POLÍTICA

SEGURIDAD DE LA INFORMACIÓN

Versión 1.0
Abril 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	12-04-2022	No Aplica	Primera versión del documento

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

INNK

Andrés Bello 2711, Ofic 2302. Las Condes. Santiago – Chile

Correo: hola@innk.cl

Web: www.innk.cl

1. OBJETIVO

La información administrada necesita ser protegida de situaciones que atentan contra su disponibilidad, integridad y confidencialidad, amenazas que en definitiva pueden poner en riesgo la continuidad del negocio y exponer a la organización a incumplimientos legales. Para mitigar estos riesgos, surge la necesidad de definir políticas de seguridad de la información al interior de la empresa, a las que deberán adherirse todos los colaboradores, permitiendo de esta forma controlar de una mejor manera el uso de los datos a los que se tiene acceso.

INNK apoya a las empresas y organizaciones a gestionar sus nuevas ideas y proyectos de forma ágil, en un ambiente digital que favorece la colaboración de los equipos y la trazabilidad de los resultados, por lo cual existe la necesidad de contar con controles y políticas para la seguridad de la información, los cuales se definen en el cuerpo de este documento.

2. ALCANCE

- Todos los colaboradores, independientemente de la relación contractual con la Organización, proveedores de servicios externos, consultores, auditores, contratistas que accedan a las instalaciones de la compañía, ya sea física o remotamente para realizar trabajos y/o empleen recursos de tecnologías de información.

- Todas las instalaciones, equipamiento (incluyendo equipos portátiles y accesorios móviles) para procesar o almacenar información y redes.

- Todo el software para el procesamiento de datos o transporte de comunicaciones, sin importar el o los medios de almacenamiento o método de procesamiento que se disponga para sus fines.

- La utilización de hardware, software y recursos de terceros que INNK tenga en propiedad o bajo su dominio o licenciamiento o derecho de uso.

- Los ambientes y recintos de INNK en los cuales se procesa información y alojan redes de comunicaciones.

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.5
- Norma NCh-ISO 27002:2013, Código de prácticas para los controles de seguridad de la información, Control 5.

4. DEFINICIONES

Confidencialidad: La información debe ser conocida únicamente por aquellas personas que estén autorizadas para acceder información específica del negocio. Esto es necesario para proteger los asuntos reservados como planes estratégicos, información legal, de recursos humanos, información de los empleados y cualquier dato sensitivo.

Integridad: La información de INNK solamente puede ser agregada, modificada o eliminada por personas y/o procesos debidamente autorizados. Esto es necesario para garantizar que la información que soporta el negocio sea precisa y completa para que las decisiones que se tomen utilizándola produzcan los resultados que se esperan.

Disponibilidad: La información debe estar cuando se necesita en el formato requerido para su procesamiento, para asegurar que los procesos de negocio y las decisiones sean oportunas.

Propietarios de la Información: Es el dueño del proceso que utiliza o genera dicha información.

Usuarios de la Información: Es aquella persona, colaborador interno o externo, que con la debida autorización introduce, borra, cambia o lee información de la compañía.

Los usuarios sólo deben tener acceso a la información a la que están autorizados para ver o procesar y las autorizaciones que se otorguen deben limitar su capacidad, de forma que no puedan realizar actividades distintas de aquellas para las que se otorgó permiso.

Activos de información: Es cualquier componente que contenga información (sea humano, tecnológico, software, etc.) que sustenta uno o más procesos de negocios de una unidad o área de negocio.

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

INNK ha decidido implementar un Sistema de Gestión de la Seguridad de la Información (SGSI), por lo cual se compromete a cumplir con los requisitos legales y los aplicables a la norma ISO 27001:2013, con el fin de conseguir la mejora continua del sistema de gestión de seguridad de la información.

Las políticas de seguridad descansan siempre en el establecimiento de responsabilidades por parte de las personas que manejan y procesan datos e información. Cualquier incidente en materia de seguridad de la información puede ocasionar perjuicios económicos a la Compañía de diversa consideración. Es por ello, que las personas relacionadas de cualquier forma con los procesos de información deben ser conscientes y asumir que la seguridad es asunto de todos y, por tanto deben conocer y respetar las normas de INNK en este aspecto.

