV.3. Método de Investigación

Se utilizó la técnica de análisis documental para recolectar la información necesaria para analizar el sistema de gestión de seguridad de activos e identificar los principales riesgos de seguridad de la información en la entidad financiera, luego se realizó un taller para implementar y educar al personal sobre las mejoras en el sistema de gestión que se deben ejecutar.

IV.4. Población y Muestra

Población: Trabajadores de los departamentos y directivos de las 15 agencias que forman parte de la entidad financiera, además de Informes de gestión, Incidentes, no conformidades, resultados de auditorías internas y externas

Muestra: Consto de 2 representante por cada departamento y 5 directivos de agencia de las 15 sedes de la entidad financiera y la documentación y archivos de registros de cada sede.

IV.5. Técnicas e instrumentos

Técnica de recolección de datos: Se realizó mediante el análisis documental de los archivos y registros de la entidad financiera, como lo son: Informes de gestión, Incidentes, no conformidades, resultados de auditorías internas y externas.

Técnica de procesamiento y análisis de datos: Se procesó los datos mediante tabulación de la información según el grupo pertinente para la información, para

analiza la información se realizó de manera estadística a partir de los cuadros resultantes de la tabulación.

Instrumentos: Los instrumentos a utilizar son las fichas de registro.

- Ficha de registro: Inventario y clasificación de activos, Análisis de riesgos

V. RESULTADOS

V.1. Analizar el sistema de gestión de seguridad de activos

V.1.1. Comprensión de la Organización

La entidad financiera regional del Perú, en la que se realizó la presente investigación, es una empresa privada que realiza actividades de intermediación financiera, regulada por la Superintendencia de Banca, Seguros y AFP's, Banco Central de Reserva del Perú y Superintendencia del Mercado de Valores; se revisó la Visión, Misión, Valores, objetivos, análisis FODA, estrategias, asimismo administra información de 830,000 clientes que hacen uso de sus productos y servicios, 135 accionistas, 5530 trabajadores y 185 proveedores.

De todas estas partes interesadas identificados, la entidad financiera recibe información que debe ser procesada, almacenada y protegida mediante un Sistema de Gestión de Seguridad de la Información dentro del marco normativo peruano y con el uso de estándares de seguridad como herramienta para lograr los objetivos salvaguardar la confidencialidad, integridad y disponibilidad.

La entidad financiera tiene 27 productos y servicios soportados por 249 procesos y subprocesos realizados por los 42 departamentos que conforman la organización. El soporte tecnológico está compuesto por el centro de procesamiento principal CPD, el centro de procesamiento alterno CPA, redes LAN/WAN, internet, enlaces a canales electrónicos (Home Banking, agentes corresponsales y ATMs) y 2,350 estaciones de trabajo.

V.1.2. Liderazgo y aprobación del proyecto

La alta dirección representado por el Directorio, tomando conocimiento de los informes del Comité de Riesgos, con los resultados de la evaluación de alineamiento del Sistema de Gestión de Seguridad de la Información a la ISO 27001 y del proyecto de optimización del Sistema de Gestión de Seguridad de la Información conteniendo los requerimientos de recursos financieros, cronograma y personal necesario, toma la decisión de aprobar el proyecto como una decisión estratégica para el logro de los objetivos institucionales.

V.1.3. Alcance del SGSI

La alta dirección determinó que dentro del alcance del SGSI todos los productos y servicios y servicios necesarios para cumplir los objetivos del negocio, incluyen los procesos y subproceso de negocio y soporte que habilitan la entrega de los productos y servicios.

V.1.4. Inventario y Clasificación de Activos

La información es suministrada a la organización por sus grupos de interés (accionistas, reguladores, clientes, proveedores y trabajadores), además es creada por la organización, utilizada y gestionada por los procesos de negocio, es un recurso importante para su operación diaria y para lograr los objetivos estratégicos, debido a su importancia, esta se convierte en un activo con valor y requiere ser tratada con la seguridad suficiente.

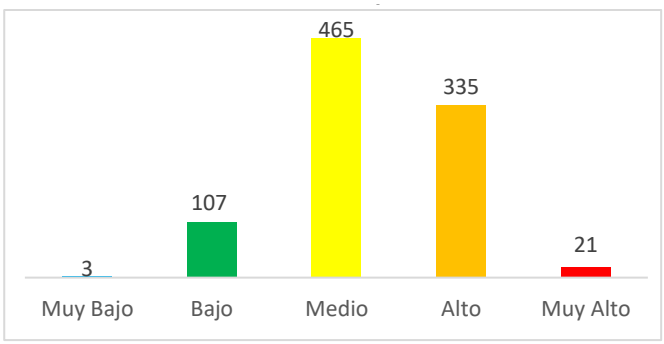
A continuación, se describe el enfoque metodológico para desplegar el inventario y la clasificación de activos:

V.1.4.1. Identificar activos de información

Habiendo sido aprobada la metodología para realizar el nuevo inventario de activos de la información en la organización, se hizo la identificación de Activos de Información utilizando el formato "SGSI-FO-01a Activos de Información Primarios", se pudo identificar un total de 931 activos primarios, para los cuales se tuvo que determinar el Propietario, Custodio, Ubicación, Requisitos Legales, Frecuencia de Uso, Sensibilidad, Valor del Activo (confidencialidad, integridad, disponibilidad) y Nivel de Tasación.

En la Figura 06 se muestra la cantidad de Activos de Información Primarios que tienen un determinado nivel de Tasación (muy bajo, bajo, medio, alto o muy alto).

Figura 6 - Cantidad Activos Primario por Nivel de Tasación



Elaboración propia

En la Tabla 05 se muestra un listado de los Propietarios y la cantidad de Activos de Información primarios por nivel de tasación que posee cada uno;

también se puede visualizar que el Gerente de Riesgos es el propietario de la mayor cantidad de Activos Primarios, y esto se debe a que el Departamento de Riesgo Crediticio, Mercado y Liquidez detallaron todos los reportes y anexos que generan, los cuales son enviados en su mayoría a las diferentes entidades regulatorias externas.

Tabla 5 - *Cantidad de Activos Primarios por Propietarios*

Propietario	Muy Bajo	Bajo	Medio	Alto	Muy Alto	Total
Gerente Ejecutivo Adjunto	2	5	22	19	1	49
Gerente Central de Administración			16	19	4	39
Gerente de División de Finanzas y Canales		11	47	65	7	130
Gerente Central de Finanzas		3	32	34	2	71
Jefe Dpto. Inspectoría de Fraude		6	9	7		22
Gerente de División de Administración	1	20	51	40	2	114
Gerente de División de Procesos y TI		14	28	18	1	61
Gerente de División Comercial		8	27	10	3	48
Gerente Central de Negocio		6	29	15		50
Gerente de División de Negocio		6	30	29		65
Gerente de Riesgos		20	137	50		207
Jefe Unidad de Auditoría Interna			10	2		12
Jefe Unidad de Cumplimiento Normativo		6	13	8		27
Jefe Unidad de Prevención			9	17	1	27
Jefe Órgano de Control Institucional		2	5	2		9
Total general	**3**	**107**	**465**	**335**	**21**	**931**

Elaboración propia

En la Tabla 06 se muestra un listado de los Custodios y la cantidad de activos primarios por nivel de tasación que posee cada uno; también se puede apreciar que el Jefe de Departamento de Riesgo Crediticio, Mercado y Liquidez es el custodio de la mayor cantidad de Activos Primarios, y esto se debe a que todos los reportes y anexos que generan, son enviados en su mayoría a las diferentes entidades regulatorias externas.

Tabla 6 - *Cantidad de Activos Primarios por Custodio*

Custodio	Muy Bajo	Bajo	Medio	Alto	Muy Alto	Total
Gerente Central de Administración			1	10		11
Gerente Central de Finanzas			1	9	2	12
Gerente Central de Negocio			11	4		15
Gerente de División Comercial		4	9	2		15
Gerente de División de Administración			1	10	2	13
Gerente de División de Finanzas y Canales			1	12	4	17
Gerente de División de Negocio			8	8		16
Gerente de División de Procesos y TI		4	3	2		9
Gerente de Riesgos		1	15	3		19
Gerente Ejecutivo Adjunto		1	2	8		11
Jefatura Zonal de Negocio		4	13	13		30

Custodio	Muy Bajo	Bajo	Medio	Alto	Muy Alto	Total
Jefe Dpto. Ahorros y Servicios		2	10	5		17
Jefe Dpto. Aprobación de Créditos		1	9	1	1	12
Jefe Dpto. Asesoría Jurídica			9	3		12
Jefe Dpto. Atención al Usuario		3	12	11		26
Jefe Dpto. Canales de Atención		4	10	8		22
Jefe Dpto. Contabilidad			3	22		25
Jefe Dpto. Finanzas		1	14	10	3	28
Jefe Dpto. Gestión de Calidad y Proyectos		7	5	1		13
Jefe Dpto. Gestión de Desarrollo Humano			6	6	4	16
Jefe Dpto. Inspectoría de Fraude		6	9	7		22
Jefe Dpto. Logística		2	10	11		23
Jefe Dpto. Marketing e Imagen Institucional	2	3	11	10		26
Jefe Dpto. Negocios No Minoristas		2	9	8		19
Jefe Dpto. Operaciones Centrales		9	17	14		40
Jefe Dpto. Planificación			19	14		33
Jefe Dpto. Recuperaciones		6	18	11		35
Jefe Dpto. Red Operaciones de Agencia	1	3	8	2		14
Jefe Dpto. Riesgo Crediticio, Mercado y Liquidez		8	86	35		129
Jefe Dpto. Riesgo Operacional		3	15	6		24
Jefe Dpto. Segmento Microempresa			5	5		10
Jefe Dpto. Segmento Pequeña Empresa		3	5	1		9
Jefe Dpto. Segmento Personas		1	8	2	3	14
Jefe Dpto. Seguridad		6	15	3		24
Jefe Dpto. Tecnología de la Información		3	20	15	1	39
Jefe Dpto. Tesorería		4	9	8		21
Jefe Órgano de Control Institucional		2	5	2		9
Jefe Unidad de Auditoría Interna			10	2		12
Jefe Unidad de Cumplimiento Normativo		6	13	8		27
Jefe Unidad de Prevención			9	17	1	27
Oficial de SI y CN		8	21	6		35
Total general	**3**	**107**	**465**	**335**	**21**	**931**

Elaboración propia

Después de identificar y definir los Activos de Información Primarios, se procedió a identificar los Activos de Información de Soporte.

Utilizando el formato “FO-01b Activos de Información de Soporte”, se pudo identificar un total de 385 Activos de Información de Soporte, para los cuales se determinó el tipo, propietario y custodio; en la Figura 07 se muestra como se el peso y el nivel de tasación que tienen los Activos de Información de Soporte, esto dependió del mayor nivel de tasación de los activos de información primarios que soporta.

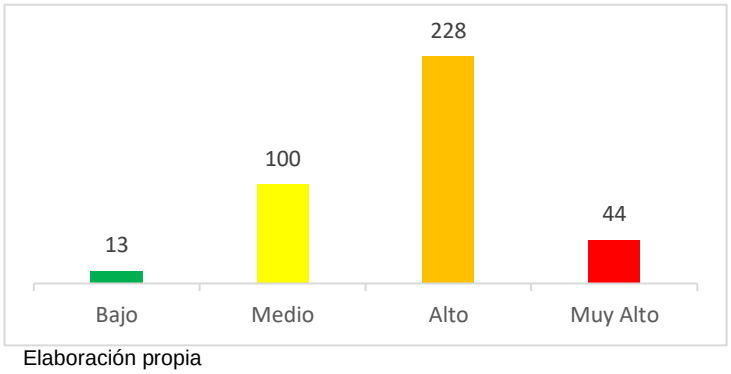
Figura 7 - Activo de Soporte vs. Activo Primario

Activo de Soporte					Activo Primario			
Código	Nombre	Nivel	Valor	Peso	Código	Nombre	Valor	Nivel
AYS-S04	Carpeta Comp. Local AYS	3.67	Alto	11	AYS-P01	Seguros	3.67	Alto
AYS-S04	Carpeta Comp. Local AYS			11	AYS-P02	Base de Ahorros	3.33	Alto
AYS-S04	Carpeta Comp. Local AYS			11	AYS-P03b	Informes estatus de producto - electrónico	3.00	Medio
AYS-S04	Carpeta Comp. Local AYS			11	AYS-P04b	Informe de Nueva Campaña - electrónico	2.67	Medio
AYS-S04	Carpeta Comp. Local AYS			11	AYS-P05b	Informe de Mejora - electrónico	2.67	Medio
AYS-S04	Carpeta Comp. Local AYS			11	AYS-P06	Informe de gestión	3.33	Alto
AYS-S04	Carpeta Comp. Local AYS			11	AYS-P07	Seguimiento Agencia	2.00	Bajo
AYS-S04	Carpeta Comp. Local AYS			11	AYS-P08	Gestión de Agencias	2.00	Bajo
AYS-S04	Carpeta Comp. Local AYS			11	AYS-P09	Reporte Comisiones Convenios	3.00	Medio
AYS-S04	Carpeta Comp. Local AYS			11	AYS-P10	Plan Comercial	2.33	Medio
AYS-S04	Carpeta Comp. Local AYS			11	AYS-P11	Propuestas de un nuevo seguro	2.67	Medio
AYS-S04	Carpeta Comp. Local AYS			11	AYS-P12	Clientes de Ahorros	3.33	Alto
AYS-S04	Carpeta Comp. Local AYS			11	AYS-P13	Lista Clientes Inactivos	3.33	Alto
AYS-S04	Carpeta Comp. Local AYS			11	AYS-P14	Activos de Información	2.67	Medio
GDA-S02	Archivador GDA	4.33	Muy Alto	13	GDA-P02a	Informes de Postulaciones	3.33	Alto
GDA-S02	Archivador GDA			13	GDA-P03a	Informes Estratégicos	3.33	Alto
GDA-S02	Archivador GDA			13	GDA-P04a	Informes Comerciales	3.33	Alto
GDA-S02	Archivador GDA			13	GDA-P06a	Informe de Aprobación de Propuestas	3.33	Alto
GDA-S02	Archivador GDA			13	GDA-P07a	Informes de baja de empleados	4.33	Muy Alto

Elaboración propia

En la Figura 08 se muestra la cantidad de Activos de Información de Soporte que tienen un determinado nivel de Tasación (muy bajo, bajo, medio, alto o muy alto). Se puede apreciar que la mayor parte de Activos de Información de Soporte tienen un Nivel de Tasación Alto, y esto se debe a que las diferentes unidades organizacionales de la entidad financiera hacen uso de diferentes medios para almacenar y procesar activos de información primarios muy importantes, los cuales deben poseer medidas de seguridad, controles y medios de respaldo.

Figura 8 - Cantidad Activos de Información de Soporte por Nivel de Tasación



Elaboración propia

En la Tabla 07 se muestra un listado de Propietarios y la cantidad de Activos de Información de Soporte por nivel de tasación que posee cada uno de ellos.

Tabla 7 - *Cantidad de Activos de Soporte por Propietario*

Propietario	Bajo	Medio	Alto	Muy Alto	Total
Gerente de División de Negocio	2	6	23	3	34
Gerente de División de Procesos y TI	3	16	32	10	61
Gerente Ejecutivo Adjunto		8	19	3	30
Gerente de División de Administración	3	15	27	3	48
Gerente Central de Administración		9	10	5	24
Gerente de Riesgos	1	11	25		37
Gerente de División de Finanzas y Canales	1	7	32	11	51
Gerente Central de Finanzas	1	7	14	1	23
Jefe Dpto. Inspectoría de Fraude		1	7		8
Gerente de División Comercial	1	7	13	4	25
Gerente Central de Negocio	1	2	11		14
Jefe Órgano de Control Institucional		1	4		5
Jefe Unidad de Auditoria Interna		9	4		13
Jefe Unidad de Cumplimiento Normativo			4		4
Jefe Unidad de Prevención		1	3	4	8
Total general	**13**	**100**	**228**	**44**	**385**

Elaboración propia

En la tabla 08 se muestra la lista de los custodios y la cantidad de Activos de Información de Soporte por nivel de tasación que posee cada uno de ellos. En esta tabla se puede visualizar que el Jefe de Departamento de TI es el custodio de la mayor cantidad de Activos de Soporte, y esto se debe, a que las diferentes unidades organizacionales, detallaron que sus activos de información primarios los almacenan en el correo corporativo, carpetas compartidas y para procesarlo hacen de uso de los diferentes módulos del SICMACT y otras herramientas de ofimática, las cuales se encuentran alojadas en determinados servidores custodiados por el Departamento de TI.

Tabla 8 - *Cantidad de Activos de Soporte por Custodio*

Custodios	Bajo	Medio	Alto	Muy Alto	Total
Gerente Central de Administración			2		2
Gerente Central de Finanzas			1	1	2
Gerente Central de Negocio		1	3		4
Gerente de División Comercial	1	3	5		9
Gerente de División de Administración				3	3
Gerente de División de Finanzas y Canales				3	3
Gerente de División de Negocio			3		3
Gerente de División de Procesos y TI			3		3
Gerente de Riesgos		2	3		5
Gerente Ejecutivo Adjunto		2	7		9
Jefe Dpto. Ahorros y Servicios		1	4		5
Jefe Dpto. Aprobación de Créditos		3	1	3	7
Jefe Dpto. Asesoría Jurídica		5	5		10

Custodios	Bajo	Medio	Alto	Muy Alto	Total
Jefe Dpto. Atención al Usuario	1	5	4		10
Jefe Dpto. Canales de Atención	1	1	6		8
Jefe Dpto. Contabilidad		1	14		15
Jefe Dpto. de Gestión de Calidad y Proyectos		4	1		5
Jefe Dpto. Finanzas			2	7	9
Jefe Dpto. Gestión de Desarrollo Humano		4	3	4	11
Jefe Dpto. Inspectoría de Fraude			7		7
Jefe Dpto. Logística			9		9
Jefe Dpto. Marketing e Imagen Institucional		1	11		12
Jefe Dpto. Negocios No Minoristas			4		4
Jefe Dpto. Operaciones Centrales	2	3	12		17
Jefe Dpto. Planificación		2	9		11
Jefe Dpto. Recuperaciones	1	1	8		10
Jefe Dpto. Red Operaciones de Agencia		3	2		5
Jefe Dpto. Riesgo Crediticio, Mercado y Liquidez	1	9	11		21
Jefe Dpto. Riesgo Operacional			6		6
Jefe Dpto. Segmento Microempresa			3		3
Jefe Dpto. Segmento Pequeña Empresa		4	2		6
Jefe Dpto. Segmento Personas			3	4	7
Jefe Dpto. Seguridad	1	8	4		13
Jefe Dpto. Tecnología de la Información	3	17	33	14	67
Jefe Dpto. Tesorería		4	6	1	11
Jefe Órgano de Control Institucional		1	4		5
Jefe Unidad de Auditoria Interna		9	4		13
Jefe Unidad de Cumplimiento Normativo			4		4
Jefe Unidad de Prevención		1	3	4	8
Jefe Zonal de Negocio	2	5	11		18
Oficial de SI y CN			5		5
Total general	**13**	**100**	**228**	**44**	**385**

Elaboración propia

V.1.4.2. Consolidación de Activos de Información de Soporte

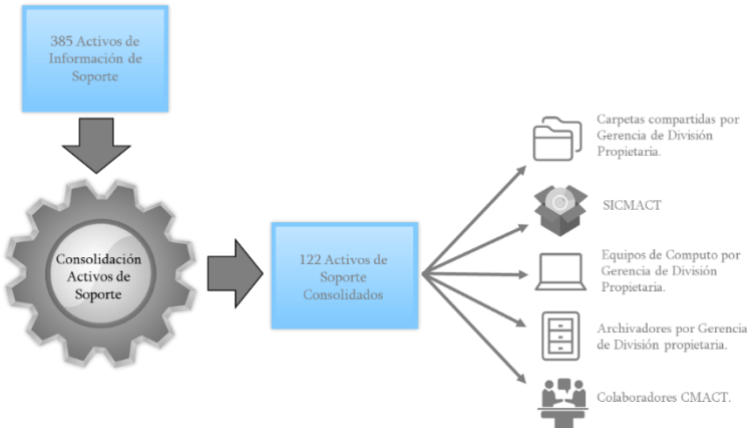
Una vez identificado los activos de información de soporte se procedió a realizar la consolidación de dichos activos.

