Política de Seguridad de la Información y Ciberseguridad

Jefe de Ciberseguridad

Gerencia de Administración y Finanzas

Cód.: GETI-PO-21-1

Elaborado por:	Aprobado por:	Fecha Liberación:	Fecha Próxima Actualización:
Jefe Ciberseguridad	Gerente de Adm. Y Finanzas	04/11/2024	04/11/2025

INDICE

Página

1. Introducción.

Para Esmax Distribución, Red e Industrial, en adelante Esmax, contar con una sólida gestión de seguridad de la información y un gobierno robusto, es cada vez más relevante a medida que crece la dependencia en la información para el desarrollo de la estrategia de negocio.

La información debe ser tratada con el mismo cuidado, precaución y prudencia que recibe cualquier otro activo o recurso esencial para el funcionamiento de Esmax.

Tomando en consideración la envergadura y grado de sofisticación de las amenazas que pueden provocar impactos en la organización, resulta imprescindible elaborar, desarrollar y fomentar, aquellos mecanismos de protección que permitan resguardar los activos, y junto con ello, desarrollar los elementos que garanticen la protección de estos.

El presente documento establece la Política de Seguridad de la Información y Ciberseguridad de Esmax, en concordancia con las directrices emitidas por su Directorio, recogiendo la filosofía y los principios de gobierno de Esmax en materia de gestión de riesgo, seguridad de la información y ciberseguridad y en línea con las mejores prácticas, estándares técnicos internacionalmente aceptados, regulaciones específicas y protección de los activos de información de Esmax, que aseguren su confidencialidad, integridad y disponibilidad.

Para la gestión de la seguridad de la información, tanto física, tecnológica como en el ciberespacio, Esmax organiza los roles y responsabilidades bajo las tres líneas de defensa para la gestión de riesgo, las cuales dependen de gerencias independientes entre sí.

2. Objetivo.

El objetivo de esta política es definir los criterios y lineamientos esenciales para la administración, custodia y uso de la información y medios requeridos para su tratamiento, con el fin de velar por su disponibilidad, confidencialidad e integridad.

Sus lineamientos sientan las bases del Sistema de Gestión de Seguridad de la Información de **Esmax** que considera el Gobierno y la organización, así como los procesos para una adecuada gestión de riesgos de seguridad de la información y ciberseguridad, que permitan identificar los riesgos, vulnerabilidades y amenazas inherentes a la información, un adecuado tratamiento, reporte y revisión continua, de modo de mejorar continuamente este sistema de gestión.

3. Alcance.

El alcance de esta Política es de carácter corporativo y aplicable a todos los procesos y colaboradores de Esmax y Terceras partes que interactúen con el Sistema de gestión de seguridad de la información.

Esta política aplica a todos los colaboradores de Esmax, personal externo, proveedores de servicios, consultores y auditores que acceden a las instalaciones o tengan acceso a la información de Esmax.

4. Responsabilidades.

4.1 Gerencia General de Esmax

- Aprobar esta política.
- Definir al responsable por la gestión de esta política.
- Asegurar el cumplimiento de los compromisos de la Política de Seguridad de la Información y Ciberseguridad.
- Disponer la divulgación de la Política de Seguridad de la Información y Ciberseguridad de la Compañía a toda la fuerza de trabajo hasta el nivel operativo.
- Garantizar el aprovisionamiento de recursos para la seguridad de la información.
- Asegurar la mejora continua en materia de Ciberseguridad y seguridad de la información.
- Ser facilitador respecto a la estrategia de ciberseguridad, según lo definido por el directorio.

4.2 Jefe de Ciberseguridad

- Administrar esta política, lo que incluye su desarrollo, implantación, control, evaluación y mejora continua.
- Obtener la aprobación de esta política.
- Cumplir la actividad de revisión y actualización de esta política.
- Identificar necesidades de capacitación en el contenido de la presente Política.
- Promover las acciones necesarias para la divulgación y aplicación de este documento.
- Asesorar a las Gerencias de la empresa en los temas relativos a Seguridad de la Información y Ciberseguridad.
- Velar por el cumplimiento de las normas legales que dicen relación con Seguridad de la Información.
- Reportar a la Gerencia General de **Esmax** los eventos relevantes relacionados con la Seguridad de la Información.
- Verificar que las normas y controles desarrollados para preservar la Seguridad de la Información se cumplan de manera adecuada.

