POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

SURA ASSET MANAGEMENT CHILE

POLÍTICA TRANSVERSAL

Tabla de contenido

Glosario de Términos

Oficial de Seguridad de la Información (ISO por sus siglas en inglés): Es el responsable de implementar y supervisar el cumplimiento de la presente Política de Seguridad de la Información y Ciberseguridad. Además, es el responsable de planificar, desarrollar, controlar y gestionar procedimientos y acciones con el fin de mejorar la Seguridad de la Información y Ciberseguridad, dentro de los pilares fundamentales de Confidencialidad, Integridad y Disponibilidad.

Políticas de Seguridad de la Información: Conjunto de directivas, regulaciones, reglas y prácticas que prescriben como la organización administra, protege y distribuye la información. Fuente: SP 800-53, SP 800-37, SP 800-18, CNSSI-4009.

Seguridad de la Información: La protección de la información y sistemas de información contra accesos, uso, divulgación, disrupción, modificación o destrucción no autorizados, con el fin de proveer confidencialidad, integridad y disponibilidad. Fuente: SP 800-37, SP 800-53, SP 800-53A, SP 800-18, SP 800-60, CNSSI-4009, FIPS 200, FIPS 199, 44 U.S.C., Sec. 3542

Clasificación de la Información: Proceso que permite determinar cualitativamente el valor o la criticidad de un activo de información, en términos de seguridad de la información. Fuente ISO/IEC 27000:2013

Activo de Información: Cualquier información o medio relacionado con su tratamiento que tenga valor para la organización y que debe ser protegida en términos de confidencialidad, integridad y disponibilidad. Fuente: ISO/IEC 27000:2013

Propietarios de Información (Asset Owner): Son los responsables de la información y de los procesos que la manipulan, sean estos manuales, mecánicos o electrónicos. Deben participar activamente en la clasificación de los activos de la información para el negocio, de manera que se puedan definir los controles apropiados para protegerla.

Acceso: Capacidad para hacer uso de cualquier recurso de un sistema de información. Fuente: SP 800-32

Control de Acceso: El proceso para garantizar o negar peticiones específicas para: 1) obtener y usar información e información relacionada al procesamiento de servicios; y 2) ingresar hacia instalaciones físicas específicas (Ej. Edificios federales, establecimientos militares, entradas fronterizas). Fuente: FIPS 201; CNSSI-4009

Capacidad y medios para comunicase o bien interactuar con un sistema, utilizar recursos del sistema para manejar información, para ganar conocimiento de la información que un sistema contiene, o para controlar componentes y funciones de un sistema. Fuente: CNSSI-4009.

Ciberseguridad: Es el cambio de enfoque de las medidas de inteligencia de seguridad, de un enfoque reactivo a proactivo, para hacer frente a las distintas amenazas internas/externas sobre los activos (digitales) y operaciones de una organización. Fuente: World Economic Forum

También, es la protección de activos de información a través de la gestión de amenazas a la información procesada, almacenada y transportada a través de sistemas de información interconectados. Fuente: ISACA – Cybersecurity Fundamentals Glossary.

Cifrado: Conversión de texto plano en texto cifrado a través del uso de algoritmos criptográficos. Fuente: FIPS 185

Alternativamente, el proceso de cambiar texto plano en texto cifrado con los propósitos de seguridad y privacidad. Fuente: SP 800-21, CNSSI-4009

Concienciación y Capacitación en Seguridad: Explica las reglas apropiadas de comportamiento en el uso de información y sistemas de información. El programa comunica las políticas y procedimientos de seguridad que deben ser seguidos. Fuente: SP 800-50

Evento de seguridad de la información: Materialización de un riesgo de seguridad de la información y ciberseguridad no deseado con efectos negativos poco relevantes para la compañía.

Incidente de seguridad de la información: Materialización de un riesgo de seguridad de la información y ciberseguridad no deseado con efectos negativos considerables para la compañía.

Amenaza: Cualquier peligro potencial que pueda ser la causa de un incidente o evento no deseado que ocasiona daños o perjuicios a la información de la compañía.

Vulnerabilidad: Debilidad de un activo o ausencia de un control de seguridad de la información y ciberseguridad, que puede ser explotado por una o más amenazas informáticas.

Control de Seguridad de la Información: Toda acción que tiende a minimizar los riesgos de Seguridad de la información, Ciberseguridad y/o del ambiente de TI, proporcionando seguridad razonable a la información del negocio para el logro de sus objetivos.

SGSI: Sistema de Gestión de Seguridad de la Información.

Grupos de Interés: para el cumplimiento de nuestro propósito e impactar de modo positivo a nuestro entorno, Sura tiene definido como grupos de interés externos los siguientes: Clientes, Academia y gremios, Líderes de opinión, Proveedores, Estado y reguladores, medios de comunicación y Comunidad. Para efectos de los grupos de interés internos se cuenta con: Colaboradores, Accionistas e Inversionistas y directores.
Las partes interesadas esperan del SGSI de Sura, un manejo responsable de la información, y que en el desarrollo de su gestión, haya sido suministrada, procesada, almacenada o transferida por la entidad de forma segura en todo el ciclo de vida de esta. Adicionalmente las partes interesadas creen en que a través del establecimiento, implementación y mejora continua del SGSI, la entidad asegurará la integridad, disponibilidad y confidencialidad de la información, y el cumplimiento estricto de los requisitos legales, contractuales, regulatorios y normativos.

Definiciones asociadas a la gestión de riesgos de información

Riesgo de Seguridad de la Información y Ciberseguridad: Es la posibilidad de materialización de un evento no deseado, relacionado con la seguridad de la información que pueda afectar el logro de nuestras metas y objetivos.

Riesgo Inherente: Riesgo antes de la existencia de controles que lo mitigan.

Riesgo Residual: Riesgo remanente luego de considerar los controles (mitigantes).

Gestión de Riesgos de Seguridad de la Información, Ciberseguridad: Identifica los riesgos, amenazas y vulnerabilidades de la información y del ambiente de TI; evalúa y determina el impacto atribuible a la confidencialidad, integridad y disponibilidad en el negocio.

Apetito de Riesgo: Es el nivel máximo de riesgo aceptado por la Compañía a fin de lograr los objetivos del negocio para el conjunto de eventos que se puedan materializar. El apetito de riesgo de la compañía es un Nivel Medio.

1. Introducción

La información, aplicaciones, bases de datos e infraestructura tecnológica (*TI*) que soportan a los procesos de negocio son activos importantes de Sura, y tal como otros activos de información importantes, deben ser protegidos. La Integridad, Confidencialidad, Disponibilidad y Privacidad de los activos de Información son esenciales para mantener nuestra ventaja competitiva, al momento de entregar un servicio de calidad a los clientes (*Externos e Internos*), dando como resultado una mayor rentabilidad al negocio y sustentabilidad a Sura, siempre cumpliendo con las normativas legales, industriales y gubernamentales.

La defensa y protección de los activos de información es una tarea esencial para asegurar la continuidad y el desarrollo de los objetivos de Sura, así como para mantener el cumplimiento normativo y regulatorio aplicable, además genera confianza a las partes interesadas. Cuanto mayor es el valor de la información, mayores son los riesgos asociados a su pérdida, deterioro, manipulación indebida o malintencionada. Por lo anterior, Sura ha establecido un Sistema de Gestión de Seguridad de la Información (SGSI) el cual al adopta una metodología para la identificación y valoración de los activos de información, y una metodología para la evaluación y tratamiento de los riesgos; siendo éste el medio más eficaz de tratar, gestionar y minimizar los riesgos, considerando el impacto para la entidad y los grupos de interés.

Así mismo, el SGSI define políticas y procedimientos eficaces y coherentes con la estrategia de la entidad, como desarrollo de los controles adoptados para el tratamiento de los riesgos, los cuales están en continuo seguimiento y medición, a través del establecimiento de indicadores que aseguran la eficacia de los controles; apoyado en los programas de auditoría y la revisión por la dirección, que concluyen en la identificación de oportunidades de mejora las cuales son gestionadas para mantener la mejora continua del SGSI.

En este contexto, una cultura que permita y apoye una correcta gestión de la información es también un tema central, por lo que desarrollar esa característica en todos los colaboradores es fundamental para que los lineamientos que se deriven de esta política permeen a toda la organización.

2. Objetivo

Establecer los lineamientos en materia de seguridad de la información y ciberseguridad, para preservar la confidencialidad, integridad y disponibilidad de la información en Sura, de sus Clientes, colaboradores y de sus proveedores.

2.1 Objetivo del SGSI

De acuerdo con la definición de los grupos de interés, definidas en puntos anteriores, la cual se encuentra alienada al objetivo estratégico de Sura, podemos definir como los objetivos del SGSI como las siguientes:

- ✓ Garantizar la confidencialidad, integridad y disponibilidad de la información en Sura para todos sus clientes, colaboradores y proveedores definidos dentro del alcance.
- ✓ Generar planes de continuidad operativa de los Servicios y/o procesos de Sura, que nos permitan mantener la continuidad efectiva al negocio cuando suceden contingencias (como, por ejemplo: desastres y se pierde la conectividad de sistemas de Información, instalaciones, personas, Ciberataques etc.), permitiéndonos seguir trabajando, en forma transparente a clientes y usuarios.
- ✓ Incorporar dentro de los nuevos servicios implementados y de los servicios y/o procesos ya definidos en Sura la seguridad de la información en todo el proceso.
- ✓ Velar por el cumplimiento de las obligaciones legales, reglamentarias y contractuales de la compañía.
- ✓ Mantener un ambiente de control interno adecuado.
- ✓ Velar por la protección de los activos de Información críticos de la compañía.
- ✓ Proteger a la infraestructura y los procesos de Sura ante riesgos que afecten la seguridad de la información.
- ✓ Demostrar a inversionistas e interesados que se protege adecuadamente la información y las tecnologías empleadas para los negocios de la empresa, de acuerdo con el estándar ISO/IEC 27001:2013.

2.2 Objetivo de la gestión de riesgos de seguridad de la información

Describir el detalle de los procedimientos necesarios para elaborar una evaluación de riesgos adecuada para los riesgos de la Compañía, junto con garantizar el cumplimiento de los lineamientos definidos en la presente política, así como mantener un proceso de gestión de riesgos de seguridad de la información y ciberseguridad adecuado, incluyendo la clasificación de la información de la empresa y valoración del impacto en el negocio.

3. Ámbito

El ámbito de esta Política incluye las directrices de tratamiento de los activos de información y las revisiones del cumplimiento de éstas. Además, de contar con los procedimientos necesarios para asegurar la Integridad, Confidencialidad y Disponibilidad de los activos de información de acuerdo con estándares internacionales y las leyes chilenas. Dicha política se encuentra alineada al marco regional MSIC (Modelo de seguridad de la Información y Ciberseguridad).

