Política de Sistema de Gestión de Seguridad y Privacidad de la Información

Código de documento: SEC004
Versión: V 6.0
Vigente desde: 25/08/2025

Tabla de contenido

1.
Objetivo

Política de Sistema de Gestión de Seguridad y Privacidad de la Información

La alta dirección de **Talana**, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad y privacidad de la información buscando establecer un marco de confianza en el ejercicio de sus servicios con sus clientes y proveedores, todo enmarcado en el cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

El objetivo de este documento es establecer las políticas, prácticas y lineamientos internos aplicables para el Sistema de Gestión de Seguridad y Privacidad de la Información (de ahora en más SGSPI) para Talana.

2.
Alcance

El siguiente documento impacta a los procesos y controles que sirven para el cumplimiento del Sistema de Gestión de la Seguridad y Privacidad de la Información y la protección de datos personales en aplicaciones del entorno de nube, incluidos en el alcance definido por la organización.

3.
Lineamientos

3.1 Comprender a la organización y su contexto

Talana ha determinado su papel como responsable y/o encargado de datos personales, así como los asuntos internos y externos que son relevantes para su propósito y que intervienen en el logro de los resultados esperados.

Para esto, se aplicaron los siguientes análisis:

Análisis del entorno

Esto incluye cualquier cosa **fuera** de la organización que pueda influir en su operación.

El contexto externo incluye cualquier elemento dentro de la organización que pueda influir en la forma en que una organización administra su riesgo de seguridad y privacidad de la información.

En el contexto sociopolítico actual, nuestros clientes consideran que las remuneraciones de su personal, y sobre todo de la gerencia, son uno de los conjuntos de datos más delicados de la empresa. Por ello, debemos tener sumo cuidado en evitar fugas de esta información.

Adicionalmente, existe nueva legislación asociada a la Protección de Datos personales, que tiene una inspiración muy profunda en la GDPR europea, publicada el 2024. Esto impacta de manera profunda los datos que se consideran datos personales, y cómo se debe lidiar con ellos.

Por último, en el contexto del impulso al teletrabajo y la digitalización de las empresas, las empresas han puesto un foco de atención mucho mayor en la ciberseguridad. Es por ello que debemos mantener una actitud proactiva en cautelar la seguridad y privacidad de nuestra plataforma.

Político Política gubernamental	**Económico** Economía y finanzas	**Social** Cultura	**Tecnológico** Avances e innovación	**Legal** Leyes y regulaciones
El continuo trabajo de digitalización del estado realiza cambios a la normativa de la Dirección del Trabajo, los cuales exigen que Talana se adapte a ellos actualizando nuestro software y nuestro modelo de operación.	Mayor impulso a la digitalización de las empresas ha puesto el foco en la seguridad y privacidad de la información en plataformas en la nube.	La evolución social producto de los avances tecnológicos ha potenciado la necesidad de parte de las empresas a adoptar modalidades de trabajo híbrido debiendo adaptar sus procesos internos incorporando herramientas tecnológicas para satisfacer los requisitos de los trabajadores. Cambio climático. Pandemias.	Nuevos cambios a las tecnologías y nuevos ataques hacen imprescindible revisar permanentemente las herramientas y frameworks subyacentes a nuestro sistema.	El cumplimiento con la Ley de protección de datos, la nueva ley marco de ciberseguridad, ley Karin, entre otras, así como también los cambios requeridos por la dirección del trabajo influyen directamente en la evolución de nuestro software. Detalles en matriz de requisitos legales.

Análisis FODA

Esto incluye cualquier cosa **fuera** y **dentro** de la organización que pueda influir en su operación.

Fortalezas	Debilidades
• SGSPI implementado y certificado. • Compromiso con la empresa. • Vasta experiencia y conocimiento de tecnologías cloud. • Colaboración con otros equipos / áreas.	• Poca conciencia de documentación y procesos internos, • Falta de concientización del riesgo en el uso de los datos personales. • Falta de automatización en tareas repetitivas.
Oportunidades	**Amenazas**
• Alta capacidad de aprendizaje. Capacidad de moldear la cultura de seguridad y procesos desde las etapas tempranas del onboarding. • Programas internos de capacitación o certificación.	• Gran volúmen de datos personales. • La cantidad de clientes que manejamos nos transforma en un objetivo para los ciberdelincuentes. • Rotación de personal o fuga de talento.

3.2 Comprender a las partes interesadas

La organización ha determinado las partes interesadas que son pertinentes para el SGSPI y sus requisitos para la seguridad de la información y el tratamiento de datos personales.

Identificar a las partes interesadas

Categoría	Interesados identificados
Partes internas	Gerente General - CEO, Alta Dirección
	Comité de Seguridad y Privacidad de Información/ C-Levels
	Chief Information Security Officer (CISO) / Data Protection Officer (DPO)
	Líderes de los Procesos/Servicios
	Personal Operativo de los Procesos, Desarrolladores

	Personal Interno de Talana
Personas Externas	Clientes / Responsables de datos personales
	Usuarios Finales / Titulares de datos personales
	Inversionistas
	Postulantes
	Proveedores de Servicios
Administrativos, legales y regulatorios	Requisitos Legales
	Reguladores Estatales

Analizar los requisitos de las partes interesadas que se abordan en el SGSPI:

ALTA DIRECCIÓN, C-LEVELS Y/O COMITÉ DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

- Un ambiente de trabajo seguro y apropiado.
- Un SGSPI exitoso.
- Empleados concientizados e involucrados.
- Un entorno de nube seguro y protegido.