4.3 Gerencia de Administración y Finanzas

- Proveer y mantener los recursos tecnológicos necesarios para el cumplimiento de las normas de Seguridad de la Información
- Asegurar que los activos de información administrados por el área cumplen con los criterios, requisitos y disposiciones establecidas en el marco normativo de seguridad de la información.

4.4 Usuarios y a todos los Colaboradores de Esmax

- Cumplir la Política de Seguridad y Ciberseguridad de la Información de **Esmax**.

- Reportar al gerente inmediato superior y a la Jefatura de Ciberseguridad, los incidentes de seguridad que afecten a los negocios y a la imagen de la empresa, y que sean de su conocimiento.

5. Política.

Esmax está comprometido con la protección de la información, a través del tratamiento continuo de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados, estableciendo estrategias para el desarrollo de las capacidades necesarias para prevenir, detectar, defender y recuperarse, velando por la implementación de funciones de identificación, protección, detección, respuesta y recuperación de sus activos de información, estableciendo también la ciberseguridad como un foco relevante para Esmax.

Una adecuada gestión de la seguridad de la información y de la ciberseguridad contribuye no solamente a velar por la disponibilidad, confidencialidad e integridad de la información de Esmax, sino que además permite generar un ambiente de control óptimo para prevenir que los propios colaboradores de la empresa incurran en conductas que podrían ser constitutivas de delitos informáticos.

5.1 Definiciones

Información: cualquier forma de registro o dato físico, electrónico, óptico, magnético o en otros medios similares, susceptible de ser procesado, distribuido y almacenado.

Seguridad de la Información: se refiere al conjunto de medidas y técnicas utilizadas para controlar y preservar la confidencialidad, integridad y disponibilidad de los datos y la información que se maneja dentro de la entidad.

Ciberseguridad: La ciberseguridad se refiere a las prácticas, medidas y tecnologías implementadas para proteger los sistemas informáticos, redes, dispositivos electrónicos y datos contra amenazas, ataques, intrusiones y actividades maliciosas en el entorno digital. El objetivo principal de la ciberseguridad es garantizar la confidencialidad, integridad y disponibilidad de la información, así como prevenir el acceso no autorizado, el robo de datos, el sabotaje, la destrucción o la alteración de sistemas y recursos tecnológicos.

Confidencialidad: propiedad que dice relación con que la información esté disponible solo para quienes estén debidamente autorizados.

Integridad: Es la propiedad que garantiza que la información se mantenga precisa, completa y sin alteraciones durante todo su ciclo de vida.

Disponibilidad: propiedad correspondiente a que la información esté disponible a tiempo y en la forma que se necesite.

Activo de información: Componente, recurso o bien económico que sustenta uno o más procesos de negocio de la entidad. Los activos varían de acuerdo con la naturaleza de la actividad desarrollada, los que pueden ser primarios como la información (física y lógica) y los procesos y actividades de negocio, o de soporte como hardware; software; redes de comunicación; personal; entre otros. recurso que contiene información de valor para Esmax, clientes y otros grupos de interés, que le permite alcanzar sus objetivos y se debe proteger. La información se encuentra en medios tecnológicos y/o no tecnológicos.

Activo crítico de ciberseguridad: Se define como aquellos activos de información que son considerados críticos para el funcionamiento del negocio, incluidos los componentes físicos tales como hardware y sistemas tecnológicos que almacenan, administran y soportan estos activos, los que, de no operar adecuadamente, pueden afectar la continuidad operacional de los procesos de negocio, exponen a la entidad a riesgos que afecten la confidencialidad, integridad y disponibilidad de la información.

Clasificación de Información: proceso donde se evalúa y se cataloga el nivel de protección que requiere cada activo de información que será almacenado manipulado o compartido en Esmax dependiendo de su nivel de confidencialidad.

