



POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

FALABELLA	Política General de Seguridad de la Información	PL-01
Fecha Revisión: 09/09/2025	Versión: 3.7	Página

Índice

1. Objetivo.	3
2. Alcance.	3
3. Documentos relacionados.	3
4. Generalidades.	4
4.1. Responsabilidad del documento.	4
4.2. Mantención del documento.	4
4.3. Cumplimiento.	4
4.4. Roles y responsabilidades generales.	4
4.5. Definiciones.	4
5. Política general de seguridad de la información.	5

F A L A B E L L A	Política General de Seguridad de la Información	PL-01
Fecha Revisión: 09/09/2025	Versión: 3.7	Página

1. Objetivo.

La presente política general de seguridad de la información tiene por objetivo definir los lineamientos generales de seguridad de la información, que permitan garantizar el adecuado uso y protección de todos los activos de información en los negocios de **Falabella**.

Representar los intereses de la dirección ejecutiva para la administración y utilización, que los usuarios o colaboradores internos y externos deben hacer de los activos de información de la organización, así como las medidas que se adopten para proteger dichos recursos.

Promover a nivel del grupo, la cultura de seguridad de la información y la comprensión de sus responsabilidades sobre ésta.

2. Alcance.

Esta política tiene como alcance y debe ser aplicada por todos los negocios de **Falabella**.

3. Documentos relacionados.

- Política de Organización de Seguridad de la Información de **Falabella**.
- Política de Seguridad de Recursos Humanos de **Falabella**.
- Política de Gestión de Activos de **Falabella**.
- Política de Criptografía de **Falabella**.
- Política de Control de Acceso Lógico de **Falabella**.
- Política de Seguridad Física y Ambiental de **Falabella**.
- Política de Gestión de las Operaciones de **Falabella**.
- Política de Gestión de las Comunicaciones de **Falabella**.
- Política de Adquisición, Desarrollo y Mantenimiento de Sistemas de Información de **Falabella**.
- Política de Gestión de proveedores de **Falabella**.
- Política de Administración de Incidentes de Seguridad de Información de **Falabella**.
- Política de Administración de Continuidad de Negocio de **Falabella**.
- Política de Ciberseguridad de **Falabella**.
- Política de Cumplimiento de **Falabella**.
- Política de Gestión de la Nube de **Falabella**.
- Política de Gestión de Seguridad de la Información de FTC de **Falabella**.
- Política de Gestión de Identidades de **Falabella**.

F A L A B E L L A	Política General de Seguridad de la Información	PL-01
Fecha Revisión: 09/09/2025	Versión: 3.7	Página

4. Generalidades.

4.1. Responsabilidad del documento.

Será responsabilidad del oficial de seguridad de la información corporativo (CISO) aprobar y garantizar la actualización y difusión de esta política y será responsabilidad de cada gerencia incluir en sus procesos las disposiciones aquí presentadas.

4.2. Mantención del documento.

Este documento se debe actualizar al menos una vez al año o frente a cambios significativos del entorno y cada vez que existan nuevas disposiciones relacionadas al gobierno de seguridad de información corporativo.

4.3. Cumplimiento.

Todos los colaboradores de los negocios de **Falabella** deberán cumplir con esta política, además de contratistas y empresas externas que presten servicios y tengan acceso a los activos de información de **Falabella**.

4.4. Roles y responsabilidades generales.

Los roles y las responsabilidades incluidas (pero no limitadas) en esta política son:

- Se entenderá que las políticas específicas de seguridad forman parte integral de esta política.
- El oficial de seguridad de la información corporativo (CISO), es responsable de aprobar y dirigir la revisión periódica de esta política.
- El Oficial de seguridad de información de la vertical de negocio (BISO), es el responsable de difundir al interior de su vertical de negocio el Marco Normativo Corporativo de seguridad de la información.
- El oficial de seguridad de información local (LISO) es el responsable de difundir al interior de su negocio el Marco Normativo Corporativo de seguridad de la información.
- Las gerencias legales son responsables de identificar las normas y regulaciones vigentes de los negocios e informarlas al oficial de seguridad de la información corporativo (CISO) y al oficial de seguridad de la información local (LISO).
- Las gerencias de recursos humanos son responsables de ejecutar programas de capacitación y concientización, al interior de sus negocios, con temas relacionados a la seguridad de la información y al cumplimiento del Marco Normativo Corporativo de seguridad de la información.

4.5. Definiciones.

Las definiciones utilizadas en este documento se encuentran en el instructivo IN-1SA-01-00-01-01 - Glosario de términos del SGSI.