Identificación de requerimientos de CISO/DPO

- Implementar y mantener el SGSPI.
- Mantener el cumplimiento normativo.
- Mejoramiento continuo del SGSPI.
- Implementar y mantener la seguridad y privacidad de la información.
- Implementar y mantener la seguridad en las aplicaciones en el entorno de nube.

LÍDERES DE PROCESOS / SERVICIOS

- Protección y privacidad de la información y datos personales involucrada en los procesos / servicios.
- Documentación pertinente sobre los procesos / servicios.
- Atención de los incidentes reportados en los procesos / servicios.
- Dar servicio de mantenimiento en condiciones (24/7/365)
- Cumplir con los requisitos de ISO 27.001 y 27.701
- Disponibilidad de Sistemas 99.7%
- SLA de respuesta a incidentes: 4 horas desde recepción de comunicaciones en centro de contacto.

- Brindar una plataforma operacionalmente eficiente.

PERSONAL OPERATIVO DE LOS PROCESOS, Desarrolladores

- Proporcionar un ambiente de trabajo seguro y apropiado.
- Recibir capacitación y apoyo requeridos.
- La compañía especifica claramente sus requisitos y expectativas de los trabajadores.
- Protección de su información personal.
- La compañía paga justamente por el trabajo.
- Continuidad del empleo
- Oportunidades para el avance y desarrollo profesional

CLIENTES / Responsables de datos personales

- Protección de los datos personales de sus empleados en su calidad de responsable del tratamiento.
- Respetar el uso de los datos personales para los fines estipulados en los contratos de prestación de servicios y su descarte al término de la relación contractual.
- Productos y servicios con soporte y mantenimiento:
  - de acuerdo con los requisitos contractuales,
  - de acuerdo con los requisitos legales aplicables,
  - de acuerdo con los requisitos adicionales de la industria aplicables.
- Disponibilidad de los sistemas alcanzados por el SGSPI.
- Cumplir con los requisitos de seguridad de la información.

USUARIOS FINALES/POSTULANTES/ Titulares de datos personales.

- Servicios disponibles:
  - Sistemas de apoyo ante interrupciones
  - Mantener servicios de soporte ante interrupciones
- Protección de datos personales: los productos y servicios protegen adecuadamente los datos de los usuarios finales/Postulantes cumpliendo los requisitos legales tanto para los datos de contacto como para los datos personales.
- Disponibilidad de las plataformas
- Integridad de la información entregada

INVERSIONISTAS

Los Inversionistas serán entidades que apoyan a Talana con recursos económicos para la consecución de los objetivos de la organización.

- Proveer una plataforma segura, confidencial, disponible y privada para las partes interesadas.
- Correcto uso de los recursos entregados.
- Plataforma operacionalmente eficiente.
- Protección de los datos personales custodiados por Talana.
- Cumplir con los requisitos de seguridad de la información.
- Compartir la información necesaria, tanto técnica como comercial, enfocada a la venta de los productos y servicios.
- Cumplir con los acuerdos contractuales.
- Los socios serán empresas que contratan nuestras aplicaciones para dar servicio a usuarios finales:
- Cumplir con los requisitos de desarrollo de Software según los acuerdos firmados
- Cumplir con los acuerdos de confidencialidad firmados
- Proporcionar información técnica y soporte suficiente que les permita desarrollar y mejorar su Interfaz de Programación de Aplicaciones (API)
- Proporcionar la formación necesaria tanto técnica como comercial enfocada a la venta de los productos y servicios
- Cumplir los acuerdos contractuales especialmente en los tiempos de entrega acordados.

PROVEEDORES

- Cumplir con los requisitos de seguridad de la información.
- Cumplir con los acuerdos contractuales
- Cumplir con las formas de pago acordadas
- Cumplir con los acuerdos de confidencialidad firmados NDA
- Velar por la protección de datos personales.

PERSONAL INTERNO DE TALANA

- Proporcionar un ambiente de trabajo seguro y apropiado.
- Recibir capacitación y apoyo requeridos.
- Recibir de la compañía los requisitos y expectativas de los trabajadores específica y claramente
- Protección de sus datos personales.
- La compañía paga justamente por el trabajo.
- Continuidad del empleo
- Oportunidades para el avance y desarrollo profesional
- Cumplir con los requisitos de desarrollo de Software según los acuerdos firmados
- Cumplir con los acuerdos de confidencialidad firmados

- Proporcionar información técnica y soporte suficiente que permita desarrollar y mejorar la Interfaz de Programación de Aplicaciones (API), para brindar servicio a nuestros clientes clientes externos.
- Proporcionar la formación necesaria tanto técnica como comercial enfocada a la venta de los productos y servicios
- Cumplir los acuerdos contractuales especialmente en los tiempos de entrega acordados.

Identificación de requisitos de ADMINISTRACIÓN, LEGALES Y REGULATORIOS

- Cumplir con políticas y procedimientos internos de la organización.
- Cumplir con los requisitos de las leyes de protección de datos.
- Identificar y cumplir con los requisitos legales propios de cada tipo de negocio emprendido
  - Normativas de la Dirección del Trabajo
  - Normativas que rigen al SII
  - Otras
- Información mediante planes de comunicación y procedimientos establecidos para mitigar su impacto.
- Se debe implementar y operar el SGSPI y/o sus equivalentes, contar con la aprobación de su documentación y producir los registros requeridos por la norma:
  - ISO/IEC 27001:2013 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información Requisitos.
  - ISO/IEC 27701:2019 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Privacidad de la Información. Extensiones de la ISO/IEC 27001:2013 para la protección de datos personales.