En la Figura 09 se muestra los activos de información primarios y los medios que permiten su procesamiento y almacenamiento.

Figura 9 - Consolidación Activos 1

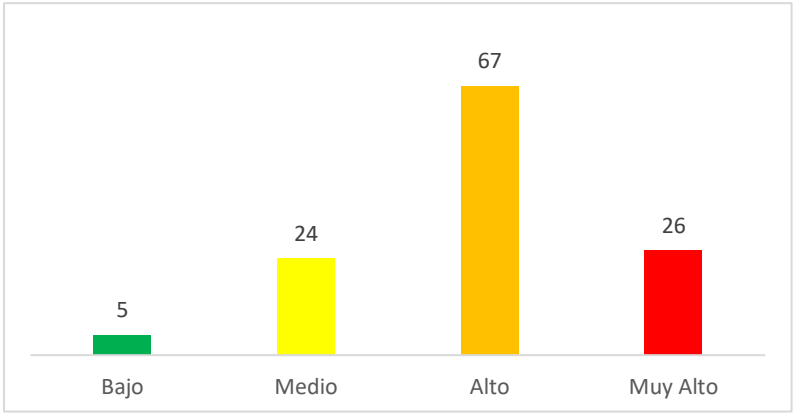
En la Figura 10 se muestra la consolidación de los activos de información de soporte, y el nuevo nombre que recibió cada una de estas consolidaciones, basándonos en el tipo y propietario de los activos de soporte que fueron agrupados de acuerdo a la consolidación.

Figura 10 - Consolidación Activos 2



Como resultado de la consolidación se obtuvo un total de 122 Activos de Soporte Consolidados; en la Figura 11 se muestra la cantidad de Activos de Soporte Consolidados que tiene un determinado nivel de tasación; este nivel de tasación fue determinado en base al mayor nivel de tasación que posee los activos de soporte que fueron agrupados de acuerdo a la consolidación.

Figura 11 - Activos de Soporte Consolidado por Nivel de Tasación



Elaboración propia

Para cada Activo de Soporte Consolidado se determinó un Propietario y Custodio respectivamente; en la Tabla 09 se muestra la lista de los Propietarios y la cantidad de Activos de Soporte Consolidado por nivel de tasación que posee cada uno de ellos; mientras que en la Tabla 10 se muestra la lista de los Custodios y la cantidad de Activos de Soporte Consolidado por nivel de tasación que posee cada uno de ellos.

Tabla 9 - *Cantidad de Activos de Soporte Consolidado por Propietario*

Propietario	Bajo	Medio	Alto	Muy Alto	Total
Gerente Central de Administración	1	4	4	3	12
Gerente Central de Finanzas		2	4		6
Gerente Central de Negocio	1	1	3		5
Gerente de División Comercial			2	1	3
Gerente de División de Administración		1	3	3	7
Gerente de División de Finanzas y Canales			7	4	11
Gerente de División de Negocio	1		8	1	10
Gerente de División de Procesos y TI	1	6	11	12	30
Gerente de Riesgos	1		9		10
Gerente Ejecutivo Adjunto		3	8	1	12
Jefe Dpto. Inspectoría de Fraude		1	2		3
Jefe Órgano de Control Institucional			2		2
Jefe Unidad de Auditoria Interna		4	1		5
Jefe Unidad de Cumplimiento Normativo		1	2		3
Jefe Unidad de Prevención		1	1	1	3
Total general	**5**	**24**	**67**	**26**	**122**

Elaboración propia

Tabla 10 - *Cantidad de Activos de Soporte Consolidad por Custodio*

Custodio	Bajo	Medio	Alto	Muy Alto	Total
Jefe Dpto. Asesoría Jurídica			1		1
Jefe Dpto. Canales de Atención			1		1
Jefe Dpto. Gestión de Desarrollo Humano				1	1
Jefe Dpto. Logística			2		2
Jefe Dpto. Seguridad		5	3		8
Jefe Dpto. Tecnología de Información	5	18	42	23	88
Jefe Dpto. Tesorería			2		2
Oficial de SI y CN			3		3
Por definir		1	13	2	16
Total general	**5**	**24**	**67**	**26**	**122**

Elaboración propia

En la Tabla 10 se puede observar que el Jefe de Departamento de TI es el Custodio de la mayor cantidad de Activos de Soportes Consolidados, debido a que las diferentes unidades organizacionales hacen uso de diferentes medios tecnológicos (carpetas compartidas locales, buzón de correo) para almacenar información de mucho valor.

V.1.5. Análisis del Sistema de Gestión de Seguridad de la Información

Como parte del proceso de entendimiento de la organización, se hace necesario conocer la efectividad de los controles existentes que forman parte del Sistema de Gestión de Seguridad de la Información, por esta razón, fueron sometidos a una evaluación preliminar comparando objetivos de control y controles de referencia propuestos en el Anexo A de la NTP-ISO/EIC27001:2014, los resultados los mostramos en la tabla 11.

Tabla 11 - Resultado de evaluación de controles existentes con los requerimientos de la ISO27001

Cumplimiento	Controles	Porcentaje	Comentario
Satisfactoriamente	21	17.36	
Parcialmente	90	74.38	Requiere de: • Modificación de manuales de gestión • Mejor y/o implementación de controles • Generación, análisis y almacenamiento de evidencias de control
No Cumple	10	8.26	Requiere de: • Creación de procedimientos en manuales • Implementación de controles • Generación, análisis y almacenamiento de evidencias de control
	121	100.00	

Elaboración propia

Como se evidencia los resultados de la evaluación, se hace necesario la optimización del Sistema de Gestión de Seguridad de la Información en la entidad financiera regional del Perú para alinearlo a la NTP-ISO/EIC27001:2014.

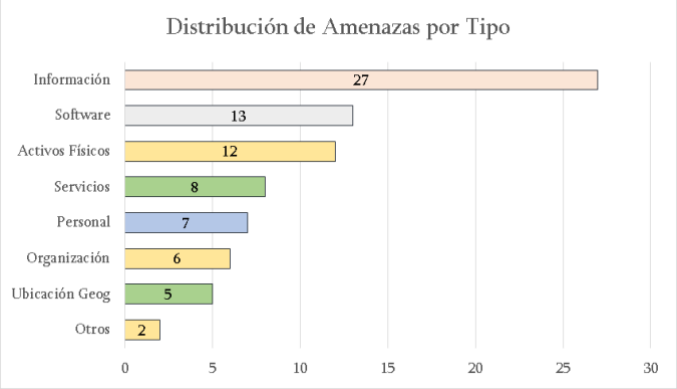
V.2. Riesgos de Seguridad de la información

En la etapa de análisis de riesgos de seguridad de la información se identificaron y evaluaron los riesgos potenciales en base de las amenazas y vulnerabilidades, se identificaron y evaluaron los controles y se determinó el riesgo residual.

V.2.1. Identificar Amenazas y Vulnerabilidades

Se identificaron las principales amenazas que tienen el potencial de dañar el activo de soporte. Las 80 amenazas identificadas se catalogaron en 8 tipos, como son amenazas a la información, al software, y personas, entre otros, tal como muestra la Figura 12.

Figura 12 - Distribución de Amenazas por Tipo

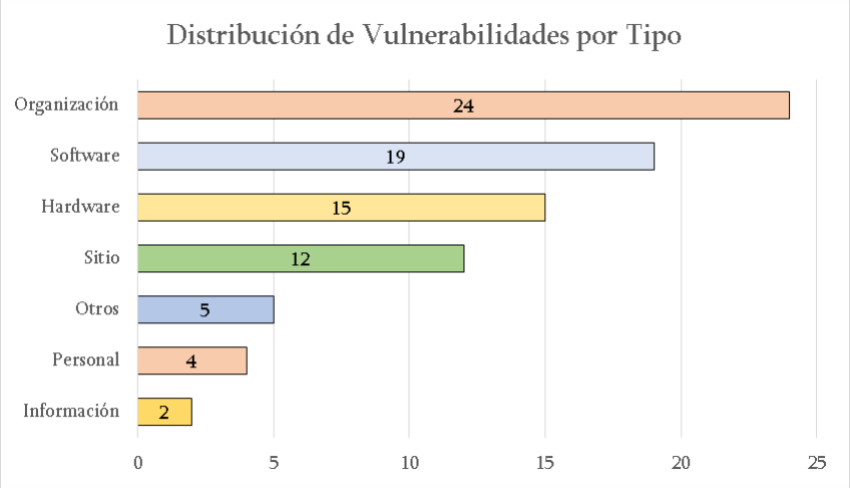


Elaboración propia

La categoría Información es la que tiene mayor cantidad incidencias con 27 de amenaza, entre las que destacan Ataques Informáticos, Robo de información sensible y Gestión errónea de la información, entre otras.

Asimismo, se identificaron un total de 81 vulnerabilidades, de las cuales 24 (30%) son del tipo organización, en donde se presentan con mayor incidencia la Falta o insuficiencia en el acuerdo de nivel del servicio, Falta de procedimientos para el manejo de información clasificada, deficiencia en los acuerdos de confidencialidad y manejo de información sensible, carencia de mecanismos de monitoreo, entre otros.

Figura 13 - Distribución de Amenazas por Tipo



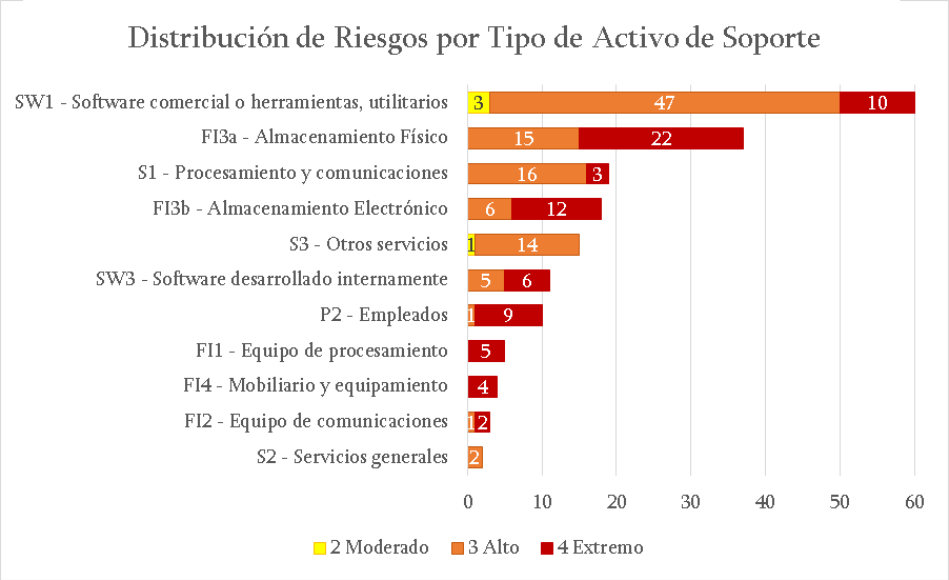
Elaboración propia

V.2.2. Identificar Riesgos de Seguridad de Información

Con cada par de amenaza y vulnerabilidad identificada para un activo de soporte, se procedió a identificar y describir cada riesgo de seguridad de información que tiene la capacidad de afectar la integridad, confidencialidad y disponibilidad del activo de soporte consolidado.

Se identificaron un total de 184 riesgos para los 67 activos de soporte consolidados analizados; en la Figura 13 se puede ver la distribución de riesgos identificados para un tipo de activo de soporte y el nivel que posee cada riesgo.

Figura 14 - Distribución de Riesgos por Tipo de Activo de Soporte

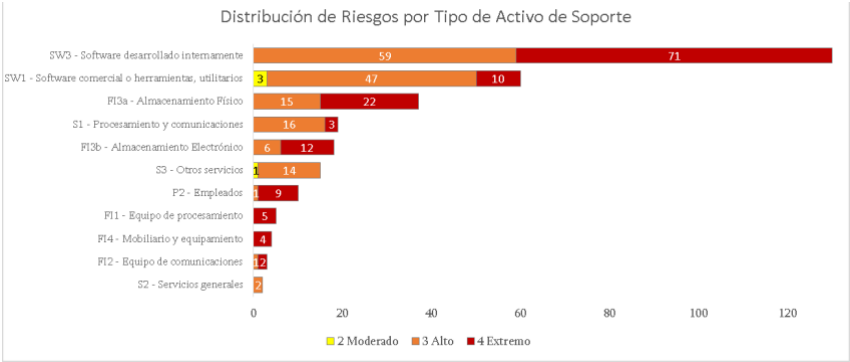


Elaboración propia

En la Figura 13 se puede observar que el 33% de los riesgos (60 de 184) es del tipo software de terceros (SW1), esta situación es consistente con el hecho de que los activos de soporte de la categoría software de tercero (SW1) son el 26% (18 de 69) de los activos.

Esta situación se debe a que las aplicaciones y los módulos desarrollados de manera interna se tuvieron que consolidar en una sola, la cual fue “SIFC”, debido a que no se contó con la arquitectura detallada de cada módulo que forma parte del SIFC; y esto originó que se definieran riesgos de manera general, caso contrario el número de riesgos definidos para este tipo de software (software desarrollado internamente) hubiese sido mayor a 130 riesgos, debido a que cada módulo del SIFC tiene funcionalidades distintas y por ende riesgos definidos, esto lo puedes se puede ver en la Figura 15.

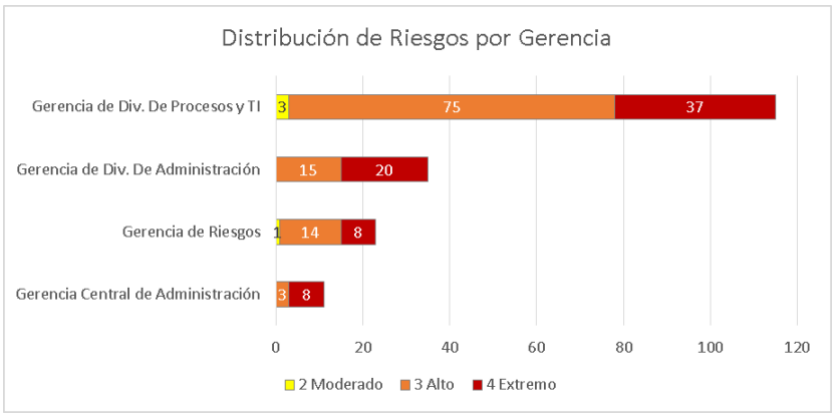
Figura 15 - Distribución de Riesgos por Tipo de Activo de Soporte - Extendido



Elaboración propia

Para cada riesgo, se identificó un propietario, quien tendrá la responsabilidad y autoridad para gestionar el riesgo; en la Figura 15 se muestra un gráfico de barras con la distribución de riesgos por Gerencias propietarias y el nivel de riesgo.

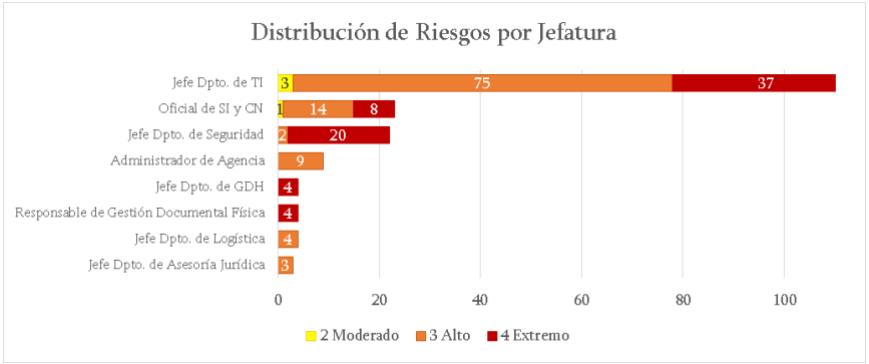
Figura 16 - Distribución de Riesgos por Gerencia



Elaboración propia

En la Figura 16 se puede observar que se identificaron 4 riesgos de nivel extremo, sobre los cuales no se ha identificado un propietario formal con responsabilidades asignadas, estos riesgos corresponden al Activo de Soporte Consolidado “Archivadores”.

