Política de Seguridad y Privacidad de la Información

Código de documento: SEC005
Versión: V 6.0
Vigente desde: 20/08/2026

talana

Tabla de contenidos

1. Objetivo

El objetivo de este documento es establecer todos los lineamientos de seguridad y privacidad aplicados por Talana para proteger sus activos y garantizar la confidencialidad, integridad, disponibilidad y privacidad de su información alineados a la misión, visión y valores de la organización.

2. Alcance

El presente documento es aplicable en todas las fases del ciclo de vida de la información, el cual incluye desde la creación o generación, distribución, almacenamiento, procesamiento, transporte y consulta, hasta su destrucción, así como también alcanza a todos los sistemas involucrados, áreas y personal, tanto interno como externo que trabaja o manipula de algún modo activos e información de la empresa.

3. Lineamientos

3.1 Gestión con instituciones de seguridad de la información

La gestión con instituciones de seguridad de la información tiene como objetivo establecer y mantener un contacto con organizaciones especializadas que puedan proporcionar apoyo para la implementación y mantenimiento del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI).

Considerando los requisitos de las partes interesadas y las regulaciones aplicables, Talana mantiene contacto con las siguientes organizaciones para la comunicación y reporte de los incidentes de seguridad:

Organizaciones	Contacto
Agencia Nacional de Ciberseguridad (ANCI)	Tel: 1510; https://www.csirt.gob.cl/ +56447711131 ayuda@anci.gob.cl
Policía de investigaciones, PDI	134; https://www.pdichile.cl
NGT Tecnologias SpA (Resility)	Slack, Resility (#talana-cybersoc) https://resility.io/
Google	Tel: 1-929-270-4297 https://console.cloud.google.com/support/

Otras instituciones que deben ser contempladas en el SGSPI en caso de emergencias en Talana son:

Chile:

Organizaciones	Contacto
Carabineros de Chile	• Tel: 133; https://www.carabineros.cl
Bomberos de Chile	• Tel: 132
Ambulancias	• Tel: 131
Seguridad municipal Las Condes	• Tel: 1402, www.lascondes.cl/seguridad/seguridad.html

Perú:

Organizaciones	Contacto
Policía Nacional del Perú (PNP)	• Emergencias: 105 • Comisaría de Miraflores: (01) 445-7943 • Alerta Miraflores (Serenazgo y Policía): (01) 755-0100 o vía WhatsApp a los números 992087510 / 964108837.
Bomberos Voluntarios del Perú	• Emergencias: 116 • Central del Bomberos de Miraflores (B-28): (01) 445-7447 y (01) 242-5823.
Ambulancias	• Emergencias: 116
Municipalidad de Miraflores	• Central Telefónica: (01) 313-3000 • Línea de Servicio al Ciudadano (Aló Miraflores): (01) 313-3030

Para asegurar la concientización y el conocimiento de los colaboradores, la empresa también mantiene contacto con grupos de interés especial que les permite capacitarse y estar actualizados sobre las mejores prácticas, nuevas amenazas, alertas y/o vulnerabilidades de seguridad.

Organizaciones	Contacto
Fundación Sochisi	www.sochisi.cl
Hackmetrix	https://www.hackmetrix.com
Google	Tel: 1-929-270-4297 https://console.cloud.google.com/support/
SocRadar	www.socradar.com

3.2 Gestión de protección de datos personales

Talana comprende la importancia de la protección de datos personales y el cumplimiento de las normativas de seguridad y privacidad aplicables al SGSPI.

La seguridad implementada para la protección de datos de identificación personal es de manera general y consistente para toda la información de la empresa, sin distinción de la que contiene o no datos personales.

Con lo anterior garantiza que se permee la integridad, confidencialidad y disponibilidad en los datos personales que gestiona, todo de acuerdo con la Política

de Privacidad y Tratamiento de Datos Personales y Política de Seguridad de la Información en la Nube.

Además, Talana implementa los siguientes métodos de enmascaramiento de datos para garantizar su protección:

- Cifrado.
- Anulación o eliminación de caracteres.
- Variación de números y fechas.
- Sustitución (cambiar un valor por otro).
- Sustitución de los valores por su hash.

En caso de que sea necesario eliminar el vínculo y asociación del titular con sus datos personales, se implementa el Procedimiento de Anonimización de Datos Personales definido por la organización.

Todos los lineamientos establecidos en la presente política ayudan, en diferentes niveles, con la prevención de fuga de datos..

3.3 Gestión de los dispositivos móviles y el teletrabajo

La gestión de los dispositivos móviles y el teletrabajo tiene como objetivo asegurar el buen uso por parte de los colaboradores o partes externas, de los activos, la información de la compañía y los datos personales que procesan.

Por lo que Talana establece las siguientes medidas de seguridad y privacidad en relación a los dispositivos:

- Contar con inicios de sesión seguros utilizando un usuario y contraseña robusta.
  - En casos de teléfonos móviles y tablets, se implementa el acceso por medio de huella, patrón, reconocimiento facial u otro factor adicional de autenticación robusto.
- Eliminar el software innecesario.
- Actualizar el sistema operativo y aplicaciones de forma regular.
- Mantener el antivirus y firewall encendido en todo momento.
- Colocar todos los documentos y archivos en repositorios oficiales de la empresa para que estén respaldados y disponibles.
  - En la medida de lo posible, no se descargan archivos de manera local en los dispositivos. Y de hacerlo, éstos se eliminan una vez que ya no se necesiten.
- Mantener el cifrado de disco encendido.
- Mantener un área de trabajo segura y sin información confidencial a la vista.