El SGSI debe cumplir con la regulación vigente en materias de seguridad de la información y ciberseguridad asociadas a la legislación local, como las siguientes leyes: Ley N°19.799, de abril 2012 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, Ley N°19.223, de junio 1993 tipifica figuras penales relativas a la informática, delitos informáticos, sistemas de información, Ley N°19.628, de agosto 1999 sobre protección de la vida privada y derecho a la privacidad y la nueva Ley N°21.459 sobre delitos informáticos publicada el 20 de junio del 2022.

4. Alcance de la Política.

Para efectos de los lineamientos de seguridad de la información aplica a todos los colaboradores, clientes y proveedores involucrados operativamente y/o funcionalmente en los procesos.

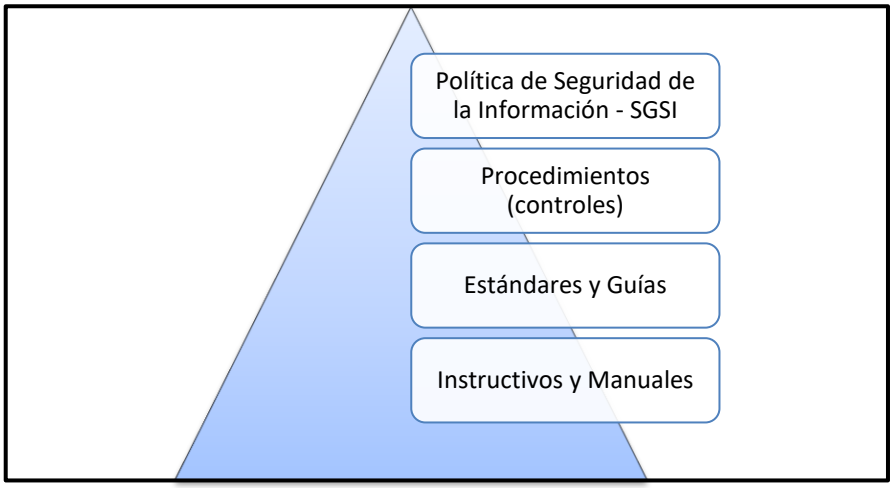
Para efectos de la gestión de riesgos de información, estos aplican de forma interna para Sura (análisis y evaluación de los riesgos de información y culmina con la valoración de los mismos a nivel de la operación del negocio).

5. Documentación de la política

El presente documento deberá ser revisado sobre una base anual o toda vez que exista un cambio mayor (modificación al documento que sea de fondo y no de forma). Estas revisiones/actualizaciones, serán presentadas al Comité de Riesgo Tecnológico, Seguridad de Información y Ciberseguridad, Comités de Riesgo y Directorios.

El control de las actualizaciones es registrado en cuadro "*hoja de modificaciones*", al final de este documento.

Los procedimientos, estándares e instructivos de Seguridad de la Información se apoyan en la Política de seguridad de la Información de Sura. Estos documentos describen en forma específica una actividad o un proceso, para crear o modificar documentos se sigue lo descrito en el Procedimiento 0177 CA Procedimiento Elaboración y actualización de documentos



Política de Seguridad de la Información y Ciberseguridad

Generales

Sura está comprometida con la Gestión de la Seguridad de Información y Ciberseguridad en todos sus aspectos, impulsando una cultura de protección de la información, a fin de asegurar la confidencialidad, integridad y disponibilidad de la información propia y de terceros, cumpliendo el marco normativo y legal, lo cual es gestionado mediante el sistema de gestión de Seguridad de la Información.

Sura diseña y ejecuta estrategias para prevenir, controlar y reducir riesgos que puedan afectar la operación de la compañía, por ende, los intereses de sus clientes. Sura reconoce que la información es uno de los activos más importantes para cumplir las funciones y objetivos que han sido definidos por la compañía, de ahí la importancia de realizar un análisis del contexto interno y externo de la entidad, con relación a seguridad de la información, para identificar cuáles son los riesgos que pueden o afectan su capacidad para lograr los resultados esperados frente al SGSI; así como identificar cuáles son las necesidades y expectativas de las parte interesadas.

Sura dentro del SGSI evaluará de forma permanente el contexto externo e interno de la organización dentro del modelo de gestión y presentando al menos de forma anual el análisis del contexto en el directorio de la compañía. El análisis del contexto interno y externo deberá contar con instancias para identificar, evaluar y tratar los riesgos de forma oportuna, usando planes de tratamientos establecidos en la metodología de la gestión de riesgos de Seguridad

de la Información y Ciberseguridad. Se establece que para efectos del contexto interno se deben considerar, aspectos administrativos, de comercialización, de recursos humanos, operacionales, financieros, de investigación, culturales y tecnológicos entre otros. Para efectos del contexto externo se deben considerar, aspectos políticos, sociales, tecnológicos, legales, ambientales y sanitarios, entre otros.

6. Organización de Seguridad de la Información y Ciberseguridad

6.1. Organización Interna

6.1.1. Roles y Responsabilidades de la seguridad de la Información

Comité de Riesgos Tecnológico, Seguridad de la Información y Ciberseguridad

En su calidad tal, dicho Comité responde ante la Alta Administración, por la existencia y cumplimiento de las medidas orientadas a mantener un nivel de Seguridad de la Información y Ciberseguridad acorde con las necesidades de Sura.

Este comité cuenta con un estatuto, el cual define el alcance, sus miembros, gobierno, funciones, entre otros. Parte de sus funciones del comité son:

- Revisar, evaluar y pre aprobar actualizaciones a esta Política.
- Monitorear el desarrollo y mantenimiento del BCP.
- Temas relevantes relacionados con Seguridad de la Información y Ciberseguridad.
- Seguimiento a las observaciones Tecnológicas de Auditoria Interna y Externa.
- Seguimiento de Incidentes Tecnológicos.
- Seguimiento a los avances en temas de Ciberseguridad.
- Monitoreo y seguimiento de las métricas de seguridad.

Mensualmente el Comité de Riesgo Tecnológico, Seguridad de la Información y Ciberseguridad, sesionará con el objetivo de analizar y evaluar los eventos de Riesgos de Seguridad de la Información y Ciberseguridad y los resultados de los análisis y monitoreos realizados, así como nuevas actividades o cambios en los procesos o avances en proyectos y/o iniciativas en materia de ciberseguridad.

Comité de Riesgos

Dar seguimiento a cualquier proceso, evento o incidente de Ciberseguridad y Seguridad de la información que deba ser reportado a la alta administración, en este mismo comité o directorio, desde el comité de riesgo tecnológico.

Directorio

Aprobar la Política de Seguridad de la Información y Ciberseguridad y sus modificaciones para asegurar que la compañía vele porque exista una adecuada gestión del riesgo de Seguridad de la información y por el cumplimiento de los requisitos de los grupos de interés.

Oficial de Seguridad de la Información (ISO)

- Realizar un monitoreo de cumplimiento de la política de Seguridad basados en la información que arrojan los controles de Seguridad de esta Política
- Evalúa los sistemas, procesos y procedimientos mecanizados existentes en relación con su confiabilidad y eficacia, incluyendo la adecuada utilización de los equipos.
- Responsable de capacitar, supervisar y asesorar a los colaboradores de Sura en temas relacionados a Seguridad de la Información y Ciberseguridad.
- Implica la responsabilidad de mantener un nivel adecuado de protección de la información de la compañía, orientando la gestión a cumplir los objetivos de integridad, confidencialidad y disponibilidad de la Información.
- Planificar, desarrollar, controlar y gestionar las políticas y acciones con el fin de mejorar la Seguridad de la Información dentro de sus pilares fundamentales de confidencialidad, integridad y disponibilidad.
- Soporte (con su equipo) a las áreas de Sura en la identificación de riesgos claves y mejoramiento de procesos, así como en la mitigación de riesgos según las mejores prácticas de seguridad del mercado, la normativa vigente y siguiendo las bases de los requerimientos de la compañía.
- Asesoría a la primera línea en la interpretación de Políticas de Seguridad de la Información y Ciberseguridad, dictar lineamientos de Seguridad en general, así como en las acciones mitigatorias.

Colaboradores de Sura

Dar estricto cumplimiento a las directrices establecidas en la presente política y los procedimientos establecidos sobre esta materia, entendiendo que es el principal actor, responsable y motor en la prevención de incidentes de seguridad, que puedan afectar el normal desenvolvimiento de la compañía.

Además, tienen la obligación de alertar de manera inmediata a su jefatura directa y al ISO de la Compañía (cibex@sura.cl), cualquier situación que atente contra lo establecido en esta política o pueda poner en riesgo la Seguridad de la Información, junto con realizar y asistir a todas las concientizaciones que se dicten por parte de Sura en términos de seguridad de la Información y Ciberseguridad.

Propietarios de Información (Asset Owner)

Son los responsables de la información y de los procesos que la manipulan, sean estos manuales, mecánicos o electrónicos. Deben participar activamente en la clasificación de los activos de la información para el negocio, de manera que se puedan definir los controles apropiados para protegerla.

Custodio de la Información

Es cualquier persona que mantiene bajo su responsabilidad información de la cual no es el Propietario. Es responsable de aplicar las medidas de seguridad que se definan de acuerdo con la clasificación de los activos de información.

6.1.2. Segregación de funciones

Segregación de áreas generales

Esta Política es administrada por el modelo de Gobierno Corporativo asumido por esta Compañía, reflejado en el siguiente esquema

Cada línea de defensa tiene funciones y responsabilidades específicas y trabajan en estrecha colaboración para identificar, evaluar y mitigar los riesgos de seguridad de la información y ciberseguridad respecto de los objetivos de negocio y las operaciones de SURA. Considerando lo anterior, las funciones y responsabilidades para cada línea de defensa se entenderán de la siguiente manera:

• 1ra Línea de Defensa: Posee y gestiona los riesgos de seguridad de la información y ciberseguridad, a la vez que desarrolla, implementa y ejecuta diariamente los controles definidos para abordar las deficiencias de control y mitigar los riesgos de seguridad de la información y ciberseguridad, a su vez asumen las consecuencias de las afectaciones ocasionadas por los riesgos que sean materializados.

• 2da Línea de Defensa: Ayuda a formular las estrategias, políticas y estructuras organizacionales que permitan administrar los riesgos de seguridad de la información y ciberseguridad. Realiza actividades de monitoreo. Identifica, en conjunto con la 1ra línea de

defensa, las necesidades, regulaciones y políticas aplicables. Identifica y transmite las leyes, regulaciones y normas emitidas en materia de seguridad de la información y ciberseguridad, y monitorea su cumplimiento.

• 3ra Línea de Defensa: Auditoría Interna (Evaluación del Sistema de Control) proporciona una evaluación independiente del diseño y efectividad de los controles internos sobre los riesgos de seguridad de la información y ciberseguridad, para el desempeño del negocio. Adicionalmente, provee recomendaciones específicas para mejorar el proceso de gestión de seguridad de la información y ciberseguridad, en alineación al Gobierno y Gestión del Riesgo en Sura.

Más detalle sobre la gestión de riesgos de información se encuentra en anexo 1 Gestión Riesgos Seguridad de la Información y Ciberseguridad.

