Política del sistema de gestión de seguridad de la información

TECHNOKEY

Implementación: 15/09/2023

1. Introducción

Los lineamientos determinados en este documento hacen referencia a una serie de medidas que buscan la protección de la información existente en la organización por su naturaleza de negocio, comprendiendo desde su creación, almacenamiento, transferencia y eliminación, así mismo su alcance incluye el manejo en papel (físico) o electrónico.

Dicha protección de la información como compromiso del Sistema de gestión de seguridad de la información se implementa para afrontar las diversas amenazas que puedan repercutir en la continuidad del negocio, minimizar los riesgos, retornar la inversión y generar oportunidades de negocio.

2. Alcance del SGSI

El Sistema de gestión de seguridad de la información para Technokey SAS. comprende todas las áreas, procesos y activos involucrados en la prestación de servicios de soluciones digitales como HUB, la comercialización de SealMail (Notificaciones Electrónicas Certificadas) y Factel; asegurando la disponibilidad, integridad y confidencialidad de la información soportada, administrada y procesada en infraestructura de computación en la nube. La sede principal de Technokey está ubicada en la ciudad de Bogotá, Colombia Calle 68 # 11-48.

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].

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 identificar, evaluar y tratar los riesgos

que comprometan la seguridad de la información 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 la protección y preservación de la confidencialidad, disponibilidad e integridad de la misma, con la responsabilidad de mejorar continuamente.

5.2 Objetivos de seguridad de la información

- Cumplir con los requisitos aplicables y correspondientes a la seguridad de la información.
- Percibir y tratar los riesgos de seguridad de la información con el fin de llevarlos a niveles aceptables para la organización.
- Establecer las medidas para la adecuada preservación y administración de la información gestionada por Technokey S.A.S. Así mismo los medios usados para su procesamiento y que estén relacionados con la seguridad de la información y la ciberseguridad.
- Generar cultura y compromiso del debido cuidado y diligencia con los miembros de la organización y proveedores involucrados en la prestación de servicios de Technokey S.A.S.
- Definir y operar los mecanismos para la identificación de oportunidades de mejora continua con el fin de aportar en la maduración del SGSI.

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 aprueba la presente política, además es responsable de la conformidad de sus modificaciones.

Con el propósito de asegurar la asignación de responsabilidades y autoridades para la adecuada planificación, implementación, operación, seguimiento, mantenimiento y mejora del SGSI; 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 la implementación y mantenimiento del SGSI al cargo **IT Security Officer,** quien a su vez también estará a cargo de coordinar las acciones del Comité Primario en términos de seguridad de la información, promover la implementación y cumplimiento de la presente política 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.

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
2023/09/18 11:35:32

CEO
Technokey