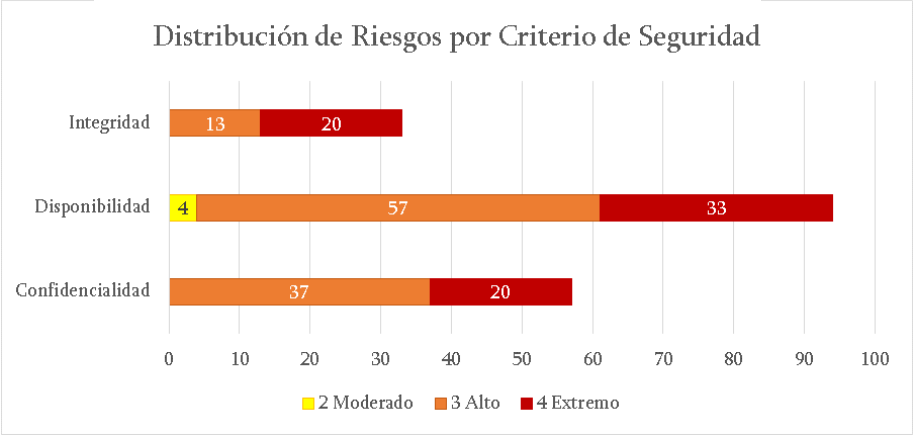
Figura 17 - Distribución de Riesgos por Jefatura



Elaboración propia

En la Figura 17 se muestra un gráfico con la distribución de riesgos sobre las dimensiones de la seguridad de la información como son confidencialidad, disponibilidad o integridad.

Figura 18 - Distribución de Riesgos por criterio



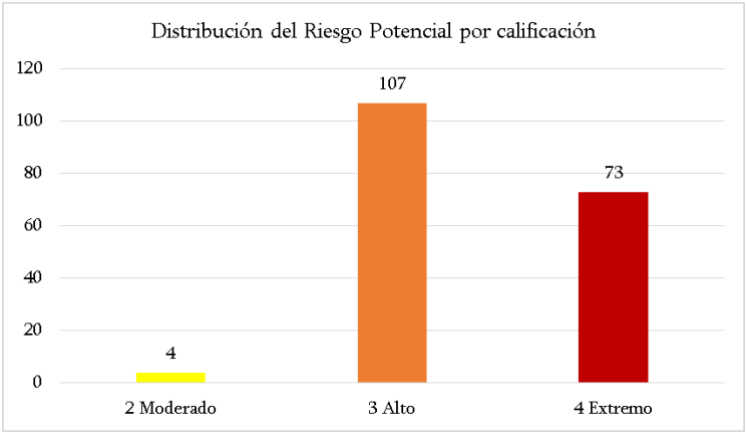
Elaboración propia

En la distribución de los riesgos de la Figura 18 se observa un gran sesgo hacia la identificación de riesgos que centran en la disponibilidad de los activos de soporte. Este sesgo deber ser corregido buscando identificar riegos que afectan a la integridad y la confidencialidad de los activos.

Junto con la identificación de cada uno de los 184 riesgos se procedió a estimar el nivel de riesgo potencial, sobre la base de la frecuencia en que se puede manifestar la amenaza y vulnerabilidad y la severidad del impacto que fue relaciona del valor del activo, tal cual lo definen los lineamientos del Manual de Gestión del SGSI.

En la Figura 19 se observa cómo en la distribución del nivel de riesgo potencial de los 184 riesgos, solo el 2% es “2 Moderado” (4), mientras que el 98% de los riesgos identificados se encuentran con un nivel de riego potencial de “3 Alto” (107) o “4 Extremo” (73) debido principalmente al nivel de tasación del activo de soporte.

Figura 19 - Distribución del Riesgos Potencial por calificación



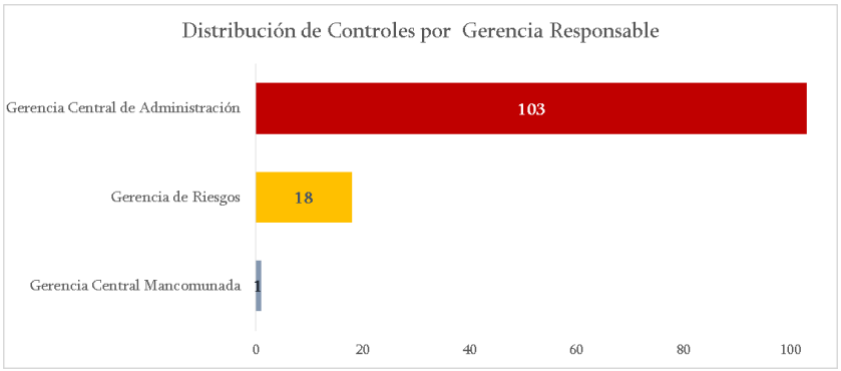
Elaboración propia

V.2.3. Identificar y Evaluar Controles

Para cada uno de 184 riesgos identificados, se procedió a identificar 122 controles existentes o planificados que permiten gestionar el riesgo. Se definió un código único, nombre, descripción, responsable del control, y una referencia a uno más controles ISO.

En la Figura 20 se muestra un gráfico de barras con la distribución de los controles por responsable a nivel de Gerencia Central, en donde se observa que la Gerencia Central de Administración es responsable del 84% de los controles (103 controles del total).

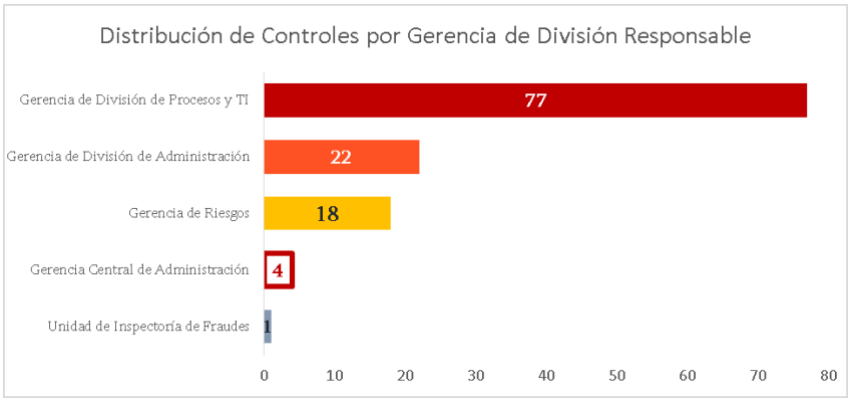
Figura 20 - Distribución de Controles por Responsable de Ejecución - Gerencia Central



Elaboración propia

En la Figura 21 se muestra un gráfico de barras con la distribución de los controles por responsable a nivel de Gerencia de División, en donde se observa que la Gerencia de División de Procesos y TI es responsable del 63% de los controles (77 controles del total).

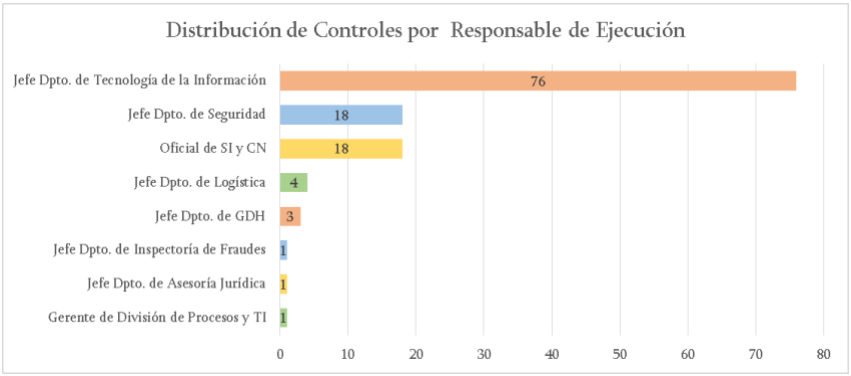
Figura 21 - Distribución de Controles por Responsable de Ejecución – Gerencia de División



Elaboración propia

En la Figura 22 se muestra un gráfico de barras con la distribución de los controles por responsable a nivel de Jefaturas, en donde se observa Jefe de Departamento de Tecnología de la Información es el responsable del 62% de los controles (76 controles del total).

Figura 22 - Distribución de Controles por Responsable de Ejecución – Jefaturas

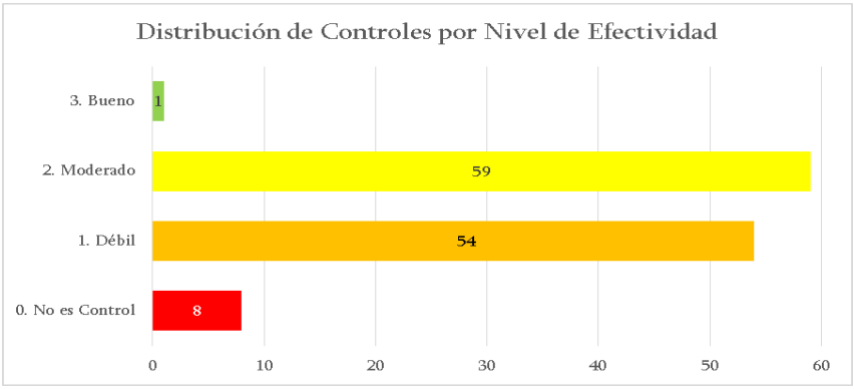


Elaboración propia

Luego de identificado el control, esté de manera individual fue evaluado calificando y registrando criterios de diseño y ejecución obteniendo un valor del control. Luego de la evaluación individual se le asignó un peso a cada control asociado al riesgo y se evaluó la efectividad de los controles en conjunto.

En la Figura 23 se muestra una gráfica de barras con el nivel de efectividad individual de los 122 controles, en donde se observa que el 51% (62 de 122) de los controles son débiles o no son controles y requieren un rediseño del control. Asimismo, que el 48% (59 de 122) son moderados y requieren mejora.

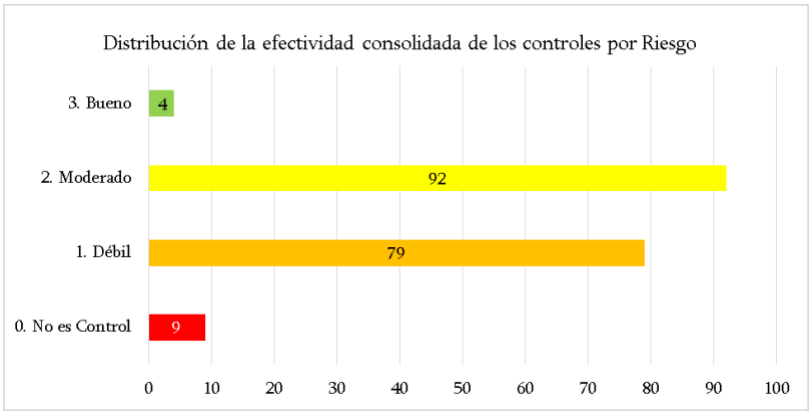
Figura 23 - Distribución de Controles por nivel de efectividad



Elaboración propia

En la Figura 23 se muestra una gráfica de barras con el nivel de efectividad grupal de los controles para los 184 riesgos, en donde se observa que el 48% (79 controles débiles más 9 que no son controles del total) necesitando una optimización del control para que funcionen apropiadamente. Asimismo, que el 50% (92 de 184) son moderados y requieren mejora. El nivel de efectividad de los controles evaluados de manera individual y grupal para un riesgo es similar, en ambos casos requieren rediseño del control y mejora.

Figura 24 - Distribución de la efectividad consolidada de los controles por Riesgo



Elaboración propia

Una de las principales debilidades que se observa en los controles identificados, es que los mecanismos tecnológicos que pueden ser calificados como moderados o buenos tienen limitaciones en el diseño, al no tener procedimientos documentados que definan claramente los responsables del control, la frecuencia de ejecución, y los registros que se deben generar. Esta limitación de diseño conlleva a las deficiencias de ejecución en la oportunidad al no tener definida la frecuencia y trazabilidad al no tener un procedimiento que defina los registros del control.

V.3. Mejoras del Sistema de Gestión de Seguridad de la Información

Para el proceso de optimización del sistema de Gestión de Seguridad de la Información se tiene que elegir una metodología estructurada para gestionar el proyecto que permita cubrir todos los requisitos mínimos para la implementación del sistema de gestión.

En la figura 25 se propone los pasos a seguir para gestionar la Implementación de un Sistema de Gestión de Seguridad, los pasos a seguir se adaptan al alcance, requerimientos, tamaño y complejidad de la organización.

Figura 25 - Marco Metodológico para Gestionar el Proyecto de Implementación del SGSI

Fuente ISO 27001

Siendo una decisión estratégica la optimización del Sistema de Gestión de Seguridad de la Información, se gestiona como proyecto con los siguientes parámetros:

V.3.1. Requerimientos

El nuevo Sistema de Gestión de Seguridad de la Información debe cumplir los requerimientos normativos de los siguientes supervisores:

- Superintendencia de Banca, Seguros y AFPs
- Banco Central de Reserva del Perú
- Superintendencia del Mercado de Valores
- Ministerio de Justicia
- Levantar observaciones de auditorías internas, externas y organismos supervisores.

Alinearse, en forma voluntaria, a las siguientes normas ISO:

- ISO27001: Sistemas de Gestión de Seguridad de la Información. Requisitos.

- ISO27002: Código de prácticas para controles de seguridad de la información.
- ISO27003; Gestión de riesgos de la seguridad de la información. Implementación.
- ISO27005: Gestión de riesgos de la seguridad de la información.

V.3.2. Involucrados

Se crean los siguientes equipos de trabajo para la implementación de las mejoras y sus respectivas responsabilidades:

- Directorio
  - Asegura que la entidad cuente con un Sistema de Gestión de Seguridad de la información de acuerdo a su tamaño y complejidad.
  - Aprobar la política de seguridad de la información, alcance y lineamientos generales que orientan la gestión de seguridad de la información
  - Asegurar los recursos necesarios para el mantenimiento del sistema de gestión de seguridad de la información
- Comité de riesgos
  - Asistir técnicamente al Directorio para proveer de un marco normativo apropiado para el Sistema de Gestión de Seguridad de la Información.
  - Aprobar las políticas, alcance, estructura organizacional, manuales y metodología del SGSI
  - Aprobar el plan anual de operación, capacitación, concientización e implementación de controles del SGSI,
  - Aprobar los recursos necesarios para mantener el SGSI
  - Evaluar los indicadores de gestión de seguridad de la información y los informes de avance de las actividades planificadas.
  - Informar periódicamente al Directorio respecto a la Gestión de Seguridad de la Información.
- Gerencia General
  - Implementar la gestión de seguridad de la información conforme a las disposiciones del Comité de Riesgos y del Directorio.
  - Asegurar el cumplimiento de las políticas y procedimientos del Sistema de Gestión de Seguridad de la Información.
  - Asegurar el uso racional de los recursos económicos, logísticos y humanos que soportan el Sistema de Gestión de Seguridad de la Información.
- Gerencia de Riesgos
  - Liderar el desarrollo e implementación del Sistema de Gestión de Seguridad de la Información en la organización.

- Proponer las políticas generales del SGSI al comité de riesgo operacional, así como verificar el cumplimiento de las mismas.
- Asegurar que el SGSI se realice de manera consistente de acuerdo a las políticas y procedimiento establecidos para la gestión de riesgos de Seguridad de la Información.
- Dirigir la implementación y desarrollo de la estructura organizacional de la Oficialía de Seguridad de la Información y Continuidad de la entidad, como un componente de la administración del riesgo operacional en la organización.
- Asegurar la suficiencia de los recursos, sistemas e información para proveer un SGSI apropiado para el tamaño y complejidad de la organización.
- Administrar la suficiencia de los recursos, sistemas e información para proveer un SGSI apropiado para el tamaño y complejidad de la institución.
- Aprobar el plan de capacitación de la Oficialía de Seguridad de la Información y Continuidad del Negocio y el plan de capacitación y concientización de la Institución en su conjunto.
- Informar al Comité de Riesgos el grado de exposición al riesgo de Seguridad de la Información de acuerdo a las políticas y procedimientos establecidos.
- Evaluar situaciones de riesgos de Seguridad de la Información e informar a los Comités respectivos.

- Comité de Riesgo Operacional

  - Asistir al Comité de Riesgos en la revisión y validación técnica de las políticas, organización, metodología, planificación anual, procedimientos de control y mejora del SGSI y proponer para su aprobación.
  - Revisar y proponer las políticas, alcance, estructura organizacional, manuales y metodología del SGSI.
  - Revisar y aprobar el plan de operación y el plan de capacitación y concientización y plan de implementación de controles del SGSI.
  - Revisar y proponer informes de resultados del: inventario, clasificación y valoración de activos, análisis de riesgo y tratamiento de riesgos.
  - Revisar y proponer las estrategias de la institución con respecto a la implementación de normas y estándares internacionales referidos a la Seguridad de la Información.
  - Proveer los recursos necesarios para implementar las acciones correctivas decididas por el Comité de Riesgos para atender y subsanar las observaciones formuladas referidas a la gestión de Seguridad de la Información.
  - Validar los resultados de indicadores de desempeño del SGSI.

- Asegurar la comunicación al personal sobre la Política y Objetivos de Seguridad de la Información, la importancia de su cumplimiento, así como sus responsabilidades de acuerdo a Ley y la necesidad de una mejora continua.
- Monitorear y controlar las implementaciones de los controles de Seguridad de la Información y el estado del SGSI, reportando periódicamente al Comité de Riesgos el desempeño obtenido.
- Revisar los informes de avance de ejecución de planes de capacitación y desempeño y proponer acciones correctivas.
- Revisar las implementaciones de las acciones correctivas y mejora continua en la metodología, planificación y procedimientos del SGSI.

- Oficial de Seguridad de la Información

  - Establecer y mantener un mecanismo de monitoreo de los controles implementados para asegurar el nivel suficiente de protección para los datos personales para el cumplimiento de la normatividad aplicable.
  - Elaborar y proponer las políticas de Seguridad de la Información, alcance, manuales, procedimientos y metodología, apropiadas para el SGSI, para su revisión en el Comité de Riesgo Operacional.
  - Elaborar y proponer estructura de roles y responsabilidades del SGSI, para su revisión en el Comité de Riesgo Operacional.
  - Administrar eficientemente las actividades de los colaboradores y los recursos asignados a la Oficialía de Seguridad de la Información y Continuidad del Negocio.
  - Establecer y mantener un mecanismo de monitoreo para garantizar la creación, actualización y control de la información documentada, determinada como necesaria por la organización para la efectividad del SGSI.
  - Elaborar el plan anual de Seguridad de la Información, plan de capacitación y concientización y plan de aseguramiento de implementación de controles del SGSI.
  - Monitorear el cumplimiento del plan anual de Seguridad de la Información, plan de capacitación y concientización, plan de aseguramiento de implementación de controles del SGSI y reportar el avance al Comité de Riesgo Operacional.
  - Asegurar razonablemente la implementación del SGSI conforme a las políticas de Seguridad de la Información aprobadas por el Directorio y/o Comité de Riesgo para proteger la integridad, disponibilidad y confidencialidad de los activos de información.