Como parte de las exigencias en materia de seguridad de la información, es fundamental que todos los colaboradores conozcan sus responsabilidades con precisión. Todo colaborador es responsable de cumplir las políticas, estándares, directrices y procedimientos que, en materia de seguridad de la información, estén vigentes en cada momento, así como también notificar a su nivel jerárquico superior o al responsable de seguridad ante una excepción de alguna norma particular y de las causas que lo motivan.

Igualmente, esta exigencia se aplicará a terceras personas que tengan acceso o que procesen información de INNK.

La información confidencial y la propia del negocio no pueden ser difundidas fuera del ámbito en que ésta debe ser tratada.

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

Lo anterior se sustenta en el cumplimiento de los siguientes compromisos del Sistema de Gestión de Seguridad de la Información y sus respectivos objetivos, por parte de INNK:

- Mejorar continuamente la efectividad del Sistema de Gestión de Seguridad de la Información (SGSI).
    - Implementar planes de acción para incidentes de seguridad de la información y no conformidades que resuelvan de raíz los problemas identificados.
- Cumplir con los requisitos legales y los aplicables a la seguridad de la información, según lo establecido en la norma ISO 27001:2013
    - Mantener igual o sobre 60 el valor del NPS (Net Promoter Score) en el indicador relativo a Seguridad de la Información (confidencialidad, disponibilidad e integridad) de la evaluación realizada a nuestros clientes.
    - Mantener vigente el Sistema de Gestión de la Seguridad de la Información implementado por la norma ISO 27001:2013.
- Proteger la confidencialidad de la información sensible relacionada con la empresa y sus clientes.
    - Implementar planes de acción para tratamiento de incidentes de seguridad de la información y no conformidades relacionadas con afectación de la confidencialidad
- Garantizar la integridad de la información de la empresa, que la misma sea precisa y completa.
    - Implementar planes de acción para tratamiento de incidentes de seguridad de la información y no conformidades relacionadas con afectación de la integridad
- Asegurar la disponibilidad de la información cuando se necesite, para asegurar la continuidad de los procesos.
    - Implementar planes de acción para tratamiento de incidentes de seguridad de la información y no conformidades relacionadas con afectación de la disponibilidad.
- Promover en sus colaboradores el conocimiento de dicha Política de Seguridad de la Información, así como la importancia de su contribución a la eficacia del SGSI.
    - Difundir el Sistema de Seguridad de la Información por medio de la ejecución de un Plan de difusión anual.

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

- Capacitar en Seguridad de la Información por medio de la ejecución de un Plan de capacitación anual.

6.1. ROLES Y RESPONSABILIDAD EN SEGURIDAD DE LA INFORMACIÓN (A.6.1.1)

INNK ha definido y asignado las responsabilidades relativas a la seguridad de la Información, definiendo para cada puesto de trabajo, tanto las funciones del personal que lo ocupa como sus responsabilidades, todo ello se realizará conforme al documento general perfiles de cargo.

Se han definido y asignado las responsabilidades relativas a la seguridad de la información, definiendo para cada perfil los accesos, autorizaciones y responsabilidades que le corresponden de según la Política de Control de Acceso, la cual se encuentra bajo el amparo de la presente Política de Seguridad de la Información.

6.2. SEGREGACIÓN DE FUNCIONES (A.6.1.2)

Los usuarios tendrán únicamente acceso a la información necesaria para el desarrollo de su actividad, para reducir el riesgo y evitar manipulaciones no autorizadas, se realiza una segregación de las tareas de responsabilidad en la gestión de la información de acuerdo con el rol que desempeñan. Existen perfiles en las distintas plataformas que se utilizan en la empresa. Cada perfil solo puede revisar la información limitada a su cargo. Por ejemplo: Jefe de área de Desarrollo, Devops, Desarrolladores, etc.

En caso de necesitar otra información se tendrá que contactar con su jefe inmediato para verificar su aplicabilidad y correspondiente justificación, para realizar la solicitud correspondiente.

En caso de clientes, cuando éstos tengan necesidad de acceder a la red de la Compañía o a las plataformas, esto se debe gestionar por medio de requerimientos al área de Desarrollo de INNK. Todas estas solicitudes tienen que ser solicitadas al Coordinador de Sistema de Gestión de Seguridad de la Información.

