

Política de Seguridad de la Información

Marco general del SGSI: principios y lineamientos para proteger la información y otros activos asociados de LegalTalent, sus clientes y terceros. Aplica a todas las partes interesadas.

IDENTIFICACIÓN DEL DOCUMENTO

Código	LT-SGSI-POL-002
Título	Política de Seguridad de la Información
Tipo de documento	Política
Versión	1.0
Estado	Vigente
Clasificación	Público
Elaboró	Agustina Moraes — responsable del Sistema de Gestión
Revisó	Maximiliano Bendinelli — CISO
Aprobado por	Nicolás Zanoni — Dirección
Fecha de emisión	03/ 09/ 2026
Alcance organizacional	Todas las partes interesadas

Historial de versiones

Toda modificación al documento debe registrarse en esta tabla antes de su publicación. La versión más reciente encabeza el histórico.

VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO
1.0	03/09/2026	Emisión inicial (consolida versiones internas previas).

Distribución y acceso

Indique quién debe conocer el documento, dónde se publica y con qué nivel de acceso.

AUDIENCIA	MEDIO DE PUBLICACIÓN	NIVEL DE ACCESO
Todo el personal	Repositorio del SGSI (SharePoint)	Lectura
Proveedores y terceros	Página web	Lectura

CONTENIDO

1. Objetivo

Establecer los principios y lineamientos generales para gestionar la seguridad de la información en LegalTalent, protegiendo la confidencialidad, integridad y disponibilidad de la información de la organización, sus clientes y terceros.

Proporcionar el marco de referencia para la implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), mediante la gestión de los riesgos de seguridad de la información y el cumplimiento de los requisitos legales, regulatorios y contractuales aplicables.

2. Alcance

Esta política aplica a:

- Todo el personal, contratistas y colaboradores de LegalTalent.
- Todos los sistemas, aplicaciones, plataformas, servicios e infraestructura utilizados por la organización.
- Toda la información generada, procesada, almacenada o transmitida por LegalTalent.
- Los proveedores y partes interesadas que tengan acceso a información o sistemas bajo responsabilidad de la organización.

3. Definiciones y abreviaturas

TÉRMINO	DEFINICIÓN
SGSI	Sistema de Gestión de Seguridad de la Información.
CID	Confidencialidad, integridad y disponibilidad de la información.
Activo de información	Todo dato, sistema o recurso con valor para la organización que requiere protección.
Parte Interesada	Personas, grupos u organizaciones que pueden afectar, verse afectados o tener interés en las decisiones y actividades de la organización.

4. Roles y responsabilidades

ROL	RESPONSABILIDAD
Dirección	Aprobar la Política de Seguridad de la Información y los objetivos de seguridad; asegurar la disponibilidad de los recursos necesarios para el SGSI; demostrar su compromiso con la seguridad de la información y promover la mejora continua del sistema.
Referente de Seguridad de la Información (CISO)	Actuar como referente experto en seguridad de la información: orientar y acompañar la elaboración y revisión de las políticas del SGSI, asesorar en la gestión de riesgos e incidentes, aportar criterio técnico sobre los controles a implementar y recomendar mejoras al marco de seguridad.

ROL	RESPONSABILIDAD
Responsable del SGSI	Elaborar, mantener y revisar las políticas y demás documentación del SGSI con la guía del CISO; implementar los controles de seguridad, mantener la infraestructura y las aplicaciones de forma segura, gestionar vulnerabilidades y cumplir con los lineamientos de desarrollo seguro.
Usuarios, colaboradores y contratistas	Cumplir con las políticas de seguridad, proteger las credenciales y dispositivos asignados, y reportar incidentes o situaciones de riesgo.
Proveedores y terceros	Cumplir con los requisitos de seguridad establecidos contractualmente y proteger la información a la que tengan acceso.

5. Desarrollo

5.1 Objetivos de la política

- Proteger la confidencialidad de la información contra accesos no autorizados.
- Preservar la integridad de la información y de los sistemas.
- Garantizar la disponibilidad de los servicios críticos.
- Cumplir con los requisitos legales, regulatorios y contractuales aplicables.
- Gestionar los riesgos de seguridad de manera proporcional al impacto potencial sobre el negocio.
- Promover una cultura de seguridad y mejora continua.
- Mejorar continuamente el SGSI, evaluando su desempeño y eficacia y tomando las acciones necesarias para su mejora.

5.2 Principios generales

- Seguridad basada en riesgos: los controles se implementan considerando los riesgos identificados y la criticidad de los activos.
- Mínimo privilegio: los accesos se asignan únicamente en función de las responsabilidades de cada usuario.
- Defensa en profundidad: se implementan múltiples capas de protección para reducir la probabilidad e impacto de los incidentes.
- Seguridad por diseño: los requisitos de seguridad se consideran desde las etapas iniciales de diseño, desarrollo e implementación de sistemas.
- Mejora continua: los controles y procesos se revisan periódicamente para adaptarse a cambios tecnológicos, regulatorios y de negocio.

5.3 Marco de gestión de seguridad

LegalTalent implementa controles y procesos de seguridad según riesgos, requisitos aplicables y necesidades de las partes interesadas.

LegalTalent establece, implementa, mantiene y mejora continuamente su Sistema de Gestión de Seguridad de la Información (SGSI), mediante la gestión de los riesgos de seguridad de la información y la implementación de controles de seguridad acordes con los riesgos identificados, los requisitos legales, regulatorios y contractuales aplicables y las necesidades de la organización.

5.4 Protección de la información

La información se clasifica y protege conforme a su sensibilidad y criticidad. Los datos personales, la información confidencial y los activos críticos están sujetos a controles reforzados de acceso, monitoreo y protección.

5.5 Gestión de accesos

El acceso a sistemas e información se otorga conforme al principio de mínimo privilegio y se revisa periódicamente. Los accesos a sistemas críticos cuentan con mecanismos apropiados de autenticación y control.

5.6 Gestión de riesgos

La organización mantiene un proceso formal para identificar, evaluar, tratar y monitorear los riesgos de seguridad de la información. Las decisiones de tratamiento de riesgos se documentan y revisan periódicamente.

5.7 Gestión de incidentes

Todo incidente o evento que pueda comprometer la seguridad de la información se reporta y gestiona conforme a los procedimientos establecidos. Se mantienen registros de incidentes y se promueven acciones correctivas y preventivas para evitar recurrencias.

5.8 Protección de datos personales

LegalTalent trata los datos personales conforme a los principios de privacidad, minimización y seguridad establecidos en la normativa aplicable y en sus políticas internas.

5.9 Continuidad del negocio

La organización implementa medidas de continuidad y recuperación que permiten restablecer los servicios críticos ante incidentes o desastres que afecten su operación.

5.10 Seguridad de proveedores

Los proveedores que accedan a información o sistemas de LegalTalent cumplen requisitos de seguridad acordes a los riesgos asociados al servicio prestado.

5.11 Concientización y responsabilidad

Todos los integrantes de LegalTalent son responsables de proteger la información bajo su control y de cumplir las políticas de seguridad vigentes. La organización promueve la concientización y la adopción de buenas prácticas

6. Rutinas de Control

- Revisiones por la Dirección
- Auditorías Internas