IFA: un activo expuesto a internet, o "internet-facing asset", se refiere a un activo de soporte perteneciente a la Esmax que está directamente accesible desde Internet para entregar servicios, información a colaboradores, clientes, no clientes, proveedores o cualquier tercero que acceda desde internet (por ejemplo: www.esmax.cl). Esto incluye, por ejemplo, servidores web, bases de datos en línea, aplicaciones, correo electrónico, VPN y cualquier otro recurso que pueda ser accesado o interactuado desde la web.

Activo Tecnológico: Corresponde al componente o medio para acceder a un activo de información, también son considerados como activos de soportes los que permiten el acceso a los activos de información. Son activos de soporte, por ejemplo: Sistemas, Aplicaciones, Servidores, Laptops, Equipos de Colaboradores, Firewalls, Dispositivos de comunicación, etc.

Vulnerabilidad: debilidad de un activo de información que puede ser explotada por una o más amenazas.

Amenaza: cualquier circunstancia o evento que puede explotar, intencionalmente o no, una vulnerabilidad específica de un activo, resultando en una pérdida de confidencialidad, integridad o disponibilidad de la información que maneja.

Estructura de Gobierno de Seguridad de la Información: Un Sistema de Gestión de Seguridad de la Información con una estructura de tres líneas de defensa con roles y responsabilidades, normas, procedimientos, recursos y procesos dispuestos para establecer, implementar, operar, monitorear, revisar y mejorar continuamente la seguridad de la Información de Esmax.

5.2 Disposiciones Generales

La información es un recurso necesario para los procesos y para el desarrollo de la estrategia de negocios, en consecuencia, Esmax considera que la información es un activo valorado donde todos los colaboradores tienen el deber de proteger. De acuerdo con lo anterior, Esmax asume el compromiso de protección permanente de esa información, tanto propia como de clientes y otras partes interesadas.

Para un adecuado sistema de gestión de seguridad de la información y ciberseguridad se establecen los siguientes lineamientos:

Un gobierno basado en tres líneas de defensa, donde la primera línea está conformada por todas las unidades operativas y de contacto con terceros, fortalecidas con las herramientas administradas directamente por las Subgerencia de Sistemas TI como de Ciberseguridad donde se encuentra el rol de jefe de Ciberseguridad de Esmax. La segunda línea de defensa está conformada por la Jefatura de Riesgo Operacional y la tercera línea de defensa está representada por la Gerencia de Auditoría Interna. Esta estructura está conformada por colaboradores especializados y dedicados, con atribuciones y competencias necesarias para gestionar la seguridad de la información y ciberseguridad.

El Sistema de Gestión de Seguridad de la Información tiene definidos y establecidos los siguientes objetivos de seguridad:

- Continuidad operacional total para los Activos Críticos.
- Evitar el robo/fuga de Información.
- Evitar Accesos no autorizados a la red.
- Evitar Accesos no autorizados a la Información.
- Reducir los eventos de fraude relacionados a Phishing.
- Detectar y responder a los Incidentes de seguridad.
- Cambios en plataformas deben ser siempre autorizados.
- Proteger a Esmax de contaminación por malware.
- Gestionar adecuadamente las vulnerabilidades de seguridad en aplicaciones.
- Establecimiento de un Comité de Gestión de Crisis.
- Identificación de los activos de información a resguardar incluyendo los activos de información expuestos a internet (IFA Internet Facing Asset) categorizándolos en base a los criterios de clasificación de la información, manteniendo un inventario regularmente actualizado considerando al menos los activos críticos, consistente con el mapa de procesos de Esmax.

Consideraciones importantes:

Aquellos IFAs que son propiedad de terceros no serán considerados IFAs, sin embargo, deben ser gestionados de acuerdo con los lineamientos establecidos de dicho ámbito.

Se considera la seguridad de la información como un proceso que forma parte del negocio, esencial para la competitividad y el desempeño de la empresa y está constituida por las siguientes directrices las cuales se encuentran organizadas en ámbitos:

5.2.1 Directorio

5.2.1.1 El Directorio es informado regularmente respecto de los riesgos relevantes a que está expuesto Esmax en términos de seguridad de la información y ciberseguridad, así como del cumplimiento de la administración y del tratamiento de incidentes de seguridad de la información y ciberseguridad, procurando mejorar su gestión y prevención.