3.3 Determinar el alcance del SGSPI

La información relacionada a los análisis internos y externos del SGSPI han ayudado a delimitar el alcance del SGSPI con respecto a:

- Características del negocio
- Procesos operativos
- Estructura organizacional de SI
- Ubicación
- Protección y tratamiento de datos personales y aplicaciones en el entorno de nube

Talana define como alcance de su sistema de gestión de seguridad, privacidad y protección de datos personales en la nube, Las plataformas Mi Talana (Software as a Service alojado en la nube orientado a usuarios administradores de procesos de Personas & Cultura) y Talana Next (aplicación móvil orientada a la experiencia del colaborador con su empresa) que incluyen los módulos de Gestión de Personas, Firma Digital, Remuneraciones, Asistencia y Turnos, Reclutamiento y Selección, Desarrollo Organizacional, Comunicaciones, Capacitación y otros, los cuales son soportados por las áreas de Producto, Desarrollo, Implementación, Soporte a Cliente, Operaciones de TI, y Site Reliability Engineering, que incluye los procesos de, soporte a clientes, implementación e integración de clientes, soporte de producto, desarrollo de software, y Operaciones TI, incorporando los controles de seguridad para servicios en la nube (ISO/IEC 27017:2015) y controles para datos personales en nubes públicas (ISO/IEC 27018:2019). Lo anterior, en calidad de encargados del tratamiento de datos personales, de acuerdo a la Declaración de aplicabilidad vigente, versión 5.0, código de documento SEG014.
.

Características del negocio

El negocio de **Talana** se encuentra en la industria de la tecnología para Recursos Humanos. El servicio provisto es el siguiente:

Descripción General

Talana es una plataforma de Gestión de Personas y de Human Capital Management. Su modelo de operación es el de SaaS (Software as a Service), por lo cual la administración y operación de los servidores y elementos de software que lo componen son responsabilidad de nuestra empresa.

La Plataforma está compuesta por los siguientes módulos:

Plataforma de Gestión de Personas

La plataforma de Gestión de Personas maneja la información personal y laboral de los trabajadores de las empresas que contratan el servicio. Esta incluye datos tales como rut, dirección, teléfono, e-mail personal, el número de cuenta corriente e información de familiares; todo esto con el objetivo de dar cumplimiento a la ley, y mantener una buena relación empresa- trabajador. Este módulo opera como base para el resto de las funcionalidades de Talana, por lo que está habilitado para todos nuestros clientes.

Este módulo también se encarga del registro, gestión y flujos de aprobación de vacaciones, permisos y otros tipos de ausentismos, los que se comunican a través de e-mail, el portal del trabajador, o el app para teléfono móvil.

Por último, maneja también la “carpeta digital” con la documentación laboral asociada a cada trabajador.

Plataforma de Remuneraciones

Utilizando la información del módulo de Gestión de Personas, la plataforma permite el cálculo de las remuneraciones de los trabajadores, la generación de archivos de transferencia bancaria, el cálculo de la centralización contable, además archivos de transferencia de leyes sociales.

Plataforma de Control de Asistencia

Nuestro sistema registra las marcas diarias de asistencia de los trabajadores registrados y enrolados. Estos pueden marcar el inicio y fin de su jornada laboral, ya sea utilizando un reloj control, algún otro dispositivo proporcionado por la empresa, o su teléfono móvil y el app Talana Next. En este caso, la marcación incluye adicionalmente una “selfie” del trabajador, su ubicación georreferencial e información acerca del modelo del teléfono utilizado. La recopilación de esta información está cubierta en los documentos “Políticas de Privacidad” y “Términos y Condiciones” que el trabajador debe aprobar antes del primer uso del App.

Plataforma de Firma Digital

Permite el enrolamiento de los trabajadores y el proceso de firma, utilizando el sistema de firma electrónica simple implementado por Talana, sobre los documentos de la carpeta del trabajador.

Procesos operativos

El SGSPI aplica a todas las funciones, servicios, actividades y activos de información, de los procesos detallados a continuación, los que son parte de la Cadena de Valor definido en el Plan Estratégico de Talana.

Procesos y/o servicios internos alcanzados	Área	Procesos con dependencia / interacción
Proceso de soporte a clientes	Soporte	●Proceso de implementación e integración de clientes ●Proceso de soporte de producto ●Proceso de desarrollo de software ●Proceso de Operaciones TI

Proceso de implementación e integración de clientes	Operaciones	●Proceso de soporte de producto, ●Proceso de desarrollo de software ●Proceso de Operaciones TI
Proceso de soporte de producto	Producto	●Proceso de soporte a clientes ●Proceso de desarrollo de software ●Proceso de Operaciones TI
Proceso de desarrollo de software	Producto	●Proceso de soporte a clientes ●Proceso de Operaciones TI
Proceso de Operaciones TI	Tecnología	●Proceso de soporte a clientes ●Proceso de implementación e integración de clientes