- Diseñar y elaborar una metodología para la implementación del SGSI considerando la evaluación de riesgo de Seguridad de la Información y tratamiento de riesgo de Seguridad de la Información.
- Desplegar la metodología y asistir como asesor metodológico de las Gerencias y Jefaturas de Departamentos de la organización.
- Asistir metodológicamente a las jefaturas de los departamentos en la elaboración del inventario, clasificación y valoración de los activos de información, análisis de riesgo, tratamiento del riesgo y controles adecuados.
- Monitorear la implementación y funcionamiento de los controles conforme a la metodología aprobada en el SGSI e informar el desempeño al Comité de Riesgos Operacional.
- Asegurar la difusión y desarrollo cultural de la Seguridad de la Información, velando por cubrir las necesidades de capacitación, difusión y sensibilización en Seguridad de la Información en coordinación con los distintos departamentos.
- Asegurar la consistencia y coherencia de los resultados obtenidos de la aplicación de la metodología en la Institución.
- Monitorear e informar el avance del despliegue de la metodología según planes anuales de operación para la Gerencia de Riesgo y el Comité de Riesgo Operacional, alertando cualquier desviación importante para la toma de acciones correctivas
- Monitorear y asegurar los planes de acción de Seguridad de la Información en coordinación con las diferentes áreas a fin de mitigar los riesgos de seguridad dentro de los niveles aceptados por la organización.
- Realizar en forma periódica el diagnóstico y evaluación de vulnerabilidades técnicas de los sistemas de información y plataformas informáticas, asegurando la implementación de mecanismos de monitoreo y registros de auditoría.

- Gerencia de TI

  - Administrar las soluciones y plataformas de seguridad interna y externa en todos los perímetros de la institución, así como la seguridad para protección de información, alojada en los activos de TI. Implementar y administrar el proceso de privilegios y gestión de acceso e identidades de los sistemas de información, servicios informáticos y plataformas tecnológicas.
  - Administrar en los procesos del ciclo de vida de desarrollo de software, adquisiciones, mantenimiento e implementación de sistemas de información, servicios y plataformas tecnológicas con la finalidad de

asegurar el cumplimiento de los estándares de Seguridad de la Información definidos.

- Facilitar la ejecución de servicios de análisis de vulnerabilidades técnicas para los servicios tecnológicos y asegurar el tratamiento de las vulnerabilidades detectadas.
- Velar por la operatividad y seguridad física de acceso al centro de datos principal y/o contingencia.
- Coordinar con la Oficialía de Seguridad de la Información y Continuidad del Negocio charlas de concientización al personal sobre aspectos de desarrollo seguro.
- Gestionar los riesgos e incidentes de seguridad informática.
- Administrar los procedimientos, controles y llaves vinculados a los dispositivos de criptografía.
- Asegurar la integridad, coherencia y veracidad de la información utilizada para el análisis de riesgos, garantizando la calidad de los resultados de la evaluación de riesgos y valoración de riesgos, tratamiento de riesgos y selección de controles, utilizando la metodología del SGSI.
- Asegurar la adecuada implementación de los controles de Seguridad de la Información, a fin de cumplir con los requerimientos.
- Cumplir con las responsabilidades descritas en las Jefaturas de Departamento.

- Gerencia de Recursos Humano

  - Verificar los antecedentes de todos los candidatos a ser empleados en concordancia con las leyes y regulaciones y ética relevantes, y ser proporcional a los requisitos de la institución, la clasificación de la información a la que se tendrá acceso y los riesgos percibidos.
  - Verificar los acuerdos contractuales con los empleados y personal temporal, contratados por la organización, deben estipular responsabilidades de éstos y de la organización respecto a la Seguridad de la Información.
  - Garantizar que desde el inicio laboral todos los colaboradores entiendan sus responsabilidades y sean idóneos en los roles para los cuales son considerados.
  - Requerir a todos los empleados y personal temporal, contratados por la organización, aplicar la Seguridad de la Información en concordancia con las políticas y procedimientos establecidos por la institución.
  - Garantizar que la inducción a los nuevos colaboradores incluya temas de Seguridad de la Información.

- Garantizar un proceso disciplinario formal y comunicado para tomar acción contra empleados que hayan cometido una infracción a la Seguridad de la Información.
- Ejecutar los procesos disciplinarios en caso de incumplimiento de las políticas de Seguridad de la Información, en conformidad con la legislación laboral vigente.
- Implementar y mantener los controles para el cumplimiento de los requerimientos regulatorios relacionados con la Seguridad de la Información y el personal.
- Asegurar los recursos necesarios a fin de desplegar los programas anuales de capacitación y concientización en Seguridad de la Información.
- Coordinar con la Oficialía de Seguridad de la Información y Continuidad del Negocio la ejecución del programa anual de capacitación y concientización en Seguridad de la Información.
- Reportar al Comité de Riesgos el cumplimiento de los controles de Seguridad de la Información relacionado a la seguridad de los recursos humanos.
- Asegurar que las políticas y procedimientos de desvinculación de personal incorpore la entrega de activos de información, claves y otros otorgados al colaborador.

- Jefe de Seguridad

  - Garantiza mecanismos de control de acceso y protecciones físicas y ambientales apropiadas para prevenir el daño o pérdida de los activos de información, a fin de prevenir el acceso no autorizado, daño, e interferencia, eventos o causas de índole ambiental que afecten negativamente los activos de la información e instalaciones de procesamiento de la organización. Liderar en la ejecución de control de acceso físico a las instalaciones de la institución.
  - Cumplir con las responsabilidades descritas en las Jefaturas de Departamentos.

- Jefes de departamento

  - Asegurar el cumplimiento de las políticas de Seguridad de la Información para promover el buen uso, funcionamiento y protección de los activos de información a su cargo a fin de que cumpla con los objetivos de la organización.
  - Garantizar la participación del personal de su departamento en el plan anual de capacitación y concientización del SGSI.
  - Liderar la participación de su personal en las actividades del análisis de riesgo y evaluación del riesgo.

- Asegurar la protección de los activos de información mediante controles para salvaguardar los activos de información a su cargo
- Participar activamente en la difusión de la cultura de Seguridad de la Información en coordinación con la Oficialía de Seguridad de la Información.
- Aplicar la metodología de Seguridad de la Información, para el inventario y clasificación de los activos de información, de acuerdo a la política.
- Garantizar la identificación de las amenazas, vulnerabilidades y controles, a fin de identificar el riesgo.
- Administrar los riesgos de su competencia, a través de la identificación, tratamiento y control de los mismos, relacionados al logro de los objetivos de la dependencia a su cargo, dentro de las políticas establecidos por el Comité de Riesgo Operacional.
- Garantizar a implementación de las acciones correctivas y mejora continua del SGSI dentro de su departamento.
- Colaborar y disponer de su tiempo para atender las consultas o reuniones solicitadas por la Oficialía de Seguridad de la Información.

- Personal de la organización

  - Independiente de la modalidad de contrato, el personal de la organización tiene la responsabilidad de cumplir y hacer cumplir al personal a su cargo, a los proveedores de servicios y a los terceros con quienes coordina, las políticas de Seguridad de la Información que apliquen de la presente directiva, garantizando el correcto uso de la información exclusivamente para fines laborales.
  - Asegurar la entrega de conocimientos, información y datos confiables, actualizados y consistentes como insumo para las actividades de evaluación de riesgos y tratamiento de riesgos de Seguridad de la Información.
  - Reportar cualquier evento, vulnerabilidad o debilidad que se observe o sospeche a través de los canales adecuados de gestión de incidentes de información física y/o tecnológica.
  - Participar activamente en los eventos del programa de capacitación y concientización en Seguridad de la Información.
  - Mantener la confidencialidad, disponibilidad e integridad de la información en cualquiera de sus formas (física y electrónica) de la Organización.

- Unidad de Auditoría

  - Realizar anualmente un proceso de auditoría independiente al SGSI con la finalidad de comprobar que las políticas y procedimientos están siendo realizados eficazmente.

- Auditar la vigencia de los planes de Seguridad de la Información y recursos asignados para cada área.
- Asegurar que la sociedad auditora externa incluya en su revisión independiente la validación del cumplimiento de las políticas, procedimientos y metodología de la organización.

V.3.3. Gestión de documentos

El Sistema de Gestión de Seguridad de la Información debe tener un sistema interno de gestión de documentos que lo conforman, que cumpla los requerimientos del departamento de procesos de la organización y los requisitos de la ISO27001.

Los objetivos principales de la gestión de documentos son los siguientes:

- Desarrollar y mantener la documentación necesaria para garantizar un sistema eficaz de gestión adaptado a las necesidades específicas de la organización.
- Garantizar el control y la adecuación de la documentación del SGSI
- Garantizar el control y la adecuación de los registros del SGSI

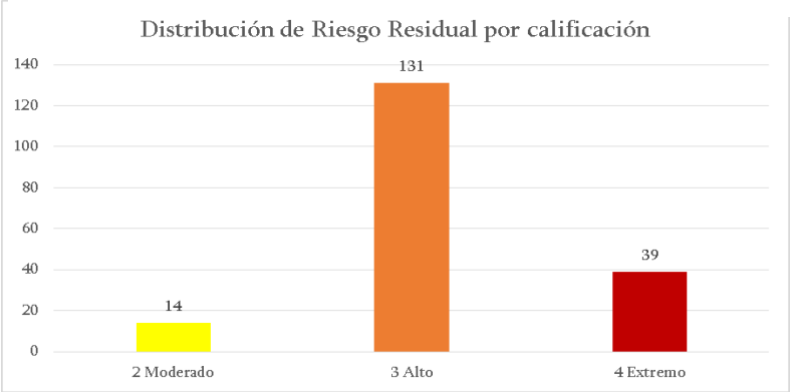
Los documentos que han sido seleccionados inicialmente para la optimización del Sistema de Gestión de Seguridad de Información son los siguientes:

- Manual de Gestión de Seguridad de la Información
- Planificación y control operativo
- Informes de seguimiento y resultado de mediciones
- Informes de Procedimientos internos de auditoría y control de auditoría.
- Resultados de revisión por la Dirección
- Informes de No conformidades, acciones correctivas y resultados
- Presupuesto de funcionamiento del SGSI
- Plan de concientización y capacitación del SGSI

V.3.4. Evaluar Riesgo Residual

En la Figura 26 se observa cómo 170 (92%) de los riesgos analizados se encuentran con un nivel de riego residual “4 Extremo” (39) y “3 Alto (131)”, debido principalmente al grado de efectividad de los controles antes expuestos, permitiendo disminuir el daño potencial de los riesgos sólo en un 6% de los casos identificados, encontrándose fuera del apetito de riesgos de la entidad financiera regional, siendo inaceptables y por lo tanto requieren tratamiento adicional.

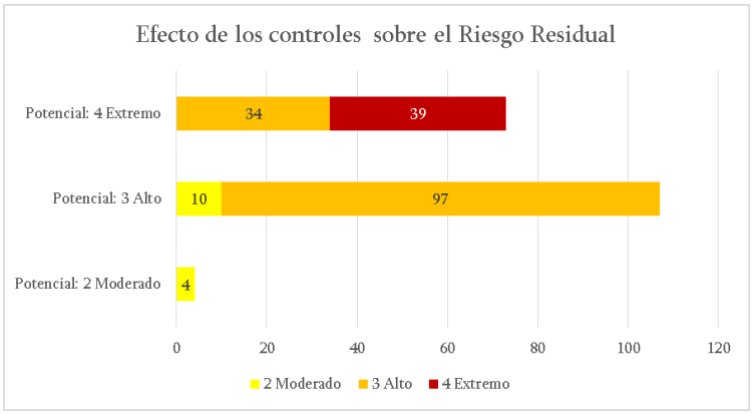
Figura 26 - Distribución de Riesgo Residual por calificación



Elaboración propia

En la Figura 27 se muestra el efecto de los controles sobre el riego residual, en la barra superior con la etiqueta "Potencial: 4 Extremo" que representa a los 73 riesgos potenciales con nivel "4 Extremo", se observa que 34 de ellos disminuyen a un nivel "3 Alto" por la efectividad de sus controles, mientras que 39 permanecen sin cambio (controles débiles). Asimismo, para los 107 riesgos potenciales con nivel "3 Alto", solo 10 de ellos disminuyen a un nivel "2 Moderado" por la efectividad de sus controles, mientras que 97 permanecen sin cambio (controles débiles).

Figura 27 - Efecto de los controles sobre el riesgo Residual



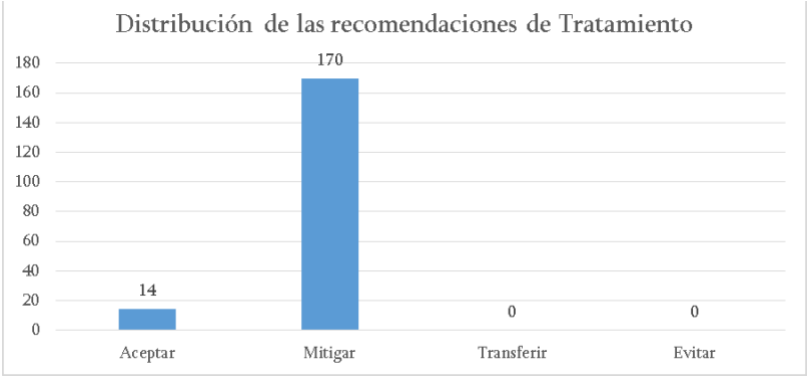
Elaboración propia

V.3.5. Tratamiento de Riesgo

Una vez efectuada la evaluación del riesgo y obtenido el nivel de riesgo residual, se definió una opción de tratamiento para cada uno de los 170 riesgos con nivel "3 Alto" (131) o "4 Extremo" (39), conforme a lo señalado en la Políticas de gestión de riesgos de seguridad de la información. Las opciones fueron para aceptar, mitigar, transferir o evitar el riesgo.

En la Figura 28 se observa la aplicación de las opciones de tratamiento, aceptando los 14 riesgos con nivel "2 Moderado" y mitigando 170 riesgos con nivel "3 Alto" o "4 Extremo", no tomaron las opciones de transferir o evitar el riesgo.

Figura 28 - Distribución de las recomendaciones de Tratamiento



Elaboración propia

V.3.6. Propuesta de Controles

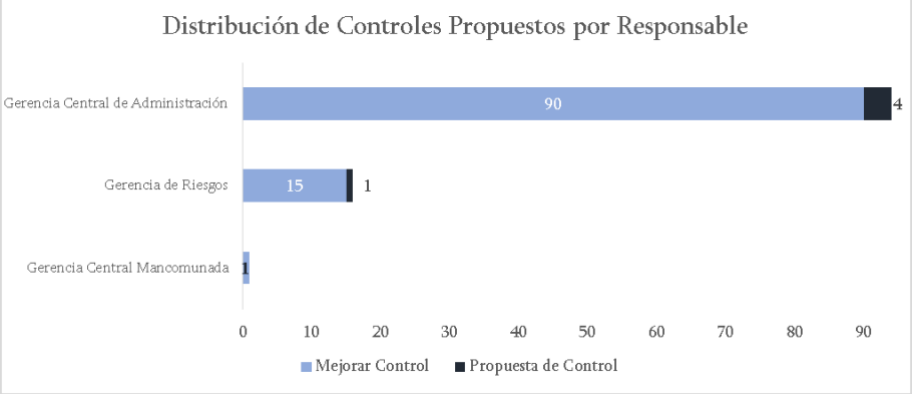
Para cada uno de los 170 riesgos residuales que requieren ser tratados a través de la mitigación, durante los talleres con los especialistas participantes se identificaron 106 controles existentes que requieren mejorar para mitigar efectivamente los riesgos, y la necesidad de 5 controles nuevos para lograr el grado de mitigación de acorde a las políticas de la entidad financiera regional. Estos controles son necesarios, a fin de lograr cerrar la brecha de exposición al riesgo inaceptable de acuerdo con sus políticas.

De acuerdo con la metodología, la información fue registrada utilizando el formato SGSI-FO-03, en el cual se registró el código de control (C) / Propuesta de control (PC), nombre de control, descripción del control, referencia del control del Anexo A de ISO 27001, y responsable de implementación del control.

Las propuestas y nuevos controles pueden ser utilizados por uno o más riesgos por lo cual se mantienen 360 registros.

En la figura 28, se presenta un gráfico en donde se aprecian a las distintas Gerencias Centrales que son responsables de implementar las mejoras o los nuevos controles. Aquí se observa que la Gerencia Central de Administración tiene la responsabilidad de implementar el 85% (94 controles del total) de las propuestas de mejora o nuevos controles.

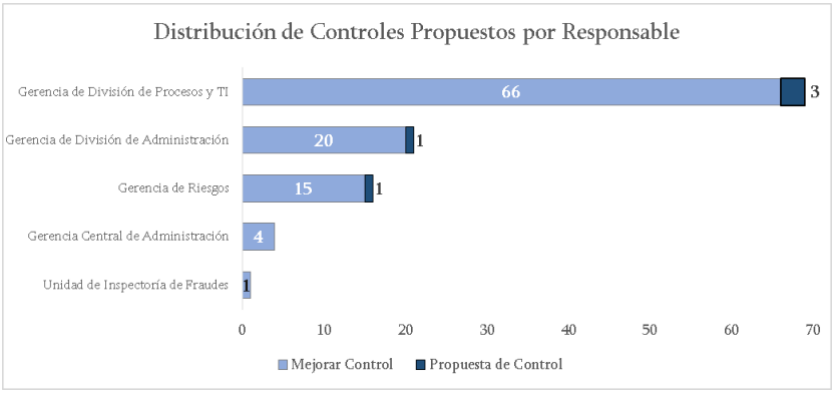
Figura 29 - Distribución de Controles Propuestos por Responsable - Gerencia Central



Elaboración propia

En la Figura 29, se presentan a las distintas gerencias de división que son responsables de implementar las mejoras o los nuevos controles y las cantidades de controles a tratar. A nivel gerencia también se observa que la Gerencia de Procesos y TI destaca al tener la responsabilidad de implementar el 62% (69 de 111) de las propuestas de mejora o nuevos controles.