- Generar copias de seguridad de manera periódica siguiendo los lineamientos establecidos en la Política de Tecnología y Operaciones de TI y en el Procedimiento de Gestión de Backups definidos por la empresa.
- Limitar la conexión con redes públicas para realizar actividades de trabajo.
    - Cuando el uso de estas redes sea muy necesario, se debe utilizar una VPN.
- Transmitir información sólo por medio de redes seguras y páginas web con protocolos HTTPS, y aplicar los lineamientos establecidos en la Política de Tratamiento de la Información definida por la empresa.
- Habilitar el rastreo y borrado remoto para los posibles casos de robo o extravío.
    - Al ocurrir un robo o extravío, el colaborador debe informar de inmediato a su jefe directo y a las autoridades pertinentes.
- En casos de urgencia donde surja la necesidad de utilizar equipos de terceros, se utiliza una sesión o ventana en modalidad “incógnito” para asegurar que no se puedan rastrear las direcciones web y que no se registre una trazabilidad de las claves o contraseñas utilizadas.
- Para los dispositivos propios de los colaboradores se deben implementar los lineamientos establecidos en la Política de BYOD definida por la empresa.
- No comprometer los DP a los que se tenga acceso.

3.3.1 Consistencia con la clasificación de la información

Al trabajar de forma remota o en movimiento, los colaboradores y partes externas se aseguran que la información es manejada de manera coherente respecto a su clasificación asignada, y de acuerdo con lo establecido en esta política.

3.3.2 Lineamientos de seguridad sobre el entorno

Talana establece las siguientes medidas de seguridad y privacidad para proteger sus activos de información en cualquier tipo de entorno:

- Garantizar un nivel de privacidad adecuado y asegurar que personas externas no puedan ver documentos, archivos o pantallas en los que se pueda visualizar información confidencial.
- Implementar los lineamientos establecidos en la Política de Escritorios Limpios definida por la empresa.

3.4 Gestión de los recursos humanos

La gestión de los recursos humanos tiene como objetivo seleccionar a las personas más adecuadas, mantener e incluso reforzar sus competencias, conocimientos,

habilidades y comportamientos éticos y garantizar la seguridad y privacidad de la información de la empresa.

Para esto, Talana realiza las siguientes actividades:

- Diseña e implementa un Procedimiento de Preselección y Selección de Personal que:
  - Valora el talento de las personas.
  - Respeta la igualdad de oportunidades y no promueven la discriminación de ningún tipo.
  - Asegura que la selección de personal se realiza con base en los criterios profesionales del candidato y alineados a las necesidades reales de la organización.
  - Cumple con la legislación laboral vigente.
  - Garantiza la confidencialidad y protección de los datos personales.

- Realiza la investigación de los candidatos de acuerdo a las regulaciones aplicables para validar la información proporcionada en la solicitud de empleo, como lo puede ser:
  - Los datos de identificación de la persona.
  - Las referencias personales, familiares y laborales.

Y una vez seleccionados los candidatos adecuados, se diseña e implementa un Proceso de Contratación y Desvinculación de Personal que:

- Asegura el establecimiento de los términos y condiciones de la relación laboral en el contrato acordado con el colaborador, incluyendo aquellos relacionados con las sanciones administrativas, la desvinculación y la devolución de todos los activos provistos por la compañía completando y firmando el Formato de Devolución de Equipos.
  - Puede ocurrir el caso en que personal interno o externo incurra en alguna desviación o incumplimiento de los lineamientos de seguridad y privacidad establecidos por la empresa, lo cual será motivo de sanciones administrativas e incluso legales, las cuales quedan por escrito en los contratos celebrados. Esto involucra un proceso disciplinario que considera:

- La identificación de la actividad o comportamiento inapropiado, o la violación de las políticas internas de la organización.
- La investigación adecuada para determinar la causa y el impacto de lo ocurrido.
- La definición de las acciones disciplinarias apropiadas a implementar, las cuales pueden incluir una advertencia verbal, por escrito, una suspensión temporal, una terminación del contrato, una acción legal o una combinación de estas medidas.
- El registro y documentación de las acciones disciplinarias tomadas.

➔ Formaliza un compromiso de confidencialidad y lealtad con el colaborador para proteger la información de la empresa.

➔ Brinda la inducción y concientización pertinente a los colaboradores sobre sus responsabilidades de seguridad y privacidad de la información y los riesgos asociados a sus funciones, así como también de la misión y visión de la empresa.

- Para esto además implementa un programa anual de capacitación y concientización sobre seguridad y privacidad de la información para todos los colaboradores, tanto internos como externos.

➔ Proporciona las políticas y procedimientos pertinentes que deben ser de conocimiento del colaborador para su lectura y comprensión.

➔ Entrega anualmente la política de seguridad y privacidad de la información a toda la empresa para su lectura y comprensión.

➔ Otorga los accesos y permisos pertinentes de acuerdo al puesto asignado, siguiendo los lineamientos establecidos en esta política y el Procedimiento de Gestión de Accesos definido por la empresa.

➔ Entrega anualmente la política de seguridad y privacidad de la información a toda la empresa para su lectura y comprensión. Para su aceptación firma el Documento de Aceptación de Política de Aceptación de la Política de Seguridad y Privacidad,

3.5 Gestión y clasificación de los activos de información

Los activos de información de la empresa y los recursos que le dan soporte son identificados, inventariados y clasificados en función de los requerimientos del negocio y del programa de seguridad y privacidad de la empresa.