Ubicación

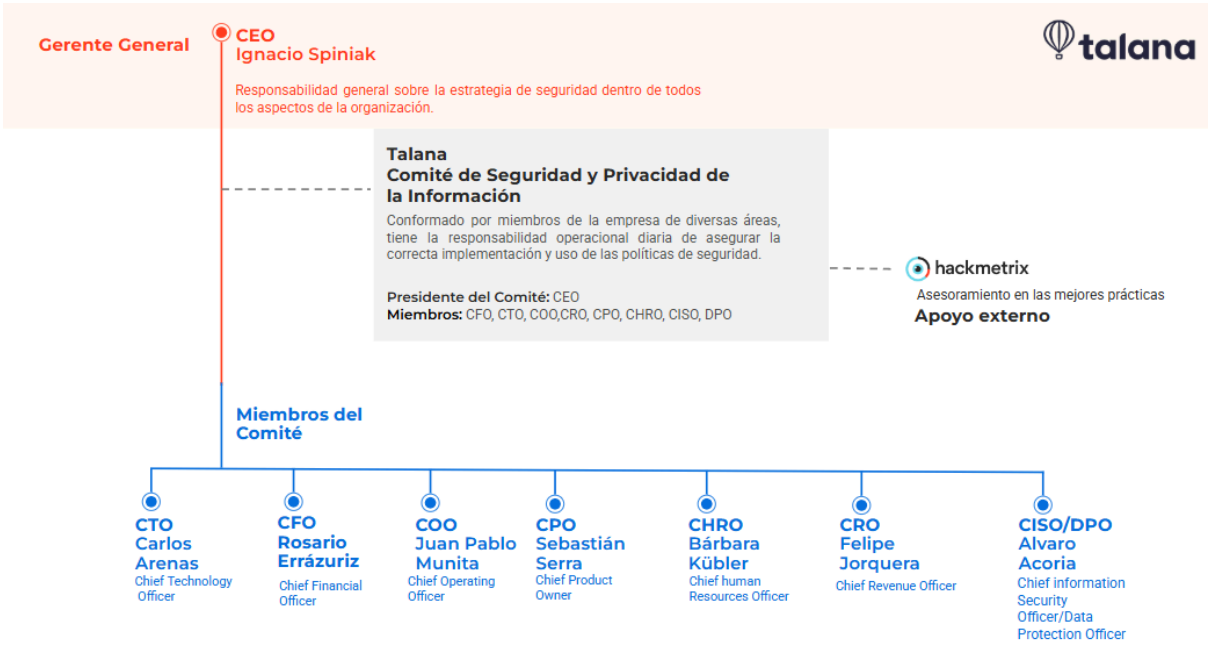
Las instalaciones donde se desarrollan los procesos alcanzados corresponden a la siguiente ubicación geográfica:

- Los Militares 4777, Piso 10 - Las Condes, Santiago - Chile.
- C. Las Orquídeas 675 Urb. Jardin int. 201, San Isidro - Lima - Perú.

Sin embargo, el teletrabajo es una práctica permitida en nuestra empresa, por lo que parte de los servicios pueden ser entregados desde la residencia de los trabajadores de Talana.

Estructura organizacional de SI

Talana cuenta con una estructura que presenta a los distintos órganos y las relaciones que existen entre ellos representado mediante el siguiente organigrama:



Para un detalle más específico de las relaciones funcionales que existen se cuenta con los descriptivos de los roles y responsabilidades de la empresa en el repositorio corporativo.

3.4 Sistema de gestión de la seguridad y privacidad de la información

Talana establece, implementa, mantiene y mejora un SGSPI siguiendo los lineamientos de esta política, los lineamientos de la Política de Seguridad de la Información en la Nube, los lineamientos establecidos para la Privacidad de la información, incluyendo los procesos necesarios y sus interacciones.

3.5 Liderazgo y compromiso

La Alta Gerencia y los miembros del Directorio de Talana demuestran su liderazgo y compromiso con el Sistema de Gestión de Seguridad y Privacidad de la Información mediante las siguientes acciones:

- Reconociendo y suscribiendo la Política de Seguridad de la Información y la Declaración de Objetivos de Seguridad de la Información, revisando y validando que son compatibles con la Dirección estratégica de la organización.

- Asegurando la integración de la seguridad y la privacidad dentro de los procesos de la organización mediante la aprobación y comunicación de documentos del SGSPI.
- Garantizando los recursos necesarios para el SGSPI mediante la aprobación de un presupuesto.
- Comunicando, mediante los canales que considere pertinente, la aceptación de las políticas y procedimientos de seguridad de la información para la adecuación de la empresa a los requisitos del SGSPI.
- Garantizando que el SGSPI logre sus resultados esperados mediante las revisiones periódicas del sistema, como lo son las auditorías, los indicadores y métricas, entre otros.
- Dirigiendo a la empresa a tomar acciones que aporten al éxito del SGSPI y promuevan la mejora continua.
- Dando recomendaciones de mejora continua para el SGSPI.
- Brindando apoyo mediante el respaldo a las convocatorias y los cambios requeridos para la operación y mejora del SGSPI.
- Comunicando su claro apoyo a la seguridad y protección de las aplicaciones y datos personales en el entorno de nube.

3.6 Política general de seguridad y privacidad de la información

La Seguridad y Privacidad de la Información en Talana es parte fundamental del negocio para así entregar confianza a nuestros clientes y usuarios sobre las tecnologías de la información que operamos. La data, con base en nuestra clasificación de la información, es gestionada con los más altos estándares según las mejores prácticas disponibles en el mercado, lo cual es una base para nuestro crecimiento y sustentabilidad organizacional.

La Seguridad y Privacidad de la Información en Talana es posible dado el compromiso de la alta dirección promoviendo una cultura de mejora continua, facilitando los recursos y herramientas necesarias.

La alta dirección entiende y atiende la importancia y beneficios de mantenerse en cumplimiento, no solo con los requerimientos de ISO 27001, ISO 27701, ISO 27017, ISO 27018 y mejores prácticas de seguridad y protección de datos personales, sino además con otros requisitos legales, contractuales y gubernamentales relevantes para el contexto de la organización.

