Sistema de gestión de seguridad de la información

Política de Seguridad de la Información

Fecha de vigencia: ***abril 2026***
Versión 1.1
Aprobado por ***Dirección de SSPV***

Política de seguridad de la información - Índice

Propósito

El propósito de esta política es establecer un marco de gestión de la seguridad de la información en la organización, para asegurar la confidencialidad, integridad y disponibilidad de los activos de información.

Alcance

Esta política aplica a todos los empleados, contratistas, proveedores y terceros que tienen acceso a los activos de información de la empresa. Abarca todos los sistemas de información, redes, aplicaciones, ubicaciones físicas y cualquier otro medio utilizado para procesar, almacenar o transmitir información.

Nuestro alcance asociado al SGI

Diseño, desarrollo, mantenimiento y soporte de software, en modalidad SaaS (software como servicio), orientados a brindar herramientas de gestión operativas a compañías de seguro y brokers.

Principios de Seguridad de la Información

- **Confidencialidad**: La información es accesible únicamente por personas autorizadas.
- **Integridad**: La información es precisa y completa, y sus métodos de procesamiento son correctos.
- **Disponibilidad**: La información está disponible para los usuarios autorizados cuando es necesario.

Objetivos de Seguridad de la Información

- **Proteger la Información**: Protegemos la información asegurando la confidencialidad, integridad y disponibilidad de toda la información que gestionamos en la organización.
- **Gestión de Riesgos**: Gestionamos los riesgos identificando, evaluando y mitigando aquellos relacionados con la seguridad de la información.
- **Respuesta a Incidentes:** Respondemos a incidentes mediante procedimientos eficaces para la detección, notificación y gestión de incidentes de seguridad de la información.
- **Formación y concienciación**: Aseguramos que todos los empleados comprendan y cumplan con las políticas y procedimientos de seguridad de la información a través de la formación y concienciación continua.
- **Continuidad del Negocio**: Implementamos y mantenemos planes de continuidad del negocio y recuperación ante desastres para minimizar el impacto de interrupciones y asegurar la disponibilidad de la información.

- **Mejora Continua**: Revisamos y mejoramos continuamente el sistema de gestión de seguridad de la información para adaptarnos a los cambios en el entorno, las tecnologías y las amenazas.

Responsabilidades

- **Alta Dirección**: Responsable de asegurar el apoyo y el compromiso con la seguridad de la información, proporcionando los recursos necesarios y realizar la aprobación y revisión periódica de la política de seguridad de la información.
- **Gerente de tecnología**: Responsable de la implementación y gestión del sistema de gestión de seguridad de la información (SGSI).
- **Empleados**: Responsables de cumplir con las políticas y procedimientos de seguridad de la información, reportar incidentes de seguridad y participar en las capacitaciones requeridas.

Gestión de Riesgos

Llevamos a cabo análisis de riesgos de forma periódica para identificar, evaluar y gestionar cualquier posible amenaza a la seguridad de la información. Este proceso nos permite comprender mejor las vulnerabilidades a las que estamos expuestos y tomar decisiones informadas sobre cómo abordarlas. Una vez identificados los riesgos, implementamos controles específicos y adecuados para mitigar su impacto y probabilidad de ocurrencia.

Estos controles no solo se limitan a la tecnología, sino que también incluyen medidas organizativas, humanas y procedimentales que fortalecen nuestro enfoque integral de gestión de riesgos.

Además, revisamos regularmente la efectividad de estos controles, asegurando que se mantengan alineados con la evolución de las amenazas y los cambios en el entorno empresarial. Este enfoque proactivo nos permite mantener un entorno seguro y resiliente, adaptado a las necesidades de nuestro negocio y a las exigencias de nuestros clientes y partes interesadas.

Control de Acceso

Nos aseguramos de que el acceso a los activos de información esté estrictamente controlado y se realice únicamente bajo autorización, siempre alineado con las necesidades del negocio y basado en los roles específicos de los usuarios. Adoptamos el principio de privilegio mínimo, lo que significa que cada usuario solo tiene acceso a la información y los recursos necesarios para cumplir con sus responsabilidades, minimizando así el riesgo de accesos innecesarios o indebidos.

Para garantizar la seguridad, utilizamos métodos de autenticación robustos que incluyen contraseñas seguras y autenticación multifactor. Estos mecanismos añaden capas adicionales de protección, reduciendo la posibilidad de accesos no autorizados incluso en caso de que las credenciales sean comprometidas.

Además, hemos implementado controles de acceso tanto físicos como lógicos. Los controles físicos limitan el acceso a nuestras instalaciones y a los dispositivos que almacenan o procesan información sensible, mientras que los controles lógicos se centran en proteger los sistemas y redes a través de firewalls, cifrado y políticas de acceso basadas en permisos. Este enfoque integral de control de acceso nos permite salvaguardar la integridad, confidencialidad y disponibilidad de la información, manteniendo un entorno seguro para nuestros activos críticos.