Talana establece una adecuada gestión de sus activos y su clasificación, por medio de las siguientes acciones:

- La identificación y mantenimiento de un inventario de activos de información que abarca todos los dispositivos utilizados para las actividades de la empresa, ya sean de su propiedad o en casos excepcionales, de los colaboradores.
- La asignación de propietarios de los activos de información.
- La clasificación de la información en función a sus niveles de confidencialidad, integridad y disponibilidad.
- El acceso, manejo y tratamiento adecuado de los activos de información acorde a su clasificación asignada.

Lo anterior aplica indistintamente si el origen de la información es:

- Interna: Documentación generada por Talana, que cumpla con los requisitos de formato y uso de marca de la organización.
- Externa: Esto incluye información que no incorpore el formato de marca de Talana y/o formato corporativo.

Talana establece las siguientes categorías de clasificación:

- Pública: Es información que se puede hacer pública, sin que implique consecuencias negativas para la empresa, como es la información que es de conocimiento público.
- Confidencial de los empleados: Esto incluye información como, registros médicos, remuneraciones, datos personales del empleado, entre otros.
- Confidencial de la compañía: Como contratos, códigos fuente, contraseñas para sistemas críticos de TI, contratos de clientes, cuentas, planes de negocio, información de nuevos productos, información sensible del mercado, información que involucra datos personales del cliente, empleados o proveedores, etc.
- Confidencial del cliente: Esto incluye información de identificación como nombre, dirección, claves de acceso al sistema, remuneraciones, información que involucra datos personales de los empleados o reclutados, etc.

La empresa realiza la clasificación de su información dentro de los registros de su Inventario de Activos.

3.5.1 Etiquetado de los activos de información

Talana etiqueta sus activos de información con base en su clasificación asignada para identificarlos fácil y rápidamente.

Los métodos para el etiquetado de la información que pueden ser utilizados por la empresa son:

- **Versionado**, es decir indicando la clasificación de la información dentro del control de versiones que se encuentra en la documentación.

- **Encabezado o pie de página**, incluyendo en la parte superior o inferior dentro de la documentación la clasificación de la información correspondiente en todas las hojas que contenga.

Nota importante: Toda la información que no cuente con un etiquetado explícito será considerada como información confidencial de la Compañía.

Los datos personales son cualquier información concerniente a una persona física identificada o identificable, los sensibles son aquellos datos personales que afectan a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o un riesgo grave para éste. Éstos datos se etiquetan con base en su clasificación asignada.

3.5.2 Intercambio de información con partes externas

Talana implementa políticas, procedimientos y controles formales para proteger el intercambio de información a través de distintos medios de comunicación y acorde con la clasificación de la información a intercambiar.

La empresa define los lineamientos del intercambio de información en su Política de Tratamiento de la Información.

3.5.3 Saneamiento/ destrucción de activos y eliminación de información

Talana reconoce la necesidad de sanear, destruir o eliminar los activos y la información que ya no se consideren necesarios para la organización.

La información almacenada en sistemas de información, dispositivos o en cualquier otro medio de almacenamiento se elimina de forma segura por medio de:

- Sobreescritura electrónica.
- Borrado criptográfico.
- Herramientas de borrado seguro que estén previamente autorizadas y configuradas correctamente.
- Eliminación de versiones, copias y archivos temporales de todas las ubicaciones donde se encuentren.

Talana define los siguientes métodos de saneamiento y destrucción para garantizar que la reutilización o eliminación de activos y la información o datos personales contenida en ellos sea segura:

Tipo de activo de información	Saneamiento	Destrucción
Papel	No aplica.	Triturar.

Dispositivos móviles	Borrar manualmente toda la información almacenada: contactos, SMS, etcétera. Restaurar los valores predeterminados del fabricante.	No aplica; el equipo es reutilizado.
Servidores virtuales	Utilización de imagen maestra	Destrucción de la máquina lógica.
Equipo de cómputo	Restaurar configuración desde imagen de inicio, borrado de datos de usuario. Proceso de borrado seguro.	No aplica; el equipo es reutilizado.
USB / Discos Duros	Proceso de borrado seguro.	Triturar/destruir.

3.6 Gestión de los riesgos de seguridad y privacidad

La gestión de los riesgos de seguridad y privacidad dentro de la organización tiene como objetivo facilitar la identificación y evaluación de los eventos potenciales que podrían provocar la pérdida, ya sea operativa o tecnológica, que afecten la confidencialidad, integridad y/o disponibilidad de la información.

Otro de sus objetivos es establecer y priorizar planes de tratamiento adecuados que minimicen el impacto de los riesgos dentro de las operaciones de la compañía.

Talana establece un proceso formal dentro de su Metodología de Gestión de Riesgos que contempla lo siguiente:

- El alcance del proceso de gestión de riesgos y su necesidad de adaptación al contexto más actual de la empresa.
- La implementación de métodos para la identificación y evaluación de los riesgos de seguridad y privacidad de la información.
- El análisis y decisión de los planes de tratamiento de riesgo.
- La definición del umbral de tolerancia y los criterios de aceptación de los riesgos.
- La evaluación y aceptación del nivel de riesgo residual.
- La planificación y evaluación periódica de los riesgos, la cual se realiza por lo menos una vez al año o cuando ocurran cambios significativos dentro de la empresa.