Segregación de áreas tecnológicas y operacionales

En Sura existen funciones y áreas con responsabilidades segregadas para reducir los riesgos de modificaciones no autorizadas, mal uso de la información o los servicios (deliberadas o accidentales), por falta de independencia en la ejecución de funciones críticas.
También, existe una estructura organizacional divida acorde a los roles y funciones, con recursos dedicados.
El área de tecnología está dividida en 3 áreas: Gestión de aplicaciones, Proyectos tecnológicos, Servicios y operaciones IT. Por otro lado, se encuentran los usuarios de las áreas operativas quienes son los responsables de explotar y operar los sistemas desarrollados y mantenidos por el área de tecnológica.

6.2. Dispositivos móviles y Teletrabajo.

6.2.1. Política de dispositivos móviles

Sura cuenta con una política de dispositivos móviles, la cual define lineamientos específicos para gestionar los riesgos presentados al usar dispositivos móviles y la seguridad de la Información en el uso de computación móvil para el personal autorizado.

La computación móvil se define como los equipos portátiles end point (Notebook, Netbook, celulares y/o smartphone, Tablets, otros) utilizados por los usuarios.

6.2.2. Trabajo Remoto

Sura ha implementado procedimientos que aplican controles de seguridad en relación con los riesgos específicos que presentan modalidades de trabajo remoto, con el objetivo de proveer seguridad a la información.

7. Seguridad de los Recursos Humanos

El área de Talento Humano incluye las funciones relativas a la Seguridad de la Información y Ciberseguridad en las descripciones de puestos de los colaboradores e informará a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de esta Política, gestionará los compromisos de confidencialidad con el personal y coordinará las tareas de capacitación de usuarios.

7.1. Previo al empleo

7.1.1. Selección

El área de Talento Humano cuenta con los procedimientos adecuados para el proceso de selección de candidatos tanto externo e interno, los cuales cumplen con las leyes, regulaciones y normas éticas pertinentes a Seguridad de la Información.

7.1.2. Términos y condiciones de la relación laboral

Como parte de las obligaciones contractuales, colaboradores, proveedor y externos, acuerdan y suscriben los términos y condiciones de la relación con Sura, entre los cuales se incluyen las responsabilidades y sanciones respecto de la seguridad de la información.

El responsable del Área de Recursos Humanos debe informar a todo el personal que ingresa a la organización de sus obligaciones respecto del cumplimiento de la Política y Normas de Seguridad de la Información.

Los términos y condiciones de empleo reflejan la política de seguridad de Sura, además de aclarar y enunciar:

a) que todos los colaboradores, proveedor y usuarios de terceras partes a los cuales se les dé acceso a información sensible, deben firmar un acuerdo de confidencialidad o de no-divulgación, previamente a ser otorgado el acceso a las instalaciones de procesamiento de información

b) las responsabilidades y derechos legales de colaboradores, proveedor y otros usuarios, en especial las relativas a derechos de copia o legislación de protección de datos

c) responsabilidades para la clasificación de información y gestión de activos de la Organización asociados a sistemas y servicios de información administrados por el empleado, el proveedor o el usuario de terceras partes

d) responsabilidades del empleado, proveedor o usuario de terceras partes por la administración de información recibida de otras organizaciones o partes externas

e) acciones a ser tomadas si el empleado, proveedor o usuario de terceras partes, desatiende los requisitos de seguridad de la Organización

7.2. Durante el empleo

La alta administración es responsable de asegurar que la seguridad se aplica a lo largo del empleo de un individuo dentro de la organización. Para ello, se provee a todos los colaboradores, proveedor y terceras partes interesadas un nivel adecuado de concientización, educación, y formación en procedimientos de seguridad y en el uso correcto de instalaciones de procesamiento de información, con el fin de minimizar los posibles riesgos de seguridad.

Por otra parte, durante el periodo de duración del contrato de empleo o de servicios, las normas y procedimientos deben asegurar, que los colaboradores, proveedor y usuarios de terceras partes, estén conscientes de las amenazas y vulnerabilidades de seguridad, de sus responsabilidades y obligaciones, y estén equipados para cumplir la política de seguridad de la Organización en el curso de su trabajo normal, y para reducir el riesgo de errores humanos.

7.3. Desvinculación y cambio de empleo

Se deben definir y asignar con claridad las responsabilidades ante la finalización o cambio de las relaciones contractuales con colaboradores, proveedor y terceros.

Las responsabilidades y obligaciones subsistentes con posterioridad a la terminación del empleo deben estar incluidas en los contratos de los colaboradores, proveedor y externos.

El cambio de responsabilidades o empleo dentro del ámbito de Sura no significa que deban superponerse los privilegios de ambas funciones, sino que debe manejarse como la finalización de una responsabilidad y el inicio de una nueva bajo los términos de los controles pertinentes para las nuevas funciones.

8. Administración de Activos de Información

Los dueños de activos de información son los encargados de clasificarla de acuerdo con su grado de sensibilidad y criticidad, y mantener actualizada la clasificación efectuada, además de definir las funciones que deberán tener permisos de acceso a la información.

El ISO de Sura es el encargado de asegurar que los lineamientos para la utilización de los recursos de la tecnología de información contemplen los requerimientos de seguridad establecidos según la criticidad de la información que procesan.

Cada dueño de activo de información supervisará que el proceso de clasificación y rótulo de información de su área de competencia sea realizado de acuerdo con lo establecido en la presente Política.

8.1. Inventario de activos

Se deben identificar todos los activos asociados a cada sistema de información, sus respectivos propietarios y su ubicación, ya sean físicos o lógicos. Además, se debe elaborar un inventario con dicha información. El mismo será actualizado ante cualquier modificación de la información registrada y revisado con una periodicidad no mayor a 1 año.

El dueño del activo de información es el responsable de gestionar la identificación y clasificación de los activos de información de la compañía, por otro lado, el área de tecnológica es el responsable de mantener el inventario de Activos de Información de Sura, junto con la implementación de controles de seguridad en base a la clasificación para el resguardo de la información.

8.2. Clasificación de los Activos de Información

La clasificación de los activos de información debe efectuarse con base en los niveles de Confidencialidad, Integridad y Disponibilidad que se desea proteger en los activos, de acuerdo con la política de clasificación de activos de Sura.

9. Control de Acceso

9.1. Administración de Accesos de Usuarios

Se definirá un proceso de administración de acceso a los sistemas, datos y servicios de información, así como un equipo responsable del proceso. El proceso debe documentarse y considerar la aprobación de los dueños de los sistemas para la creación de cuentas y asignación de permisos.

9.2. Registro de Usuarios

El área de tecnología debe definir un procedimiento formal de registro de usuarios para otorgar, modificar y revocar el acceso a todos los sistemas, bases de datos, red y servicios de información de Sura.

9.3. Administración de Permisos de Acceso a los Sistemas de Información

Los dueños del activo de información deben aprobar el acceso a los sistemas de los que son responsables, así como de la asignación de los perfiles o permisos mínimos necesarios para cumplir las funciones de sus cargos. El área de tecnología otorgará los accesos según las autorizaciones realizadas.

9.4. Administración de Cuentas de Usuario

La asignación de cuentas se controlará a través de un proceso de administración formal. El área de tecnología es el responsable de documentar los controles adecuados, el Oficial de Seguridad de la Información por otro lado debe monitorear el cumplimiento de los controles diseñados por el área de tecnología

9.4.1. Administración de cuentas Privilegiadas

Existen cuentas de usuarios con las cuales es posible efectuar actividades críticas, por ejemplo, la instalación de plataformas o sistemas, habilitación de servicios, actualización de software, etc. Dichas cuentas no serán de uso habitual (diario), sino que sólo serán utilizadas ante una necesidad específica para realizar alguna tarea que lo requiera y se encontrarán protegidas por contraseñas con un mayor nivel de complejidad, la cual tendrá como mínimo exigido, 10 caracteres, con uso de mayúsculas y minúsculas, alfanumérico y caracteres especiales.

9.4.2. Revisión de Cuentas de Acceso

A fin de mantener un control eficaz del acceso a los datos y servicios de información, el Asset Owner debe llevar a cabo un proceso formal de revisiones, a lo menos una vez al año calendario, a fin de revisar las cuentas de accesos de los usuarios internos y externos, como mínimo para las aplicaciones de negocio clasificadas como altas o críticas.
Además, el Asset Owner y dueños plataformas debe validar a los usuarios que accesos a sus sistemas, con una periodicidad anual.

9.5. Responsabilidades del Usuario

9.5.1. Uso de Contraseñas

Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas y cumplir las reglas que se impartan para tales efectos. El mínimo exigido en la complejidad de contraseñas para este tipo de cuentas será: 10 caracteres, con uso de mayúsculas y minúsculas, alfanumérico y caracteres especiales.
Además, queda estrictamente prohibido compartir las contraseñas personales, siendo definido como una falta grave, tanto para el colaborador que las comparte como para el colaborador que accede a los sistemas con credenciales ajenas.

10. Criptografía

El área de tecnología es la responsable de implementar herramientas y técnicas criptográficas para la protección de la información, con base en las definiciones de control sobre los activos de información que determinen los propietarios de la información y el ISO con el fin de asegurar

una adecuada protección de su confidencialidad e integridad y disponibilidad solo para personas autorizadas para estos efectos.

Se deben ofuscar o encriptar de acuerdo a cada todos los datos sensibles del negocio como por ejemplo datos personales, contraseñas, cotizaciones de clientes, información estratégica de Sura.

10.1. Política sobre el uso de controles Criptográficos

Sura cuenta con procesos sobre el uso de controles criptográficos para la protección de la información sensible, ya sea información en la red (transito), almacenada en bases de datos o log.

10.2. Privacidad de Datos de Clientes

La Gerencia de Riesgos en conjunto con la Alta Gerencia y los Dueños de la Información deberán definir el apetito de riesgo de la Compañía en el ámbito del resguardo de la privacidad de datos de los clientes. Se deben acordar los alcances y procedimientos de disociación de datos personales de manera que la información que se obtenga no pueda asociarse a una persona determinada.

El área de tecnología es la responsable de implementar las herramientas de despersonalización de los datos de clientes en ambientes de desarrollo y QA, de acuerdo a lo definido, así como de la gestión del proceso de despersonalización de datos definido por el marco de gobierno de privacidad, de manera de proteger la información privada de los clientes en dichos ambientes.

10.3. Gestión de claves

Sura cuenta con un proceso sobre el uso, protección y vida útil de las claves criptográficas.

10.4. Parámetros mínimos de duración y rotación de claves en distintas plataformas.

Sura cuenta con una Política para la configuración de claves del Active Directory, la cual debe tener 10 caracteres, 60 días de duración y no se pueden utilizar las ultimas 10 contraseñas utilizadas anteriormente, esta política aplica para todas las plataformas que se autentican contra el AD, a excepción de aquellas plataformas que tengan una configuración distinta y no se autentiquen contra el AD.