En Talana nuestras políticas y procedimientos en cuanto a la Seguridad y Privacidad de la Información son del conocimiento general de los empleados, cuando aplique. En la medida de lo posible y con base al Plan de Comunicación del SGSPI definido, nuestras partes interesadas clave serán informadas de nuestros lineamientos y mejores prácticas.

3.7 Roles, responsabilidades y autoridades

La alta dirección de Talana ha definido los roles y ha asignado sus responsabilidades asociadas al SGSPI dentro del documento de **Descriptivo de Roles y Responsabilidades,** que establece, entre otras cosas, lo siguiente:

- Todos los roles necesarios para llevar a cabo las actividades requeridas por la ISO 27001, ISO 27701, ISO 27017 e ISO 27018.
- Las responsabilidades que asume cada uno de los roles involucrados en el SGSPI.
- La responsabilidad del Chief Information Security Officer (CISO), el Data Protection Officer (DPO), en conjunto con el Comité de Seguridad y Privacidad es, entre otras, velar por el cumplimiento del SGSPI y de informar sobre su desempeño a la alta dirección y a la organización.
- Además, dentro de la Política del Comité de Seguridad y Privacidad de la Información se establecen las funciones de los integrantes del comité definido por la organización.
- Garantías que el SGSPI logre sus resultados esperados mediante las revisiones periódicas del sistema, como lo son las auditorías, los indicadores y métricas, entre otros.
- Las acciones para dirigir a la empresa a tomar acciones que aporten al éxito del SGSPI y promuevan la mejora continua.
- Dando recomendaciones de mejora continua para el SGSPI.
- Brindando apoyo mediante el respaldo a las convocatorias y los cambios requeridos para la operación y mejora del SGSPI.
- Comunicando su claro apoyo a la seguridad y protección de las aplicaciones y datos personales en el entorno de nube.

Así como también dentro de la Política del Comité de Seguridad y Privacidad de la Información donde se establecen las funciones de los integrantes del comité definido por la organización.

3.8 Acciones para dirigir los riesgos y oportunidades

3.8.1 General

Talana planifica la gestión de riesgos y oportunidades del SGSPI, tomando como base lo analizado en **3.1 Comprender a la organización y de su contexto** y en **3.2 Comprender las necesidades y expectativas de las partes interesadas.**

Esta planificación está orientada a:

- Identificar nuevos controles para garantizar el logro de resultados del SGSPI, que se evidencia mediante las mediciones de los controles.

- Anticiparse a los riesgos para evitar o reducir efectos perniciosos, que se evidencia con el análisis, evaluación y tratamiento de riesgos.
- Constituir una fuente de robustecimiento del SGSPI, apoyando a la mejora continua, que se evidencia durante la implementación de los nuevos controles que se han definido en el Plan de Tratamiento de Riesgos.
- Evitar o reducir efectos no deseados, que se demuestra con el análisis, evaluación y tratamiento de riesgos.
- Fortalecer el SGSPI apoyando el logro de los resultados previstos y la mejora continua.
- Fortalecer la seguridad y la privacidad de la información.
- Fortalecer la seguridad y protección de las aplicaciones y los datos personales en el entorno de nube.

Esta planificación tiene como objetivos:

- Definir las acciones para evaluar y tratar los riesgos y oportunidades.
- Definir la forma en que se integrarán e implementarán estas acciones dentro de los procesos del SGSPI.
- Definir la forma en que serán medidas estas acciones en cuanto a su efectividad.

Para los riesgos y oportunidades identificados, la empresa establece:

- Las acciones para manejarlas.
- La forma en que se implementarán en los procesos mediante Plan de Tratamiento de Riesgos.
- La forma en que serán medidas en cuanto a su efectividad.

3.8.2 Evaluación de los riesgos de seguridad de la información y privacidad de la información

Talana dispone de la realización de una evaluación de riesgos, que considera lo siguiente:

- Definir los criterios de aceptación y de evaluación de los riesgos.
- Establecer una metodología objetiva para la evaluación de los riesgos que arroje resultados consistentes, válidos y comparables.
- Identificar y analizar riesgos de seguridad de la información (asociados a la pérdida de confidencialidad, integridad y disponibilidad y privacidad) y a sus responsables dentro del SGSPI, así como también aquellos riesgos asociados con el tratamiento de datos personales.
- Determinar el nivel de riesgo mediante la valorización de su probabilidad e impacto.
- Evaluar los riesgos comparando los resultados del análisis con los criterios establecidos en la metodología y priorizarlos.

- Asegurar la relación entre la seguridad de la información y la protección de datos personales, y gestionar adecuadamente esto durante los procesos de valoración de riesgos.

Estas actividades se encuentran documentadas en la Metodología de Gestión de Riesgos y en los registros asociados:

- Módulo de Activos.
- Módulo de Riesgos.

3.8.3 Tratamiento de los riesgos de seguridad de la información

Talana establece el tratamiento de los riesgos de seguridad y privacidad de la Información considerando:

- Tomar los resultados de la evaluación de riesgos para seleccionar opciones de tratamiento.
- Asociar los controles de seguridad del anexo A de la ISO 27001 y las guías y controles adicionales de ISO 27701, ISO 27017 e ISO 27018 para implementar la opción de tratamiento seleccionada, verificando que no existan omisiones.
- Elaborar la declaración de aplicabilidad donde se indiquen los controles necesarios ya implementados dentro de Talana e identificar aquellos que sean necesarios implementar y los que no para el SGSPI, así como la justificación de su inclusión/exclusión para ambos casos.
- Proponer un plan de tratamiento y documentarlo dentro de la matriz de riesgos.
- Obtener la aprobación de los responsables de riesgos sobre el plan de tratamiento y sus riesgos residuales.