Talana, además garantiza que los riesgos de seguridad se abordan de manera efectiva en la gestión de proyectos y durante todo su ciclo de vida, considerando los siguientes aspectos:

- La evaluación y tratamiento de los riesgos de seguridad de la información debe realizarse en una fase temprana del ciclo de vida del proyecto y con revisiones periódicas.
- Se debe evaluar y monitorear el progreso y efectividad del tratamiento de los riesgos.

3.7 Gestión de los accesos

La gestión de los accesos tiene como objetivo asignar y controlar los roles y permisos de los usuarios del personal o partes externas, utilizados para acceder a la información, sistemas, datos personales o aplicaciones de la empresa.

Para esto, Talana establece los siguientes lineamientos:

- Los colaboradores cuentan con un usuario único.
- Las altas, bajas y modificaciones de usuarios y/o permisos se realizan siguiendo el Procedimiento de Gestión Accesos definido por la empresa.
    - Al dar de alta a un nuevo usuario se otorgan los accesos y permisos estrictamente necesarios para llevar a cabo sus tareas de trabajo y garantizar una adecuada segregación de funciones.
    - Ante un cambio de funciones se eliminan los accesos relacionados con la función anterior y se asignan los accesos necesarios para las nuevas responsabilidades.
    - Al dar de baja a un usuario se eliminan o deshabilitan todos los accesos asociados a la persona.
- Los privilegios de administrador de los sistemas de la empresa son restringidos solo a personal capacitado y previamente autorizado.
- Los accesos son revisados periódicamente por lo menos una vez al año.
- El registro de los roles y permisos otorgados dentro de la empresa se realiza dentro de la Matriz de Accesos, la cual se actualiza conforme a los cambios que van ocurriendo.
- Las cuentas compartidas sólo están autorizadas cuando son necesarias por objetivos comerciales y/o operativos debidamente justificados.
- El acceso a entidades externas debe ser previamente autorizado por el propietario de la información y/o del activo correspondiente, y la necesidad del acceso debe estar debidamente justificada y ser coherente con la clasificación de la información definida por la empresa.
- La información almacenada en el entorno de nube puede estar sujeta al acceso y la gestión por parte del proveedor, por lo que para protegerla adecuadamente

se debe solicitar la aprobación del acceso al CTO, en conjunto con el Comité de Seguridad de la Información.
- Los usuarios desactivados o caducados para los sistemas y servicios que tratan los datos personales no deben volver a ser activados.
- Si el tratamiento de los datos personales es un servicio por parte de Talana, el cliente puede ser responsable de algunos o todos los aspectos de la gestión de la identificación del usuario.
- Si se sospecha que los usuarios que administran u operan sistemas y/o servicios que procesan datos personales están comprometidos, éstos deberán ser dados de baja de acuerdo al Procedimiento de Gestión Accesos de la organización.
- Si el usuario tiene acceso a los datos personales, se debe requerir información adicional para la autenticación como una pregunta de seguridad o un número PIN.

3.8 Gestión de contraseñas e información de autenticación

La gestión de contraseñas e información de autenticación tiene como objetivo asegurar la protección de la información sensible de la empresa por medio de contraseñas robustas y siguiendo las mejores prácticas de la industria.

Para esto, Talana establece los siguientes lineamientos, los cuales deben ser aplicados tanto por usuarios normales como por usuarios privilegiados:

- Está prohibido compartir información de autenticación o contraseñas, así como también el compartir credenciales en texto plano por medios no seguros.
- Las contraseñas por defecto que proporciona el proveedor, o que son generadas automáticamente, son robustas y únicas para cada persona y se cambian después del primer uso.
- Las contraseñas son personales e intransferibles, y es responsabilidad del usuario hacer un buen uso de ellas.
- Las contraseñas se cambian de manera regular cada 90 días y cuando se detecta actividad sospechosa.
- No se utiliza la misma contraseña para más de un sistema o aplicación.
- Las contraseñas tienen una longitud mínima de 12 caracteres y contienen minúsculas, mayúsculas, números y símbolos.
- Se determina la obligatoriedad de uso de los gestores de contraseñas aprobados por el área de Seguridad.
- Se configura el segundo factor de autenticación (2FA) para todas los sistemas y aplicaciones donde exista factibilidad técnica.
- No se escriben ni resguardan PINs o contraseñas al lado de computadores, teléfonos, en libretas, notas, etcétera.

3.9 Gestión de la criptografía

La gestión de la criptografía tiene como objetivo proporcionar un nivel más alto de seguridad y privacidad de la información para que ésta no pueda ser leída por personas no autorizadas.

Y para esto, Talana utiliza métodos criptográficos que protegen la confidencialidad, privacidad e integridad de su información y de los datos personales, no solo durante su almacenamiento, sino también durante su transferencia y recepción.

Estos métodos son aplicados en los siguientes elementos:

- Credenciales de accesos.
- Información compartida por medios no oficiales (archivos, correos electrónicos, etcétera).
- Información interna restringida para la mayoría de los empleados.
- Bases de datos.
- Todos los datos personales sensibles.
- Los siguientes datos personales generales:
  - De identificación
  - Laborales
  - Académicos
  - Tránsito y movimientos migratorios
  - Patrimoniales

Además, para ejecutar un protocolo de seguridad de criptografía eficiente, Talana considera lo siguiente:

- El establecimiento y gestión de las claves públicas y privadas, lo cual se realiza siguiendo el Procedimiento de Gestión de Claves Públicas y Privadas definido por la empresa.
- La autenticación de los usuarios.
- La aplicación de cifrado de mensajes y métodos de no repudio.

