Política seguridad de la información

TECHNOKEY

Implementación: 06/09/2024

1. Introducción

En un mundo digitalmente interconectado y en constante evolución, se genera un contexto de crecientes amenazas cibernéticas y regulaciones de privacidad cada vez más estrictas. Ante este escenario, es necesario que la organización establezca una política, en la que la organización se compromete a adoptar medidas de seguridad para salvaguardar los activos digitales y la información cuya responsabilidad sea inherente a su objeto de negocio y a sus procesos.

Así mismo establecer medidas para la ciberseguridad y protección de la privacidad y los derechos de clientes, empleados, proveedores y demás partes interesadas.

2. Alcance del SGSI

Comercializar y gestionar la Información que soporta los servicios de las soluciones digitales HUB (Firma Electrónica), SealMail (Notificación Electrónica Certificada) y Factel (Facturación Electrónica), asegurando la Confidencialidad, Integridad y Disponibilidad de la Información almacenada y procesada en infraestructura de nube.

3. Responsables

Los lineamientos de seguridad de la información establecidos en este documento son de obligatorio cumplimiento por parte de todos los funcionarios, contratistas y proveedores de Technokey S.A.S.

4. Definiciones

Confidencialidad: Propiedad de la información que la hace no disponible o sea divulgada [Fuente: NTC-ISO/IEC 27000:2017].

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos [Fuente: NTC-ISO/IEC 27000:2017].

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad autorizada [Fuente: NTC-ISO/IEC 27000:2017].

Propietario de la información: Parte designada por la organización, cargo, proceso o grupo de trabajo que son responsables de garantizar que la información y los activos asociados se clasifican adecuadamente, revisan periódicamente las restricciones y clasificaciones de acceso, teniendo en cuenta la política de control de acceso [Adaptado: GTC-ISO/IEC 27002:2015].

Custodio: Parte designada por la organización, cargo, proceso o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya establecido [Adaptado: GTC-ISO/IEC 27002:2013].

Usuario: Persona, grupo, entidad o sistema automatizado que genere, obtenga, transforme, conserve o utilice información en papel o medio digital, físicamente o a través de la red de datos y los sistemas de información de la organización, para fines de uso corporativo o en cumplimiento de sus funciones [Adaptado: Guía para la Gestión y Clasificación de Activos de Información. Min TIC].

Información: Es un conjunto de datos con un significado para la organización [Adaptado del libro: «Introducción a la Teoría General de la Administración», Séptima Edición, de Chiavenato Idalberto, McGraw-Hill Interamericana, 2006, Pág. 110.].

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información. Nota: Adicionalmente puede abarcar otras propiedades como la autenticidad, la rendición de cuentas, el no repudio y la confiabilidad [Fuente: NTC-ISO/IEC 27000:2017].

Ciberseguridad: El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. [Fuente: Rec-UIT-

T X.1205 2008]

Protección a la privacidad: Aporta garantías de seguridad sobre los tratamientos de los datos personales. [Fuente: Blog ¿Conoces la nueva norma para la gestión de la privacidad? INCIBE].

5. Política de seguridad de la información

5.1 Generalidades

Technokey consciente de la importancia de la información para la eficaz gestión de todos sus procesos y como lo define su propuesta de valor, se compromete desde la alta dirección a establecer la presente política y definir los objetivos de seguridad de la información que sean compatibles con la dirección estratégica de la organización.
Adicionalmente identificar, evaluar y tratar los riesgos y oportunidades que afecten la seguridad de la información, el ciberentorno y la protección de la privacidad de datos; proveniente del desarrollo de procesos internos y de la prestación de servicios de soluciones digitales a terceros; de manera que se implementen controles o mecanismos que contribuyan a:

- El cumplimiento de requisitos de relacionados de seguridad de la información.
- La protección y preservación de la confidencialidad, disponibilidad e integridad de la información.
- La responsabilidad de mejorar continuamente.

5.2 Objetivos de seguridad de la información

- Examinar la exhaustividad de los requisitos de seguridad de la información que serán abordados mediante el sistema de gestión de seguridad de la información.
- Estimar la exposición de la organización a los riesgos de seguridad de la información.
- Evaluar el cumplimiento de la disponibilidad de la información en los servicios ofrecidos por la organización.
- Medir el conocimiento de los colaboradores en temas de seguridad de la información.

- Implementar medidas de mejoramiento al sistema de gestión de seguridad de la información.

6. Evaluación actual y proyectada de amenazas de seguridad de la información

La evaluación del entorno de la organización respecto a la seguridad de la información se debe realizar antes de iniciar la fase de planificación y actualizarlo posterior a la fase de evaluación de desempeño identificando los avances de implementación del modelo del sistema de gestión, mediante herramientas de autodiagnóstico.

La organización debe abordar amenazas identificadas en la actualidad y proyectadas concernientes a seguridad de la información, teniendo en cuenta los reportes de grupos de interés especial, foros y asociaciones profesionales especializadas en seguridad.

7. Organización para la seguridad de la información

La Alta Dirección es responsable de la aprobación de la presente política, de los objetivos de seguridad de la información planteados, además de la conformidad de sus modificaciones. Asignar a los lideres de proceso la responsabilidad de implementar requisitos aplicables, con el fin de asegurar la integración de los requisitos del SGSI en los procesos.