5.2.2 Compromiso con la Seguridad de la Información

5.2.2.1 Esmax se compromete a mejorar continuamente el sistema de gestión de seguridad de la información, proporcionar los recursos y formación que sean necesarios para la implementación y mantenimiento de dicho sistema.

5.2.2.2 La Información transmitida o almacenada en Activos Tecnológicos puede ser monitoreada en cualquier momento cuando existan propósitos comerciales legítimos para hacerlo.

5.2.3 Roles y Responsabilidades en Seguridad de la Información

5.2.3.1 Los roles y responsabilidades en materia de seguridad de la información se deben establecer a fin de gobernar, gestionar, mantener y mejorar la seguridad de la información en Esmax.

5.2.3.2 Esmax declara que la responsabilidad por la seguridad de la información recae en todos los colaboradores de la organización.

5.2.3.3 Esmax cumple con las políticas y estándares de ciberseguridad aplicables para proteger la información de la empresa del Grupo Aramco.

5.2.3.4 Esmax cumple con clasificar y/o manejar datos de acuerdo con las políticas aplicables de Grupo Aramco.

5.2.3.5 Esmax debe destruir o triturar registros en papel que contengan información confidencial de acuerdo con las políticas aplicables del Grupo Aramco.

5.2.3.6 Esmax debe informar de inmediato el acceso no autorizado, el uso indebido o la divulgación que comprometa de otro modo la información a la entidad responsable dentro del departamento o unidad de negocio organizacional correspondiente del Grupo Aramco.

5.2.4 Concientización en Seguridad de la Información

5.2.4.1 Esmax debe aprovisionar los recursos suficientes para sensibilizar, capacitar y entrenar al personal en materias de seguridad de la información al menos una vez al

año y al ser contratados, declarando que leyeron y entendieron esta política, para que conozcan las amenazas que la afectan y sus consecuencias, y estén preparados para cumplir la presente política y sus normas relacionadas. La planificación de la concientización via correos es creada por Comunicaciones Internas de Esmax, con la información enviada por el equipo de Ciberseguridad. Otros métodos de concientización serán via Videos informativos y capsulas dispuestas por el equipo de RRHH en cursos preparados para los colaboradores. Es de vital importancia concientizar además no tan solo a los colaboradores antiguos, sino que, a los recién contratados, sobre el uso de la información (tarjeta de crédito, Rut, cuentas, etc)

5.2.5 Clasificación de la Información

5.2.5.1 La información debe ser clasificada y protegida en forma apropiada, de acuerdo con su sensibilidad e importancia que posee para el negocio.

5.2.6 Resguardo y Uso Aceptable de activos de información

5.2.6.1 Esmax debe gestionar la seguridad de la información en el ámbito interno y externo a la organización, a fin de asegurar la confidencialidad, integridad y disponibilidad de los activos de información de la organización.

5.2.6.2 Los recursos tecnológicos puestos a disposición por Esmax, incluyendo equipos y accesos, son herramientas de trabajo y deben ser usados para actividades de interés de la Empresa.

5.2.7 Inversiones

5.2.7.1 El plan anual de inversiones en tecnologías de procesamiento, seguridad de la información y ciberseguridad está alineado con la estrategia definida para estos efectos, con especial énfasis en mitigar los riesgos operacionales y tecnológicos

5.2.8 Control de Acceso

5.2.8.1 Las credenciales físicas, tales como tarjetas, claves o contraseñas de identificación personal para accesos y uso de las instalaciones, equipos, información y recursos de Esmax son de carácter intransferible.

5.2.8.2 Las autorizaciones para acceso y uso de las instalaciones, sistemas y recursos de información deben ser formalmente solicitadas por el Líder inmediato del usuario que necesite tal acceso para desempeñar sus actividades o en su defecto responsable del proceso donde se necesite habilitar el acceso, y también se deben promover las revisiones periódicas de las autorizaciones concedidas.

5.2.8.3 Se deben utilizar mecanismos y controles para verificar el uso indebido de las credenciales de autenticación.

5.2.8.4 Todo el personal interno o externo, que preste sus servicios a Esmax, ya sea en forma directa o a través de proveedores, sólo debe acceder a la información estrictamente necesaria para el cumplimiento de sus funciones.