11. Seguridad Física y del Ambiente

11.1. Perímetro de Seguridad física

Sura cuenta con procedimientos de acceso físico adecuado para el acceso físico casa matriz como a sucursales de Sura, gestionado por el área de administración, estos cuentan con los controles adecuados para el acceso físico y de factores medioambientales.

Por otro lado, para el acceso físico al datacenter provisto por IBM, estos son gestionados por el área de tecnología, y a su vez IBM cuenta con procedimientos específicos para el

acceso a este, también se consideran controles para el acceso físico y medioambientales para el resguardo de los servicios prestados por IBM.

11.2. Equipamiento

El equipamiento es ubicado y protegido para reducir los riesgos ocasionados por amenazas y peligros ambientales y oportunidades de acceso no autorizado.

Los controles definidos por el área de tecnología para el equipamiento son provistos por el proveedor para el caso de servidores productivos, de desarrollo y control de calidad.
Para el caso de la casa matriz y sucursales son provistos por el área de administración, dentro de los controles que se consideran para ambos casos, podemos señalar los siguientes:

- Suministro de energía
- Seguridad del cableado
- Mantenimiento del equipo (detectivo, preventivo y correctivo)

11.3. Escritorios y Pantallas Limpias

Se adopta una política de escritorios limpios para proteger documentos en papel y dispositivos de almacenamiento removibles y una política de pantallas limpias en las instalaciones de procesamiento de información, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo.

Toda vez que un funcionario o externo se ausente de su lugar de trabajo, junto con bloquear su estación de trabajo, debe guardar en lugar seguro cualquier documento, medio magnético u óptico removible que contenga información confidencial o sensible.

12. Seguridad de las Operaciones

Establecer responsabilidades y procedimientos para su gestión y operación, incluyendo instrucciones operativas y seguridad de las instalaciones de procesamiento de la información.

12.1. Procedimientos y Responsabilidades Operativas

12.1.1. Documentación de los Procedimientos Operativos

Se debe documentar y mantener actualizados los procedimientos, sus cambios deberán ser autorizados.

12.1.2. Control de Cambios en las Operaciones

Deben existir procedimientos para el control de los cambios en el ambiente operativo y de comunicaciones. Todo cambio deberá ser evaluado previamente en aspectos técnicos y de seguridad. El ISO participará activamente del comité que apruebe los cambios a las plataformas tecnológicas procurando que no comprometan la seguridad de estos ni de la información que soportan.

12.1.3. Separación entre Ambientes

El área de tecnología debe asegurar que los ambientes de Desarrollo, QA y Producción estén separados, y se definirán y documentarán las reglas para la transferencia de software entre los distintos ambientes.

12.2. Protección contra código malicioso

12.2.1. Controles contra código malicioso

Sura cuenta con controles de detección, prevención y recuperación para proteger los activos de información contra código malicioso, junto con los procedimientos adecuados.

12.3. Respaldos

12.3.1. Respaldos de Información

Sura cuenta con procedimientos para el respaldo de información, el que contemple las copias de respaldo y pruebas de recuperación de la información, de acuerdo con un procedimiento de respaldo necesaria para el negocio.

12.4. Registro y monitoreo

Sura cuenta con los registros de eventos de las actividades sobre plataforma y actividades del cliente.

Estos registros son protegidos adecuadamente para realizar seguimiento de eventos de seguridad de la información

12.4.1. Sincronización de relojes

Todos los relojes de los sistemas de información y las plataformas que lo soportan de Sura se encuentran sincronizados a una sola fuente horario, con el fin de poder realizar un seguimiento y gestión adecuada ante una falla de seguridad de la información.

12.5. Control del software de operacionales

12.5.1. Instalación del software en sistemas operacionales

Sura cuenta con procedimientos para el control en la instalación de software en los sistemas operacionales.

12.5.2. Lineamientos para software de escritorios

Sura tiene como lineamiento que todo software escritorio debe estar integrado con la herramienta Active Directory. SAAS = Software as a Service.

12.6. Gestión de vulnerabilidades técnicas

12.6.1. Gestión de las vulnerabilidades técnicas

El área de tecnología es el responsable de obtener la información acerca de las vulnerabilidades técnicas de los sistemas de información usados, evalúa la exposición de la organización a esas vulnerabilidades y toma las medias apropiadas para abordar el riesgo asociado. Se presentan todas las vulnerabilidades altas y críticas en el comité de riesgos tecnológico para realizar el seguimiento.

12.6.2. Restricciones sobre la instalación de software

Sura cuenta con procedimientos para el control en la instalación de software por parte de los usuarios. Para esto existe un proceso formal de instalación de software, el cual realiza una evaluación del software por parte del área de IT e ISO para su autorización e instalación.

13. Seguridad de las Comunicaciones

13.1. Controles de Red

El área de tecnología definirá un proceso de administración de acceso a la red, así como un equipo responsable del proceso. El proceso debe documentarse y considerar el acceso a la red desde fuera de la organización.

13.2. Administración y Seguridad de los Medios de Almacenamiento

13.2.1. Administración de Medios de Almacenamiento Externo

El uso de medios de almacenamiento extraíbles será restringido a menos que una necesidad del negocio basada en un análisis de riesgo sea realizada, documentada y aprobada.

13.2.2. Eliminación de Medios de Información

El área de tecnología debe definir procedimientos para la eliminación segura de los medios de información respetando la normativa vigente. Realizándose previamente las respectivas copias de resguardo.

13.3. Seguridad del Correo Electrónico

13.3.1. Correo Electrónico

El área de tecnología junto con el ISO, deben definir y documentar normas y procedimientos claros con respecto al uso del correo electrónico, que incluya al menos los siguientes aspectos:

a) Protección contra ataques al correo electrónico, por ejemplo, virus, intercepción, etc.

b) Protección de archivos adjuntos de correo electrónico.

c) Retención de mensajes que, si se almacenaran, pudieran ser usados en caso de litigio.

d) Controles adicionales para examinar mensajes electrónicos de origen dudoso o sospechoso.

e) Aspectos operativos para garantizar el correcto funcionamiento (ej.: tamaño máximo de información transmitida y recibida, cantidad de destinatarios, tamaño máximo del buzón del usuario, etc.).

f) Definición de los alcances del uso del correo electrónico por parte de los colaboradores.

13.4. Sistemas de Acceso Público

El área de tecnología toma los recaudos pertinentes para la protección de la integridad, confidencialidad y disponibilidad de la información publicada electrónicamente, a fin de prevenir la modificación no autorizada.

13.5. Otras Formas de Intercambio de Información

El área de tecnología implementará normas, procedimientos y controles para proteger el intercambio de información.

14. Adquisición, Desarrollo y Mantenimiento de Sistemas

Requerimientos de Seguridad de los Sistemas

14.1.1. Análisis y Especificaciones de los Requerimientos de Seguridad

Se implementa para incorporar seguridad a los sistemas de información (propios o de terceros) y a las mejoras o actualizaciones que se les incorporen. Los requerimientos para nuevos sistemas o mejoras a los existentes especificarán la necesidad de controles. Estas especificaciones deben considerar los controles automáticos a incorporar a los sistemas de información, como así también controles manuales de apoyo dependiendo de su clasificación.

14.2. Seguridad en procesos de desarrollo y soporte

14.2.1. Controles de Procesamiento Interno

El área de tecnología debe definir un procedimiento para que, durante la etapa de diseño, se incorporen controles de validación a fin de eliminar o minimizar los riesgos de fallas de procesamiento.

14.2.2. Autenticación de Mensajes

El propietario de la aplicación debe asegurar que cuando una aplicación tenga previsto el envío de mensajes que contengan información clasificada como secreta, se implementen controles criptográficos en la trasmisión del mensaje.

14.3. Seguridad de los Archivos del Sistema

El área de tecnología debe garantizar que los desarrollos y actividades de soporte a los sistemas se lleven a cabo de manera segura, controlando el acceso a los archivos de este, de acuerdo con lo establecido en los siguientes 4 puntos.

14.3.1. Control del Software Operativo

Toda aplicación, desarrollada por Sura o por terceros, tendrá un único responsable designado formalmente.

Ningún programador o analista de desarrollo y mantenimiento de aplicaciones, podrá acceder a los ambientes de producción.

14.3.2. Protección de los Datos de Prueba del Sistema

Las pruebas de los sistemas se efectuarán sobre datos extraídos del ambiente de desarrollo. Para proteger los datos de prueba se establecerán normas y procedimientos a tal efecto.

14.3.3. Control de Cambios a Datos Operativos

Las modificaciones, actualizaciones o eliminaciones de los datos operativos serán realizadas de acuerdo con el esquema de control de cambios implementado.

14.3.4. Control de Acceso a las Bibliotecas de Código Fuente de las Aplicaciones

El área de tecnología definirá un proceso de gestión del versionamiento del código fuente, que incluya la administración de acceso del código fuente, así como un equipo responsable del proceso.

14.4. Seguridad de los Procesos de Desarrollo y Soporte de Aplicaciones

14.4.1. Procedimiento de Control de Cambios

El área de tecnología definirá un proceso de Control de Cambios a las Aplicaciones, así como un equipo responsable del proceso. El proceso debe documentarse, facultar la segregación de funciones incompatibles y considerar la aprobación de los dueños de las aplicaciones para la modificación de las aplicaciones.

14.4.2. Restricción del Cambio de Paquetes Cerrados de Software

Previamente a la modificación de paquetes de software suministrados por proveedores se deberá:

a) Analizar los términos y condiciones de la licencia a fin de determinar si las modificaciones se encuentran autorizadas.

b) Evaluar el impacto que se produce si Sura se hace cargo del mantenimiento.

15. Relaciones con los Proveedores

15.1.1. Desarrollo Externo de Software

Para el caso que se considere la tercerización del desarrollo de software, se establecerán normas y procedimientos que contemplen los siguientes puntos:

a) Acuerdos de licencias, propiedad de código y derechos conferidos.

b) Requerimientos contractuales con respecto a la calidad del código y la existencia de garantías.

c) Procedimientos de certificación de la calidad y precisión del trabajo llevado a cabo por el proveedor, que incluyan pruebas, revisión de código para validar uso de buenas prácticas de desarrollo, verificación del cumplimiento de los requerimientos de seguridad del software definidos, etc.

d) Acuerdos de custodia de los códigos fuentes que son propiedad del proveedor del software (y cualquier otra información requerida) en caso de quiebra o venta del proveedor que está realizando dicho desarrollo.

e) La arquitectura y códigos para utilizar por el proveedor.

16. Gestión de Incidentes de Seguridad de la Información y Ciberseguridad

16.1.1. Procedimientos de Manejo de Incidentes Tecnológicos

El área de tecnología debe establecer funciones y procedimientos de manejo de incidentes garantizando una respuesta rápida, eficaz y sistemática a los incidentes. El ISO, deberá estar presentes en todos los canales de información de incidentes.

16.2. Generar las instancias para asegurar el adecuado tratamiento a los incidentes que comprometan la Seguridad de la información y Ciberseguridad.