La instalación, uso, copia o venta de software y de otro tipo de información no autorizado bajo licencia del fabricante o dueño, constituye una infracción a los derechos de propiedad y queda estrictamente prohibida. La instalación y uso de software libre, debe tener una justificación de negocio y la aprobación formal de la jefatura correspondiente, habiéndose además comprobado debidamente la autenticidad del software y el cumplimiento de las condiciones para su uso.

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

El software debe instalarse de acuerdo a las políticas de seguridad correspondientes, incluyendo su revisión por medio de una versión actualizada del antivirus estándar de la Empresa.

6.3 CONTACTO CON LAS AUTORIDADES (A.6.1.3)

Es necesario centralizar el contacto con autoridades según distintas circunstancias según lo especificado en el siguiente anexo que se utiliza en caso de ocurrir algún siniestro, se especifican las autoridades que deben ser contactadas bajo ciertas circunstancias como: incendios, inundaciones, robos, asaltos, interrupción o intermitencia de internet, telefonía, electricidad u otros.

AUTORIDAD	CIRCUNSTANCIA	DETALLES DE CONTACTO
Administración Edificio	• Incendio. • Inundación (vía de agua). • Aviso de explosivos. • Rescate en ascensores. • Fallas de aire acondicionado. • Otras fallas del edificio.	Contacto del encargado **Nombre:** Gerardo Wielandt B. **Teléfono:** 22345673 **Correo:** gwielandt@costavita.cl
Bomberos	• Incendio. • Rescate en altura. • Rescate en ascensores • (Rescate Edificio).	Teléfono: **132**
Carabineros	• Robo. • Asalto. • (Evento en Edificio).	Teléfono: **133**
Soporte Técnico -Movistar	• Interrupción o intermitencia en Conexión a Internet.	**Ejecutivo:** Julio Guerrero **Teléfono:** 6006000280 **Correo**: jcguerreros@empresas.movistar.cl
Enel	Electricidad: • Interrupción. • Emergencia.	Llamar al: **600 696 0000** o al **22 696 0000** desde celulares. Ingresar a sitio web (www.enel.cl) para reportar emergencia indicando el número de cliente del holding Solunegocios. Oficina 1201: **3042486-7** Oficina 1203: **3042488-3** Oficina 1204: **3042489-1**

		https://www.enel.cl/es/clientes/servicios- en-linea/reporte-de-emergencia.html

Debe revisarse periódicamente para verificar que el listado de autoridades a contactar y que los datos de cada contacto están actualizados. Debe estar impreso y a la vista en:

- Oficinas administrativas.

Los registros que evidencian la operación de este procedimiento son las llamadas, correos y tickets enviados cuando se presentan las situaciones que se detallan en la Tabla adjunta
En el caso de llamados a bomberos, Carabineros y similares, no existirá registro de la llamada, dada que se tratan de emergencias. Sin embargo, se tomarán como evidencia de operación (registro) los correos electrónicos internos o con terceros donde se mencionen dichas llamadas.

En el caso de comunicaciones con proveedores de comunicaciones (internet), serán evidencia de operación (registros) los correos electrónicos y/o llamadas realizadas a los proveedores por parte del Jefe de Administración y Finanzas.

Dentro de la mejora continua, esta tabla debe ser revisada constantemente, a partir de la fecha de entrada en vigencia.

6.4 CONTACTO CON GRUPOS DE INTERÉS (A.6.1.4)

En cuanto al contacto con grupos especiales de interés, INNK se apoya de forma interna con grupos especiales de colaboradores con fortalezas técnicas, quienes están permanentemente involucrado en participación de foros, capacitaciones y charlas relativas a seguridad de la información.

Hay una revisión particular del personal en temas relacionados a desarrollo de software, tecnologías devops, ingeniería de software, entre otros.

Se mantiene contacto con empresas de ethical hacking quienes emiten consejos de seguridad, envían alertas tempranas de avisos y parches de seguridad relacionados con ataques, vulnerabilidades y otros.

6.5 SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS (A.6.1.5)

INNK aborda la seguridad de la información en la gestión de proyectos de la organización, sin importar el tipo de proyecto en cuestión, a través de cada uno de los procedimientos operativos.

