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

Código de documento: SEC004
Versión: V 4.0
Vigente desde: 07/11/2024

Tabla de contenido

1.
Objetivo

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

La 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.
Responsabilidades

- **Comité de Seguridad.** Aprobar y proporcionar los recursos necesarios para el desarrollo, implementación y cambios de esta política.

  Garantizar que estas políticas sean conocidas por todos y apoyar a su divulgación, conocimiento y carácter obligatorio.

- **Oficial de Seguridad/Oficial de Protección de Datos.** Tiene la responsabilidad de supervisar la adecuada ejecución de la presente política.

Gestionar la capacitación sobre el contenido de la presente política.

Establecer, documentar y distribuir la presente política.

Resolver posibles controversias originadas por la política.

Gestionar los recursos otorgados para la implementación de la política.

- **Empleados de la organización**. Cumplir con los lineamientos de la presente política, apegándose a los procedimientos establecidos. Alertar de inmediato sobre incumplimientos a esta política.

4.
Autoridad de emisión, revisión y publicación

Esta Política ha sido aprobada por el Comité de Seguridad de la Información de Talana.

Se revisará de manera periódica, una vez al año.

5.
Términos y definiciones

- **Acción Preventiva**: Acción tomada para eliminar la causa de una no conformidad potencial u otra situación potencial no deseable.
- **Aceptación del Riesgo:** Decisión de aceptar un riesgo.
- **Activo de Información:** Entidad, objeto o artefacto que genera, almacena o transmite información que tiene valor para la empresa.
- **Análisis del Riesgo:** Uso sistemático de la información para identificar fuentes y estimar el riesgo.
- **Gestión del Riesgo:** Actividades coordinadas para dirigir y controlar una organización en relación con el riesgo.
- **Integridad**: Propiedad de salvaguardar que la información no sufra alteraciones conservando su exactitud.
- **Riesgo:** Combinación de probabilidad de un evento y sus consecuencias.
- **Políticas**: Intenciones globales y orientación tal como se expresan formalmente por la Dirección.
- **Procedimiento**: Forma especificada para llevar a cabo una actividad o un proceso.
- **Registro**: Documento que presenta resultados obtenidos o proporciona evidencias de actividades desempeñadas.
- **Riesgo de Seguridad de la Información:** Posibilidad que una amenaza explote vulnerabilidades de un activo o de un grupo de activos y por lo tanto cause daño a la Institución.
- **Seguridad de la Información**: Preservación de la confidencialidad, integridad y disponibilidad de la información.
- **Sistema de Gestión**: Marco de políticas, procedimientos, guías y recursos asociados para lograrlos objetivos de la Institución.
- **Sistema de Gestión de la Seguridad y Privacidad de la Información (SGSPI)**: Parte del sistema de gestión global, basado en un enfoque hacia los riesgos del

negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad y privacidad de la información.

6.
Reglas de aplicación al SGSPI

6.1 Comprender la organización y su contexto

Talana ha determinado los objetivos, asuntos internos y externos que son relevantes para su propósito y que intervienen en el logro de los resultados esperados.

6.1.1 Declaración de Objetivos

La organización declara los siguientes objetivos de seguridad y privacidad de la información alineados a la estrategia establecida en el Plan Estratégico de **Talana** .

- Garantizar la seguridad, privacidad y confidencialidad de los datos de nuestros clientes en nuestra calidad de responsable del tratamiento
- Operar de acuerdo a las buenas prácticas de protección de datos
- Minimizar el impacto de acciones maliciosas sobre la plataforma
- Visibilizar los riesgos en materia de Seguridad y Privacidad de la Información a la Alta Gerencia

Lo anterior, asociado al alcance definido para el sistema de gestión de seguridad y privacidad de la información el cual contempla, 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 y otros, son soportadas por las áreas de Producto, Desarrollo, Implementación, Soporte a Cliente, Operaciones de TI, y Site Reliability Engineering, lo anterior, en calidad de encargados del tratamiento de datos personales.