5.2.8.5 Los colaboradores de Esmax, no deben utilizar las credenciales proporcionadas (ID de red o dirección de correo electrónico) y la combinación de contraseña para iniciar

sesión en sitios web, sistemas o activos tecnológicos no operados por el Grupo Aramco.

5.2.9 Controles de Seguridad

5.2.9.1 Esmax debe mantener controles adecuados, a fin de proteger los activos de información de la sustracción, pérdida, daño o compromiso de la confidencialidad e integridad, y que puedan poner en riesgo la normal operación del negocio.

5.2.9.2 Realización regular de auditorías al proceso de gestión de la seguridad de la información y ciberseguridad, con la profundidad y alcance necesario, que considere aspectos tales como el cumplimiento de las políticas y la eficacia de los procedimientos y controles definidos en estas materias

5.2.10 Herramientas corporativas

5.2.10.1 Las herramientas corporativas actualmente vigentes son todas las de la suite de Microsoft y sus plataformas colaborativas y de comunicación que nos permiten compartir información de manera segura. No está permitido el uso de correo electrónico u otras herramientas de tecnología de mensajería de usuario final para compartir información sensible para la compañía (tales como números de tarjeta de crédito, Rut, números de cuenta, correos electrónicos o los que se encuentren dentro de la Política de Protección de Datos Personales) que utilicen cuentas que no son administradas por Esmax.

5.2.11 Leyes y Normativas

5.2.11.1 El proceso de gestión de la seguridad de la información y ciberseguridad implementado procura el cumplimiento de las leyes y normativas vigentes tales como la protección de los datos de carácter personal y los derechos de propiedad intelectual.

5.2.12 Gestión de Incidentes de Seguridad

5.2.12.1 Los incidentes que afecten la seguridad de la información deben ser notificadas por el personal, tanto interno como externo, a través de un canal de gestión apropiado, con el fin de investigar sus causas, minimizar los daños, monitorear y aprender de tales incidentes.

5.2.13 Continuidad de Negocios

5.2.13.1 Se debe asegurar la continuidad de las funciones críticas del negocio, y la disponibilidad de las funciones relativas a la seguridad de la información.

5.2.14 Cumplimiento y Revisión

5.2.14.1 Las disposiciones relacionadas con las normas sobre la seguridad de la información deben ser debidamente controladas en su cumplimiento por el área de Ciberseguridad de Esmax.

5.2.14.2 Esmax declara su decisión de cumplir con la normativa y legislación vigente en temas de seguridad de la información y ciberseguridad.

5.2.14.3 Esmax, está facultada de tomar todas las medidas necesarias para evitar, mitigar, sancionar y protegerse de los efectos de cualquier utilización de sus recursos, que viole la legislación aplicable, las normas internas o el derecho propio o de terceros.

5.2.14.4 El sistema de gestión de seguridad de la información debe ser auditado periódicamente para atestar su eficacia.

5.2.15 Almacenamiento y transmisión de datos de tarjeta

5.2.15.1 Esmax no almacena datos de tarjetas de pago en su entorno. En caso de ser necesario, solo podrá almacenarse el PAN truncado y como máximo los primeros 6 dígitos y los últimos 4 dígitos del PAN.

5.2.15.2 Esmax mantendrá un inventario de ubicaciones donde se almacenan datos truncados de las tarjetas de pago.

5.2.15.3 Esmax no almacena datos confidenciales de autenticación, ni durante la autorización, así como tampoco en forma posterior a la autorización de la transacción.

5.2.15.4 La transmisión de datos de tarjetahabientes a través de las redes de Esmax solo está permitida en el caso de utilización de cifrado de extremo a extremo, implementado por el proveedor de la solución Host-to-Host, de manera que Esmax no tenga acceso ni conocimiento de las claves de cifrado utilizadas y, por consiguiente, no tenga la posibilidad de descifrar la información transmitida.

5.2.15.5 El proveedor de la solución Host-to-Host deberá estar certificado bajo la norma PCI DSS y será responsable de implementar y mantener los mecanismos de seguridad necesarios para proteger la transmisión de los datos de los titulares de tarjetas mediante criptografía robusta.