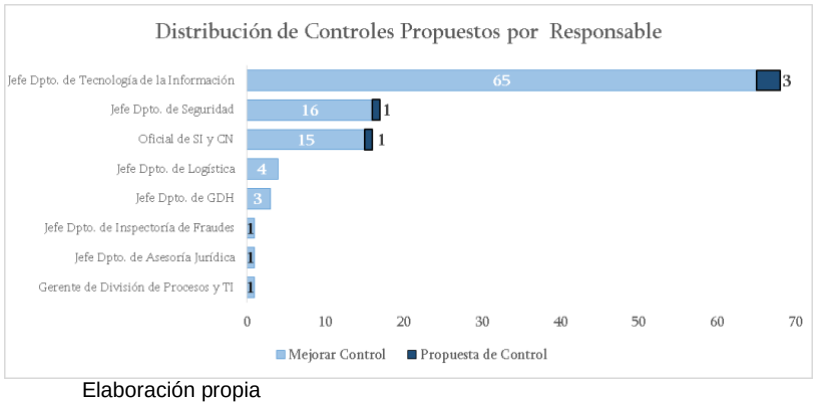
Figura 30 - Distribución de Controles Propuestos por Responsable - Gerencia de División



Elaboración propia

En la Figura 30, se presenta un gráfico en donde se aprecian a las distintas jefaturas departamentales que son responsables de implementar las mejoras o los nuevos controles. Aquí se observa que la Jefatura del departamento de TI tiene la responsabilidad de implementar el 61% (68 de 111) de las propuestas de mejora o nuevos controles.

Figura 31 - Distribución de Controles Propuestos por Responsable - Jefaturas



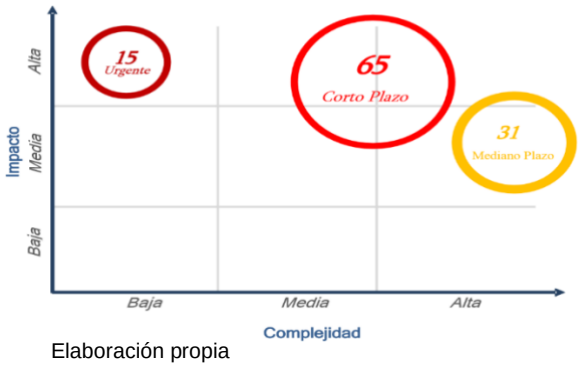
Elaboración propia

V.3.7. Plan de Tratamiento

Sobre la base de la propuesta de controles (formato SGSI-FO-03) se elaboró un listado único de 111 planes de acción para implementar las mejoras necesarias para cerrar las brechas de los distintos riesgos. Los datos de incluidos en el Plan de Tratamiento se registraron utilizando el formato SGSI-FO-04, en donde se definió un código, nombre, descripción, riesgos que mitiga este tratamiento, responsable de implementación, nivel de urgencia de implementación, fecha estimada de inicio y fin de implementación, costo estimado, situación de implementación, y observaciones.

Considerando la cantidad de 111 planes de acción, y con el fin de obtener resultados importantes en un corto plazo, se decidió dividir el nivel de urgencia de corto plazo (2. Corto Plazo) en un nivel adicional denominado “1. Urgente” el cual se asigna a actividades que se estima tienen mayor impacto para gestionar el riesgo y a su vez se estima tienen menor complejidad de implementación, en la práctica se les denomina “Quick Wins” o logros importantes en un periodo corto. El mayor impacto se estima identificado a los riesgos que serán mitigados por el control y sumando un peso asignado a su nivel de riesgo (10 para Extremo, 6 para Alto, 3 para Moderado y 1 para Bajo). En la Figura 31 se puede observar la forma en cómo se encuentran distribuidos los planes de acción de acuerdo con el nivel de urgencia de implementación.

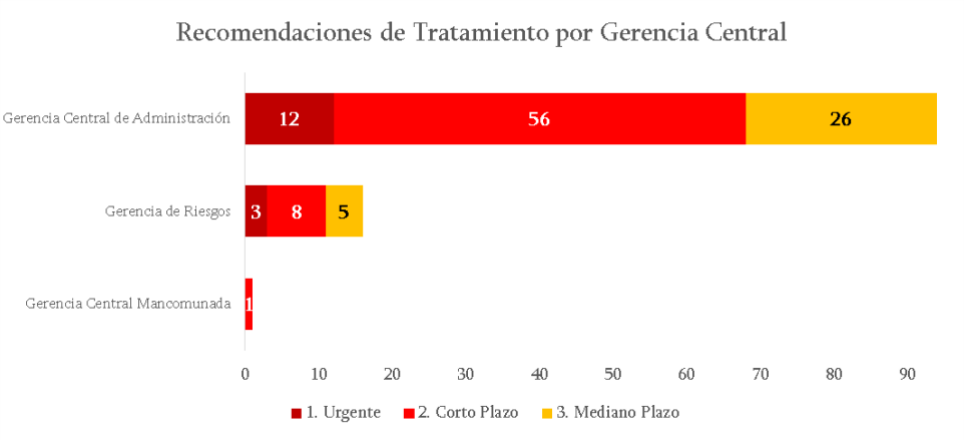
Figura 32 - Distribución de Planes de acción



Elaboración propia

En la figura 33 se observa que la Gerencia Central de Administración, tiene a su cargo la implementación de 94 propuestas de tratamiento. Asimismo, que existen 15 acciones de tratamiento del nivel urgente que se recomienda reciban la prioridad necesaria.

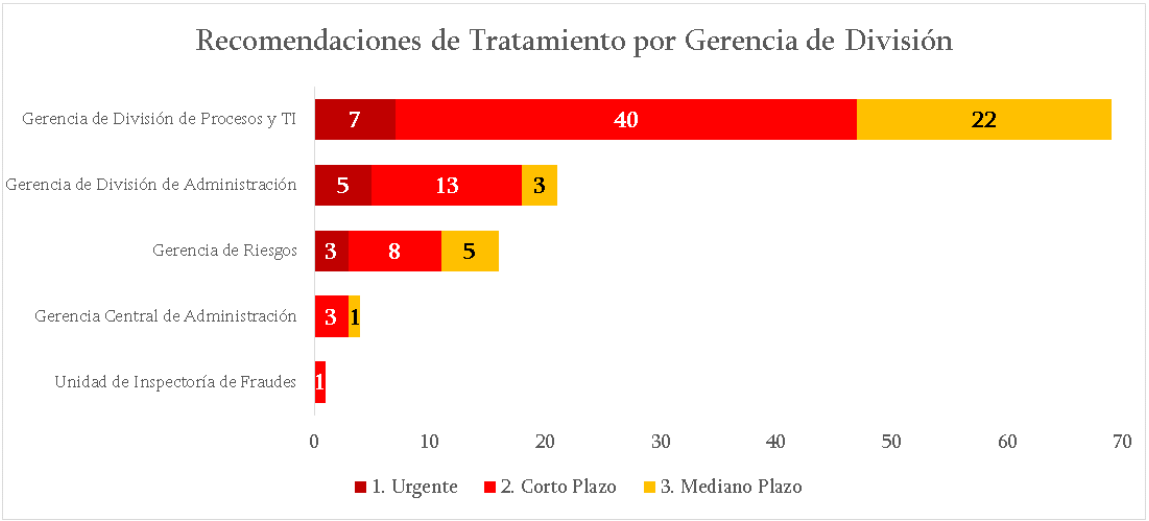
Figura 33 - Recomendaciones de Tratamiento por Gerencia Central



Elaboración propia

En la Figura 33 se observa que la Gerencia de División de Procesos y TI, tiene a su cargo la implementación de 69 propuestas de tratamiento. Asimismo, que existen 7 acciones de tratamiento del nivel urgente que se recomienda reciban la prioridad necesaria.

Figura 34 - Recomendaciones de Tratamiento por Gerencia de División

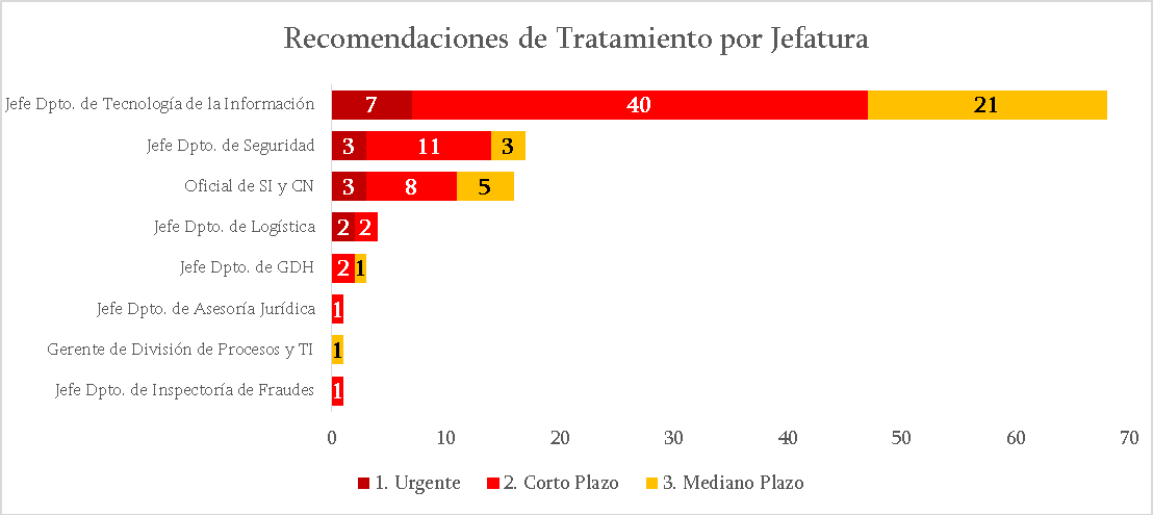


Elaboración propia

En la Figura 35 se observa que el jefe del Departamento de Tecnología de la Información tiene a su cargo la implementación de 68 propuestas de tratamiento.

Asimismo, que existen 7 acciones de tratamiento del nivel urgente que se recomienda reciban la prioridad necesaria.

Figura 35 - Recomendaciones de Tratamiento por Jefatura



Elaboración propia

VI. DISCUSIÓN

En los resultados obtenidos de la investigación se evidenció e identificó un total de 122 activos consolidados, consolidados en un grupo de 67 activos de Información – ASC, en la que se demuestra el uso excesivo de carpetas de red, disco duro, equipo locales, documentos físicos y archivadores dando pie a identificar la raíz de la situación problemática tal como se evidencia en la investigación de Garcia y Huamani (2019) en la que se tuvo que definir, gestionar y monitorear el uso adecuado y control de la información de manera tangible e intangible para tomar mejores decisiones y reducir los gastos para la entidad financiera, por lo que se debe tener en cuenta que para las organizaciones el uso excesivo de activos de la información de manera tangible no será más que el inicio de una problemática para la gestión de seguridad.

De igual manera Guamán (2015) al realizar el diseño del sistema de gestión de la seguridad de la información, incorpora estándares internacionales que se ajustan al rubro de su organización con la intención de implementar de manera eficaz las responsabilidades de seguridad de la información, para evitar debilidades como las presentes en la investigación con respecto a las cintas de Backup, en la que se indican la perdida repentina de datos totales que atenta contra la disponibilidad, siendo al mes alrededor de 30 a 40 eventos documentados de MDB, ya que no existe un personal a cargo de mantener la seguridad de esta data.

En la entidad analizada se observó también la ausencia de operaciones de TI y falta de evidencias de la aplicación de controles en la documentación que son como mínimo exigido para el desarrollo de software, producción comunicación y operación, es por ello que investigaciones como la de Moncada e Israel (2018) que diseñaron un modelo que permite gestionar la seguridad de la información de tal manera que la gestión de los activos incremente en un 22% al presente en la entidad con un enfoque rentable que le dé frente a los riesgos de recursos cumpliendo los planes de seguridad pertinentes.

Molano (2017) identifico que al implementar un sistema de seguridad para la información se debe incluir además un comité que supervise el cumplimiento, funcionamiento y éxito total del sistema, de la misma manera para la presente investigación ya que el alto riesgo de pérdida o deterioro de la información física se debe a la ausencia de un personal responsable formalizado del sistema documental físico presente en la entidad.

Uno de los principales riesgos identificados estaban vinculados a la disponibilidad por encima de los diversos factores existentes claves como la integridad y confidencialidad, cuantificando en un 51% los riesgos asociados a la disponibilidad de la información, causando altas inversiones en herramientas de diversos tipos como enmascaramiento de datos y confidencialidad, para esta problemática Cruz y Fukusaki (2017) implantan un sistema de seguridad de gestión de la información con la intención de lograr la confidencialidad, integridad

y sobre todo disponibilidad de la información, priorizado que cada SGSI esté acorde con el tamaño y madurez de los procesos de la empresa para evitar la aplicación de gastos incensarios en diversos sistemas múltiples.

Por último se determina que se requiere mejorar 106 controles además e implementar 5 controles nuevos para lograr el nivel de mitigación adecuado para el tamaño, complejidad y riesgos de entidad financiera, tal como lo hizo Niño (2018) obteniendo como resultado que la seguridad de la información es un apoyo para la dirección de la organización manteniendo el control de los sistemas, transparencia en los procesos y el uso adecuado de los recursos, colaboradores e información operaria, de esta manera aceptando la hipótesis de su investigación al igual que la presente que optimiza el sistema de gestión de seguridad de la información disminuye los riegos de la seguridad de la información de una entidad.

VII. CONCLUSIONES

El desarrollo de la presente tesis logró determinar de qué manera se debe optimizar el Sistema de Gestión de Seguridad de la Información en una entidad financiera regional del Perú. Esto quedó evidenciado de la siguiente manera:

- Se analizó el sistema de gestión de seguridad de activos, siendo los resultados más relevantes la presencia de un alto sesgo de los colaboradores de la entidad financiera regional por ver los problemas de disponibilidad como único objetivo de la seguridad de la información; evidenciando una tendencia vinculada a la disponibilidad por encima de los otros factores claves como integridad y confidencialidad, por ello el 51% de los riesgos identificados se asocian a la disponibilidad de los activos de información.
- Se Identificó los riesgos potenciales de seguridad de la información en la entidad financiera, considerándose el más relevante los niveles altos con un 71.20% además de las brechas existentes de Seguridad de la Información evaluando la efectividad de los controles existentes teniendo que solo el 50% de ellos son moderados y el 42% débiles.
- Se determinó las mejoras del Sistema de Gestión de Seguridad de la Información en una entidad financiera regional del Perú. La mejora en la cual se hizo énfasis fue seleccionar los controles y objetivos de control, que forman parte del el Sistema de Gestión de Seguridad de la Información con la versión de la norma ISO 27001:2014, correspondientes a las cláusulas de Seguridad Organizacional, Gestión de activos, Seguridad en los recursos humanos, Seguridad física, Gestión de comunicaciones, Control de accesos, etc. Aplicados según la tabla Declaración de aplicabilidad del SGSI, objetivos de control y controles por la que serán mantenidos, ejecutados y auditados bajo la aprobación de la alta dirección de la organización.
- Se concluye que la propuesta de Optimización del Sistema de Gestión de Seguridad de la Información para disminuir los riesgos de la seguridad de la información en una entidad financiera regional del Perú está conformada por solución de gestión de seguridad de activos y su visibilidad, además de selección de controles que se adecuen a los objetivos de la entidad.

VIII. RECOMENDACIONES

1. El Sistema de Gestión de Seguridad de la Información optimizado para la organización alineado a la ISO27001 en una entidad financiera regional del Perú, debe seguir su implementación y mejora continua para asegurar una correcta cuantificación de los riesgos existentes en activos de información para preservar la confidencialidad, integridad y disponibilidad en niveles aceptables por la organización.
2. Documentar los registros, análisis y reportes de gestión generados por el funcionamiento del nuevo Sistema de Gestión de Seguridad de la Información para evidenciar los resultados y proponer las mejoras.
3. Implementar los planes de acción propuestos en la evaluación de riesgos para activos de información para reducir las brechas existentes detectadas con la nueva metodología de identificación y evaluación de riesgos, asimismo, capacitar a los participantes del Sistema de Gestión de Información para que participen con eficiencia en los roles y responsabilidades asignados.
4. Implementar y optimizar los controles de seguridad propuestos para mantener un nivel de protección adecuada a los activos de información generando los registros de evidencia de su operatividad para su próxima evaluación de efectividad y mejora.
5. Los demás sistemas de gestión que cuente la organización como: Continuidad del Negocio y atención al cliente debe alinearse a las ISO para utilizar parte de la estructura organización implementada en la organización.

IX. LISTA DE REFERENCIAS

Bermúdez, K & Bailón, E (2015) Análisis en seguridad informática y seguridad de las información basado en la norma ISO/IEC 27001 – Sistemas de Gestión de Seguridad de la Información Dirigido a una Empresa de Servicios Financieros. Universidad Politécnica Salesiana, Guayaquil.

Bsigroup. ¿Qué son las sistemas de gestión?, 2012. disponible en: https://www.bsigroup.com/es-MX/Sorry-we-could-not-find-that-page/

Conexión Esan (2019) Marco de Basilea: todo lo que necesitas saber dentro de la gestión de riesgos: Conexión Esan. Recuperado de: https://www.esan.edu.pe/apuntes-empresariales/2019/03/marco-de-basilea-todo-lo-que-necesitas-saber-dentro-de-la-gestion-de-riesgos/

Deming, W. (2008). Saliendo de la crisis. Boston: MIT Press.

Gastulo, Ayala & López (2019) Diseño e implementación de la ISO 27035 (gestión de incidentes de seguridad de la información) para el área de plataforma de servicios de una entidad del estado peruano (Tesis de licenciatura). Universidad Tecnológica del Perú, Lima.

GESCONSULTOR. ISO 27001 – Sistema de Gestión de la Seguridad de la Información, [consultado el 2 de mayo de 2018. Disponible en Internet: http://www. http:/wwwgesconsultor.com/iso-27001.html

INACAL (2017) NTP-ISO 27001 Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos.

INACAL (2017) NTP-ISO 27002 Tecnología de la Información. Técnicas de Seguridad, Código de prácticas para controles de seguridad de la Información.

INACAL (2018) NTP-ISO/IEC 27005 Tecnología de la Información. Técnicas de Seguridad, Gestión de riesgos de la seguridad de la información.

INACAL (2018) NTP-ISO 31000 Gestión del Riesgo. Directrices. 2da edición.

ISO 27001 "ISO Survey 2018 Certicates". Disponible en: https://isotc.iso.org/livelink/livelink?func=ll&objId=20719433&objAction=browse&viewType

J. C. García Porras and S. C. Huamani Pastor, "Modelo de gestión de riesgos de seguridad de la información para pymes en el Perú," Universidad Peruana de Ciencias Aplicadas (UPC), Lima, Perú, 2019.