Estas actividades se encuentran documentadas en la Metodología de Gestión de Riesgos y en los registros producidos como resultado del proceso:

- Plan de Tratamiento de Riesgos incluído en la Matriz de Riesgos.
- Declaración de Aplicabilidad.
- Reporte de análisis de riesgos.
- Minuta de sesión de comité.

3.9 Objetivos de seguridad de la información y planificación para alcanzarlos

Talana establece sus Objetivos de Seguridad y Privacidad, bajo un enfoque de alto nivel, pero estrechamente relacionado a los objetivos institucionales. Los objetivos del SGSPI deben:

- Ser consistentes con la Política de Seguridad y Privacidad de la Información y la Política de Privacidad y Tratamiento de Datos Personales.
- Estar relacionados directamente con las métricas del SGSPI, lo cual permite su medición, si aplica.
- Contemplar los resultados de la evaluación y los planes de tratamiento de los riesgos.
- Contemplar los requisitos de seguridad y privacidad de la información aplicables y los resultados de la apreciación y tratamiento de los riesgos.
- Ser monitoreados, publicados y comunicados según lo establece el Plan de Comunicación del SGSPI.
- Estar disponibles y documentados.
- Ser actualizados, cuando sea requerido.

Se determina dentro de la Metodología de Indicadores de Seguridad de la Información qué se hará, qué recursos se usarán, quién será el responsable, cuándo y cómo se evaluarán los objetivos y sus métricas.

Talana declara los siguientes objetivos de seguridad de la información y privacidad alineados al SGSPI y a su estrategia:

- Garantizar que la organización cumpla con las leyes y regulaciones aplicables en materia de protección de datos personales y seguridad en la nube.
- Establecer procesos y procedimientos para evaluar y mejorar continuamente el SGSPI y la protección de las aplicaciones y datos personales en el entorno de nube de la organización.
- Asegurar que los datos personales se mantengan confidenciales y sólo sean accesibles por las personas autorizadas dentro de la organización.
- Mantener un uptime de 99,7% anual para nuestra plataforma SaaS. el cual se controla mensualmente.
- Realizar revisiones de seguridad sobre el aplicativo móvil y plataforma SaaS al menos anualmente, abordardando la mitigación de los hallazgos detectados dentro del ciclo de desarrollo siguiente.
- Realizar búsqueda de actualizaciones de seguridad sobre la infraestructura que soporta al SaaS al menos mensualmente, abordardando la aplicación de las que se declaren como críticas durante los 30 días siguientes a su descubrimiento.
- Realizar revisiones independientes de auditoría de forma anual para identificar y mitigar brechas en nuestro sistema de gestión.
- Asegurar y mantener la confidencialidad, integridad, disponibilidad y privacidad de la información de la empresa, de nuestros trabajadores, de nuestros clientes y sus colaboradores
- Asegurar la disponibilidad de la plataforma.
- Entregar un servicio seguro y confiable.

3.10 Planificación de cambios

Talana determina que cualquier cambio que se considere necesario para el SGSPI, éste debe llevarse a cabo de manera planificada. Además, debe ser aprobado por la alta dirección y comunicado a la organización y partes interesadas.

3.11 Recursos

Talana elabora una vez al año el Presupuesto Anual, en el que también se consideran los recursos requeridos para el establecimiento, implementación, mantenimiento y mejora continua del SGSPI. Dicho Presupuesto es aprobado por la Alta Gerencia.

Asimismo, se garantiza la participación de los recursos humanos necesarios para el SGSPI, mediante decisión del Comité de Gestión de Seguridad y Privacidad de la Información. También se cuenta con el nombramiento formal del Oficial de Seguridad.

La alta dirección de Talana, dispone de los recursos de infraestructura tecnológica y física (si corresponde), que han sido establecidas en el apartado 3.3 Determinar el alcance del sistema de gestión de la seguridad y privacidad de la información de este documento.

3.12 Competencia

Talana dispone lo siguiente:

- Ha determinado las competencias necesarias de las personas que operan y asumen funciones específicas dentro del SGSPI, las cuales han sido definidas en el documento Roles y Responsabilidades del SGSPI.
- Se ha asegurado el cumplimiento de estas competencias mediante la capacitación y concientización del personal, lo que se ha documentado en el Plan de Capacitación y Concientización en Seguridad. Este plan puede ser actualizado si se detectan deficiencias en el conocimiento del personal, de manera que se programan capacitaciones adicionales. Para identificarlas se cuenta con métricas que evalúan el know how adquirido.
- Ha realizado una investigación de las competencias y habilidades de los candidatos previo a su contratación, lo cual se define en el procedimiento de preselección y selección de personal.

3.13 Concientización

Las charlas de concientización son realizadas según lo especificado en el Plan de Capacitación y Concientización de Seguridad y Privacidad:

- Difusión de la Política de Seguridad y Privacidad de Información mediante envío de dicho documento por Slack, Talana Next, y su publicación en Coda, a todo el personal de la empresa. Cabe resaltar que, la política forma parte de los temas tratados en las charlas de sensibilización.
- Importancia de las acciones del personal para la efectividad del SGSPI.
- Beneficios de las mejoras en el desempeño del SGSPI.
- Las implicancias de la empresa acerca de una no conformidad sobre el SGSPI.