La organización establece que los métodos criptográficos a implementar son:

Activo de información	Método criptográfico	Especificaciones
Firma de documentos digitales	Firma electrónica	DocuSign
Firma de documentos laborales	Firma Digital Aprobada por DT	Talana

Almacenamiento de información en la nube	Cifrado simétrico	AES
Accesos a plataformas en trabajo remoto.	VPN	CATO
Mensajería por correo electrónico confidencial	Cifrado asimétrico	Estándar Open PGP
Datos personales sensibles	Cifrado simétrico	AES
Datos personales generales	Cifrado simétrico	AES

3.10 Gestión de la seguridad física

La gestión de la seguridad física tiene como objetivo proteger adecuadamente las instalaciones de la empresa y sus activos de información.

Para esto, Talana implementa las siguientes medidas de seguridad:

- Perímetro de seguridad física de las instancias y oficinas de la organización, considerando la protección contra amenazas externas y ambientales.
- Las instalaciones y oficinas de la empresa cuentan con los señalamientos pertinentes de seguridad para identificar salidas de emergencia, rutas de evacuación, extintores, etcétera.
- Las instalaciones y oficinas de la empresa son monitoreadas continuamente con herramientas como video vigilancia, guardias de seguridad y alarmas.
- Controles de acceso físico que generan registros de las entradas y salidas de colaboradores y visitantes.
    - Estos registros contienen fecha, hora de entrada y de salida, y en caso de ser proveedores o visitantes, el motivo de visita.
- Tanto los colaboradores como los visitantes deben portar una identificación visible mientras se encuentren en las instalaciones de la empresa.
- Aseguramiento de los activos de información, oficinas, instalaciones y centro de procesamiento de datos de la empresa con accesos biométricos, credenciales de acceso y/o puertas con códigos de acceso.
- Mantenimiento periódico del suministro de electricidad y agua, de los servicios de telecomunicaciones, alcantarillado, ventilación, aire acondicionado, etcétera.
- Designación de áreas para entrega y carga de material.
- Seguridad en el cableado estructurado.
- Mantenimiento periódico de los equipos y los procedimientos adecuados para autorizar su retiro de las instalaciones de la empresa.

- El mantenimiento de los equipos solo es realizado por personal autorizado.

- Separación de las instalaciones de procesamiento de información de las demás áreas de la empresa.

3.11 Gestión de la tecnología y las operaciones

La gestión de la tecnología y las operaciones considera todos los procesos operativos con el objetivo de garantizar la implementación de la seguridad y privacidad de la información en las operaciones y servicios del negocio.

Talana establece los lineamientos para estos procesos dentro de la Política de Tecnología y Operaciones de TI.

3.12 Gestión de la seguridad en los sistemas y aplicaciones

La gestión de la seguridad en los sistemas, aplicaciones, plataformas o cualquier otra herramienta usada por la empresa tiene como objetivo implementar y controlar la seguridad en todos los entornos que soportan los servicios y operaciones del negocio.

Y para esto, Talana implementa, configura y utiliza los siguientes sistemas:

- Servicio de seguridad en correos electrónicos: (Google Workspace).
- Antimalware: (Bitdefender antimalware y EDR).
- Antivirus: (Antimalware).
- Firewall: (Fortinet, Google Cloud Armor y Cloudflare).

La correcta instalación y configuración de los sistemas mencionados anteriormente abarcan a los siguientes elementos:

- Sistemas operativos.
- Estaciones de trabajo y dispositivos móviles.
- Sistemas de almacenamiento.
- Bases de datos.
- Correo electrónico e internet.
- Aplicaciones en la nube con datos personales.
- Aplicaciones en general.
- Sistemas, servicios y aplicaciones de nube.

Además, Talana implementa las medidas de hardening proporcionadas por los proveedores y las contenidas en la Documentación de Hardening de la organización.

Esto permite:

- La detección de programas informáticos no autorizados.
- La detección de sitios web maliciosos o sospechosos.
- La reducción de explotación de vulnerabilidades técnicas.
- La validación automatizada y periódica de los sistemas utilizados en los procesos críticos de la organización.
- El escaneo de archivos, datos, descargas, páginas web, etcétera para validar que no sean maliciosos.

Los lineamientos que se aplican a nivel de sistema operativo y de aplicaciones se encuentran definidos en la Política de Seguridad por Capas de la empresa.

3.12.1 Filtrado web

Talana gestiona y restringe el acceso a todos sus colaboradores y personal externo que trabaje con activos y/o información de la organización de los siguientes tipos de sitios web para reducir y evitar la exposición a contenido malicioso:

- Sitios que tienen una función de carga de información que no está autorizada por la organización.
  - La carga de información a sitios web debe estar justificada por razones comerciales válidas.
- Sitios maliciosos conocidos o sospechosos que distribuyen malware o contenido de phishing.
- Servidores de mando y control.
- Sitios maliciosos identificados a partir de inteligencia de amenazas, sección 3.21 Gestión de la inteligencia de amenazas de seguridad.
- Sitios web que comparten contenido ilegal.

3.13 Gestión de los registros de eventos (logs)

La gestión de los registros de eventos también llamados logs, tiene como objetivo registrar y monitorear las actividades realizadas en los sistemas de información de la empresa para la detección de acciones inusuales o accesos no autorizados a tiempo que permitan la prevención de incidentes de seguridad y privacidad.

