POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

FECHA	VERSIÓN	MODIFICADO POR	DESCRIPCIÓN DE LA MODIFICACIÓN
12/01/2023	V1.0	Francisco Espinel	Documento Inicial
26/04/2023	V1.1	Mayra Medrano	Descripción Base del Documento
26/06/2023	V1.2	Francisco Espinel	Responsabilidades Equipo Implementador
07/08/2023	V1.3	Mayra Medrano	Actualización Responsable & Aprobado
18/08/2023	V1.4	Mayra Medrano	Actualización Etiquetado

Tabla de contenido

1. Objetivo, alcance y usuarios

El propósito de esta Política de alto nivel es definir el objetivo, dirección, principios y reglas básicas para la gestión de la seguridad de la información.

Esta Política se aplica a todo el (SGSI), según se define en el documento del alcance de este.

Los usuarios de este documento son todos los Colaboradores de CONECTA, como también terceros externos a la organización.

2. Documentos de referencia

- Norma ISO/IEC 27001 SGSI
- Documento sobre el alcance del SGSI.
- Metodología de evaluación y tratamiento de riesgos.
- Declaración de aplicabilidad.
- Lista de obligaciones legales, normativas y contractuales.

3. Terminología básica sobre seguridad de la información

Confidencialidad: característica de la información por la cual solo está disponible para personas o sistemas autorizados.

Integridad: característica de la información por la cual solo puede ser modificada por personas o sistemas autorizados y de una forma permitida.

Disponibilidad: característica de la información por la cual solo pueden acceder las personas autorizadas cuando sea necesario.

Seguridad de la información: es la preservación de la confidencialidad, integridad y disponibilidad de la información.

SGSI: parte de los procesos generales de gestión que se encarga de planificar, implementar, mantener, revisar y mejorar la seguridad de la información.

4. Gestión de la seguridad de la información

4.1. Objetivos y medición

Los objetivos generales del SGSI son los siguientes:

- Creación de una cultura enfocada a la seguridad de información mediante la implementación de ISO 27001 para generar una ventaja competitiva en el mercado de software.
- Gestionar los requisitos de seguridad de la información en los servicios mediante la evaluación de los riesgos informáticos.
- Disminuir la probabilidad de ataques de la seguridad de la información manteniendo una buena imagen y reputación.

Las metas están en línea con los objetivos comerciales, con la estrategia y los planes de negocio de la organización.

El Oficial de seguridad de la información es el responsable de revisar estos objetivos generales del SGSI y de establecer nuevos en caso de ser necesarios.

Los objetivos para controles individuales de seguridad o grupos de controles son propuestos por Oficial de seguridad de la información y son aprobados por la alta dirección en la Declaración de Aplicabilidad.

Todos los objetivos deben ser revisados al menos una vez al año.

CONECTA medirá el cumplimiento de todos los objetivos. El Oficial de seguridad de la información es el responsable de definir el método para medir el cumplimiento de los objetivos; la medición se realizará al menos una vez al año y el Oficial de seguridad de la información analizará y evaluará los resultados y los reportará a alta dirección como material para la revisión por parte de la Gerencia.

Todos los procesos estratégicos del alcance de certificación interna del producto CTRL+ buscan promover y cumplir los objetivos del SGSI. Los procesos estratégicos tienen como fin la determinación de políticas internas, estrategias de trabajo, objetivos y metas de la compañía, así como también velar por el cumplimiento de todo lo mencionado anteriormente dentro de la organización y del alcance del sistema.

4.2. Requisitos para la seguridad de la información

Esta Política, y todo el SGSI, deben cumplir los requisitos legales y normativos importantes para la organización en el ámbito de la seguridad de la información, como también con las obligaciones contractuales.

Todos los colaboradores que pertenezcan a CONECTA deben conocer y aplicar las políticas de seguridad de la información.

Las soluciones ofertadas para Banca digital y canales digitales deben cumplir con las mejores prácticas de seguridad de la información.

Mantener la fidelidad de los clientes garantizando que las futuras decisiones se basen en preservar la confidencialidad, integridad y disponibilidad de los servicios.

4.3. Controles de seguridad de la información

Los controles seleccionados y su estado de implementación se detallan en la Declaración de aplicabilidad.