De acuerdo a la Declaración de aplicabilidad SEG014, versión 3.0, Fecha: 10/11/2023

6.1.2 Contexto de SGSPI

Con el fin de definir los parámetros externos e internos que deben tenerse en cuenta al gestionar el riesgo, se analiza el contexto interno y externo de la organización.

Análisis externo

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, desde hace algunos años el parlamento está trabajando en una nueva legislación de Protección de Datos personales, que tiene una inspiración muy profunda en la GDPR europea, por lo que esperamos que se publique durante el 2024. Esto impactará de manera profunda el qué 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 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	Nuevos cambios a las tecnologías y nuevos ataques hacen imprescindible revisar permanentemente las herramientas y frameworks subyacentes a nuestro sistema.	Se espera la proclamación de la nueva ley de protección de datos, la nueva ley marco de ciberseguridad, ley Karin así como también los cambios requeridos por la dirección del trabajo.

Análisis interno

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

Fortalezas	Debilidades
• Compromiso con la empresa. • Vasta experiencia y conocimiento tecnológico • Amplio conocimiento de tecnologías cloud	• Poca conciencia de documentación y procesos internos • Comportamiento poco adecuado en función de la criticidad de información porcesada.
Oportunidades	**Amenazas**
• Alta capacidad de aprendizaje. • Gran número de personas ingresando a la empresa cada mes, que pueden ser concientizados desde el principio	• Gran volúmen de datos personales • La cantidad de clientes que manejamos nos transforma en un objetivo para los ciberdelincuentes

6.1.3 Contexto de Gestión de Riesgos

Los lineamientos acerca de esta gestión son considerados en la **Política de Seguridad de la Información, sección Política de Gestión de Riesgos,** donde se encuentran las definiciones pertinentes al tema.

6.2 Comprender las necesidades y expectativas de 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.

6.2.1. Identificación y Análisis de las Partes Interesadas

Categoría	Interesados identificados
Personal Interno	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
Personas Externas	Clientes
	Usuarios Finales
	Inversionistas
	Usuarios Analistas
	Trabajadores de empresas clientes/Titulares de datos
	Empresas de outsourcing de remuneraciones
	Postulantes
Proveedores	Proveedores de Servicios
	Proveedores de Tecnologías: Servidores en la nube, Sistemas de Alarma Ambiental, Máquinas Virtuales, Software de Monitoreo, Software de Gestión de TI, Certificados Digitales.
Administrativos, legales y regulatorios	Requisitos Legales

6.2.2. Identificación y Análisis de los Requerimientos del Negocio de Partes Interesadas

Identificación de requerimientos de 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.

Identificación de requerimientos de 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.

Identificación de requerimientos de CLIENTES

- 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.
- Entregar productos y servicios con soporte y mantenimiento:
  - de acuerdo con los requisitos contractuales,
  - en caso de interrupciones,
  - cumpliendo los requisitos legales aplicables,
  - cumpliendo los requisitos adicionales de la industria aplicables.
- 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.

Identificación de requerimientos de 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

Identificación de requerimientos de 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.

Identificación de requerimientos de PROVEEDORES

- 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.

Identificación de requerimientos de 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.

6.2.3 Determinar el alcance del sistema de gestión de la seguridad y privacidad de la información

La información relacionada a los análisis internos y externos (contexto) del SGSPI que intervienen y afectan al logro de sus objetivos y que fueron desarrollados en la sección **6.1.2 Contexto de SGSPI**. Esta información ha sido usada para definir el alcance respecto a:

- Protección y tratamiento de datos personales y aplicaciones en el entorno de nube
- Procesos
- Características del Negocio

- Organización
- Ubicación
- Activos
- Tecnología
- Justificación de la Exclusión

De manera similar, de la sección **6.2.2, Identificación y Análisis de los Requisitos del Negocio de Partes Interesadas,** se tomarán en cuenta los Requisitos de Seguridad de la Información y Privacidad que provienen de los involucrados y afectados por el SGSPI para delimitar el alcance de:

- Activos
- Justificación de la Exclusión

Finalmente, las dependencias de las actividades de otras organizaciones que, como en el caso anterior, también influyen en el alcance de:

- Procesos
- Características del Negocio

El siguiente texto definirá el alcance aplicable a la certificación:

Talana define como objeto de su sistema de gestión de seguridad y privacidad de la información, 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 y otros, son soportadas por las áreas de Producto, Desarrollo, Implementación, Soporte a Cliente, Operaciones de TI, y Site Reliability Engineering, lo anterior, en calidad de encargados del tratamiento de datos personales.

De acuerdo a la Declaración de aplicabilidad vigente, código de documento SEG014.

Procesos y servicios

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	Dependencias/Interfaces
Proceso de soporte a clientes	Soporte	Clientes

Proceso de integración de clientes	Operaciones	Implementación Integración
Proceso de soporte de producto	Producto	Proceso de Soporte a Clientes
Proceso de desarrollo de software	Producto	Proceso de Soporte a Clientes
Proceso de Operaciones TI	Tecnología	Soporte de Producto Desarrollo de software

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.

Para poder acceder y utilizar Talana basta con un navegador web moderno y una conexión a Internet de una velocidad razonable de acuerdo a los estándares de hoy. Sin embargo, atendiendo a la necesidad de nuestros clientes de conocer en mayor detalle la arquitectura de servidores y de software de nuestra solución es que hemos preparado este documento explicativo.

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 nuestro servicio. Esto incluye datos como su rut, su dirección, teléfono y e-mail personal, el número de su cuenta corriente e información de sus 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, más las “novedades del mes”, es decir, gastos, descuentos, bonos, etc. nuestra plataforma permite el cálculo de las remuneraciones de los trabajadores, la generación de archivos de transferencia bancaria, el cálculo de la centralización contable y otra información que se entrega al ERP de la empresa, y el cálculo y archivos de transferencia de leyes sociales.

Plataforma de Control de Asistencia

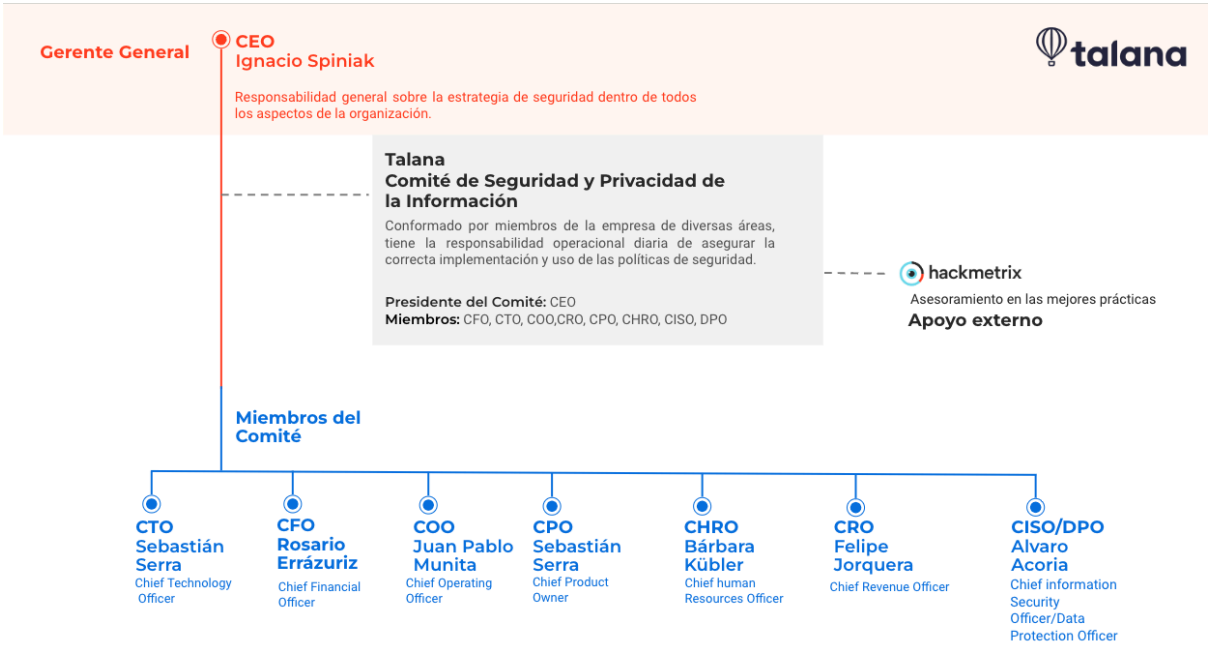
Nuestro sistema registra las marcas diarias de asistencia de los trabajadores registrados y enrolados. Estos pueden marcar el inicio y fin de su jornada laboral, ya sea utilizando un reloj control, algún otro dispositivo proporcionado por la empresa, o su teléfono móvil y el app Talana Next. En este 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.