5.2.15.6 Cualquier otra forma de transmisión de datos de titulares de tarjetas a través de las redes de Esmax está estrictamente prohibida.

5.2.16 Marco Normativo de Seguridad

5.2.16.1 A partir de esta política se articularán un conjunto de políticas de seguridad específicas y sus respectivas herramientas de implementación y monitoreo, las que deben ser aprobadas por la Gerencia al igual que las excepciones a ellas.

5.2.17 Prohibiciones

5.2.17.1 Los colaboradores de Esmax, no deben

- Facilitar o participar en la grabación no autorizada y/o encubierta (por ejemplo, voz y/o vídeo) de conferencias, reuniones o debates del Grupo Aramco.
- Facilitar o participar en la fotografía o videografía no autorizada de instalaciones restringidas del Grupo Aramco.
- Publicar información del Grupo Aramco sin obtener la aprobación de una entidad autorizada y de acuerdo con las políticas y procedimientos establecidos de la empresa del Grupo Aramco.

- Usar logotipos, marcas comerciales, derechos de autor u otra propiedad intelectual del Grupo Aramco (incluido en todo momento cualquier logo de Saudi Aramco) sin obtener la aprobación previa, tal como se define en las políticas y procedimientos establecidos del Grupo Aramco.
- Respaldar, identificar o citar públicamente a Terceros con quienes el Grupo Aramco realiza cualquier negocio, excepto cuando se obtenga aprobación previa.
- Divulgar especificaciones confidenciales relacionadas con el trabajo y publicar información técnica detallada relacionada con el negocio del Grupo Aramco en las redes sociales o cualquier plataforma de red profesional.
- Publicar declaraciones en nombre de la empresa del Grupo Aramco o expresar opiniones públicas en nombre del Grupo Aramco, a menos que esté autorizado para hacerlo.

5.2.18 Monitoreo y Privacidad

Esmax deberá monitorear todas las actividades relacionadas con el uso de Activos Tecnológicos e Información de acuerdo con las políticas corporativas y de acuerdo con la ley aplicable. La información recopilada como parte de dicho seguimiento podrá utilizarse en caso de una investigación o procedimiento disciplinario y para fines legítimos de ciberseguridad, como los que se enumeran a continuación:

5.2.18.1 Detectar o prevenir actividades ilegales, delitos y violaciones de las políticas de Esmax, incluida la detección del uso no autorizado de información y/o activos tecnológicos, la protección contra virus y piratas informáticos y la investigación de fraude.

5.2.18.2 Para prevenir actividades ilegales en los Sistemas, para proteger a las personas de daños, abuso y explotación.

5.2.18.3 Realizar investigaciones internas relacionadas con incidentes de ciberseguridad.

5.2.18.4 Colaborar en el mantenimiento de la seguridad, el rendimiento, la integridad y la disponibilidad de la Información, los Activos Tecnológicos, los Sistemas, los servicios y las instalaciones.

5.2.18.5 Para reunir pruebas en caso de un posible reclamo, acción de cumplimiento, auditoría u otra disputa.

5.2.18.6 Proteger la confidencialidad, integridad y disponibilidad de las personas, los datos, la red, los activos, las instalaciones, la reputación y los intereses competitivos del Grupo Aramco.

5.2.18.7 Al llevar a cabo las actividades de monitoreo descritas anteriormente, Esmax no se dirigirá a Personal específico, a menos que exista una razón legítima para hacerlo, como una sospecha de incidente de abuso, un incidente de seguridad o cuando esté obligada a hacerlo, por ley. En la medida de lo posible, Esmax se abstendrá de realizar revisiones humanas y de acceder a correos electrónicos o archivos (incluido cualquier dato personal contenido en activos tecnológicos, información y sistemas).

5.2.18.8 Se garantizará la confidencialidad en todas las investigaciones que involucren datos personales, excepto en la medida en que se requiera una divulgación más amplia

para dar seguimiento a infracciones, cumplir órdenes judiciales o facilitar una investigación criminal.

5.2.18.9 Las empresas del Grupo Aramco garantizarán la confidencialidad de todas las investigaciones que involucren Datos Personales. Sólo se permitirá una divulgación más amplia si es necesaria para cumplir con órdenes judiciales o para facilitar una investigación criminal.