Kosutic, D. (2014). La lógica básica de la norma ISO 27001. Noviembre 12, 2014, de 27001 Academy, Recuperado de: https://advisera.com/27001academy/knowledgebase/the-basic-logic-of-iso-27001-how-does-information-security-work/

Moncada, M & Israel, O. (2018) “Diseño de un sistema de gestión de la seguridad de la información (SGSI) para la Cooperativa de Ahorro y Crédito ABC, basado en la norma ISO 27001:2013,” Universidad Peruana de Ciencias Aplicadas (UPC). Lima

Niño, N. (2018) MODELO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN – SGSI, PARA FORTALECER LA CONFIDENCIALIDAD, INTEGRIDAD, DISPONIBILIDAD Y MONITOREAR LOS ACTIVOS DE INFORMACIÓN PARA EL INSTITUTO NACIONAL DE ESTADÍSTICA E INFORMÁTICA - INEI FILIAL LAMBAYEQUE, Universidad Nacional “Pedro Ruiz Gallo”. Lambayeque.

Recovery Labs (2019) Delitos informáticos: Computer Forensic. Recuperado de: https://delitosinformaticos.info/

Vergara, G (2009) ¿Que es un sistema de gestión? disponible en: http://mejoratugestion.com/mejora-tu-gestion/que-es-un-sistema-de-gestion/

ANEXOS

Anexo 01 Catálogo de amenazas

Tipo	N°	Tipología de Amenaza
Amenazas a la información	1	Acceso no autorizado a la información
	2	Modificación no autorizada de la información
	3	Eliminación no autorizada de la información
	4	Robo de activos contenedores de información
	5	Inadecuada eliminación de activos contenedores de información
	6	Corrupción de datos por error de procesamiento
	7	Uso extra laboral de la información
	8	Ataques de hacking/cracking sobre la información
	9	Virus informáticos que alteran o eliminan la información
	10	Fuga de Información
Amenazas al software	11	Adulteración intencional del software (bombas lógicas, sabotaje)
	12	Cambios no autorizados sobre el software (mantenimientos)
	13	Actualizaciones no controladas del software (parches)
	14	Instalación de software no licenciado o autorizado
	15	Copia no controlada del código fuente del software
	16	Saturación de la operación del software
	17	Hacking/cracking
	18	Virus informáticos
	19	Error humano en los cambios en el software (bugs)
	20	Incompatibilidad en la operación con otros softwares
Amenazas a activos físicos (equipos)	21	Corto circuito
	22	Filtraciones de agua
	23	Filtración de polvo
	24	Corrosión de equipos
	25	Congelación de equipos
	26	Desconexión de equipos
	27	Saturación de humedad en ambientes
	28	Fallas del sistema de aire acondicionado
	29	Radiación electromagnética
	30	Robo de equipos o de sus componentes
	31	Incumplimiento del plan de mantenimiento
	32	Uso inadecuado de los equipos
	33	Desconfiguración del equipo
	34	Obsolescencia de los componentes del equipo
Amenazas a servicios	35	Falla de servicios para las telecomunicaciones
	36	Degradación de servicios para las telecomunicaciones
	37	Falla de la provisión de energía eléctrica
	38	Incumplimiento de fechas por parte de proveedores

Tipo	N°	Tipología de Amenaza
	39	Provisión de servicios defectuosos (personal)
	40	Provisión de recursos defectuosos (materiales)
	41	Falla en servicios de información provistos por clientes
Amenazas a personal	42	Contaminación del ambiente por gases
	43	Uso de credenciales falsificadas
	44	Bloqueo del acceso al centro de trabajo
	45	Dificultad en el desplazamiento hacia el centro de trabajo
	46	Asaltos/secuestros
	47	Enfermedad
Amenazas a ubicaciones físicas	48	Sismo
	49	Inundación
	50	Hundimiento de suelos
	51	Incendio
	52	Destrucción intencional de los ambientes (protestas)

Anexo 02 Catálogo de vulnerabilidades

Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Hardware	Mantenimiento insuficiente/instalación fallida de medios de almacenamiento	Ruptura de la mantenibilidad del sistema de información
	Falta de esquema de reemplazo periódicos	Destrucción de equipos o medio
	Susceptibilidad a la humedad, al polvo y a la suciedad	Polvo, corrosión, congelamiento
	Sensibilidad a la radiación electromagnética	Radiación electromagnética
	Falta de control eficiente del cambio de configuración	Error en el uso
	Susceptibilidad a variaciones de voltaje	Pérdida de suministro eléctrico
	Susceptibilidad a variaciones de temperatura	Fenómeno meteorológico
	Almacenamiento no protegido	Robo de medios o documentos
	Falta de cuidado al descartarlo	Robo de medios o documentos
	Copia no controlada	Robo de medios o documentos
Software	Pruebas al software inexistentes o insuficientes	Abuso de derechos
	Errores conocidos en el software	Abuso de derechos
	No hacer "logout" cuando se sale de la estación de trabajo.	Abuso de derechos
	Disposición o reutilización de medios de almacenamiento sin borrar apropiadamente	Abuso de derechos
	Falta de evidencias de auditoría	Abuso de derechos
	Asignación equivocada de derechos de acceso	Abuso de derechos
	Software ampliamente distribuido	Corrupción de datos
	Aplicar programas de aplicación a datos incorrectos en términos del tiempo	Corrupción de datos
	Interfaz de usuario complicada	Error en el uso
	Falta de documentación	Error en el uso

Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
	Configuración incorrecta de parámetros	Error en el uso
	Fechas incorrectas	Error en el uso
	Falta de mecanismos de identificación y autentificación como la autentificación de usuarios	Falsificación de datos
	Tablas de claves no protegidas	Falsificación de datos
	Mala administración de claves	Falsificación de datos
	Habilitación de servicios incensarios	Procesamiento ilegal de datos
	Software inmaduro o nuevo	Mal funcionamiento del software
	Especificaciones no claras o incompletas para los desarrolladores	Mal funcionamiento del software
	Falta de control de cambios eficaz	Mal funcionamiento del software
	Descarga y uso incontrolado de software	Adulteración del software
	Falta de copia de respaldos	Adulteración del software
	Falta de protección física del edificio, puertas y ventanas	Robo de medios o documentos
	No producir informes de gestión	Uso no autorizado del equipo
	Falta de prueba de envío o recepción de un mensaje	Mediación de acciones
	Líneas de comunicación no protegidas	Intercepción
	Tráfico delicado no protegido	Intercepción
	Juntas malas en el cableado	Falla del equipo de telecomunicaciones
	Punto de falla único	Falla del equipo de telecomunicaciones
Red	Falta de identificación y autentificación de receptor y destinatario	Falsificación de derechos
	Arquitectura de red insegura	Espionaje remoto
	Transferencia de claves en claro	Espionaje remoto
	Gestión inadecuada de la red (capacidad de recuperación del ruteo)	Saturación del sistema de información
	Conexiones no protegidas de la red pública	Uso no autorizado del equipo
Personal	Ausencia de personal	Ruptura de la disponibilidad del personal
	Procedimientos inadecuados de reclutamiento	Destrucción de equipos o medio
	Capacitación de seguridad insuficiente	Error en el uso
	Uso incorrecto del software y hardware	Error en el uso
	Falta de conciencia de seguridad	Error en el uso
	Falta de mecanismos de monitoreo	Procesamiento ilegal de datos
	Trabajo no supervisado del personal externo o de limpieza	Robo de medios o documentos
	Falta de políticas para el uso correcto de medios de telecomunicaciones y mensajería	Uso no autorizado del equipo
	Uso inadecuado o negligente del control de acceso físico a edificios y habitaciones	Destrucción de equipos o medio
Sitio	Ubicaciones en un área susceptible a las inundaciones	Inundación

Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
	Red inestable de energía eléctrica	Pérdida de suministro eléctrico
	Falta de protección física del edificio, puertas y ventanas	Robo de equipos
Organización	Falta de un procedimiento formal para el registro y baja de los usuarios	Abuso de derechos
	Falta de proceso formal para revisar el derecho de acceso (supervisión)	Abuso de derechos
	Disposiciones inexistentes o insuficientes (respecto de la seguridad) en contratos con clientes y/o terceros	Abuso de derechos
	Falta de procesamiento de monitoreo de las instalaciones de procesamiento de la información	Abuso de derechos
	Falta de auditorías regulares(supervisión)	Abuso de derechos
	Falta de procesamiento de identificación y evaluación del riesgo	Abuso de derechos
	Falta de informes de fallas registradas en los registros del administrador y del operador.	Abuso de derechos
	Respuesta inadecuada del mantenimiento del servicio	Ruptura de la mantenibilidad del sistema de información
	Inexistencia o insuficiencia de acuerdo sobre el nivel del servicio.	Ruptura de la mantenibilidad del sistema de información
	Falta de procedimiento de control de cambios	Ruptura de la mantenibilidad del sistema de información
	Falta de procedimiento formal para el control de la documentación	Corrupción de datos
	Falta de procedimiento formal para la supervisión del registro	Corrupción de datos
	Falta de proceso formal para autorización de información pública disponible	Datos de fuentes no confiables
	Falta de asignación apropiada de responsabilidades de seguridad en la información	Negación de acciones
	Falta de planes de continuidad	Falla del equipo
	Falta de una política de uso de correos electrónicos	Error en el uso
	Falta de procedimientos para introducir software en sistema operativos	Error en el uso
	Faltas de registros en los historiales del administrador y del operador	Error en el uso
	Falta de procedimientos para manejo de la información clasificada	Error en el uso
	Falta de responsabilidades sobre la seguridad de la información en las descripciones de puesto	Error en el uso
	Ausencia o insuficiencia de disposiciones (concernientes a la seguridad de la información en contratos con empleados)	Procesamiento ilegal de datos

Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
	Falta de proceso disciplinario definido en caso de incidentes en la seguridad de la información	Robo de equipos
	Falta de política formal sobre el uso de computadoras portátiles	Robo de equipos
	Falta de control de activos que se encuentran fuera del local	Robo de equipos
	Inexistencia o insuficiencia de la política de "Escritorios despejado y pantalla despejada"	Robo de medios o documentos
	Falta de autorización al acceso a las instalaciones de procesamiento de la información	Robo de medios o documentos
	Falta de mecanismos de monitoreo establecidos para las rupturas de la seguridad.	Robo de medios o documentos
	Falta de revisiones regulares de la gestión	Uso no autorizado del equipo
	Falta de procedimientos para reportar debilidades en la seguridad	Uso no autorizado del equipo
	Falta de procesamiento sobre el cumplimiento de disposiciones respecto de derechos intelectuales	Uso de software falsificada o copiado

Anexo 03 Criterios para evaluar controles

Dimensión	Peso	Criterio	Peso	Nivel de cumplimiento	Peso
Diseño	40%	Frecuencia	35%	1. No se establece frecuencia	30%
				2. Se hace más veces de lo necesario	60%
				3. Se hace menos veces de lo necesario	75%
				4. Se hace tantas veces como se necesita	100%
		Documentación	30%	1. No documentado formalmente	70%
				2. Documento desactualizado	80%
				3. Documentado, pero no cumple criterios	90%
				4. Documentado cumple todos los criterios	100%
		Responsabilidad	35%	1. Asignación múltiple e informal	50%
				2. Asignado, pero no es su función	80%
				3. Asignado, pero no formalizado	95%
				4. Formalmente asignado	100%
Ejecución	60%	Implementación	20%	1. Manual	95%
				2. Manual con soporte automatizado	98%
				3. Automatizado	99%
		Oportunidad	40%	1. Se omite la ejecución del control	0%
				2. Incumplimiento de la frecuencia de ejecución	50%
				3. Se cumple la ejecución en un momento distinto al proceso	90%
				4. Se cumple en frecuencia y momento de ejecución	99%
		Trazabilidad	40%	1. Se omite la documentación que sustente la ejecución	0%
				2. Se documenta de manera incompleta	50%

				3. Se documenta, pero faltan firmas	90%
				4. Se documente de acuerdo al diseño	99%

Anexo 04 Ejemplo de Descripción del Escenario de Riesgo

Elemento	Ejemplo de Narración
Activo de Información	Archivos de configuración lógica de switches y router
Amenaza	Acceso no autorizado a los archivos de configuración lógica de switches y router, por parte de atacantes internos y/o atacantes externos.
Vulnerabilidad	Los archivos de configuración lógica de switches y router, no están protegidos con algún de software de encriptación en los discos duros de los administradores.
Impacto / Severidad	Impacto en las operaciones dado que la información puede ser aprovechada por un hacker para futuros ataques.
Escenario de Riesgo	**Si** ocurre un acceso no autorizado a los archivos de configuración lógica de switches y router, **entonces** puede causar un impacto en las operaciones dado que la información puede ser aprovechada por un hacker para futuros ataques debido a que no se guardan los archivos de configuración lógica de switches y router con algún de software de encriptación en los discos duros de los administradores.

Anexo 05 Controles que conforman la declaración de aplicabilidad

Código	Nivel	Nombre del Control	Descripción	Aplica	Descripción
05.1.1	Control	Políticas de la seguridad de la información	La gerencia debe definir, aprobar, publicar y comunicar a los trabajadores y partes externas involucradas, una serie de políticas para la seguridad de la información.	Si	Requerido por Circular G-140 Artículo 3.
05.1.2	Control	Revisión de las políticas de seguridad de la información.	Las políticas de seguridad de la información deben ser revisadas en intervalos planificados o si ocurren cambios significativos, para garantizar su idoneidad, adecuación y efectividad continuos.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
06.1.1	Control	Funciones y responsabilidades de la seguridad de la información.	Se debe definir y asignar todas las responsabilidades de la seguridad de la información.	Si	Requerido por Circular G-140 Artículo 4.
06.1.2	Control	Segregación de tareas.	Tareas o áreas de responsabilidad en conflicto deben ser segregadas para reducir las oportunidades de modificación no autorizada o involuntaria o el uso inadecuado de los activos de la organización.	Si	Requerido por Circular G-140 Artículo 4.
06.1.3	Control	Contacto con las autoridades.	Se debe mantener contacto adecuado con las autoridades respectivas.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
06.1.4	Control	Contacto con grupos especiales de interés.	Se debe mantener contacto con grupos especiales de interés u otros fórums y asociaciones de profesionales especializados en seguridad.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
06.1.5	Control	Seguridad de la información en la gestión del proyecto.	La seguridad de la información debe adaptarse a la gestión del proyecto, independientemente del tipo de proyecto.	Si	Aplica para mitigar los riesgos identificados de los activos de información.

Código	Nivel	Nombre del Control	Descripción	Aplica	Descripción
06.2.1	Control	Política de los equipos móviles	Se debe adoptar políticas y medidas de soporte de seguridad para el manejo de los riesgos derivados del uso de equipos móviles.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
06.2.2	Control	Trabajo a distancia.	Se debe implementar políticas y medidas de soporte de seguridad para proteger la información a la que se accede, procesa o almacena en los lugares de trabajo a distancia.	SI	Aplica para mitigar riesgos para trabajo a distancia.
07.1.1	Control	Selección	Se debe llevar a cabo la verificación de los antecedentes de todos los candidatos al empleo de acuerdo a las leyes y regulaciones vigentes y a la ética; y debe ser proporcional a los requisitos del negocio, la clasificación de la información a la que tendrá acceso y los riesgos que se perciban.	Si	Requerido por Circular G-140 Artículo 5.2.
07.1.2	Control	Términos y condiciones del empleo.	Los acuerdos contractuales con los trabajadores deben fijar sus responsabilidades y las de la organización con respecto a la seguridad de la información.	Si	Requerido por Circular G-140 Artículo 5.2.
07.2.1	Control	Responsabilidades de la Gerencia.	La dirección debe solicitar a todos los empleados y contratistas que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
07.2.2	Control	Concientización, educación y capacitación sobre seguridad de la información.	Todos los empleados de la organización, y en donde sea pertinente, los contratistas deben recibir formación adecuada en concientización y actualizaciones regulares en políticas y procedimientos organizacionales, pertinentes para su función laboral.	Si	Requerido por Circular G-140 Artículo 5.2.
07.2.2.B	Control	Alcance y registro de las capacitaciones sobre seguridad de la información	Mantener la información utilizada en las capacitaciones sobre seguridad de la información y mantener un registro de asistencia.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
07.2.3	Control	Procesos disciplinarios	Debe haber un proceso disciplinario formal que debe ser comunicado en	Si	Requerido por Circular G-140

Código	Nivel	Nombre del Control	Descripción	Aplica	Descripción
			el lugar, para tomar acción contra los trabajadores que comentan alguna infracción contra la seguridad de la información.		Artículo 5.2.
07.3.1	Control	Término o cambio de responsabilidad en el empleo	Se debe definir, comunicar y reforzar a todos los trabajadores y contratistas, las responsabilidades y tareas de seguridad de la información que permanecerán válidos después del término del empleo.	Si	Requerido por Circular G-140 Artículo 5.2.
08.1.1	Control	Inventario de activos.	Se debe identificar los activos y las instalaciones asociados a la información y al procesamiento de la información y se debe diseñar y mantener un inventario de dichos activos.	Si	Requerido por Circular G-140 Artículo 5.4.
08.1.2	Control	Propiedad de los activos.	Los activos que se encuentren identificados en el inventario deben de ser asignados a un “propietario”.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
08.1.3	Control	Uso aceptable de los activos.	Se debe identificar, documentar e implementar las reglas para el uso aceptable de la información y de los activos relacionados a la información y a las instalaciones de procesamiento de la información.	Si	Requerido por Circular G-140 Artículo 5.4.
08.1.4	Control	Retorno de los activos	Todos los trabajadores y usuarios internos y externos deberán devolver todos los activos de la organización que estén en su posesión una vez terminado su empleo, contrato o acuerdo.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
08.2.1	Control	Clasificación de la información.	La información debe ser clasificada en términos de los requisitos y valores legales, siendo crítica y sensible ante la divulgación y modificación no autorizada.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
08.2.2	Control	Etiquetado de la información.	Se debe desarrollar e implementar una serie de procedimientos adecuados para el etiquetado de la información, de acuerdo al esquema de clasificación de la información adoptado por la organización.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
08.2.3	Control	Manejo de los activos	Se debe desarrollar e implementar procedimientos de manejo de los	Si	Requerido por Circular G-140

Código	Nivel	Nombre del Control	Descripción	Aplica	Descripción
			activos de acuerdo al esquema de clasificación de la información adoptado por la organización.		Artículo 5.4.
08.3.1	Control	Gestión de medios removibles	Se deberían implementar procedimientos para la administración de medios extraíbles de acuerdo con el esquema de clasificación adoptado por la organización	Si	Aplica para mitigar los riesgos identificados de los activos de información.
08.3.2	Control	Eliminación de medios	Los medios se deberían eliminar de manera segura cuando ya no se necesitan, a través de procedimientos formales.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
08.3.3	Control	Transferencias física de los medios	Los medios de comunicación que contienen información deben ser protegidos contra el acceso no autorizado, mal uso o corrupción durante su transporte.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
09.1.1	Control	Política de control de acceso	Se debe establecer, documentar y revisar la política de control del acceso en base a los requisitos del negocio y de la seguridad de la información.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
09.1.2	Control	Acceso a la redes y a los servicios de las redes	Los usuarios deben tener acceso únicamente a la red o a los servicios de redes a los que han sido autorizados a usar.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
09.2.1	Control	Registro y cancelación de registro de usuarios	Se debería implementar un proceso formal de registro y cancelación de registro de un usuario para permitir la asignación de derechos de acceso.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
09.2.2	Control	Provisión de acceso al usuario.	Se debe implementar un proceso formal de provisión de acceso al usuario, para asignar o revocar los derechos de acceso a todos los tipos de usuarios a todos los sistemas y servicios.	Si	Requerido por Circular G-140 Artículo 5.1.
09.2.3	Control	Gestión de derechos de accesos privilegiados	La asignación y el uso de derechos de acceso privilegiado se deberían restringir y controlar.	Si	Requerido por Circular G-140 Artículo 5.1.
09.2.3.B	Control	Gestión de perfiles de acceso	Implementar un proceso formal para la gestión de perfiles en los sistemas informáticos y mantener una matriz de perfiles para cada	Si	Requerido por Circular G-140 Artículo 5.1.