Organización

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.

Ubicación

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

Los Militares 4777, Piso 10 - Las Condes, Santiago - Chile.

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.

Activos

Los activos de información de **Talana** dentro del alcance y límites del SGSPI están sujetos al proceso de Gestión de Riesgos, por lo que estos son inventariados, clasificados y valorizados en base al procedimiento de Gestión de Riesgos vigente, y pueden ser encontrados en el Inventario de Activos que se produce a partir de la ejecución del mencionado procedimiento y teniendo en cuenta los lineamientos de la Gestión de Activos y Clasificación de la Información de la Política de Seguridad de la Información y Privacidad.

Tecnología

Los activos se encuentran a su vez soportados por una estructura tecnológica compleja, la cual cuenta con hardware, software, infraestructura y servicios que permiten procesar, almacenar y transmitir la información del proceso. Los componentes tecnológicos más importantes están listados en el Inventario de Activos vigente.

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

Talana establece, implementa, mantiene y mejora un SGSI siguiendo los lineamientos de esta política, los lineamientos de la Política de Seguridad de la Información en la Nube y los lineamientos establecidos para la privacidad de la información.

6.3 Liderazgo

6.3.1. 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.

6.3.2. 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.

6.3.3. Roles, responsabilidades y autoridades

La alta dirección de Talana ha definido los roles y 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.

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.

6.4 Planificación

6.4.1 Acciones para tratar los riesgos y oportunidades

Talana planifica la gestión de riesgos y oportunidades del SGSPI, tomando como base lo analizado en **6.1 Comprender a la organización y de su contexto** y en **6.2 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 está orientada a:

- 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.

Evaluación de los riesgos de seguridad y privacidad de la información

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

- 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.
- Identificar y analizar riesgos de seguridad y privacidad de la información (asociados a la pérdida de confidencialidad, integridad, 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 priorizándolos.
- Asegurar la relación entre la seguridad de la información, aplicaciones y protección de datos personales en el entorno de nube, 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:

- Inventario de activos de Información.
- Matriz de riesgos

Tratamiento de los riesgos de la seguridad y privacidad 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.

6.4.2 Objetivos de Seguridad y Privacidad de 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. Estos objetivos:

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

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

- Mantener un uptime de 99,7% anual para nuestra plataforma SaaS. el cual controlaremos mensualmente.
- Realizar revisiones de seguridad sobre nuestro aplicativo móvil y plataforma SaaS al menos anualmente y abordar 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 y abordar 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.

De esta forma 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

6.5 Apoyo / Soporte

6.5.1 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 **6.2.3 Determinar el alcance del sistema de gestión de la seguridad y privacidad de la información** de este documento.

6.5.2 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.

6.5.3 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.