El área de tecnología en conjunto con el ISO debe contar con los adecuados canales de comunicación, que permitan conocer in situ los incidentes tecnológicos que comprometan la seguridad de la información, tanto por las áreas técnicas de tecnología, como las áreas de Riesgo Tecnológico y de Seguridad de la Información.

16.3. Monitoreo de eventos de seguridad y ciber inteligencia de amenazas

El área de tecnología debe contar con un monitoreo activo de eventos y debilidades en activos de información, así como consumo de fuentes de ciber inteligencia de amenazas como parte de una estrategia de prevención de incidentes de Seguridad de la Información y Ciberseguridad. Este monitoreo de eventos de seguridad debe considerar la identificación de comportamientos inusuales por parte de personal crítico como parte de un programa de analíticos de seguridad.

17. Gestión de la Continuidad de Negocio

El ISO participará activamente en la definición, documentación, prueba y actualización de los planes de Continuidad de Negocio. El área de tecnología, los Propietarios de la Información y el ISO cumplirán las siguientes funciones:

a) Identificar las amenazas que puedan ocasionar interrupciones de los procesos y/o las actividades.

b) Evaluar los riesgos para determinar el impacto de dichas interrupciones.

c) Identificar los controles preventivos y detectivos.

d) Desarrollar un plan estratégico para determinar el enfoque global con el que se abordará la continuidad de las actividades.

e) Elaborar los planes de contingencia necesarios para garantizar la continuidad de las actividades y el resguardo de la información en dichos planes.

18. Cumplimiento

18.1. Cumplimiento de Requisitos Legales

Identificación de la legislación aplicable. Se definirán y documentarán claramente todos los requisitos normativos y contractuales pertinentes para Sura. Del mismo modo se definirán y documentarán los controles específicos y las responsabilidades y funciones individuales para cumplir con dichos requisitos.

18.2. Derechos de Propiedad Intelectual

Se implementarán procedimientos adecuados para garantizar el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual.

18.2.1. Derecho de Propiedad Intelectual del Software

El área de tecnología con la asistencia del Área Legal y el ISO si aplica, analizará los términos y condiciones de la licencia, e implementará los siguientes controles:

a) Definir normas y procedimientos para el cumplimiento del derecho de propiedad intelectual de software, que defina el uso legal de productos de información y de software.

b) Mantener un adecuado registro de activos.

c) Conservar pruebas y evidencias de propiedad de licencias, discos maestros, manuales, etc.

d) Verificar que sólo se instalen productos con licencia y software autorizado, los que no sean parte de esta definición, quedan prohibidos de instalación.

e) Elaborar y divulgar un procedimiento para el mantenimiento de condiciones adecuadas con respecto a las licencias.

18.3. Protección de los Registros de Sura

Los registros críticos de Sura se protegerán contra pérdida, destrucción y falsificación. Algunos registros pueden requerir una retención segura para cumplir requisitos legales o normativos, así como para respaldar actividades esenciales.

18.4. Protección de Datos y Privacidad de la Información Personal

Sura cuenta con los procesos adecuados para asegurar la privacidad y protección de la información, de acuerdo con la legislación vigente.

18.5. Recolección de Evidencia

Es necesario contar con adecuada evidencia para respaldar una acción contra una persona u organización. Siempre que esta acción responda a una medida disciplinaria interna, la evidencia necesaria estará descrita en los procedimientos internos.

18.6. Sanciones

Sura cuenta con un reglamento interno de orden, higiene y seguridad, que establece sanciones que se pueden aplicar a colaboradores al cometer faltas leves o faltas graves.

Faltas leves:

- Caer en ejercicios preventivos de Phishing
- Uso incorrecto de correo corporativo para temas personales
- Mantener sesión abierta del PC sino se está presente
- Instalación de Software no autorizado y modificar las configuraciones del equipo corporativo.

Faltas Graves:

- Uso indebido de contraseñas de terceros
- Caer reiteradamente en ejercicios preventivos (Mas de tres veces)
- Acumular más de tres cartas de amonestación.

19. Excepciones a la Política

Toda desviación parcial o total de algún punto de esta política, deberá ser revisada y validada por Comité de Riesgo Tecnológico, Seguridad de la Información y Ciberseguridad y los respectivos Directorios.

El ISO resguardará el registro de todas las excepciones a la política que hayan sido aprobadas.

20. HOJA DE MODIFICACIÓN

Nº	Modificaciones efectuadas	Fecha	Realizado por	Revisado y aprobado
1	Primera Edición	Mar. 2011	Sabrina Otero	CRO
2	Rebranding y adaptación nuevo modelo	Sep. 2012	Seguridad de la Información	CRO
3	En Punto 3.2 Evaluaciones de Riesgo de la Información, página 3, se agrega cuadro con detalle de responsables según tipo de activos.	Nov. 2012	Seguridad de la Información	

	Página 9, se agrega punto 5.10 Auditoría Externa			
3.1	Se agrega portada, dado por actualización de formato documento 177.	Abr. 2013	Seguridad de la Información	
3.22	- Se incorpora punto 1.5. relacionado a periodicidad de revisión y validación del documento. - Cambios menores de redacción	Oct. 2014	RRCC (oi)	
3.23	Incorporación del nuevo marco de gestión de riesgo TI.	Julio 2015	RRCC (oi)	Comité de Riesgo y Auditoria Corporativo
3.24	Se revisa documento, no registrando actualizaciones significativas, se mantiene versión 3.24	Nov. 2016	RRCC (oi)	Comité CRA Dic. 2016 Comités de Línea Dic. 2016
3.25	Se revisa documento, no registrando actualizaciones significativas.	Oct. 2017	RRCC (oi)	Comité CRA nov. 2017 Comités de Línea nov. 2017
4.0	Se incorporan los siguientes puntos: • 3.4 Evaluación de riesgos TI de la compañia • **4.0** Modelo de cuantificación de Riesgos Tecnológicos • 5.0 Apetito de Riesgo	Nov. 2018	RRCC	Comité de Riesgo TI y Seguridad de la Información Comité de Riesgos
5.0	Actualización de contenidos	Abril 2019	RRCC	Comité de Riesgo TI y Seguridad de la Información Comité de Riesgos
5.1	Se agregaron los siguientes puntos: 14.2 Controles contra código malicioso 14.3 Respaldos de la Información 14.4 Control del software de operación 14.5 Gestión de vulnerabilidades técnicas	Noviembre 2019	Oficial de Seguridad de la Información	No Aplica, ya que son actividades que se realizan en áreas y no estaban definidas en política.
6.0	-Revisión y validación del contenido y forma de la política. -Se agregaron dominios y subdominios de acuerdo a la norma. -Se modificaron aplicación de dominios de acuerdo lo realizado en la organización.	Julio 2020	Oficial de Seguridad de la Información	Comité de Riesgo tecnológico Comité de Riesgos Directorio
7.0	Se realiza la revisión y validación del contenido de la política. Se realiza la incorporación de los siguientes apartados: - Referencia de lineamientos regionales MSIC. - Revisión anual para activos altos y críticos. - Revisión de vulnerabilidades en comité de riesgo tecnológico para altas y críticas. - Se ajusta la política de contraseñas de acuerdo con lo implementado en los sistemas.	Julio 2021	Oficial de Seguridad de la Información	Comité de Riesgo tecnológico Comité de Riesgos Directorio

8.0	Se realiza la revisión y actualización de contenidos de la política, incluyendo temas asociados al Sistema de Gestión de Seguridad de la Información (SGSI) y de detalle de la gestión de riesgos de Seguridad de la Información.	Noviembre 2021	Oficial de Seguridad de la Información	Comité de Riesgo tecnológico Comité de Riesgos Directorio
9.0	Se realiza la revisión y actualización de contenidos de la política, incluyendo la nueva ley de delitos informáticos, descripción detallada de las tres líneas de defensa, parámetros y rotación de claves en plataformas tecnológicas y sanciones del reglamento interno.	Octubre 2022	Oficial de Seguridad de la Información	Comité de Riesgo tecnológico Comité de Riesgos Directorio

Anexo 1 - Gestión Riesgos Seguridad de la Información y Ciberseguridad

1. MARCO DE TRABAJO PARA LA GESTIÓN DE RIESGOS DE INFORMACIÓN

Figura 1. Marco de Trabajo para la Gestión de Riesgo de Información.

1.1 Gobierno de Riesgos

Esta metodología traduce el gobierno corporativo en principios y políticas de gobierno del riesgo de seguridad de la información basado en la arquitectura del Sistema de Control Interno de la Compañía, el cual define además un esquema de gestión de riesgos empresariales donde la Gestión de Riesgos de Seguridad de la Información y Ciberseguridad fortalecen la estabilidad operacional de la Compañia.

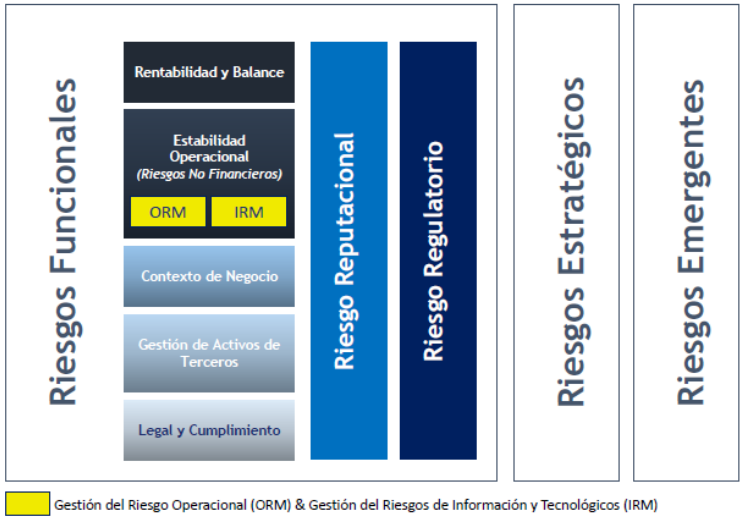


Figura 2. Esquema de Gestión de Riesgos Empresariales (ERM)

1.1.1 Principios

El Gobierno de Riesgos de Seguridad de la Información se rige por los siguientes principios:

- **Conexión con los objetivos corporativos:** la gestión de riesgos de Seguridad de la información y Ciberseguridad, así como el apetito de riesgo definido conducen a que los objetivos del negocio se cumplan.
- **Alineación ERM:** los riesgos de Seguridad de la información y Ciberseguridad son tratados como riesgos del negocio (no financieros), permitiendo un enfoque completo y multidisciplinar.
- **Balance costo/beneficio:** el riesgo de Seguridad de la información y Ciberseguridad es priorizado y gestionado de acuerdo con el apetito de riesgo de la Compañía.
- **Comunicación efectiva:** la información precisa, oportuna y transparente sobre los riesgos de Seguridad de la información y Ciberseguridad sirve como base para la toma de decisiones en todos los niveles de la Compañía.
- **Grupos de interés (Stakeholders):** las personas claves, por ejemplo, Propietarios de Negocio y Junta Directiva, están comprometidos con la gestión de riesgos de Seguridad de la información, Ciberseguridad y tecnológicos (IRM), promoviendo la cultura y el comportamiento respectivo. Toman decisiones basadas en esta gestión.
- **Enfoque coherente:** las prácticas de gestión de riesgos de Seguridad de la información, Ciberseguridad y tecnológicos se aplican continuamente, se mejoran y alinean de acuerdo con la dinámica de la Compañía.