Código	Nivel	Nombre del Control	Descripción	Aplica	Descripción
			sistema informático.		
09.2.4	Control	Gestión de información de autentificación secreta de usuarios	La asignación de la información de autenticación secreta se debería controlar a través de un proceso de administración formal.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
09.2.5	Control	Verificación de los derechos de acceso de los usuarios.	Los propietarios de los activos deben verificar los derechos de acceso de los usuarios a intervalos regulares.	Si	Requerido por Circular G-140 Artículo 5.1.
09.2.6	Control	Retiro o ajuste de los derechos de acceso.	Los derechos de acceso a todos los trabajadores y terceros a la información y a las instalaciones de procesamiento de la información deben ser retirados al término del empleo, contrato o acuerdo, o ajustado luego de un cambio.	Si	Requerido por Circular G-140 Artículo 5.1.
09.3.1	Control	Uso de información secreta de autenticación	Se debe solicitar a los usuarios seguir las prácticas de la organización sobre el uso de la información secreta de autenticación.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
09.4.1	Control	Restricción del acceso a la información	Se debe restringir el acceso a la información y a las funciones de aplicación del sistema de acuerdo a la política de control de acceso.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
09.4.2	Control	Procedimiento seguro de logeo	Si así lo requiere la política de control del acceso, se debe controlar el acceso a los sistemas y a las aplicaciones, mediante un procedimiento seguro de logeo.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
09.4.3	Control	Sistema de gestión de la clave	Los sistemas de gestión de la clave deben ser interactivos y deben asegurar la calidad de las claves.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
09.4.4	Control	Uso de programas utilitarios de privilegio.	Se debe restringir y controlar severamente el uso de programas utilitarios que puedan controlar manualmente el sistema y los controles de la aplicación.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
09.4.5	Control	Control del acceso para programar el código fuente.	Se debe restringir el acceso al programa de código fuente.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
10.1.1	Control	Política del uso	Se debe desarrollar e implementar	Si	Aplica para mitigar

Código	Nivel	Nombre del Control	Descripción	Aplica	Descripción
		de controles criptográficos	una política de uso de controles criptográficos para proteger la información.		los riesgos identificados de los activos de información.
10.1.2	Control	Gestión de las claves	Se debe desarrollar e implementar una política para el uso, protección y tiempo de vida de las claves criptográficas a lo largo de todo su ciclo de vida.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
11.1.1	Control	Perímetro de seguridad física	Se debe determinar y utilizar los perímetros de seguridad para proteger las áreas que contienen información sensible y crítica y las instalaciones de procesamiento de la información.	Si	Requerido por Circular G-140 Artículo 5.3.
11.1.2	Control	Controles físicos de los ingresos	Se debe proteger las áreas seguras mediante controles adecuados de ingreso para garantizar el ingreso de sólo personal autorizado.	Si	Requerido por Circular G-140 Artículo 5.3.
11.1.3	Control	Seguridad de las oficinas, Salas e instalaciones.	Se debe diseñar y aplicar mecanismos de seguridad física a las salas, oficinas e instalaciones.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
11.1.3	Control	Seguridad de las oficinas, Salas e instalaciones.	Se debe diseñar y aplicar mecanismos de seguridad física a las salas, oficinas e instalaciones.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
11.1.4	Control	Protección contra las amenazas externas y medioambientales.	Se debe diseñar y aplicar mecanismos de control contra los desastres naturales, ataques maliciosos o accidentes.	Si	Requerido por Circular G-140 Artículo 5.3.
11.1.5	Control	Trabajo en áreas seguras.	Se debe diseñar y aplicar procedimientos para el trabajo en áreas seguras.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
11.1.6	Control	Distribución de las zonas de carga.	Los puntos de acceso, tales como las zonas de distribución y carga y otros puntos por los que podría ingresar personal no autorizado a las instalaciones deben ser controlados, y en la medida de lo posible, alejados de las instalaciones de procesamiento de	Si	Aplica para mitigar los riesgos identificados de los activos de información.

Código	Nivel	Nombre del Control	Descripción	Aplica	Descripción
			la información para evitar el acceso no autorizado.		
11.2.1	Control	Ubicación y protección de los equipos	Los equipos deben ser ubicados y protegidos de tal forma que se reduzcan los riesgos como resultado de las amenazas y los peligros del medio ambiente, y las oportunidades de acceso no autorizado.	Si	Requerido por Circular G-140 Artículo 5.3.
11.2.2	Control	Servicios públicos de soporte.	Los equipos deben ser protegidos contra las fallas de energía y otras alteraciones causadas por las fallas en los servicios públicos de soporte.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
11.2.3	Control	Seguridad en el cableado.	Se debe proteger de cualquier interferencia, intercepción o daño al cableado de energía o telecomunicaciones que transfiere datos o que sirve de apoyo en los servicios de información.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
11.2.4	Control	Mantenimiento de los equipos	Se debe mantener de manera correcta el mantenimiento de los equipos para garantizar su disponibilidad e integridad continuas.	Si	Requerido por Circular G-140 Artículo 5.3.
11.2.4.B	Control	Revisión independiente	Realizar una evaluación independiente sobre el funcionamiento de los controles de seguridad física y ambiental implementados.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
11.2.5	Control	Retiro de los activos.	El equipo, la información o el software no puede ser retirado de su lugar sin una previa autorización.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
11.2.6	Control	Seguridad de los equipos y bienes fuera de las instalaciones	Se debe aplicar medidas de seguridad para los activos utilizados fuera de las instalaciones, tomando en cuéntalos diferentes riesgos de trabajar fuera de las instalaciones de la organización.	Si	Requerido por Circular G-140 Artículo 5.3.
11.2.7	Control	Eliminación o reutilización segura de equipos	Todos los equipos que contienen medios de comunicación de la información deben ser revisados para garantizar que se haya extraído o que se haya sobre-escrito la información sensible y la licencia del software antes de	Si	Aplica para mitigar los riesgos identificados de los activos de información.

Código	Nivel	Nombre del Control	Descripción	Aplica	Descripción
			desechar o re-usar el mismo.		
11.2.8	Control	Equipos de usuario no supervisados	Los usuarios se deberían asegurar de que los equipos no supervisados cuentan con la protección adecuada.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
11.2.9	Control	Política de escritorio y pantallas limpias.	Se debería adoptar una política de escritorio despejado para los papeles y para los medios de almacenamiento extraíbles y una política de pantalla despejada para las instalaciones de procesamiento de información.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
12.1.1	Control	Procedimientos operativos documentados	Se debe documentar los procesos operacionales y ponerse a disposición de todos los usuarios que lo necesiten.	Si	Requerido por Circular G-140 Artículo 5.5.
12.1.2	Control	Administración de cambios	Se debe mantener un control sobre los cambios en la organización, el negocio y los sistemas que afectan la seguridad de la información.	Si	Requerido por Circular G-140 Artículo 5.5.
12.1.2.B	Control	Gestión de cambios de emergencia	Implementar procedimientos formales para gestionar cambios de emergencia en los sistemas informáticos.	Si	Requerido por Circular G-140 Artículo 5.5.
12.1.2.C	Control	Gestión de nuevos productos y cambios significativos	Implementar procedimientos formales para gestionar el lanzamiento de nuevos productos y cambios significativos en el ambiente operativo.	Si	Requerido por Circular G-140 Artículo 5.5.
12.1.3	Control	Administración de capacidad	El uso de recursos se debería monitorear, ajustar y se deberían hacer las proyecciones necesarias para los requisitos futuros de capacidad y así poder garantizar el rendimiento que el sistema requiere.	Si	Requerido por Circular G-140 Artículo 5.5.
12.1.4	Control	Separación de ambientes de desarrollo, prueba y de operaciones.	Se debe separar los ambientes de desarrollo, prueba y operaciones para reducir los riesgos de acceso o cambios no autorizados dentro de ambiente de operaciones.	Si	Requerido por Circular G-140 Artículo 5.5.
12.2.1	Control	Controles contra el malware.	Se debe implementar mecanismos de control para la detección, prevención y recuperación, para proteger a la información contra el malware, junto con una concientización adecuada al	Si	Requerido por Circular G-140 Artículo 5.5.

Código	Nivel	Nombre del Control	Descripción	Aplica	Descripción
			usuario.		
12.3.1	Control	Respaldo de información	Se deberían realizar copias de la información, del software y de las imágenes del sistema y se deberían probar de manera regular de acuerdo con una política de respaldo acordada..	Si	Requerido por Circular G-140 Artículo 5.7.
12.4.1	Control	Registro de eventos	Se deberían producir, mantener y revisar de manera periódica los registros de eventos del usuario, las excepciones, las fallas y los eventos de seguridad de la información.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
12.4.2	Control	Protección de la información del logeo	Se debe proteger contra la falsificación y el acceso no autorizado a los medios de logeo y a la información del logeo.	Si	Requerido por Circular G-140 Artículo 5.5.
12.4.3	Control	Registros del administrador y del operador	Las actividades del administrador y del operador del sistema se deberían registrar y los registros se deberían proteger y revisar de manera regular.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
12.4.4	Control	Sincronización de los relojes.	Se debe sincronizar a una sola fuente de tiempo de referencia, los relojes de todos los sistemas de procesamiento de la información correspondientes dentro de la organización o del dominio de seguridad.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
12.5.1	Control	Instalación del software en los sistemas operacionales.	Se debe implementar procedimientos para controlar la instalación del software en los sistemas operacionales. Se cuenta con un procedimiento para la administración de activos de software	Si	Aplica para mitigar los riesgos identificados de los activos de información.
12.6.1	Control	Administración de vulnerabilidades técnicas	Se debería obtener la información sobre las vulnerabilidades técnicas de los sistemas de información de manera oportuna; la exposición de la organización a dichas vulnerabilidades se debería evaluar y se deberían tomar las medidas necesarias para abordar el riesgo asociado.	Si	Requerido por Circular G-140 Artículo 5.6.
12.6.2	Control	Restricciones en la instalación de software.	Se debe establecer e implementar las reglas que gobiernen la instalación de software.	Si	Aplica para mitigar los riesgos identificados de los

Código	Nivel	Nombre del Control	Descripción	Aplica	Descripción
					activos de información.
12.7.1	Control	Controles de la auditoría sobre los sistemas de información.	Se debe planificar cuidadosamente los requisitos y actividades de la auditoría que involucren la verificación de los sistemas operacionales; y acordar minimizar las alteraciones a los procesos del negocio.	Si	Requerido por Circular G-140 Artículo 5.5.
13.1.1	Control	Controles en las redes	Se debe administrar y controlar las redes para proteger la información de los sistemas y las aplicaciones.	Si	Requerido por Circular G-140 Artículo 5.5.
13.1.2	Control	Seguridad de los servicios de las redes.	Se debe identificar los mecanismos de seguridad, los niveles del servicio y los requisitos de todos los servicios de redes e incluirlos en los acuerdos de servicios de redes, ya sea que los servicios sean proporcionados por la misma organización o por un tercero.	Si	Requerido por Circular G-140 Artículo 5.5.
13.1.3	Control	Segregación en las redes	Se debe segregar grupos de servicios de información, usuarios y sistemas de información.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
13.1.3.B	Control	Monitoreo de la red	Monitorear los mecanismos y herramientas de seguridad en redes tales como: firewalls, antivirus, IPS, IDS, DLP, puertos USB, conexiones bluetooth.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
13.1.3.C	Control	Pruebas de ethical hacking	Realizar pruebas de ethical hacking interno y externo.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
13.2.1	Control	Políticas y procedimientos de la transferencia de la información.	Se debe dar lugar a las políticas, procedimientos y controles formales de transferencia a través del uso de todo tipo de equipos de comunicación.	Si	Requerido por Circular G-140 Artículo 5.5.
13.2.2	Control	Acuerdos sobre las transferencias de la información.	Los acuerdos deberán señalar la transferencia segura de la información del negocio entre la organización y terceros.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
13.2.3	Control	Mensajería electrónica	Se debe proteger adecuadamente la información enviada mediante mensajes electrónicos.	Si	Requerido por Circular G-140 Artículo 5.5.

Código	Nivel	Nombre del Control	Descripción	Aplica	Descripción
13.2.4	Control	Confidencialidad de los acuerdos de no divulgación	Se debe identificar, revisar regularmente y documentar los requisitos para la confidencialidad o acuerdos no divulgados que reflejan las necesidades de la organización sobre la protección de la información.	Si	Aplica para mitigar los riesgos identificados de los activos de información: Colaboradores de CMACT.
14.1.1	Control	Análisis y especificaciones de los requisitos de la seguridad de la información.	Se debe incluir la seguridad de la información relacionada a los requisitos en los requerimientos de nuevos sistemas de información o en el mejoramiento de los sistemas de información existentes.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
14.1.2	Control	Seguridad de los servicios de aplicación en las redes públicas.	Se debe proteger la información que pasa a través de las redes públicas de las actividades fraudulentas, controversias contractuales y divulgación y modificaciones no autorizadas.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
14.1.3	Control	Protección de las transacciones de los servicios de aplicación	Se debe proteger la información que provenga de las transacciones se los servicios de aplicación, para evitar las transmisiones incompletas, desvíos, duplicado o reproducción no autorizados de mensajes.	Si	Requerido por Circular G-140 Artículo 5.5.
14.2.1	Control	Política de desarrollo seguro	Se debe establecer y aplicar reglas de desarrollo de software y sistemas a los programas de desarrollo dentro de la organización.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
14.2.2	Control	Procedimiento de control de los cambios de sistemas.	Se debe controlar los cambios dentro del ciclo de vida de los programas de desarrollo, mediante el uso de procedimientos formales de control de cambios.	Si	Requerido por Circular G-140 Artículo 5.6.
14.2.3	Control	Revisión técnica de las aplicaciones después de los cambios en la plataforma operativa	Luego del cambio de las plataformas operacionales, se debe revisar y verificar las aplicaciones críticas del negocio, para garantizar que no haya un impacto adverso sobre las operaciones o la seguridad organizacional.	Si	Requerido por Circular G-140 Artículo 5.6.
14.2.4	Control	Restricciones a los cambios de los paquetes de software	Se debería desalentar la modificación de los paquetes de sistemas; por el contrario, se les limitará a los cambios necesarios y todos los cambios deberán ser	Si	Aplica para mitigar los riesgos identificados de los activos de información.

Código	Nivel	Nombre del Control	Descripción	Aplica	Descripción
			estrictamente controlados.		
14.2.5	Control	Principios del sistema de seguridad para la ingeniería	Se debe establecer, documentar, mantener y aplicar los principios de sistemas de seguridad para la ingeniería, a todos los esfuerzos de implementación del sistema.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
14.2.6	Control	Ambiente seguro del programa de desarrollo	Las organizaciones deben establecer y proteger adecuadamente los ambientes seguros de desarrollo de los sistemas de desarrollo y la integración de los esfuerzos a lo largo del ciclo de vida del programa de desarrollo del sistema.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
14.2.7	Control	Programa de desarrollo subcontratado.	La organización debe supervisar y monitorear las actividades de desarrollo del sistema del ente subcontratado.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
14.2.8	Control	Revisión de la seguridad del sistema.	Se debe llevar a cabo revisiones de la funcionalidad de la seguridad durante el desarrollo	Si	Aplica para mitigar los riesgos identificados de los activos de información.
14.2.9	Control	Revisión de la aceptación del sistema.	Se debe establecer programas de verificación de la aceptación y de los criterios relacionados con respecto a los nuevos sistemas de información, renovaciones y nuevas versiones.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
14.3.1	Control	Protección de los datos de prueba.	Los datos de prueba deben ser seleccionados, protegidos y controlados cuidadosamente.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
15.1.1	Control	Política de seguridad de la información sobre las relaciones con los proveedores.	Se debe acordar y documentar los requisitos de seguridad de la información para mitigar los riesgos asociados al acceso de los proveedores a los activos de la organización.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
15.1.2	Control	Consideración de la seguridad en los acuerdos con los proveedores.	Se debe establecer y acordar todos los requisitos relacionados a la seguridad de la información con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proveer con elementos	Si	Aplica para mitigar los riesgos identificados de los activos de información.

