POLÍTICA

SEGURIDAD Y PRIVACIDAD

Versión 2.0
Julio de 2022

INNK
Andrés Bello 2711, Ofic 2302. Las Condes. Santiago – Chile
Correo: hola@innk.cl
Web: www.innk.cl

Control de cambios

Versión:	Fecha:	Modificado por:	Descripción:
1.0	2020	No Aplica	Primera versión del documento
2.0	26-07-2022	Coordinador de SGSI	Actualización de política según requisitos de la Norma ISO 27001

Información de Firmas

Elaboración del documento	Revisión del documento	Aprobación del documento
Coordinador del SGSI	Coordinador del SGSI	CEO

INNK
Andrés Bello 2711, Ofic 2302. Las Condes. Santiago – Chile
Correo: hola@innk.cl
Web: www.innk.cl

Contenido

INNK
Andrés Bello 2711, Ofic 2302. Las Condes. Santiago – Chile
Correo: hola@innk.cl
Web: www.innk.cl

1. OBJETIVO

El objetivo de esta Política es establecer los lineamentos generales de seguridad y privacidad dentro de la organización.

2. ALCANCE

Esta política de seguridad aplica para INNK y sus colaboradores.

3. REFERENCIA NORMATIVA

La presente política se define considerando las recomendaciones de las siguientes normativas:

- Norma NCh-ISO 27000:2014, Sistemas de gestión de la seguridad de la información - Visión general y vocabulario.
- Norma NCh-ISO 27001:2013, Sistemas de gestión de la seguridad de la información – Requisitos A.12.3, A.12.5, A.13.2.2, A.14.1.3, A.14.2.5, A.14.2.9, A.16.1.1, A.16.1.7, A.17.1.1, A.17.1.2, A.18.1.2
- Norma NCh-ISO 27002:2013, Código de prácticas para los controles de seguridad de la información, Control 12.3, 12.5, 13.2.2, 14.1.3, 14.2.5, 14.2.9, 16.1.1, 16.1.7, 17.1.1, 17.1.2, 18.1.2.

4. DEFINICIONES

No Aplica.

5. ROLES Y RESPONSABILIDADES

CEO / Coordinador del Sistema de Seguridad de la Información: Asegurar que las materias abordadas en esta política se ejecutan y se cumplen, identificar como se manejan los no cumplimientos, promover la difusión y sensibilización de las materias abordadas en este documento, revisar periódicamente la presente política detectando y proponiendo mejoras. Recibir y dar respuesta a los incidentes de seguridad de la información ocurridos.

Colaboradores: Dar cumplimiento a la presente política de seguridad de la información y a todas las responsabilidades en materia de seguridad de la información que hayan sido definidas y asignadas.

6. DESCRIPCIÓN DE LA POLÍTICA

6.1. PROTECCIÓN, CIFRADO DE TRANSACCIONES Y MANTENCIÓN DE DATOS

6.1.1.- Los respaldos de la base de datos, tanto física como lógica, son gestionados por Heroku, nuestra plataforma en donde está montado el software. Asegurando respaldos de la BD en distintas localidades y creando backups lógicos frecuentemente de la BD.

6.1.2.- Nadie que no sea registrado como usuario de una compañía puede acceder a los datos y contenido creado por esta. A excepción del soporte de INNK.

6.1.3.- Los datos y contenido creado en una compañía no serán accesibles ni visibles para otras compañías que utilicen el software. 1

6.1.4.- INNK utiliza el protocolo HTTPS mediante un certificado SSL y un comodín al dominio de la institución (por ejemplo: institución.INNK.cl). Este protocolo cifra toda transmisión de datos garantizando que toda la información vertida en la plataforma no pueda ser consultada por agentes ajenos a ella.

6.1.5.- INNK cuenta con la extensión de seguridad DNSSEC que garantiza que el dominio no pueda ser utilizado por terceros, para evitar el riesgo de phishing (suplantación de identidad). 1.6.- Se utiliza un sistema de encriptación de contraseñas basado en el algoritmo Blowfish que dificulta intentos de robo de información de las cuentas

6.2. PRUEBAS DE SOFTWARE

6.2.1.- Un equipo especializado realiza regularmente pruebas en representación de los usuarios finales. El área de desarrollo de sistemas de INNK deberá entregar el software desarrollado con códigos fuentes al área responsable de ejecutar las pruebas, el cual es revisado para encontrar códigos mal intencionado y debilidades de seguridad, para luego ser compilado e iniciar las pruebas correspondientes.

INNK
Andrés Bello 2711, Ofic 2302. Las Condes. Santiago – Chile
Correo: hola@innk.cl
Web: www.innk.cl

6.2.2.- Los tipos de pruebas se planifican para garantizar la integridad de la información en producción. Además, estos procedimientos se realizan en un ambiente de pruebas, separado al ambiente de producción. Este sandbox es lo más idéntico, en su configuración, al ambiente real de producción.

6.3. MANTENIMIENTO DEL SOFTWARE

6.3.1.- Heroku está constantemente monitoreando el rendimiento del sistema. Si llegan a ocurrir problemas de tiempos de respuesta o fallas del sistema, entre otras cosas, Heroku avisa por medio de un correo al administrador de INNK para tomar las acciones necesarias.