5.3 Proceso de Gestión de Riesgos de Seguridad de la Información y Ciberseguridad

Para que el sistema de gestión de seguridad de la información y ciberseguridad sea efectivo y suficiente, utiliza un proceso de evaluación y gestión de riesgo que considera:

- Identificación de los activos de información.
- Identificación de las amenazas y vulnerabilidades que puedan dañar los activos de información.
- Evaluación periódica de los controles existentes de manera de conocer su efectividad y suficiencia.
- Identificación de consecuencias que puedan tener en los activos de información pérdidas de confidencialidad, integridad y disponibilidad.
- Análisis de riesgo de los activos de información que considera elementos como la evaluación de la probabilidad de ocurrencia de incidentes y su impacto, en base al grado de daño o costos causados por un evento de seguridad de la información y de ciberseguridad.
- Valoración del riesgo, entendido como una actividad donde se compara el nivel de riesgo determinado con criterios de valoración y de tolerancia previamente definidos.
- Plan de tratamiento del riesgo, donde los riesgos priorizados en la etapa de valoración permiten establecer los controles para reducir, aceptar, evitar o transferir los riesgos.
- Evaluación regular de riesgos asegurando que estos sean concordantes con la tolerancia definida.
- Comunicación periódica de los riesgos entre el equipo de Riesgo y Ciberseguridad.
- Realización de auditoría al proceso de gestión de riesgos de seguridad de la información y ciberseguridad, de manera de identificar oportunamente la necesidad de efectuar ajustes en las metodologías y/o herramientas utilizadas.

5.4 Respuesta y Recuperación de Actividades Ante Incidentes

El área de Riesgo apoya en la identificación y analiza los eventos de seguridad de la información que atenten contra la confidencialidad integridad y disponibilidad de la información, que puedan provocar una fuga o uso indebido de la información, fraude o suplantación de identidad entre otros incidentes.

El área de ciberseguridad detecta, registra y analiza los incidentes de ciberseguridad que producen interrupción parcial o total de los sistemas de información, siendo los más comunes infección por malware, ataques de ransomware y de ingeniería social entre otros.

Sin perjuicio de lo anterior, se cuenta con normas internas específicas que detallan las siguientes actividades regulares:

- Prueba regular de planes de recuperación de desastres (DRP por su sigla en inglés) para enfrentar adecuadamente los escenarios que puedan afectar la ciberseguridad, así como los equipos para dar respuesta a los ciber incidentes que se pudieran materializar. Estos planes son actualizados cada vez que se registran cambios o se materialicen eventos que amenacen la ciberseguridad.
- Plan definido de escalamiento dependiente de la severidad de un incidente de ciberseguridad que permite informar la situación a la alta administración para la toma de decisiones, el cual se debe actualizar anualmente.
- Plan de comunicaciones liderado por el Comité de Crisis, que operan ante incidentes de ciberseguridad y operacional de alto impacto, los cuales alcanzan a todas las partes interesadas, ya sea internas o externas, a fin de mantenerlas adecuadamente informadas.
- Proceso independiente de análisis forense para los ciber incidentes relevantes, que considera la identificación, recopilación, adquisición, examen y análisis de evidencias digitales, junto con la generación de documentación e informes de la investigación forense, interpretación de evidencia digital y las conclusiones del trabajo realizado, además de los requerimientos necesarios para custodiar adecuadamente las evidencias generadas.
- Base de incidentes de ciberseguridad de los activos de información presentes en el ciberespacio que es regularmente utilizada para perfeccionar la capacidad de respuesta a este tipo de eventos, dependiente del área de ciberseguridad.
- La base de incidentes es utilizada como insumo para la realización de pruebas que permitan detectar las amenazas y vulnerabilidades que pudieran existir sobre su sistema de gestión de seguridad de la información y ciberseguridad.
- Una base de conocimientos y lecciones aprendidas, con el objeto de disminuir los tiempos de respuesta cuando se repita un incidente igual o similar, identificar posibles mejoras en los procesos, facilitar el intercambio de conocimientos, y disponer de información que permita apoyar la toma de decisiones en caso de materializarse nuevos incidentes.
- Realización regular de autoevaluaciones de ciberseguridad, para determinar el grado de cumplimiento con la normativa interna y la adherencia a las mejores prácticas en ciberseguridad, de manera de determinar las vulnerabilidades de infraestructura y tomar las acciones oportunas para su mitigación, así como para prever la adopción de medidas ante escenarios de amenazas de ciberseguridad.