Talana establece los lineamientos para esto en la Política de Gestión de Logs y aplica las acciones definidas en el Procedimiento de Gestión de Logs.

La organización conserva copias de las políticas de privacidad y procedimientos conexos durante 1 año. Esto incluye la conservación de las versiones anteriores de estos documentos cuando se actualizan.

3.14 Gestión de las vulnerabilidades técnicas

La gestión de vulnerabilidades técnicas tiene como objetivo revisar constantemente los sistemas de información para identificar vulnerabilidades y posibles brechas de seguridad y privacidad que puedan ser explotadas para perjudicar a la organización, y de esta manera dar solución a ellas en el modo y momento adecuado.

Dado esto, Talana establece lo siguiente:

- Se realiza Ethical Hacking por lo menos **una vez al año** a todos los sistemas alcanzados por el SGSI, incluyendo las aplicaciones en el entorno de la nube.
- El Procedimiento de Gestión de Vulnerabilidades establecido por la empresa contempla:
  - La verificación periódica de la publicación de vulnerabilidades por parte de los fabricantes de tecnología.
  - La realización periódica de escaneos de vulnerabilidades.
  - La priorización de atención para las vulnerabilidades con respecto a su criticidad e impacto.
  - La definición de plazos para reaccionar y dar resolución a las vulnerabilidades técnicas reportadas o identificadas.
  - La generación de un plan de remediación con plazos establecidos y su seguimiento.
  - La validación de la remediación por medio de retest de vulnerabilidades.
- Para mitigar la explotación de posibles vulnerabilidades se deben mantener los sistemas actualizados en sus últimas versiones, incluyendo la instalación de los parches pertinentes.
- La instalación de software en dispositivos propiedad de la empresa debe limitarse a actualizaciones y parches de seguridad. No se permite la instalación de nuevo software para uso personal y cuya procedencia es desconocida o sin licencia.

3.15 Gestión de la seguridad en las redes

La gestión de la seguridad en las redes tiene como objetivo proteger la información y el tráfico de datos transmitidos por redes internas o externas, y para ello Talana implementa las siguientes medidas:

- Se restringen las conexiones con redes que no sean confiables.
- Se segregan en distintas redes los servicios, usuarios y sistemas de información de la empresa.
- El acceso público directo entre internet y los sistemas de la organización se realiza solo por medio de una VPN.

- Se aplican medidas de seguridad para la protección de la información transferida por medio de la mensajería electrónica contra acceso no autorizado, asegurando el correcto direccionamiento, usando canales de comunicación seguros y garantizando la disponibilidad e integridad de la información.
- Se documentan, comunican e implementan una Política de Tratamiento de la Información y un Procedimiento de Transferencia de Información por Medios Extraíbles para administrar los equipos de red, los medios extraíbles y las transferencias de información.
- Se documenta, comunica e implementa una Política de Seguridad por Capas donde se establecen las medidas aplicadas a nivel de red.
- Las transacciones en la página web de la organización se ejecutan de manera segura utilizando los protocolos de seguridad pertinentes.
    - Algunos de los protocolos aplicados son el uso de certificados, firma electrónica, autenticación de usuarios, protocolos de cifrado de comunicaciones entre las partes involucradas, etcétera.

3.16 Gestión del ciclo de vida del desarrollo

La gestión del ciclo de vida del desarrollo tiene como objetivo mantener un control adecuado de los cambios y adecuaciones, así como del mantenimiento e implementación de medidas de seguridad y privacidad durante todas las fases que contempla el desarrollo de software.

Para esto, Talana aplica las siguientes acciones:

- Se cuenta con una segregación de ambientes para el desarrollo, pruebas y producción con el fin de minimizar los riesgos latentes en los procesos de gestión de cambios. Además, se definen los requisitos para el paso entre cada uno de los ambientes y los derechos de usuario responsables de ello.
    - Para la ejecución de las pruebas, no se utilizan datos productivos de clientes.
- Se documenta, comunica e implementa una Política de Desarrollo Seguro donde se establecen los lineamientos de seguridad y privacidad pertinentes.
- Se documenta, comunica e implementa una Metodología de Ciclo de Vida de Desarrollo donde se establecen todas las actividades y controles de seguridad y privacidad realizados por la empresa durante el desarrollo.
- Se documenta, comunica e implementa un Procedimiento de Gestión de Cambios Productivos donde se establece el proceso formal para el control de los cambios aplicados en los pasos a producción.
    - Los lineamientos establecidos para la gestión de cambios productivos se encuentran dentro de la Política de Tecnología y Operaciones de TI.

3.17 Gestión de las relaciones con los proveedores

La gestión de las relaciones con los proveedores tiene como objetivo asegurar un nivel apropiado de calidad y seguridad en los servicios y/o productos obtenidos por partes externas, así como garantizar la seguridad y privacidad de los activos e información de la empresa a los que tienen acceso.