6.5.4 Comunicación

Las comunicaciones internas y externas del SGSPI son planificadas y controladas mediante el Plan de Comunicaciones, documento que es actualizado conforme se avanza con la operación del sistema, éste define:

- Comunicación
- Emisor
- Destinatarios
- Fecha de emisión
- Procesos afectados
- Estado

6.5.5 Documentación de la Información

General

El SGSPI cuenta con:

- Los documentos y registros que son requisito de la norma.
- 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).

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.
- Definición de formatos para los documentos y registros, ya sean en medio electrónico o físico.
- La especificación de quiénes elaboran, revisan y aprueban los documentos.

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.
- Condiciones adecuadas de almacenamiento y conservación.
- Control de cambios sobre los documentos, retención y disposición.

6.6 Operación

6.6.1 Planificación y control operacional

En el punto **6.4.1 Acciones para tratar los riesgos y oportunidades** de este documento se especifican los procedimientos y actividades que se llevan a cabo para planificar, implementar y controlar el proceso de Gestión de Riesgos.

Para todos los casos indicados anteriormente se cuenta con procedimientos documentados que a su vez generan registros que son evidencia de las actividades realizadas.

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

La frecuencia y condiciones para la realización de las Gestiones de Riesgo son especificadas en el procedimiento Gestión de Riesgos del SGSPI.

Los resultados de la Evaluación de Riesgos se encuentran documentados y dejan registros que evidencian su realización.

6.6.3 Tratamiento de los riesgos de seguridad y privacidad de la información

La empresa propone e implementa el Plan de Tratamiento de Riesgos, según lo dispone el procedimiento Gestión de Riesgos del SGSPI.

Las actividades del Tratamiento de Riesgos dejan registros que evidencian su realización.

6.7 Evaluación del desempeño

6.6.1 Monitoreo, medición, análisis y evaluación

Talana mide y evalúa 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 evaluarlos, para obtener resultados válidos.
- Cuándo se llevarán a cabo el monitoreo y las mediciones.
- Quién es el responsable de las mediciones.
- Cuándo se analizarán y evaluarán los resultados del monitoreo y de las mediciones.
- Quién es el responsable del análisis y evaluación de los resultados.

6.6.2. Auditorías internas

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.

Ambos puntos son realizados según se dispone en el Plan de Auditoría Interna De igual forma, la empresa establece que:

- Planifica, establece, implementa y mantiene un programa o programas de auditoría (frecuencia, métodos, responsabilidades, requisitos de planificación y reporte) 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
    - Estar certificados como auditor líder en las normas a auditar
    - Estar certificados como auditor y haber participado en al menos 1 ciclo de auditoría
    - Contar con experiencia demostrable en al menos 5 auditorías
    - Poseer una carrera afín a las normativas a auditar.
    - Liderazgo
    - Buena comunicación
    - Capacidad de análisis
    - Analítico y organizado

- Comunica 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

6.6.3 Revisión por parte de la Dirección

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 disponibilidad, adecuación y efectividad. Esta revisión comprende:

- El estado de las acciones generadas por revisiones de la Dirección previas.
- Cambios significativos internos y externos, 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 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.

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.

6.8 Mejora

6.8.1 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.

El manejo de estas condiciones para las acciones correctivas se encuentra especificado en el procedimiento Acciones Correctivas y de mejoras. Estas acciones son acordes y proporcionales a las no conformidades que las originaron.

Asimismo, se mantiene registro de las correcciones realizadas.

6.8.2 Mejora continua

Para realizar acciones de mejora continua sobre la idoneidad, adecuación y efectividad del SGSPI, Talana establece los lineamientos de Mejora Continua del SGSPI mencionados anteriormente.

7.
Versionado

Confeccionado por:	CISO/DPO - Cybersecurity Engineer
Código de documento:	SEC004
Versión:	V 4.0
Fecha última de actualización:	11/10/2024
Revisado por:	CISO/DPO
Aprobado por:	Comité de Seguridad y Privacidad de la Información
Fecha de aprobación:	07/11/2024
Clasificación:	Pública

8.
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