Gestión de Incidentes de Seguridad

Hemos establecido un procedimiento detallado para la gestión de incidentes de seguridad de la información, asegurando que cada incidente sea tratado de manera eficiente y estructurada. Todos los incidentes, sin importar su magnitud, son reportados de inmediato y gestionados conforme a este procedimiento, que incluye etapas claras desde la detección inicial hasta la resolución final y posterior análisis. Este proceso no solo nos permite responder rápidamente a las amenazas, sino también aprender de cada incidente para fortalecer nuestras defensas y prevenir futuros eventos similares. La documentación y el seguimiento exhaustivo de cada incidente garantizan que tengamos una visión completa de las vulnerabilidades y las medidas correctivas necesarias, manteniendo así la seguridad y resiliencia de nuestra organización.

Continuidad del Negocio

Hemos implementado planes de continuidad del negocio (BCP) y recuperación ante desastres (DRP) diseñados para garantizar que, en caso de una interrupción, la disponibilidad de la información y la operación de nuestros servicios críticos se mantengan o se restablezcan de manera rápida y efectiva. Estos planes cubren una amplia gama de escenarios potenciales, desde fallos técnicos hasta desastres naturales, y detallan los pasos a seguir para minimizar el impacto en nuestras operaciones y proteger los intereses de nuestros clientes y partes interesadas.

El BCP está estructurado para asegurar que las funciones esenciales del negocio continúen operando con la menor interrupción posible, mientras que el DRP se enfoca en la recuperación de la infraestructura tecnológica y la restauración de datos. Ambos planes son revisados y actualizados regularmente para reflejar cambios en el entorno, nuevas amenazas y lecciones aprendidas de ejercicios y simulaciones. De esta manera, estamos preparados para enfrentar cualquier contingencia, asegurando la resiliencia de nuestra organización y la continuidad de los servicios que ofrecemos.

Cumplimiento Legal y Regulatorio

Cumplimos rigurosamente con todas las leyes y regulaciones aplicables en materia de seguridad de la información, asegurando que nuestras prácticas estén siempre alineadas con los estándares legales y normativos vigentes. Este compromiso no solo nos permite operar dentro del marco legal, sino que también refuerza la confianza de nuestros clientes y socios en nuestra capacidad para manejar la información de manera segura y responsable.

Realizamos auditorías periódicas para verificar y asegurar el cumplimiento continuo de la norma ISO 27001, garantizando que nuestros procesos y controles de seguridad se mantengan en consonancia con los requisitos de esta certificación internacional. Estas auditorías nos permiten identificar y corregir cualquier desviación a tiempo, asegurando que nuestras políticas y procedimientos no solo cumplan con las expectativas actuales, sino que también se anticipen a futuros desafíos y cambios regulatorios.

Formación y Concientización

Proporcionamos formación periódica a todos los empleados, asegurando que comprendan y sigan las políticas y procedimientos de seguridad de la información que hemos establecido. Estas capacitaciones no solo cubren aspectos técnicos, sino que también abordan la importancia de la seguridad en el día a día, ayudando a los empleados a reconocer y manejar posibles amenazas.

Además, promovemos activamente una cultura de seguridad de la información en toda la organización. Esto implica no solo la formación, sino también la concientización constante sobre la importancia de proteger nuestros activos y datos sensibles. A través de campañas, comunicaciones y el ejemplo diario, fomentamos un ambiente en el que cada miembro del equipo se siente responsable y comprometido con la seguridad, asegurando así que la protección de la información sea una prioridad compartida por todos.

Revisión y Mejora

Llevamos a cabo auditorías internas periódicas y revisiones por parte de la alta dirección para evaluar la eficacia de nuestro Sistema de Gestión de Seguridad de la Información (SGSI). Estos procesos de revisión nos permiten identificar áreas de mejora y asegurar que nuestras prácticas y controles sigan siendo efectivos y alineados con nuestros objetivos de seguridad. Basándonos en los resultados de estas auditorías y revisiones, así como en los cambios en el entorno de riesgos, implementamos mejoras continuas en el SGSI. Este enfoque nos permite adaptarnos de manera proactiva a nuevas amenazas y desafíos, fortaleciendo constantemente nuestras defensas y capacidades de respuesta.

Comunicación

Nos aseguramos de que esta política de seguridad sea comunicada claramente a todos los empleados y partes interesadas relevantes, garantizando que comprendan su importancia y sus responsabilidades. Además, mantenemos la política siempre disponible y accesible para toda la organización, facilitando que cualquier persona pueda consultarla cuando lo necesite. Este compromiso con la transparencia y la comunicación efectiva refuerza nuestra cultura de seguridad y asegura que todos estén alineados con nuestros objetivos y prácticas de protección de la información.


sspv