Para esto, Talana implementa las siguientes medidas:

- Se mantiene una lista de los proveedores de la empresa y se realiza una evaluación anual de sus servicios, la cual se documenta en la Matriz de Evaluación de Proveedores.
  - Esta evaluación proporciona información relevante para la toma de decisiones sobre la contratación y/o renovación de proveedores, y para las evaluaciones de riesgo de la organización.
- Se cuenta con un contrato y/o términos y condiciones por escrito con cada proveedor, el cual incluye sus responsabilidades asociadas a la seguridad y privacidad de la información, acuerdos de confidencialidad y el compromiso de cumplir con las políticas de seguridad de la información de Talana.
  - El detalle de los contratos, acuerdos y/o términos y condiciones de los proveedores se registra dentro de la Matriz de herramientas tecnológicas (nube y datos personales).
- El contrato y/o términos y condiciones también define los acuerdos de niveles de servicio, las responsabilidades legales y derechos de propiedad intelectual vigentes, y las regulaciones de protección de la información de carácter personal.
- Se definen los requerimientos mínimos de seguridad para proteger la información según su clasificación asignada, y el tipo de acceso y permisos a otorgar con base en las necesidades del proveedor y del negocio.
- Se le comunican las políticas y procedimientos operativos aplicables al proveedor para cumplir con todos los requisitos de seguridad y privacidad establecidos por la empresa.
- Se gestiona adecuadamente la comunicación y el impacto de los posibles cambios que puedan presentarse en los contratos con proveedores, en sus servicios o cualquier aspecto dentro de la organización que afecte directa o indirectamente la relación con ellos.
- Se solicita al proveedor la comunicación y propagación de los requisitos de seguridad de Talana a lo largo de la cadena de suministro, en caso de que subcontraten y/o adquieran productos y/o servicios de otras partes externas para la prestación de su propio servicio.
- Se solicita al proveedor información relacionada a seguridad, configuraciones y buenas prácticas para el uso correcto de su producto y/o servicio.

3.17.1 Servicios de nube

Además de los lineamientos previamente establecidos para la gestión de las relaciones con los proveedores, que también aplican a los proveedores de servicios en la nube, Talana establece los siguientes criterios para implementar adecuadamente la seguridad en los servicios de la nube.

Criterios generales

- El uso de servicios en la nube debe ser exclusivo para el cumplimiento de las funciones laborales de cada colaborador.
  - No está autorizado el uso de servicios en la nube para fines personales.
- Está prohibido el uso de los servicios de correo electrónico y almacenamiento en la nube con fines personales que no tengan que ver con la empresa.
  - Se debe tener activado el filtro antispam para asegurar que los correos maliciosos son identificados y que no lleguen a la bandeja de entrada, así como también se debe instalar una tecnología de cifrado y firma digital para proteger la información confidencial y asegurar la autenticidad de la empresa como remitente en los correos electrónicos.
- Se debe verificar y dar mantenimiento a las redes creadas sobre la infraestructura del proveedor de servicios de nube.
- Se debe realizar monitoreo a los logs de transferencia de datos hacia la nube.
- Los procesos no deben ejecutarse en una nube virtualizada de alguno de los múltiples inquilinos de los servicios de la empresa.
- Si se requiere el almacenamiento de información clasificada como reservada, sensible o confidencial y/o información de carácter personal, ésta debe permanecer cifrada para evitar su divulgación o acceso no autorizados.
- Al contratar servicios en la nube se debe validar la protección de los datos en tránsito, incluyendo:
  - Los datos se mueven desde la infraestructura tradicional a los proveedores de nube, incluyendo público/privado, interior/exterior y otras combinaciones.
  - Los datos que migran entre los proveedores de nube.
  - Los datos que se mueven entre instancias (u otros componentes) en una nube determinada.

Criterios relacionados a los riesgos de seguridad

- En los procesos de contratación y uso de servicios en la nube se deben identificar, evaluar y gestionar los riesgos de seguridad asociados al tratamiento de información, acceso a información personal, riesgos legales, técnicos, de continuidad y todos los asociados a la transmisión de información por medio de la nube.
- Al contratar servicios de nube se deben contemplar y tratar los riesgos de pérdida de continuidad, disponibilidad e integridad por fallas en las plataformas para generar los procesos de recuperación correspondientes.
- No se deben utilizar servicios en la nube cuyo análisis de riesgo indique niveles no tolerables para la organización.
    - Los resultados del análisis y evaluación de riesgos son determinantes para aceptar o rechazar el uso de servicios en la nube, ya sean de pago o gratuitos.

Criterios relacionados a las capacidades, respaldos y gestión de cambios

- Los servicios de nube deben cumplir con los lineamientos de capacidad, respaldos y gestión de cambios establecidos en la Política de Tecnología y Operaciones de TI de la empresa.
- Los servicios de nube deben ser incluidos en el Procedimiento de Gestión de Backups, y Procedimiento de Gestión de Cambios Productivos establecidos por la empresa para que cumplan con todos los requisitos de seguridad pertinentes.
- Los cambios deben aprobarse siguiendo el Procedimiento de Gestión de Cambios Productivos.

3.18 Gestión de incidentes de seguridad y privacidad

La gestión de incidentes de seguridad y privacidad tiene como objetivo llevar un adecuado análisis, registro y tratamiento de los incidentes de seguridad y privacidad que puedan afectar las operaciones, los datos personales o servicios de la compañía.

Para esto, Talana define los siguientes lineamientos:

- Todos los colaboradores, clientes y proveedores deben reportar a la organización la identificación de posibles incidentes de seguridad y privacidad y la ocurrencia de ellos.
- Se deben analizar, definir y registrar soluciones para todo incidente de seguridad y privacidad reportado o detectado, siguiendo el Procedimiento de Gestión de Incidentes de Seguridad y Privacidad establecido por la empresa.
- Se deben asignar a los responsables más adecuados para atender y resolver los incidentes de seguridad y privacidad y otras posibles vulnerabilidades detectadas.