6.3.2.- Aparte del monitoreo de Heroku, el soporte de INNK también realiza monitoreos constantes, mejoras continuas y correcciones al software respectivamente.

6.4. PROPIEDAD INTELECTUAL Y ADMINISTRACIÓN DE DATOS

6.4.1.- Todos los derechos de propiedad intelectual de los datos y contenido creado por el cliente, son de propiedad exclusiva del cliente.

6.4.2.- El cliente puede solicitar el borrado de los datos en cualquier momento si lo estima conveniente. Una vez solicitado esto, el equipo de soporte de INNK se encargará de evaluar el tiempo necesario y, una vez informado, procederá al borrado de datos.

6.4.3.- Cualquier tipo de información interna del cliente no puede ser vendida, transferida o intercambiada con terceros para ningún propósito diferente al del servicio contratado y se cumplirá con los procedimientos de autorización internos para los casos en que se requiera.

6.5. POLÍTICA DE RECUPERACIÓN DE DESASTRES (DRP)

6.5.1.- Como INNK es un software que está en la nube y sus componentes críticos están montados en Heroku, INNK se cobija en las políticas de recuperación de desastres que posee Heroku. El cual, se encarga de mantener más de un equipo físico encargado de gestionar el servidor de INNK, su base de datos y otros componentes de INNK.

6.5.2.- En caso de fallar cualquier componente montado en Heroku por un desastre, el servicio se mantendría ininterrumpido y el componente sería reasignado para ser gestionado por otro equipo

INNK
Andrés Bello 2711, Ofic 2302. Las Condes. Santiago – Chile
Correo: hola@innk.cl
Web: www.innk.cl

de Heroku. Esta es una de las razones por la cual no podemos entregar especificaciones de la IP o ubicación física de los equipos que se encargan de gestionar los componentes de INNK, ya que Heorku los maneja dinámicamente.

6.5.3.- Los encargados de monitorear y asistir en este tipo de casos son el director de INNK Francisco Martinez (francisco.martinez@INNK.cl) y el líder de desarrollo Matías Salgado (matias.salgado@INNK.cl).

6.5.4.- En relación al RPO de INNK. Nuestro servidor ofrece la recuperación directa de los datos con un intervalo de hasta 7 días atrás desde el momento de solicitar la recuperación. También, se realizan backups de la base de datos diariamente.

6.5.5.- INNK asegura que el uptime es de un 99.9%. El RTO que se tolera para los problemas de uptime que tenga el software está especificado en los tiempos de resolución de problemas planteados en las políticas para procedimiento de soporte e incidencias informáticas de INNK, considerandose de severidad alta.

6.6. RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA

6.6.1.- Junto a todos los cifrados de transacción y protección de datos establecidos en el punto 6.1, INNK también cuenta con protección con Web Application Firewall, protección preventiva para ataques DDoS y herramientas de monitoreo de servidores.

6.6.2.- En el caso de sospecha de un ataque informático se le otorgará alta prioridad y se realizarán todos los esfuerzos para identificar el ataque monitoreando y revisando el servidor y reportes del firewall. De confirmarse éste, se enviará un reporte avisando rápidamente a los clientes que el sistema se encuentra bajo ataque y se tomarán todas las medidas para aumentar las defensas del firewall y recursos del servidor Luego, se analizará toda la información disponible relacionada al incidente para poder identificar qué sistemas, redes y datos han sido comprometidos.

6.6.3.- En caso de que se haya encontrado alguna brecha de seguridad en el software por la cual ocurrió el incidente, se procederá a la identificación y corrección de ésta, junto con un inicio de procedimiento de pruebas y ethical hacking para validar que no vuelva a ocurrir un incidente por ese medio.

6.6.4.- En caso de que se haya perdido algún dato, se utilizará el respaldo diario que realiza Heroku para restituir en lo posible los datos perdidos.

6.6.5.- Una vez determinado el alcance del incidente se enviará un segundo reporte a nuestros clientes para que estén informados. El plazo de este reporte depende del tiempo que tome determinar el alcance del ataque.

6.6.6.- Se realizarán todos los esfuerzos y herramientas posibles para identificar el o los autores del incidente para reportar a las autoridades correspondientes.

6.6.7.- Los reportes enviados a nuestros clientes serán por medio un correo electrónico en el que se indique lo sucedido y de ser necesario se adjuntarán archivos con datos necesarios asociados al reporte.

7 ACTUALIZACIÓN DE LA POLÍTICA

Dentro de la mejora continua de las políticas de seguridad de la información, esta política debe ser revisada al menos una vez al año, a partir de la fecha de entrada en vigor. El proceso se debe realizar según las definiciones del proceso PR-01 de Información Documentada.

8 DIFUSIÓN DE LA POLÍTICA

- La totalidad de las políticas deben ser informadas a las Jefaturas de la compañía para que los difundan según el nivel de acceso permitido a cada colaborador.
- El mecanismo formal de comunicación es el correo institucional de la compañía.

9 CONTROL DE REGISTROS

N°	Nombre	Responsable	Almacenamiento			
			Lugar / Responsable	Medio / Recuperación	Tiempo	Disposición final
	No Aplica	No Aplica	No Aplica	No Aplica	No Aplica	No Aplica

INNK
Andrés Bello 2711, Ofic 2302. Las Condes. Santiago – Chile
Correo: hola@innk.cl
Web: www.innk.cl