1.1.2 Establecimiento del Contexto

- La presente metodología de gestión de riesgos de información contempla dentro de su alcance los riesgos asociados a la información y al ambiente de TI, que tienen impacto en la operación del negocio.
- El equipo de Seguridad y Riesgos de Información deberá definir un plan anual de evaluación de riesgos de información y tecnológicos alineado al plan estratégico de la Compañía, considerando los subprocesos de negocio y de TI, nuevos proyectos con base tecnológica, iniciativas, requerimientos regulatorios, la clasificación de activos de información, el plan de protección de información, entre otros.

- El plan anual de evaluaciones debe ser aprobado por el comité de Seguridad de la Información, Ciberseguridad y Riesgos Tecnológicos.
- Los dueños de los subprocesos de TI deberán realizar la autoevaluación de sus subprocesos al menos una vez al año, o en caso de que hayan sufrido cambios mayores, evaluando el riesgo inherente y residual.
- La evaluación de la solidez de los controles de seguridad de información se debe realizar al menos una vez al año. Esta evaluación comprende dentro de su alcance todos los controles de seguridad.

Esta evaluación debe realizarse de acuerdo con el apetito de riesgos definido por el Comité de Riesgos y divulgado en la Política de Gestión de Riesgo Operativo, tal como se muestra a continuación:

- **Unidad de Negocio(*):**

Nivel de Riesgo	Ponderación
Crítico	4
Alto	3
Medio	2
Bajo	1

Niveles de Riesgo: Son los diferentes niveles que establece la organización para realizar una medición de la exposición que existe a los riesgos y sus impactos.
Actualmente la compañía tiene establecido los siguientes niveles de riesgo:

- **Riesgo Crítico:** El nivel de riesgo se encuentra en el umbral máximo de pérdida de acuerdo con los límites en el mapa de calor definido para la compañía. Bajo este escenario se deben tomar acciones inmediatas de mitigación.
- **Riesgo Alto:** El nivel de riesgo se encuentra en un umbral alto de pérdida de acuerdo con los límites en el mapa de calor definido para la compañía. Bajo este escenario se deben tomar acciones de mitigación en un plazo razonable.
- **Riesgo Medio:** El nivel de riesgo se encuentra en un umbral medio de pérdida de acuerdo con los límites en el mapa de calor definido para la compañía. Se debe analizar la intervención para establecer un plan monitoreo para que el nivel de riesgo no se incremente.
- **Riesgo Bajo:** El nivel de riesgo se encuentra en un umbral bajo de pérdida de acuerdo con los límites en el mapa de calor definido para la compañía. Se debe establecer un plan de mitigación en la medida en que se considere necesario y monitorear que el nivel de riesgo no se incremente.

** El Apetito de Riesgo para los riesgos de Seguridad de la Información y Ciberseguridad es Medio.*

Para la valoración de riesgos de información se consideran las siguientes definiciones para la frecuencia esperada e impacto:

- **Tabla de Frecuencia Esperada:** La siguiente tabla contempla la escala para determinar el valor de frecuencia de ocurrencia de un riesgo de información. Esta es referenciada de las definiciones de la Metodología de Riesgo Operativo:

Frecuencia Esperada	Probabilidad Anual	Ponderación
1 vez al mes	12.00	Muy Frecuente

1 vez por trimestre	4.00	Muy Frecuente
1 vez por semestre	2.00	Muy Frecuente
1 vez al año	1.00	Frecuente
1 vez cada 2 años	0.50	Frecuente
1 vez cada 3 años	0.33	Poco Frecuente
1 vez cada 4 años	0.25	Poco Frecuente
1 vez cada 5 años	0.20	Muy rara vez
1 vez cada 10 años	0.10	Muy rara vez
1 vez cada 20 años	0.05	Muy rara vez

- **Tablas de Impacto:** Determina el impacto cualitativo (Crítico, Alto, Medio o Bajo) de los riesgos analizados de acuerdo con las siguientes variables:
  - Seguridad de la Información: determinado por el impacto en la confidencialidad, integridad y disponibilidad de los activos de información.
  - Legal: determinado por una escala en el incumplimiento regulatorio que pudiera generar consecuencias adversas para la compañía.
  - Reputacional: determinado por el nivel de daño que se pudiera tener en la imagen o reputación de la compañía.

  A continuación, se detallan las tablas de impacto a considerar en la valoración de un riesgo de seguridad de la información y Ciberseguridad:

IMPACTO EN SEGURIDAD DE LA INFORMACIÓN		
Valor	**Nivel**	**Descripción**
4	Crítico	Efecto adverso en un grado y duración tales que derivan: divulgación o fuga de información secreta; cambios que afectan significativamente la exactitud y completitud de la información; y/o indisponibilidad de información crítica para la operación del negocio; generando pérdidas económicas e imagen negativa.
3	Alto	Efecto adverso en un grado y duración tales que derivan: divulgación o fuga de información secreta; cambios que afectan considerablemente la exactitud y completitud de la información; y/o indisponibilidad de información relevante para la operación del negocio; ocasionando errores en la ejecución de los subprocesos y la toma de decisiones.
2	Medio	Efecto adverso en un grado y duración tales que derivan: divulgación o fuga de información confidencial; cambios que afectan aceptablemente la exactitud y completitud de la información; y/o indisponibilidad de información básica para la operación del negocio; generando retrasos o incumplimientos en la consecución de objetivos.
1	Bajo	Efecto adverso en un grado y duración tales que derivan: divulgación o fuga de información pública; cambios que afectan mínimamente la exactitud y completitud de la información; y/o indisponibilidad de información no relevante para la operación del negocio; ocasionando una afectación no significativa.

IMPACTO LEGAL

Valor	Nivel	Descripción
4	Crítico	Intervención por parte de los órganos de control por incumplimientos legales y/o contractuales.
3	Alto	Sanciones económicas por incumplimiento de las normas establecidas por los entes reguladores. Apertura de procesos sancionatorios, disciplinarios o fiscales.
2	Medio	Llamados de atención o requerimientos realizados por los entes reguladores a nivel nacional.
1	Bajo	Llamados de atención o requerimientos realizados por los entes reguladores a nivel local o regional / No genera incumplimientos.

IMPACTO REPUTACIONAL		
Valor	**Nivel**	**Descripción**
4	Crítico	Imagen negativa en el mercado por mal servicio, prácticas inseguras y/o irregulares. Mala reputación generalizada debido a comentarios adversos ampliamente difundidos a través de medios masivos de comunicación.
3	Alto	Imagen negativa generalizada a través de las redes sociales a consecuencia de las ineficiencias operativas en los servicios, atención ineficaz o inoportuna.
2	Medio	Imagen negativa por mal servicio difundida a través de medios masivos de comunicación nacionales.
1	Bajo	Imagen negativa por mal servicio difundida a través de medios masivos de comunicación locales o regionales. / No afecta la imagen.

- **Tablas de Referencia:** A continuación, se detallan las tablas de referencia para tener en cuenta como guía y criterio, más no como lineamiento, en la mitigación de la frecuencia y del impacto inherentes:

Disminución de Frecuencia: esta tabla es una referencia para disminuir la frecuencia inherente, la cual puede estar determinada por la solidez del control" que causen el riesgo. Así mismo, el control con solidez más alta permitirá disminuir la frecuencia de acuerdo con la siguiente escala, siendo esta una guía para obtener la frecuencia residual:

Disminución de Impacto: esta tabla es una referencia para disminuir el impacto total inherente, de acuerdo con la solidez de los controles de seguridad de información tal como se muestra en la siguiente escala:

Impacto inherente	Impacto residual según la Solidez del Control		
	Fuerte	Moderada	Débil
Crítico	Medio	Alto	Crítico
Alto	Bajo	Medio	Alto
Medio	Bajo	Medio	Medio
Bajo	Bajo	Bajo	Bajo

Nota: *Si son varios controles los que ayudan a mitigar un riesgo, se escoge el que tenga mayor solidez.*

1.1.3 Marco de Gobierno de Riesgos de Información y Tecnológicos

El Marco de Gobierno de Riesgos de Seguridad de la Información y Ciberseguridad comprende un enfoque holístico, que cubre de extremo a extremo la Compañía, desde la operación de los activos TI como soporte de los activos de información hasta la consecución de los objetivos corporativos, apalancando su cumplimiento con el apoyo de catalizadores (elementos facilitadores) como la cadena de valor, las tecnologías de información, políticas, personas y habilidades, entre otros. En las figuras 3 y 4 se presenta gráficamente el marco y la relación con los catalizadores desde un enfoque de riesgos y controles.