- Se debe registrar toda la información relevante sobre los incidentes de seguridad y privacidad, incluyendo su impacto, frecuencia y forma de resolución aplicada.
  - Esto tiene como objetivo recolectar datos sobre su comportamiento y crear una base de conocimiento a la que se pueda consultar ante la ocurrencia de eventos similares en el futuro.
- Si ocurre una brecha en el procesamiento de datos personales, la organización debe actuar de acuerdo con la ley local y notificar a las autoridades y al titular de datos personales dentro de las 24 horas posteriores a la detección.

Adicionalmente, la organización habilita un canal de comunicación por medio de la **línea de ética de Talana** para denunciar de manera anónima cualquier violación a las políticas de seguridad de la organización, o cualquier anomalía que pueda generar un incidente de seguridad.

3.19 Gestión de la continuidad del negocio

La gestión de la continuidad del negocio tiene como objetivo asegurar que las operaciones de la empresa se mantengan funcionando adecuadamente aún durante eventos de crisis o de desastre.

Para esto, Talana define los siguientes lineamientos:

- La documentación, comunicación e implementación de planes de continuidad y recuperación ante desastres que garanticen la restauración de los servicios o elementos interrumpidos por eventos inesperados, y su correcto funcionamiento una vez levantados.
- La asignación de los responsables adecuados, con el conocimiento y capacitación pertinentes para la ejecución adecuada de los planes definidos por la empresa.
- El aseguramiento de los recursos necesarios para la ejecución adecuada de los planes ante un evento inesperado.
- El mantenimiento de los planes, considerando la aplicación de pruebas y la mejora continua, siguiendo los lineamientos establecidos en el Plan de Recuperación ante Desastres y el Plan de Continuidad definidos por la empresa.

3.20 Gestión del cumplimiento

La gestión del cumplimiento tiene como objetivo mantener a la empresa alineada a las diferentes regulaciones y normativas a las que está sujeta.

Para esto, Talana realiza lo siguiente:

- Identifica y documenta los requisitos, regulaciones y normativas aplicables al giro de negocio y a la empresa en general dentro de la Matriz de Evaluación de Requisitos Legales y Contractuales.
- Verifica que los acuerdos con los colaboradores, clientes y proveedores cumplan con las pautas de las regulaciones aplicables, así como también que se identifiquen los riesgos de seguridad, privacidad de la información y de los datos personales derivados del servicio prestado o asociados a la relación con cada una de estas partes.
- Establece las políticas y procedimientos necesarios para adherirse a los requisitos regulatorios y normativos.
- Realiza revisiones de cumplimiento y auditorías internas del SGSPI de manera anual.
- Cada vez que la organización realice cambios en las operaciones, debe identificar las leyes pertinentes a las que puede estar sujeto.
- Las revisiones independientes o auditorías externas sirven como evidencia para garantizar que el SGPI funciona de acuerdo con las políticas y procedimientos de la organización, estas revisiones están planificadas para realizarse anualmente.
- Las revisiones independientes o auditorías externas se encuentran documentadas en el documento Plan y Programa de Auditoría.

3.21 Gestión de la inteligencia de amenazas de seguridad

Talana implementa la inteligencia de amenazas para la examinación y análisis de datos e información relevante sobre posibles nuevas amenazas y vulnerabilidades, lo cual aporta valor en la toma de decisiones sobre el control de ellas, saber cómo prevenirlas, detectarlas y remediarlas.

Esto se realiza siguiendo el Procedimiento de Gestión de Inteligencia de Amenazas establecido por la organización, y tiene los siguientes objetivos:

- Mejora de procesos internos.
- Implementación de una gestión de riesgos de seguridad más eficiente que genere decisiones más sólidas e informadas.
- Mayor comprensión de los puntos débiles de la organización que permita la priorización adecuada de las decisiones a tomar.
- Amplio conocimiento en las amenazas que apoye la proactividad y la aplicación de medidas preventivas que impidan la ocurrencia de un ciberataque.

La información obtenida como resultado de la inteligencia de amenazas debe ser compartida en un formato comprensible a todas las personas pertinentes, partes interesadas e incluso con otras organizaciones para mejorar los procesos y sus resultados.

4. Versionado

Confeccionado por:	CISO
Código de documento:	SEC005
Versión:	V 5.0
Fecha última de actualización:	29/04/2025
Revisado por:	Comité de Seguridad y Privacidad de la Información
Aprobado por:	Comité de Seguridad y Privacidad de la Información
Fecha de aprobación:	07/11/2024
Clasificación:	Público

5. Historial de cambios

N°	Cambio introducido	Realizado por	Fecha
1	Se cambia contenido de la política a nivel general con una versión más actualizada y alineada con la ISO 27001	Cybersecurity Engineer	16/11/2022
2	Se agrega pie de con información documental, versionado e historial de cambios	Cybersecurity Engineer	25/11/2022
3	Se agregan lineamientos de privacidad de la información en concordancia a la ISO 27701	Cybersecurity Engineer	18/10/2023
4	Se agregan lineamientos relacionados a la nube en concordancia a la ISO 27017 e ISO 27018	Cybersecurity Engineer	17/10/2024
5	Se modifican datos de contactos de interés, se agregan cláusulas de seguridad cloud y se corrigen algunos datos de proveedores de	Margarita Vargas - Cybersecurity Engineer	19/05/2025

	soluciones. Se agregan los puntos 3.21 y 3.17.1		