Cada charla de capacitación y concientización programada cuenta con la Lista de Asistencia de Capacitación.

3.14 Comunicación

Las comunicaciones internas y externas del SGSPI son planificadas y ejecutadas en base al Plan de Comunicación del SGSPI. La actualización de este documento se realiza conforme a las operaciones de la empresa.

Éste plan define lo siguiente:

- Qué se va a comunicar
- Cuándo se va a comunicar
- A quién va dirigido
- Cómo se va a comunicar

3.15 Información documentada

3.15.1 General

El SGSPI cuenta con:

- Los documentos y registros que son requisito de la norma.
- Los documentos que sin ser requisito de la norma son usados por Talana para asegurar la efectividad del SGSPI (reglamentación interna, políticas específicas de seguridad y privacidad de información, documentación de controles de seguridad y privacidad de información).

3.15.2 Creación y actualización

Talana dispone para la creación y actualización de sus documentos del SGSPI:

- La identificación y descripción del documento: título, fecha de elaboración, autor, código, entre otros.
- La definición de formatos para los documentos y registros, ya sean en medio electrónico o físico.
- La especificación de los responsables de elaborar, revisar y aprobar los documentos, los cuales deben ser adecuados con respecto a los roles del SGSPI.

3.15.3 Control de la información documentada

La documentación del SGSPI de Talana es controlada y garantiza su disponibilidad e idoneidad. Adicionalmente se vela por su adecuada protección.

Esto se logra a través de la aplicación de actividades de control:

- Distribución restringida, acceso controlado, mecanismos de recuperación y restricciones de uso.
- Estar protegida contra pérdida de confidencialidad e integridad.
- Tener condiciones adecuadas de almacenamiento y conservación.
- Tener control de los cambios a los documentos, así como condiciones adecuadas de retención y disposición.
- Identificar y controlar la documentación de origen externo, que la organización determine que es necesaria para la planificación, operación y mantenimiento del SGSPI.

3.16 Control y planificación operacional

Talana planifica, implementa y controla las políticas y procedimientos necesarios donde se establecen los criterios pertinentes para cumplir los requisitos del SGSPI y las acciones de la sección **3.8, Acciones para dirigir los riesgos y oportunidades** de esta política.

Además, la empresa implementa planes para alcanzar los objetivos de seguridad de la información determinados en **3.9, Objetivos de seguridad de la información y planificación** para alcanzarlos de esta política. Esto se encuentra como información documentada en el **Listado de Métricas e Indicadores**.

3.17 Evaluación de los riesgos de seguridad de la información

La evaluación de riesgos debe ser periódica, por lo que Talana ha definido aplicarla cada año, o cuando se produzcan modificaciones importantes.

Las condiciones para la aplicación adecuada de estas evaluaciones son especificadas en la Metodología de Gestión de Riesgos.

Asimismo, los resultados de las evaluaciones de riesgos se encuentran disponibles como información documentada en la Matriz de Riesgos y sus registros asociados.

3.18 Tratamiento de los riesgos de seguridad de la información

Talana implementa el plan de tratamiento de riesgos, con base en lo definido en la Matriz de riesgos.

La implementación de los controles seleccionados en la declaración de aplicabilidad para el tratamiento de riesgos, dejan registros que evidencian su realización.

3.19 Seguimiento, medición, análisis y evaluación

Talana mide y evalúa el desempeño de la seguridad de la información y privacidad y la efectividad del SGSPI, para lo cual determina:

- Aquello que requiere ser monitoreado y medido: procesos y controles de la seguridad y privacidad de información.
- Los métodos aplicados para monitorear, medir, analizar y evaluar, para obtener resultados válidos.
- Quién es el responsable y cuándo se llevará a cabo el seguimiento y las mediciones.
- Quién es el responsable y cuándo se llevará a cabo el análisis y la evaluación de los resultados del seguimiento y las mediciones.

Las actividades descritas anteriormente se ejecutan según lo dispone la Metodología de Indicadores de Seguridad de la Información. Asimismo, los registros asociados se encuentran en el Listado de Métricas e Indicadores.

3.20 Auditorías internas

3.21 General

Talana lleva a cabo a intervalos planificados auditorías internas para determinar que el SGSPI:

- Cumpla con los requerimientos del negocio y los lineamientos del estándar ISO 27001, ISO 27701, ISO 27017 y ISO 27018
- Se encuentra implementado y se mantiene de manera efectiva.

3.22 Programa de auditoría interna

Adicionalmente, la empresa debe:

- Planificar, establecer, implementar y mantener un programa o programas de auditoría donde se defina la frecuencia, los métodos, las responsabilidades, los requisitos de planificación y la elaboración de reportes, tomando en cuenta la importancia de los procesos involucrados y los resultados de auditorías previas.
- Define los criterios y alcance de la auditoría en el Plan de Auditoría Interna.
- Contratará auditores internos o servicios externos de auditoría para ejecutar el plan.
    - Los auditores externos, podrán utilizar documentos y formatos de registro de auditoría internos de Talana o externos.
- Selecciona auditores objetivos e imparciales que cumplan con los siguientes requisitos y aptitudes:
    - El auditor interno debe mostrar que cuenta con experiencia demostrable y conocimiento para realizar auditorías de seguridad de la información (de ser posible, debe proporcionar los certificados pertinentes que lo comprueben).
    - El auditor interno debe saber aplicar sus conocimientos sobre auditorías en cualquier proceso de la empresa para verificar el cumplimiento total del sistema de gestión de seguridad de la información.
    - El auditor interno debe demostrar independencia de las funciones o procesos sobre los que se realizará la auditoría.
    - El auditor interno debe tener un buen conocimiento de los requisitos y procesos involucrados en la auditoría de certificación.
    - Liderazgo
    - Buena comunicación
    - Capacidad de análisis
    - Analítico y organizado
- Comunicar los resultados de las auditorías a los jefes involucrados y Alta Gerencia, dejando registro de ello en el Plan de Comunicaciones.
- Se mantienen registros que evidencian la planificación y ejecución de la Auditoría en el:
    - Programa Anual de Auditoría Interna
    - Plan de Auditoría Interna
    - Cronograma de Auditoría Interna
    - Acta de Reunión de Auditoría Interna
    - Informe de Auditoría Interna