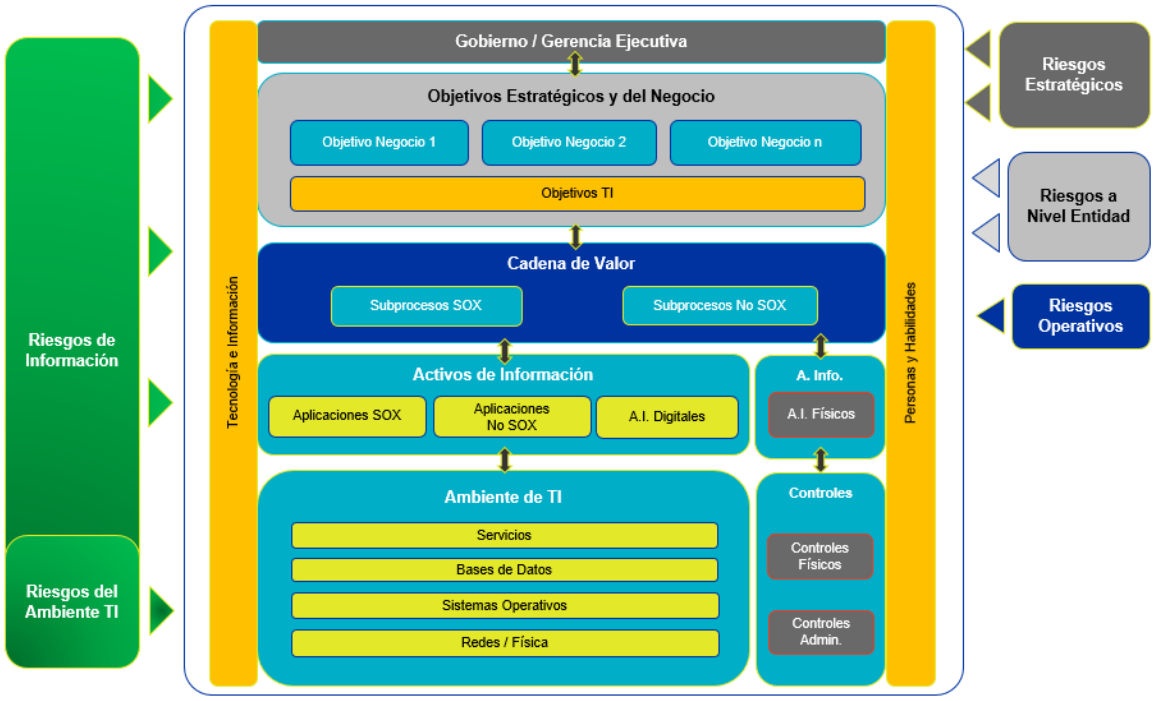


Figura 3. Enfoque holístico de riesgos

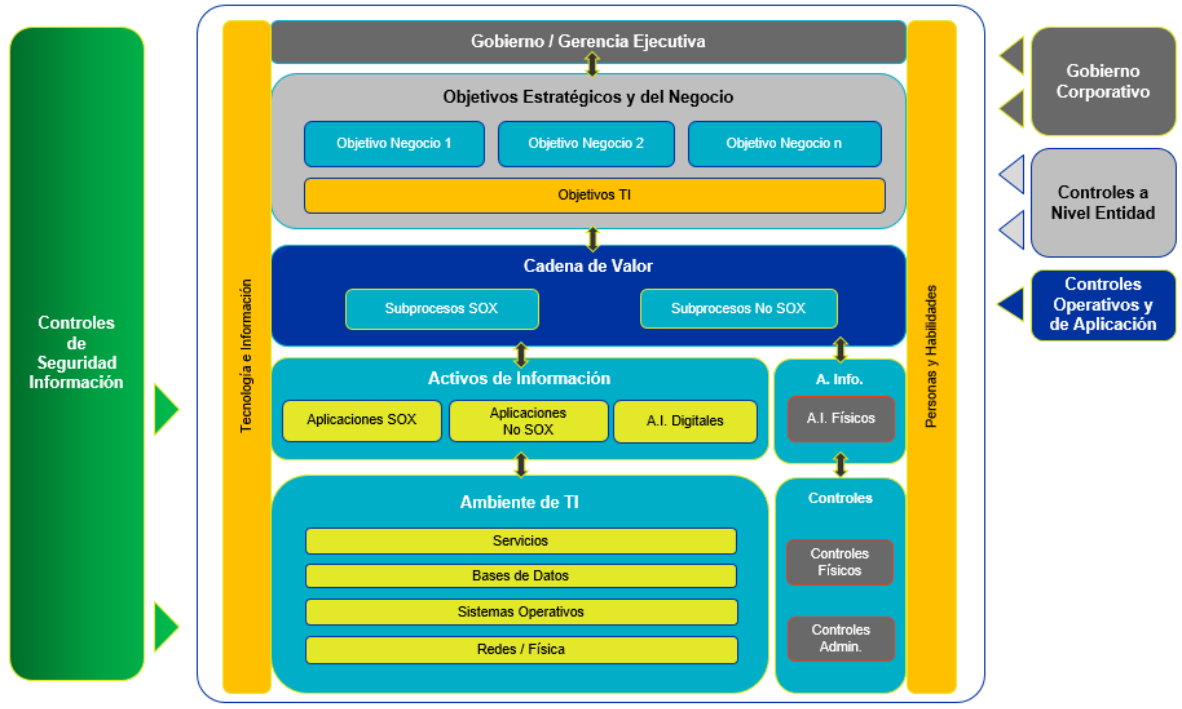


Figura 4. Enfoque holístico de controles

1.2 Identificación de Riesgos

La identificación y levantamiento de riesgos de información se realiza teniendo en cuenta los siguientes elementos que lo constituyen:

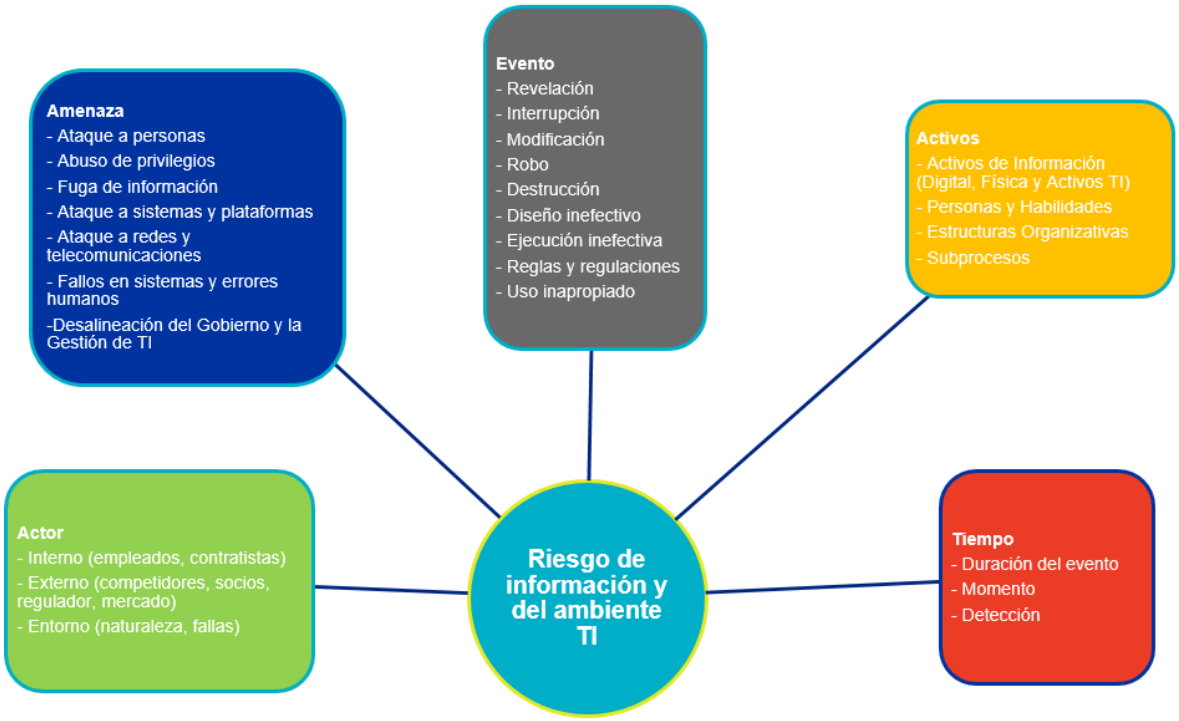


Figura 5. Elementos de Riesgos de seguridad de la Información y Ciberseguridad

Así mismo, se deben considerar los siguientes parámetros para definir cada elemento:

Riesgo:

- ✓ **Qué:** ¿qué puede suceder?, ¿qué no quiero que suceda? Se recomienda iniciar con un verbo en infinitivo o con una acción.
- ✓ **Por qué:** indicar la causa por la que se pueda materializar el riesgo. Se recomienda que contenga unidades cuantificables.
- ✓ **Cómo:** expresar el riesgo materializado. Se recomienda indicar el efecto o la consecuencia.

Objetivo de Control: Define qué se debe controlar para evitar la materialización del riesgo asociado que puede afectar el logro del objetivo del subproceso (conocido también como Práctica de Gestión).

- ✓ Iniciar con un verbo en infinitivo.
- ✓ Qué es lo que buscamos lograr con la implementación de controles. Qué es lo que se quiere controlar.
- ✓ También se considera el objetivo de control como el nivel de control deseado en un subproceso.

Control:

- ✓ **Quién**
- ✓ **Qué**
- ✓ **Cómo**
- ✓ **Para qué**
- ✓ **Cuándo**
- ✓ Se recomienda que la acción de mitigación esté enfocada en la causa del riesgo

Los riesgos de información y tecnológicos identificados, revisados y aprobados, se deben documentar en archivo de Evaluación de Riesgos de Seguridad de la Información, administrado por el área de Riesgos Tecnológicos.

1.3 Análisis / Cuantificación

La valoración de riesgos de información se realiza considerando una probabilidad de ocurrencia, el impacto cualitativo en términos de seguridad de información, legal, reputacional, así como la magnitud del impacto para cada riesgo analizado tanto inherente como residualmente, bajo los siguientes criterios:

- ➢ **Criterios para la probabilidad de ocurrencia inherente:**
  - Determinada por la periodicidad de ejecución de actividades sobre los activos de información. O en su defecto, determinada por el máximo nivel de probabilidad.
  - Puede ser determinada por históricos de incidentes, rotación de personal y/o por cambios en la estructura de la Compañía.
  - Determinada por la vulnerabilidad de los activos de información (ver tabla de referencia en la sección “1.1.3 Establecimiento del Contexto”).
- ➢ **Criterios para la probabilidad de ocurrencia residual:**

- Tener en cuenta la solidez de los controles de seguridad de información, así como las vulnerabilidades identificadas (ver tabla de referencia en la sección “1.1.3 Establecimiento del Contexto”).
- Eventos materializados.

➢ **Criterios para el impacto inherente:**
- Considerar el promedio de los impactos: en seguridad de la información, legal, reputacional. Así como la magnitud del impacto en términos cualitativos.
- Tener en cuenta los peores escenarios para la valoración.

➢ **Criterios para el impacto residual:**
- Tener en cuenta la solidez de los controles de seguridad de información (ver tabla de referencia en la sección “1.1.3 Establecimiento del Contexto”).
- Considerar los eventos materializados.

✓ 1.3.1 Solidez de Controles de Seguridad de Información

Por otro lado, se debe considerar la solidez consolidada de cada uno de los controles de seguridad de la información con el fin de conocer qué tan fuertes son en el momento de mitigar los riesgos analizados. Para obtener la solidez consolidada se diligencia la Matriz de Solidez de Control, en la cual el responsable de ejecución del control evalúa la eficiencia y la eficacia de cada control de Seguridad de la información y Ciberseguridad que hacen parte del alcance de la gestión de riesgos, teniendo en cuenta los siguientes criterios:

Eficiencia del Control: evalúa los siguientes parámetros según la escala de valores definidos:

ESCALA DE EFICIENCIA PARA AMBIENTE CONTROL DE SEGURIDAD	
Oportunidad del control	**Valor**
Preventivo	3
Detectivo	2
Correctivo	1
Naturaleza del control	**Valor**
Automático	3
Semiautomático	2
Manual (*)	1
Máximo Total Eficiencia	**6**

** La escala de naturaleza de controles manuales o de gobierno no se homologan ya que un control procedural o de gobierno normalmente es manual y **aun así puede ser un control fuerte**, por lo que puede ser re-evaluado el riesgo residual por juicio experto por el responsable del control.*

- Oportunidad del control:

- Preventivo: evita que se materialice el riesgo.
- Detectivo: identifica el evento de riesgo en el momento en que se presenta.

- Correctivo: corrige el riesgo después de materializado el evento.