5.5 Declaración general de apetito al riesgo

El Apetito de Riesgo es un marco conceptual que explicita y define los límites dentro de los cuales la administración debe ejecutar la estrategia de negocios de Esmax, de modo de optimizar la relación riesgo-retorno.

En Seguridad de la Información, Ciberseguridad y Riesgo el apetito se define:

- No se aceptarán incidentes de ciberseguridad.
- No se aceptarán incidentes de seguridad cloud.
- Por "incidentes de ciberseguridad" se reconocen los conceptos que afecten a la "confidencialidad", "integridad" y "disponibilidad" de la información o de los sistemas.

En relación con la tolerancia al riesgo, frente a incidentes que afecten la disponibilidad, la tolerancia corresponde al tiempo de recuperación objetivo (RTO por su sigla en inglés) en el plan de continuidad de negocio de tecnología de información. En relación con los incidentes que afecten la seguridad de la información y la ciberseguridad asociado a los ámbitos de integridad y confidencialidad se tendrá una tolerancia mínima asociada.

5.6 Gestión de Proveedores.

Los proveedores de servicios tecnológicos y los requisitos de seguridad de terceros son componentes esenciales por lo tanto es fundamental evaluar y seleccionar proveedores que cumplan con los estándares de seguridad establecidos, asegurando que implementen medidas adecuadas para proteger la información sensible. Además, se deben establecer acuerdos claros que definan las responsabilidades de cada parte en cuanto a la protección de datos y la respuesta ante incidentes de seguridad. La supervisión continua y las auditorías periódicas son necesarias para garantizar que los proveedores mantengan un nivel de seguridad adecuado y cumplan con las normativas vigentes.

5.7 Documentos relacionados.

Estos documentos establecen las bases para la implementación de medidas de seguridad, definen las responsabilidades y procedimientos a seguir en caso de incidentes, y aseguran que todos los actores involucrados comprendan y cumplan con los requisitos de seguridad establecidos. La actualización y revisión periódica de estos documentos es crucial para mantener la eficacia de la política de seguridad.

- ADFI-PO-6 Política de Protección de Datos Personales Esmax
- Matriz Política de Conservación y Destrucción de Datos Personales
- GETI-PO-6 Política de Adquisición Mantenimiento Infra y Desarrollo seguro
- GETI-PO-8 Política de Ciberseguridad para Teletrabajo
- GETI-PO-20 Política de Control de Acceso
- GETI-PO-16 Política de Uso Aceptable de Activos

- GETI-PO-12 Política de Seguridad en la Relación con Proveedores
- GETI-DC-12 Reglamento de Parámetros de Contraseñas

6. Frecuencia de Revisión y Actualización de la Política.

El presente procedimiento será revisado periódicamente en función de las necesidades y actualizado cada año, a partir de su entrada en vigencia, por el jefe de ciberseguridad, quien propondrán los cambios tanto de forma como de fondo correspondientes.

7. Control de Cambios.

Versión	Fecha Modificación	Aspectos Modificados
001	30-05-2019	Creación de documento
002	19-06-2021	Se modifican numeral 1, 4, 5 y 9 de la política
003	28-04-2022	Revisión anual de Procedimiento y cambio de gerencia en Promax
004	18-08-2023	Actualización de comentarios para certificación PCI DSS
005	27-11-2023	Actualización para política de protección de datos personales y remediación PCI DSS
006	10-08-2024	Actualización y cambio de nombre con información sobre ciberseguridad.

8. Anexos.

No aplica

9. Registros.

Identificación	Almacenamiento	Grado de sigilo	Protección	Recuperación	Tiempo de Retención	Descarte
Política de Seguridad de la Información y ciberseguridad.	Electrónico.	Corporativo.	Acceso al sistema por clave y contraseña y Sistema protegido por backup.	Procedimientos almacenados por código.	Permanente.	N/A