3.21 Revisión por la alta dirección

3.21.1 General

El Comité de Seguridad y privacidad de la Información y los miembros del Directorio que conforman a Talana, realizan una revisión anual del SGSPI para garantizar su conveniencia, continuidad, vigencia, adecuación y efectividad.

3.21.2 Insumos para la revisión por la dirección

La revisión por la dirección comprende lo siguiente:

- El estado de las acciones generadas por revisiones de la Dirección previas.
- Cambios significativos internos y externos, relevantes para el SGSPI.
- Cambios en las necesidades y expectativas de las partes interesadas que son relevantes para el SGSPI.
- El desempeño de la Seguridad de Información en la empresa:
  - No conformidades y acciones correctivas.
  - Resultados de métricas e indicadores.
  - Resultados de auditoría.
  - Grado de cumplimiento de los objetivos del SGSPI.
- Retroalimentación de las partes interesadas.
- Los resultados de la valoración y Gestión de Riesgos del SGSPI y el estado del Plan de Tratamiento de Riesgos.
- Oportunidades de Mejora Continua.

Todos estos elementos son preparados, presentados e informados a la Alta Dirección mediante métricas y mediciones.

3.21.3 Resultados de la revisión por la dirección

Producto de la revisión, se cuenta con evidencias documentadas de su realización en el Acta de Revisión por el Comité de Seguridad y privacidad de la Información, donde se indican los resultados y acciones definidas durante la misma.

3.22 Mejora continua

Talana realiza acciones de mejora continua sobre la idoneidad, adecuación y efectividad del SGSPI y deja registro de esto en los siguientes documentos:

- Procedimiento de Acciones Correctivas y de Mejora
- Plan de Tratamiento de Acciones Correctivas y de Mejora

3.23 No conformidad y acción correctiva

Al presentarse una no conformidad, la empresa dispone:

- ➔ Reaccionar frente a la misma, disponiendo la acción para controlarla, corregirla y atender las consecuencias de ésta.
- ➔ Considerar si es necesario y posible eliminar la causa de la no conformidad, mediante: su revisión, determinación de las causas de la no conformidad y verificación de no conformidades similares.
- ➔ Implementar las acciones planeadas.
- ➔ Revisar la efectividad de las acciones realizadas.
- ➔ Realizar cambios sobre el SGSPI, si es requerido.

La organización deja registro de esto en los siguientes documentos:

- Procedimiento de Acciones Correctivas y de Mejora
- Plan de Tratamiento de Acciones Correctivas y de Mejora
- Análisis Causa Raíz

Talana asegura que las acciones correctivas aplicadas son acordes y proporcionales a las no conformidades que se encontraron.

talana

4.
Versionado

Confeccionado por:	CISO/DPO - Cybersecurity Engineer
Código de documento:	SEC004
Versión:	V 6.0
Fecha última de actualización:	19/08/2025
Revisado por:	CISO/DPO
Aprobado por:	Comité de Seguridad y Privacidad de la Información
Fecha de aprobación:	25/08/2025
Clasificación:	Pública

5.
Historial de cambios

N°	Cambio introducido	Realizado por	Fecha
1	Se reemplaza Zulip por Slack Se actualiza Estructura del SGSPI	Cybersecurity Engineer	25/10/2022
2	Se agregó pie de página y espacio en portada con especificaciones de versión del documento.	Cybersecurity Engineer	25/11/2022
3	Se incorpora párrafo en sección 6.4.2.: "Talana declara los siguientes objetivos de seguridad de la información alineados al SGSPI y a su estrategia: → Asegurar y mantener la confidencialidad, integridad y disponibilidad de la información de la empresa, de nuestros trabajadores, de nuestros clientes y sus colaboradores. → Asegurar la disponibilidad de la plataforma. → Entregar un servicio seguro y confiable."	CISO	23/10/2023
4	Se incorporan lineamientos para el cumplimiento de la ISO 27017 e ISO 27018 Se actualiza estructura.	Cybersecurity Engineer	11/10/2024
5	Se actualiza alcance, que incluye requerimientos de ISO 27017 e ISO 27018. Se actualiza SOA a versión actual Se incorporan requisitos para parte interesada:	CISO	06/5/2025

	inversiontas		
6	Se reorganiza el documento con las adecuaciones de ISO 27001:2022	Cybersecurity Engineer	14/05/2025
7	Se actualiza el alcance, de acuerdo a la versión 5.0, se incorpora dirección de Talana Perú, se modifica Tabla Pestel, columna Legal y Regulatoria, se agregan puntos 3.17 y 3.18 requisitos del estándar y se mejora tabla de procesos, área y dependencias.	Cybersecurity Engineer	19/08/2025