6.6 SEGURIDAD EN LAS COMUNICACIONES Y OPERACIONES

6.6.1 USO DE INTERNET EN LAS OFICINAS DE LA ORGANIZACIÓN (A.13.1)

Queda prohibido que los usuarios accedan a otras redes privadas o redes de clientes sin la autorización de su Jefatura.

El acceso a Internet por los colaboradores de INNK, queda sujeto a las siguientes consideraciones:

1. El colaborador debe ser responsable y profesional en su uso.

2. Con el fin de verificar el buen uso de la misma, el empleador podrá establecer medidas de control, mediante la revisión de los logs de actividad de los usuarios. Estas medidas de control serán compatibles con el respeto de la privacidad y dignidad de los dependientes.

3. Los usuarios de los sistemas de información de la Empresa deben respetar en todo momento el derecho de propiedad intelectual, la seguridad de los sistemas de terceros y la privacidad ajena al acceder o usar la plataforma Internet

4. La Empresa posee la potestad, de restringir el acceso a materiales en Internet. Esta potestad no implica un deber de regular el contenido de la Información en Internet. En todo caso, la ausencia de dichas restricciones no implica, ni debe ser entendida como una autorización para acceder a tal material.

5. La información confidencial o sensible, patentada o interna, sólo puede ser transmitida a través de Internet previa autorización de la Jefatura correspondiente y dueño de la información.

6. Se prohíben los comentarios, bromas, insultos y comentarios de índole sexual, racial u otras, ofensivas o ilegales a través de Internet. El uso de Internet para observar, tener acceso, cargar, descargar, almacenar, transmitir, crear o manipular en otra forma materiales ofensivos, pornográficos o sexualmente explícitos.

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

7. El Empleador podrá controlar todas las conexiones a Internet mediante la instalación de servicios de Proxy para el acceso de los colaboradores y la recepción de información desde Internet a través de Firewalls y antivirus en los servidores de entrada.

8. Se prohíbe a los colaboradores no autorizados alterar, eliminar o burlar de cualquier modo, dichos servicios de Proxy, Firewalls o Antivirus de los sistemas de información de la Empresa.

6.6.2 USO DE CORREO ELECTRÓNICO (A.13.2.3)

El uso del sistema de correo electrónico está restringido a asuntos laborales. Su empleo para asuntos personales está autorizado siempre y cuando (a) consuma una mínima parte de los recursos y (b) no interfiera con el cumplimiento de las obligaciones del colaborador.

Está prohibido utilizar el sistema de correo para el desarrollo de actividades políticas, comerciales o de entretenimiento o para la transmisión de mensajes vulgares u obscenos.

El usuario deberá responsabilizarse por efectuar copia de los mensajes electrónicos si considera que contienen información de referencia o de importancia para el desempeño de las labores de éste. No se pretende que el sistema de correo electrónico sirva de método de almacenamiento de archivo.

6.6.3 CONFIGURACIÓN DE REDES (A.13.1)

Todo cambio relevante en los dispositivos que conforman las redes en INNK debe quedar debidamente documentado, considerando como cambio relevante todo aquel que se realice sobre componentes de una red, como lo son, por ejemplo:

- Routers
- Switches
- Firewall

Dichos cambios deben ser realizados por el equipo asignado por la Jefatura correspondiente.

6.6.4 RELACIÓN CON PROVEEDORES (A.15.1)

Todo proveedor externo de la compañía debe contar con un documento formal que respalde la relación con la Compañía, ya sea un acuerdo de servicios o un Contrato. En dicho documento se

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

debe abordar todos los requisitos de seguridad de información pertinentes, para mitigar riesgos asociados al acceso del proveedor a los activos de la Compañía.

Al momento de definir cada acuerdo de servicio o contrato de servicio se deben tener en cuenta los siguientes ámbitos de acción a controlar según sean los servicios por contratar:

- Control de accesos físicos.
- Control de accesos a información.
- Control de activos.
- Confidencialidad de información
- Seguridad en las operaciones y todos aquellos ámbitos regulados por la presente política de seguridad de la información.

En caso de ausencia de un documento formal, el proveedor debe aceptar explícitamente la cláusula 6.6.4 de la política de seguridad de la información de la compañía, y comprometerse a su cumplimiento.