- Naturaleza del control:

- Automático: ejercido únicamente a través de sistemas o recursos tecnológicos.
- Semiautomático: es un control manual que requiere del apoyo de un recurso tecnológico para su función (conocidos también como controles manuales dependientes de TI). Un ejemplo de este tipo de control es la gestión de cambios a través de herramientas como Jira.
- Manual: ejercidos por una o más personas sin el apoyo de los recursos tecnológicos.

- Implementación del control : El dueño del proceso declara la implementación del control de acuerdo a como fue definido es:

- Efectivo: El control se implementó según se encuentra definido.

- Inefectivo: El control no ha sido implementado.

Solidez del Control (Eficiencia X Eficacia): se calcula teniendo en cuenta el valor de la evaluación preliminar del control más la implementación del control la cual es evaluada por el responsable del control.

Solidez del control			
Implementación			
Efectiva	Moderado	Moderado	Fuerte
Inefectiva	Débil	Moderado	Moderado
Evaluación prelimilar -->	Inadecuado	Adecuado	Muy adecuado

1.3.2 Flujo de Análisis y Valoración de Riesgos de Seguridad de la Información

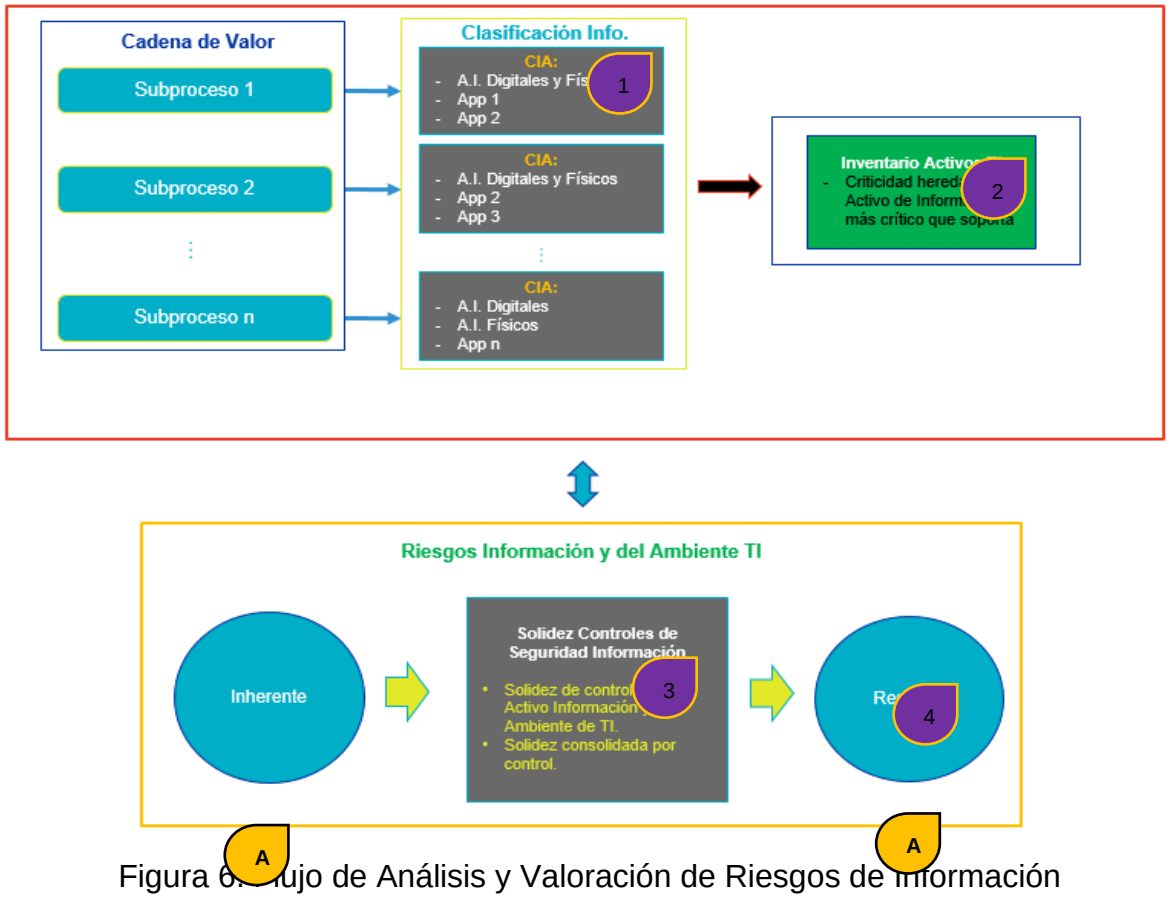


Figura 6. Flujo de Análisis y Valoración de Riesgos de Información

1. Evaluar la solidez de los controles por cada activo de información en archivo de Evaluación de Riesgos de Seguridad de la Información, administrado por el área de Riesgos Tecnológicos. La solidez consolidada del control es insumo en la Matriz de Riesgos y Controles de Seguridad de Información y Ciberseguridad para la valoración.
2. Teniendo en cuenta la solidez de los controles y de acuerdo con los criterios definidos, se realiza la valoración de la frecuencia esperado y del impacto de cada uno de los riesgos de información, con el fin de obtener el nivel de riesgo con respecto al apetito definido.

Punto A:

Para determinar el Nivel de Riesgo tanto inherente como residual, se obtiene la probabilidad de ocurrencia, se valora cada impacto cualitativo: seguridad de la información, legal, reputacional, así como se considera la magnitud del impacto, de acuerdo con los siguientes cálculos (ver ejemplo en figura 7):

- ***Probabilidad de Ocurrencia =*** *se selecciona un valor de la lista desplegable.*
- ***Impacto Cualitativo =***
  - ***Seguridad de la Información:*** *se selecciona un valor de la lista desplegable.*

- ***Legal:*** *se selecciona un valor de la lista desplegable.*
- ***Reputacional:*** *se selecciona un valor de la lista desplegable.*

Riesgo Inherente					
Probabilidad de Ocurrencia	Impacto Cualitativo				Riesgo Inherente
	Seguridad de la Información	Legal	Reputacional	Resultado Impacto	
1 vez al mes	Crítico: Efecto adverso en un grado y duración tales que derivan: divulgación o fuga de información secreta; cambios que afectan significativamente la exactitud y completitud de la información; y/o indisponibilidad de información crítica para la operación	Medio: Llamados de atención o requerimientos realizados por los entes reguladores a nivel nacional.	Alto: Imagen negativa generalizada a través de las redes sociales a consecuencia de las ineficiencias operativas en los servicios, atención ineficaz o inoportuna.	Alto	Crítico

Figura 7. Ejemplo de valoración de riesgos

La valoración de los riesgos, como la solidez de los controles deben quedar documentados en archivo de Evaluación de Riesgos de Seguridad de la Información, administrado por el área de Riesgos Tecnológicos.

1.4 Tratamiento / Respuesta

El tratamiento de los riesgos de Seguridad de la información y ciberseguridad mediante la implementación de acciones mitigantes o a través de la aceptación de estos, sigue los lineamientos definidos en el proceso de planes de remediación de Riesgo, el cual, define los siguientes criterios:

Nivel de Riesgo	Criterio	Tratamiento / Respuesta (hallazgo / planes remediación)	Aprobación de aceptación del riesgo
Crítico	Se encuentra en el umbral máximo de pérdida de acuerdo con los límites en el mapa de calor definido para la compañía. Bajo este escenario se deben tomar acciones inmediatas de mitigación.	0 a 3 meses	Autorización CEO País, VP o Responsable del riesgo o Directorio
Alto	Se encuentra en un umbral alto de pérdida de acuerdo con los límites en el mapa de calor definido para la compañía. Bajo este escenario se deben tomar acciones de mitigación en un plazo razonable.	3 a 6 meses	Autorización CEO País, VP o responsable del riesgo
Medio	Se encuentra en un umbral medio de pérdida de acuerdo con los límites en el mapa de calor definido para la compañía. Se debe analizar la intervención en la medida en que se considere necesario y monitorear que el nivel de riesgo no se incremente.	Debe ser monitoreado.	Responsable del proceso o del riesgo
Bajo	Se encuentra en un umbral bajo de pérdida de acuerdo con los límites en el mapa de calor definido para la compañía. Se debe establecer un plan de mitigación en la medida en que se considere necesario y monitorear que el nivel de riesgo no se incremente.	Podría ser monitoreado.	Responsable del proceso o del riesgo

Ver: *¡Error! No se encuentra el origen de la referencia.*

1.5 Monitoreo

- El monitoreo deberá realizarse en conjunto por la primera y la segunda línea de defensa de manera continua, basándose en las siguientes fuentes, entre otras:
  - Resultados de Auditorías Internas
  - Resultados de Auditorías Externas
  - Hallazgos de Reguladores
  - Reporte de Incidentes
  - Autoevaluaciones de Riesgo
  - Revisiones a subprocesos SOX (de acuerdo con planificación anual)

    - Centro de Operaciones de Seguridad (SOC), por ejemplo
- El dueño del subproceso TI debe monitorear las fechas compromiso de los planes de remediación de riesgos definidos, a fin de asegurar la ejecución a tiempo de las acciones comprometidas.
- El equipo de Seguridad y Riesgos de Información podrá realizar la revisión de la implementación de los planes de remediación de los riesgos de información y tecnológicos, en la fecha compromiso definida por el dueño del subproceso, a efectos de asegurar la efectividad del control implementado.
- El equipo de Seguridad y Riesgos de Información mediante el monitoreo continuo de eventos y amenazas de seguridad podrá alimentar el catálogo de riesgos de información y tecnológicos, así como asesorará al equipo de Tecnología en la implementación de medidas mitigantes.

1.6 Información y Comunicación

- Toda información relativa a la gestión o existencia de riesgos de información y tecnológicos deberá ser considerada, analizada y comunicada en forma estructurada para asegurar que las personas relevantes dentro de la Compañía estén conscientes de los riesgos y sus responsabilidades por la administración de estos.
- La primera línea de defensa deberá comunicar de forma inmediata al equipo de Seguridad y Riesgos de Información los riesgos críticos que identifique en la operación de su subproceso, así como los eventos de seguridad que identifique.
- El equipo de Seguridad y Riesgos de Información deberá suministrar al equipo de Riesgo Operativo, toda la información relevante de los riesgos de información y tecnológicos, con el fin de construir el Informe Trimestral de Riesgo Operacional a las instancias de gobierno definidas tanto localmente como regionalmente.
- La Alta Dirección aprueba la Política de Seguridad la Información y Ciberseguridad, a partir de la cual se crean procedimientos, prácticas, normas y directrices que se comunican en toda la Organización.
- La gestión de los riesgos de información se presentará por cada subproceso de negocio evaluado. Para los riesgos de seguridad de la Información y Ciberseguridad, se realizará la gestión en la matriz de riesgos y controles. Al final de las valoraciones, se deben consolidar los respectivos resultados y ser presentados los niveles promedio por cada riesgo.