4.4. Responsabilidades equipo implementador del SGSI

Las responsabilidades para el SGSI son las siguientes:

- El Oficial de seguridad de la información es el responsable de garantizar que el SGSI sea implementado y mantenido de acuerdo con esta Política.
- La Alta Gerencia debe garantizar que todos los recursos necesarios estén disponibles.
- El Oficial de seguridad de la información es el responsable de la coordinación operativa del SGSI, como también de informar su desempeño.
- La Alta Gerencia debe revisar el SGSI al menos una vez por año o cada vez que se produzca una modificación significativa; y debe elaborar minutas de dichas reuniones. El objetivo de las verificaciones por parte de la dirección es establecer la conveniencia, adecuación y eficacia del SGSI.
- El Oficial de seguridad de la información implementará programas de capacitación y concienciación de empleados sobre seguridad de la información.
- La protección de la integridad, disponibilidad y confidencialidad de los activos es responsabilidad del propietario de cada activo.
- Todos los incidentes o debilidades de seguridad deben ser reportados a la Mesa de Ayuda.
- El Oficial de seguridad de la información definirá qué información relacionada con la seguridad de la información será comunicada a qué parte interesada (tanto interna como externa), por quién y cuándo.
- El Oficial de seguridad de la información y La Gerencia de Gestión Humana es el responsable de adoptar e implementar el Plan de capacitación y concienciación, que corresponde a todas las personas que cumplen una función en la gestión de la seguridad de la información.
- El equipo implementador definirá la modificación, aprobación y publicación de cambios en la documentación del SGSI.

4.5. Responsabilidades para todo el personal de CONECTA

- Todo personal debe conocer sus roles y responsabilidades de acuerdo con el organigrama de la empresa.
- El equipamiento de dispositivos móviles que contiene información importante, sensible o crítica no debe ser desatendido y, en lo posible, debe quedar resguardado bajo llave o se deben utilizar trabas especiales para asegurarlo.
- Cuando se utiliza equipamiento de dispositivos móviles en lugares públicos, el usuario debe tener la precaución de que los datos no puedan ser leídos por personas no autorizadas.
- La persona que utiliza equipamiento de dispositivos móviles fuera de las instalaciones es responsable de revisar al finalizar la jornada, que su información se encuentre sincronizada en la nube privada de CONECTA.
- Evitar el acceso no autorizado de personas a la estación de trabajo donde se realiza la actividad de teletrabajo.
- Los Colaboradores debe conocer los acuerdos de confidencialidad, propiedad intelectual, reglamento interno, proceso disciplinario, política antisoborno y el conocimiento del SGSI.
- La Alta Gerencia debe garantizar que todos los recursos necesarios estén disponibles para desempeñar los roles y responsabilidades del puesto asignado.

- Las claves generadas por los Colaboradores no deben ser distribuidas por ningún medio (oral, escrito, electrónico, etc.); las claves deben ser cambiadas si existen indicios de que puedan estar en riesgo las mismas claves o el sistema (en ese caso, se debe informar un incidente de seguridad).
- Los Colaboradores deben colocar contraseñas que tenga como mínimo ocho caracteres, incluyendo números, letras y caracteres especiales. La clave no debe ser de palabras de uso común, y no debe estar relacionado a datos personales.
- Las claves deben ser cambiadas cada 3 meses, en el primero ingreso al sistema y no deben ser almacenadas en un sistema de registro automatizado (por ej., macros o explorador o temporales).
- No se debe colocar información en el escritorio del dispositivo tecnológico (pantallas limpias) y se debe bloquear la sesión a los 3 minutos de inactividad o al no encontrarse en la estación de trabajo.
- No se encuentra autorizado la instalación de programas que comprometan la seguridad, integridad y disponibilidad de la empresa.
- Cualquier invitado que no sea parte de CONECTA, debe ser autorizado para su ingreso, registrado y siempre debe estar acompañado en las instalaciones.
- La información de la organización puede ser intercambiada a través de correo electrónico, transferencia de datos por medio de plataformas autorizadas.

4.5. Comité de Seguridad

El Comité de Seguridad debe estar conformado por, Gerente General, Subgerente, Arquitecto de Soluciones, Gerente Financiero, Gerente de Gestión Humana y el Oficial de Seguridad de la Información. El Comité será el responsable de impulsar, velar y responder por la seguridad de la información de la empresa, mediante la mejora continua del SGSI implementado en CONECTA.

4.6. Comunicación de la Política

El Oficial de seguridad de la información debe asegurarse que todo el equipo de CONECTA, como también los participantes externos correspondientes, estén familiarizados con esta Política.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

CONECTA cumple con los requisitos legales y normativos de un SGSI basado en la ISO 27001, con el objetivo de mantener la fidelidad de los clientes garantizando que todas nuestras decisiones se basen en la mejora continua, preservando la confidencialidad, integridad y disponibilidad de los servicios.

5. Apoyo para la implementación del SGSI

A través del presente, la alta Gerencia declara que en la implementación y mejora continua del SGSI se contará con el apoyo de los recursos adecuados para lograr todos los objetivos establecidos en esta Política, como también para cumplir con todos los requisitos identificados.

6. Propiedad del documento

El propietario de este documento es el Oficial de Seguridad de la Información, que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

Responsable del SGSI:	Aprobado por:
Francisco Espinel Oficial de Seguridad de la Información Fecha 18/08/2023 Conecta/Heaven	Bolivar Bermeo Gerente General Fecha 18/08/2023 Conecta