El proveedor debe comprometerse a administrar y tratar la información de INNK con la debida confidencialidad y uso de información únicamente con fin de cumplir con las obligaciones contractuales.

Queda formalmente prohibido que los proveedores hagan uso de la información de la compañía o de sus clientes para fines personales o fuera del alcance del contrato de servicio.

En caso de tener proveedores que generen una cadena de suministro de tecnologías de información y comunicaciones, deben velar por el cumplimiento de la presente política según la aplicabilidad.

6.7 POLÍTICAS COMPLEMENTARIAS RELACIONADAS

INNK, adicional a lo mencionado en el punto anterior, donde se detalla la política de seguridad de la información, considera la definición de las siguientes políticas que son parte integral del conjunto de políticas de seguridad de la información.

6.7.1 POL-02 POLÍTICA DE SEGURIDAD Y PRIVACIDAD

Establecer los lineamentos generales de seguridad y privacidad dentro de la organización.

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

6.7.2 POL-03 POLÍTICA DE DISPOSITIVOS MÓVILES

Establecer las directrices de seguridad para los dispositivos móviles que son propiedad de INNK, o propiedad de sus colaboradores y controlar los riesgos de seguridad asociados a dichos dispositivos.

6.7.3 POL-04 POLÍTICA DE TELETRABAJO

Establecer las directrices para regular el trabajo remoto para los colaboradores y controlar los riesgos de seguridad para proteger la información a la que se accede, procesa o almacena en los lugares de trabajo remoto.

6.7.4 POL-05 POLÍTICA DE CONTROL DE ACCESO

Los usuarios sólo tendrán acceso a la información a la que están autorizados para ver o procesar y las autorizaciones que se otorguen deben limitar su capacidad, de forma que no puedan realizar actividades distintas de aquellas para las que se otorgó permiso.

6.7.5 POL-06 POLÍTICA DE PUESTO DE TRABAJO DESPEJADO Y PANTALLA LIMPIA

Establecer lineamientos y normas generales que regulen la protección y el uso de pantallas y escritorios no supervisados, durante y después de la jornada laboral, entendiendo éstos como pantallas de computador y/o escritorios que permanecen sin uso y sin un colaborador que esté vigilando y ejerciendo supervisión sobre la información que éstos contienen.

6.7.6 POL-07 POLÍTICA DE SEGURIDAD FÍSICA Y DEL ENTORNO

Establecer las políticas de seguridad física y del entorno de INNK y de sus colaboradores y evitar el acceso físico no autorizado, daños e interferencias contra las instalaciones de procesamiento de la información y la propia información

6.7.7 POL-08 POLÍTICA DE GESTIÓN DE ACTIVOS

Establecer las directrices para administrar o gestionar los activos que son propiedad de INNK, colaboradores y controlar los riesgos de seguridad asociados a dichos activos.

6.7.8 POL-09 POLÍTICA DE INTERCAMBIO DE INFORMACIÓN

Garantizar la seguridad de la información que se intercambia o transfiere dentro de INNK y con cualquier entidad externa a la misma, haciendo uso de cualquier recurso de comunicación.

6.7.9 POL-10 POLÍTICA DE RESPALDO DE DATA

La finalidad de esta política es regular la seguridad y la protección de los datos, aplicaciones, servicios informáticos contra todo tipo de fallas o accidentes tecnológicos. Estableciendo normas y políticas para el resguardo de la información, para posibilitar la recuperación de estos en el menor tiempo posible, esto a través de la restauración del respaldo.

6.7.10 POL-11 POLÍTICA DE CONTROL CRIPTOGRÁFICO

La finalidad de esta política es establecer los lineamientos para asegurar el uso adecuado y eficaz de la criptografía en INNK con el objetivo de proteger la confidencialidad, autenticidad e integridad de la información

6.7.11 POL-12 POLÍTICA DE DESARROLLO

Definir los lineamentos generales para el diseño e implementación de desarrollo seguro para aplicativos de software dentro de la organización.

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

INNK

Andrés Bello 2711, Ofic 2302. Las Condes. Santiago – Chile

Correo: hola@innk.cl

Web: www.innk.cl