Código	Nivel	Nombre del Control	Descripción	Aplica	Descripción
			de infraestructura tecnológica, información de la organización.		
15.1.3	Control	Cadena de suministro de tecnología de la información y comunicación.	Los acuerdos con los proveedores deben incluir los requisitos para el manejo de los riesgos de seguridad de la información relacionados a los servicios de tecnología de la información y la comunicación y a la cadena de suministro del producto.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
15.2.1	Control	Monitoreo y revisión del servicio de los proveedores	Las organizaciones deben monitorear, revisar y auditar regularmente la prestación de servicios del proveedor.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
15.2.2	Control	Cambios en la gestión del servicio de los proveedores	Se debe gestionar los cambios a la provisión de los servicios prestados por los proveedores, incluyendo el mantenimiento y la mejora de políticas, procedimientos y controles de la seguridad de la información, tomando en cuenta la sensibilidad de la información del negocio, los sistemas y los procesos involucrados así como la re-evaluación de los riesgos.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
16.1.1	Control	Responsabilidades y procedimientos.	Se debe establecer responsabilidades de la gerencia y procedimientos para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
16.1.2	Control	Reporte de los eventos de seguridad de la información.	Se debe reportar los eventos de seguridad de la información a través de canales adecuados lo más pronto posible.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
16.1.3	Control	Reporte de las debilidades de la seguridad de la información.	Se debe instar a los trabajadores y contratistas que hagan uso de los sistemas de información de la organización, a tomar nota e informar acerca de cualquier debilidad que se observe o sospeche con respecto a los sistemas o servicios del sistema de seguridad de la información.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
16.1.4	Control	Evaluación y decisión sobre	Se debe evaluar los eventos de seguridad de la información; y	Si	Aplica para mitigar los riesgos

Código	Nivel	Nombre del Control	Descripción	Aplica	Descripción
		los eventos de seguridad de la información.	tomar una decisión sobre si deben ser clasificados como incidentes de la seguridad de la información.		identificados de los activos de información.
16.1.5	Control	Respuesta a los incidentes de seguridad de la información	Se debe responder a los incidentes de seguridad de la información de acuerdo a los procedimientos documentados.	Si	Requerido por Circular G-140 Artículo 5.8.
16.1.6	Control	Aprendizaje de los incidentes de seguridad de la información.	Se debe usar el conocimiento obtenido del análisis y resolución de los incidentes de la seguridad de la información, con la finalidad de reducir la probabilidad o impacto de futuros incidentes.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
16.1.7	Control	Recolección de evidencia.	La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y conservación de la información que puede servir como evidencia.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
17.1.1	Control	Continuidad de los planes de seguridad de la información	La organización debe determinar sus requisitos para la seguridad de la información y para la continuidad de la gestión de seguridad de la información en situaciones adversas, e.g. durante una crisis o desastre	Si	Aplica para mitigar los riesgos identificados de los activos de información.
17.1.2	Control	Implementación de la continuidad de la seguridad de la información.	Implementación de la continuidad de la seguridad de la información.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
17.1.3	Control	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	La organización debe verificar los controles de la continuidad de la seguridad de la información establecidos e implementados, a intervalos regulares con la finalidad de asegurar la su validez y efectividad durante situaciones adversa.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
17.2.1	Control	Disponibilidad de instalaciones de procesamiento de la información.	Se debe implementar las instalaciones de procesamiento de la información con una capacidad adicional suficiente para cumplir con los requisitos de disponibilidad.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
18.1.1	Control	Identificación de la ley aplicable y de los requisitos	Se debe identificar de manera explícita, documentar y mantener actualizados todos los requisitos	Si	Aplica para mitigar los riesgos identificados de los

Código	Nivel	Nombre del Control	Descripción	Aplica	Descripción
		contractuales.	legislativos regulatorios y contractuales así como el enfoque de la organización para cumplir con estos requisitos, con respecto a cada sistema de información y a la organización.		activos de información.
18.1.2	Control	Derechos de propiedad intelectuales.	Se debe implementar procedimientos adecuados para garantizar el cumplimiento de los requisitos legislativos, regulatorios y contractuales relacionados a los derecho de propiedad intelectuales y al uso de productos registrados de software.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
18.1.3	Control	Protección de los registros.	Los registros deben ser protegidos contra la pérdida, destrucción, falsificación, acceso no autorizado y lanzamiento no autorizado, de acuerdo a los requisitos legales, regulatorios, contractuales y del mismo negocio.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
18.1.4	Control	Privacidad y protección de la información que permite identificar a las personas.	Se debe garantizar la privacidad y la protección de la información que permita identificar a las personas de acuerdo a lo requerido en la legislación y las regulaciones pertinentes, si fuera aplicable.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
18.1.5	Control	Regulación de los controles criptográficos.	Se debe hacer uso de controles criptográficos en cumplimiento con los acuerdos, las leyes y las regulaciones correspondientes.	Si	Aplica para mitigar los riesgos identificados de los activos de información.
18.2.1	Control	Revisión independiente de la seguridad de la información.	Se debe revisar, a intervalos planificados o cuando ocurre algún cambio significativo, el enfoque de la organización para gestionar la seguridad de la información y su implementación (i.e. objetivos de control, controles, políticas, procesos y procedimientos de la seguridad de la información).	Si	Aplica para mitigar los riesgos identificados de los activos de información.
18.2.2	Control	Cumplimiento de las políticas y normas de seguridad de la información.	Los gerentes deben revisar regularmente el cumplimiento de los procedimientos y del procesamiento de la información dentro de su área de responsabilidad, de acuerdo a las políticas, normas de seguridad	Si	Aplica para mitigar los riesgos identificados de los activos de información.

Código	Nivel	Nombre del Control	Descripción	Aplica	Descripción
			adecuadas y a los otros requisitos de seguridad.		
18.2.3	Control	Revisión del cumplimiento técnico.	Se debe revisar regularmente los sistemas de la información con respecto al cumplimiento de las políticas y normas de seguridad de la información de la organización.	Si	Aplica para mitigar los riesgos identificados de los activos de información.

Anexo 06 Activos de información consolidados que no posee custodio definido.

Código	Nombre Act. Sop. Consol.	Tipo	Propietario	Custodio	Ubicación	Nivel
ASC-063	Escritorio CMACT	FI4 - Mobiliario y equipamiento	Gerente Ejecutivo Adjunto	**Por definir**	Oficinas CMACT	Alto
ASC-017	Archivadores Div. Procesos y TI	FI4 - Mobiliario y equipamiento	Gerente de División de Procesos y TI	**Por definir**	Oficina de los Dptos. Usuarios	Alto
ASC-003	Archivadores Div. Finanza	FI4 - Mobiliario y equipamiento	Gerente de División de Finanzas y Canales	**Por definir**	Oficina de los Dptos. Usuarios	Muy Alto
ASC-004	Archivadores Riesgos	FI4 - Mobiliario y equipamiento	Gerente de Riesgos	**Por definir**	Oficina de los Dptos. Usuarios	Alto
ASC-005	Archivadores Insp. Fraudes	FI4 - Mobiliario y equipamiento	Jefe Dpto. Inspectoría de Fraude	**Por definir**	Oficina Dpto. Inspectoría de Fraude	Alto
ASC-006	Archivadores GCM	FI4 - Mobiliario y equipamiento	Gerente Ejecutivo Adjunto	**Por definir**	Oficinas CMACT	Alto
ASC-007	Archivadores Órgano Control Inst.	FI4 - Mobiliario y equipamiento	Jefe Órgano de Control Institucional	**Por definir**	Oficina Dpto. Órgano de Control Institucional	Alto
ASC-008	Archivadores Cumplimiento Norm.	FI4 - Mobiliario y equipamiento	Jefe Unidad de Cumplimiento Normativo	**Por definir**	Oficina Dpto. Cumplimiento Normativo	Alto
ASC-009	Archivadores Prevención	FI4 - Mobiliario y equipamiento	Jefe Unidad de Prevención	**Por definir**	Oficina Dpto. Prevención	Alto
ASC-010	Archivadores Auditoria Int.	FI4 - Mobiliario y equipamiento	Jefe Unidad de Auditoria Interna	**Por definir**	Oficina Dpto. Auditoria Interna	Medio

Código	Nombre Act. Sop. Consol.	Tipo	Propietario	Custodio	Ubicación	Nivel
ASC-011	Archivadores Div. Comercial	FI4 - Mobiliario y equipamiento	Gerente de División Comercial	**Por definir**	Oficina de los Dptos. Usuarios	Alto
ASC-012	Archivadores Div. Negocio	FI4 - Mobiliario y equipamiento	Gerente de División de Negocio	**Por definir**	Oficina de los Dptos. Usuarios	Alto
ASC-013	Archivadores Div. Administración	FI4 - Mobiliario y equipamiento	Gerente de División de Administración	**Por definir**	Oficina de los Dptos. Usuarios	Muy Alto
ASC-014	Archivadores Ger. Cent. Adm.	FI4 - Mobiliario y equipamiento	Gerente Central de Administración	**Por definir**	Oficina de los Dptos. Usuarios	Alto
ASC-015	Archivadores Ger. Cent. Fin.	FI4 - Mobiliario y equipamiento	Gerente Central de Finanzas	**Por definir**	Oficina de los Dptos. Usuarios	Alto
ASC-016	Archivadores Ger. Cent. Neg.	FI4 - Mobiliario y equipamiento	Gerente Central de Negocio	**Por definir**	Oficina de los Dptos. Usuarios	Alto

Anexo 07 Ejemplo de registro de Activos de Información Primarios

FO-01a Activos de Información Primarios — **Inventario de Activos de Información (IAI)**

Ciclo: IAI 2017-1

Código	Nombre	Descripción	Tipo	Propietario	Custodio	Ubicación		Requisitos legales	Frecuencia de Uso	Sensibilidad	Valor del activo				Nivel de Tasación
						Tipo	Lugar				C	I	D	Valor	
P0001	Activo primario X		I1 - Información electrónica			Física				Restringida	5	5	5	5.00	Muy Alto
P0002	Activo primario Y		I2 - Información escrita			Electrónica				Confidencial	4	4	4	4.00	Alto
P0003			I3 - Información hablada							Uso Interno	3	3	3	3.00	Medio
P0004			I4 - Otro tipo de información							Público	2	2	2	2.00	Bajo
P0005															
...															

Elaboración propia

Anexo 08 Ejemplo de registro de activos de información de soporte

FO-01b Activos de Información de Soporte — **Inventario de Activos de Información (IAI)**

Ciclo: IAI 2017-1

Activo Primario		Código	Nombre	Descripción	Tipo	Propietario	Custodio	Ubicación		Peso	Nivel de Tasación
Código	Nombre							Tipo	Lugar		
P0001	Activo Primario X	S0001	Base de datos XX		SW1 - Software comercial o herramientas, utilitarios			Física		11	Muy Alto
P0001	Activo Primario X	S0002	Aplicación local XX		SW2 - Software desarrollado por terceros			Electrónica		8	Muy Alto
P0001	Activo Primario X	S0003	Servidor de aplicaciones XX		FI1 - Equipo de procesamiento						Muy Alto
P0001	Activo Primario X	S0004	Caja Fuerte		FI4 - Mobiliario y equipamiento			Física	Sede Central, piso 5,		Muy Alto
P0002	Activo primario Y	S0001	Base de datos XX								Alto
P0002	Activo primario Y	S0002	Aplicación local XX		SW2 - Software desarrollado por terceros			Electrónica			Alto
P0002	Activo primario Y	S0003	Servidor de aplicaciones XX		FI1 - Equipo de procesamiento						Alto
...											

Elaboración propia

Anexo 09 Niveles de sensibilidad de activos de información

Clasificación	Detalle
Público	Pueden ser accedidos tanto por miembros de la entidad y público en general, sin estar sujetos a ningún control.
Uso interno	Pueden ser accedidos sólo por personal interno de la organización y cuyo acceso excepcional por parte de personal externo (auditores, entidades reguladoras, consultores externos) puede darse, pero se encuentra regulado y sujeto a condiciones específicas de acceso.
Confidencial	Son activos que pertenecen a un proceso, son accedidos por personal del proceso específico y cuyo acceso excepcional por parte de personal externo (auditores, entidades reguladoras, consultores externos) puede darse, pero se encuentra regulado y sujeto a condiciones específicas de acceso. Su revelación requiere la aprobación de su propietario, es de uso exclusivo de la organización, en el caso de terceros se deberá firmar acuerdo de confidencialidad y no divulgación.
Restringido	Son activos cuyo acceso es restringido a un grupo seleccionado a partir de un proyecto específico o que pertenecen a un grupo o nivel específico de poder dentro de la entidad.

Anexo 10 Escala de valor de activos

Valor	Confidencialidad (C)	Integridad (I)	Disponibilidad (D)
5 Muy alto	La información asociada al activo es restringida y solo accedida por el Directorio, Comité de Riesgos, Comité de Riesgo Operacional, Gerente Central, Gerentes de División, pues su divulgación afectaría irreversiblemente a la entidad.	La información asociada al activo es restringida y solo accedida por el Directorio, Comité de Riesgos, Comité de Riesgo Operacional, Gerente Central, Gerentes de División, pues su divulgación afectaría irreversiblemente a la entidad.	La información asociada al activo es restringida y solo accedida por el Directorio, Comité de Riesgos, Comité de Riesgo Operacional, Gerente Central, Gerentes de División, pues su divulgación afectaría irreversiblemente a la entidad.
4 Alto	La información asociada al activo es restringida y solo personal de un proyecto específico crítico para la entidad puede acceder a ella, pues su divulgación afectaría gravemente a la entidad.	La información asociada al activo es restringida y solo personal de un proyecto específico crítico para la entidad puede acceder a ella, pues su divulgación afectaría gravemente a la entidad.	La información asociada al activo es restringida y solo personal de un proyecto específico crítico para la entidad puede acceder a ella, pues su divulgación afectaría gravemente a la entidad.
3 Medio	La información asociada al activo es confidencial y solo personal de algunas áreas internas pueden acceder a ella, pues su divulgación afectaría considerablemente a la entidad.	La información asociada al activo es confidencial y solo personal de algunas áreas internas pueden acceder a ella, pues su divulgación afectaría considerablemente a la entidad.	La información asociada al activo es confidencial y solo personal de algunas áreas internas pueden acceder a ella, pues su divulgación afectaría considerablemente a la entidad.
2 Bajo	La información asociada al activo es de uso interno y solo personal de la entidad puede acceder a ella, pues su divulgación afectaría parcialmente a la entidad.	La información asociada al activo es de uso interno y solo personal de la entidad puede acceder a ella, pues su divulgación afectaría parcialmente a la entidad.	La información asociada al activo es de uso interno y solo personal de la entidad puede acceder a ella, pues su divulgación afectaría parcialmente a la entidad.
1 Muy bajo	La información asociada al activo es pública y cualquiera puede acceder a ella, pues no impacta a la entidad.	La información asociada al activo es pública y cualquiera puede acceder a ella, pues no impacta a la entidad.	La información asociada al activo es pública y cualquiera puede acceder a ella, pues no impacta a la entidad.

Elaboración propia

Anexo 10 Tasación de activo primario

$$\text{Valor del activo} = \frac{\text{Valor Confidencialidad} + \text{Valor Integridad} + \text{Valor Disponibilidad}}{3}$$

Anexo 11 Niveles de tasación de activo

Nivel de Importancia	Valor	Color	Rango del valor
Muy alto	5	Rojo	4,001 – 5,000
Alto	4	Naranja	3,001 – 4,000
Mediano	3	Amarillo	2,001 – 3,000
Bajo	2	Verde	1,001 – 2,000
Muy bajo	1	Azul	0,001 – 1,000

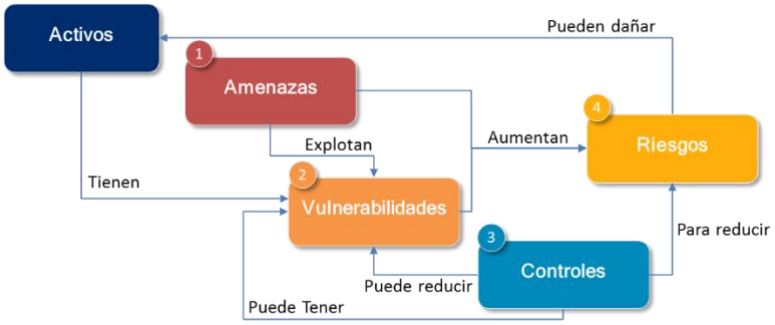
Elaboración propia

Anexo 12 Ejemplo de inventario de activos de información

FO-01d Inventario de Activos de Información — **Inventario de Activos de Información (IAI)** — Ciclo: IAI 2017-1

Código	Nombre	Descripción	Tipo	Departamento	Propietario	Custodio	Ubicación Tipo	Ubicación Lugar	Requisitos legales	Frecuencia de Uso	Sensibilidad	Valor del activo C	I	D	Valo	Nivel de Tasación
Activos de Información Primarios																
P0001	Activo primario X		I1 - Información electrónica				Física				Restringida	5	5	5	5.00	Muy Alto
P0002	Activo primario Y		I2 - Información escrita				Electrónica		LPDP		Confidencial	4	4	4	4.00	Alto
P0003			I3 - Información hablada								Uso Interno	3	3	3	3.00	Medio
P0004			I4 - Otro tipo de información								Público	2	2	2	2.00	Bajo
…												1	1	1	1.00	Muy Bajo
Activos de Soporte																
S0001	Base de datos XX		SW1 - Software comercial o												12	Muy Alto
S0002	Aplicación local XX		SW2 - Software desarrollado por												8	Alto
S0003	Servidor de aplicaciones XX		FI1 - Equipo de procesamiento												14	Alto
S0004	Caja Fuerte		FI4 - Mobiliario y equipamiento												8	Bajo
…																

Anexo 13 Relaciones entre los elementos del Análisis de Riesgos



Anexo 14 Nivel de Amenaza

Nivel de amenaza	Descripción	Valor
Raro	Nunca ha ocurrido en la empresa	1

Nivel de amenaza	Descripción	Valor
Improbable	Ha sucedido alguna vez	2
Moderado	Una vez al año	3
Probable	Una vez al mes	4
Casi certeza	Una o más veces a la semana	5

Elaboración propia

Anexo 15 Niveles de Vulnerabilidad

Nivel de vulnerabilidad	Descripción	Valor
Raro	Nunca ha ocurrido en la empresa	1
Improbable	Ha sucedido alguna vez	2
Moderado	Una vez al año	3
Probable	Una vez al mes	4
Casi certeza	Una o más veces a la semana	5

Elaboración propia

Anexo 16 Valor del control

$$\text{Valor Control} = \left((\text{Valor diseño})*40\% + (\text{Valor ejecución})*60\% \right)$$

Anexo 17 Efectividad del control

$$\text{Valor de efectividad del Control} = \left(\sum \text{Valor del Control x Peso del Control} \right)$$

Anexo 18 Matriz de riesgos

Anexo 19 Niveles de Riesgo

Riesgo	Descripción
Extremo	Riesgo extremo (no deseable): requiere acción de manera inmediata o de corto plazo, para aceptar, mitigar, transferir o evitar el riesgo, que será aprobado por el Comité de Riesgo Operacional
Alto	Riesgo alto (no deseable): requiere acción de corto o mediano plazo, para aceptar, mitigar, transferir o evitar el riesgo, que será aprobado por el Comité de Riesgo Operacional
Moderado	Riesgo moderado: son aceptados dentro del apetito de riesgos de la Organización y no requieren tratamiento adicional.
Bajo	Riesgo bajo: son aceptados dentro del apetito de riesgos de la organización y no requieren tratamiento adicional.

Anexo 20 Valor de la Frecuencia

$$\text{Valor de la frecuencia} = \frac{\text{Valor de la vulnerabilidad} + \text{Valor de la amenaza}}{2}$$