Asegurar la disponibilidad de recursos necesarios para la implementación, mantenimiento y mejora del SGSI, incluyendo recursos financieros, personal, infraestructura técnica, entre otros. Adicionalmente comunicar en la organización la importancia del SGSI, la necesidad de cumplir los requisitos aplicables.

Así mismo afirmar el respaldo adecuado a las personas designadas con roles y responsabilidades en el SGSI, para que cuenten con la capacidad de liderar y respaldar las actividades de seguridad de la información en sus respectivas áreas.

Solicitar y revisar informes sobre el estado y la eficacia del SGSI, mediante la obtención de indicadores, informes de revisión por la dirección e informes de auditoría.

Con el objetivo de garantizar la asignación clara de responsabilidades y autoridades, lo cual contribuye a la eficacia del Sistema de Gestión de Seguridad de la Información (SGSI) en todas sus fases: planificación, implementación, operación, seguimiento, mantenimiento y mejora continua; la Alta Dirección nombra al **Comité Primario** de la organización como ente responsable de asegurar la gestión adecuada en toda la organización del SGSI. Por lo tanto, cumple con las funciones de un Comité de seguridad de la información, el cual estará conformado por los siguientes cargos:

- CEO
- Technology Director
- IT Security Officer
- Otros cargos que se consideren necesarios de acuerdo con la temática de la reunión.

Por consiguiente, dentro de los **Comités Primarios** que se realicen, al menos una vez al año o cuando ocurran cambios significativos se deben revisar y actualizar esta política y demás lineamientos de seguridad de la información aplicables con el fin de cerciorar su conveniencia, adecuación y eficacia.

Sumado a esto el Comité es responsable de revisar y proponer a la Alta Dirección los lineamientos de seguridad de la información para su correspondiente aprobación.

De acuerdo con el compromiso de liderazgo adquirido por la alta dirección, asigna como responsable de coordinar el establecimiento, implementación, mantenimiento, reporte de desempeño a la alta dirección y mejora del SGSI al cargo **IT Security Officer,** quien a su vez también estará a cargo de organizar las acciones del Comité Primario en términos de seguridad de la información, promover la implementación y cumplimiento de la presente política.

Adicionalmente asesorar con relación a la evaluación y tratamiento de riesgos, diseñar procesos y sistemas, establecer estándares acerca de la determinación, configuración y operación de controles, gestionar los incidentes, revisar el SGSI y las demás que se encuentren definidas en el perfil del cargo.

Propietarios de activos de información como responsables delegados sobre la gestión del activo en su ciclo de vida deben asegurar que los activos se encuentran inventariados, clasificados y protegidos apropiadamente, de acuerdo con la Política de control de acceso y definir que usuarios deben tener permisos de acceso a la información con base en sus roles y competencia. Así mismo asegurarse del manejo apropiado de los activos cuando es eliminado o destruido y demás responsabilidades, autoridades de seguridad de la información definidas en los perfiles de cargo.

Custodios de activos de información tienen la responsabilidad de la administración diaria de la seguridad en los sistemas de información y el monitoreo de cumplimiento de las políticas de seguridad en los sistemas que se encuentran bajo su administración; es decir otorgan o deniegan los permisos y roles asignados por los propietarios en los sistemas de información y activos, en cumplimiento de las políticas de seguridad de la información, demás responsabilidades y autoridades de seguridad de la información definidas en los perfiles de cargo.

Usuarios de activos de información son los colaboradores y contratistas que durante sus actividades diarias usan la información de Technokey S.A.S. tienen como responsabilidad mantener la confidencialidad de información secreta, reportar debilidades o posibles incidentes de seguridad de la información, asegurar el ingreso de la información adecuada a los sistemas, cumplir con las políticas de seguridad de la organización al usar la información.

8. Políticas específicas de seguridad de la información

A continuación, se enlistan las políticas específicas de seguridad de la

información.
Política de control de acceso.
Política de uso aceptable de activos.
Política de uso de controles criptográficos.
Política de desarrollo de software seguro.
Política contra código malicioso.
Política de copias de respaldo.
Política de instalación de software.
Política de seguridad de las comunicaciones.
Política de seguridad de la información relación con los proveedores.
Política de tratamiento de datos personales.
Política de uso de servicios de nube.

9. Proceso para desviaciones y excepciones

Cualquier desviación a las políticas de seguridad de la información se toma como un incumplimiento a las obligaciones contractuales, por tal motivo se debe:

a) Registrar el evento o incidente de seguridad de la información (conforme al procedimiento de gestión de incidentes de SI).
b) Efectuar las indicaciones del procedimiento para comprobación de faltas y formas de aplicación de las sanciones disciplinarias establecidas en el reglamento interno de trabajo. Si es vinculante a proveedores se debe seguir con las cláusulas de suspensión temporal o terminación del contrato considerando el impacto del incumplimiento.

El manejo de excepciones debe ser validado por el IT Security Officer siempre y cuando sean evaluadas y autorizadas por el comité primario. Así mismo especificar la razón por la que no es aplicable la política, lineamiento o medida.

Firmado por:
Esteban Madiedo Bautista
2024/09/09 04:23:01

CEO
Technokey