F A L A B E L L A	Política General de Seguridad de la Información	PL-01
Fecha Revisión: 09/09/2025	Versión: 3.7	Página

5. Política general de seguridad de la información.

- **Falabella** entiende la seguridad de la información como la preservación y protección de la confidencialidad, integridad y disponibilidad de la información.
- Los negocios de **Falabella** deben proteger la información que manejan, de forma apropiada, según su valor y sensibilidad, independiente de los medios que la contengan y velando especialmente por su confidencialidad, integridad y disponibilidad.
- **Falabella** debe cumplir con todas las regulaciones, leyes y normativas de seguridad de la información vigentes en los países que opera.
- **Falabella** debe invertir en tecnologías de seguridad, procesos, recursos y personal para proteger la información sensible de la Compañía.
- **Falabella** debe implementar medidas de control consistentes con la estrategia de seguridad de la información y con los objetivos estratégicos del grupo.
- **Falabella** debe realizar de forma periódica análisis de riesgos de seguridad de la información, de modo que éstos se gestionen y traten de forma adecuada mitigando sus impactos.
- **Falabella**, a través de la Gerencia General Corporativa y sus Gerentes Generales Corporativos, para cumplir con el Marco Normativo Corporativo de Seguridad de la Información, deberán velar por la implementación y cumplimiento de las siguientes políticas específicas de seguridad de la información en cada una de sus unidades de negocio:
- **Política de organización de seguridad de información:** Define los lineamientos para administrar la seguridad de la información, establecer un marco gerencial de control e implementación y define los roles y responsabilidades de seguridad de la información dentro de **Falabella**.
- **Política de seguridad de recursos humanos:** Define los lineamientos para la selección y contratación, durante la vigencia del empleo y una vez terminada la relación contractual con los colaboradores de los negocios de **Falabella**.
- **Política de gestión de activos de información:** Define los lineamientos para mantener una adecuada protección de los activos de información de **Falabella**, en todas sus formas y medios.
- **Política de criptografía:** Define los lineamientos para el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o Integridad de la información.
- **Política de control de acceso lógico:** Define los lineamientos para controlar el acceso a la información de **Falabella**, para así, evitar el acceso no autorizado, salvaguardando su confidencialidad e integridad.
- **Política de seguridad física y ambiental:** Define los lineamientos para la seguridad física y ambiental, de modo de controlar el acceso de personas a lugares sensibles y restringidos, evitar daño en el personal y las instalaciones de **Falabella**.
- **Política de gestión de las operaciones:** Define los lineamientos para asegurar la operación correcta y segura de los medios de procesamiento de información de **Falabella**, así también, evitar la divulgación no autorizada, la corrupción y pérdida de disponibilidad; debido a

FALABELLA	Política General de Seguridad de la Información	PL-01
Fecha Revisión: 09/09/2025	Versión: 3.7	Página

procedimientos operacionales insuficientes, inadecuados o por canales de comunicación poco robustos.

- **Política de gestión de las comunicaciones:** Define los lineamientos para garantizar la protección de la información en las redes y sus instalaciones de procesamiento de información de apoyo.
- **Política de adquisición, desarrollo y mantenimiento de sistemas de información:** Define los lineamientos, para garantizar que la seguridad de la información sea una parte integral de todos los sistemas de información, desde su desarrollo/adquisición hasta el término de su vida útil.
- **Política de gestión de proveedores:** Define los lineamientos para garantizar la protección de los activos de la organización accesibles a los proveedores de la organización, evitar la divulgación de información no autorizada, la corrupción y pérdida de información.
- **Política de administración de incidentes de seguridad de información:** Define los lineamientos para llevar a cabo una correcta detección, identificación y gestión de los incidentes de seguridad de la información, que pudieran materializarse en **Falabella**.
- **Política de administración de continuidad de negocio:** Define los lineamientos para realizar una apropiada gestión de la continuidad de los sistemas; asegurando la recuperación de los procesos críticos de negocio, en plazos previamente definidos por **Falabella**.
- **Política de Ciberseguridad:** proporciona un marco de orientación para mejorar el estado de la Ciberseguridad, usando para ello los aspectos estratégicos y técnicos relevantes para esa actividad, y sus dependencias con otros dominios de seguridad.
- **Política de Cumplimiento:** Define los lineamientos para evitar violaciones a la ley vigente, normas regulatorias y responsabilidades contractuales; para asegurar el cumplimiento de las políticas, normas y estándares internos de **Falabella** y para maximizar la efectividad de los procesos de auditoría sobre los sistemas de información.
 - i. **Política de Gestión de la Nube:** Define los lineamientos y buenas prácticas de seguridad para garantizar la protección de los activos de la información de la organización en la nube, así como asegurar la correcta operación y manipulación de recursos en ambientes Cloud.
 - ii. **Política de Gestión de Seguridad de la Información de FTC:** Define los lineamientos estratégicos para definir un marco de gestión de riesgos de seguridad de la información en Falabella Tecnología Corporativa, en lo adelante FTC, que permita facilitar el logro de los objetivos estratégicos de Falabella.
 - iii. **Política de Gestión de Identidades:** Define los lineamientos que debe adoptar **Falabella** con respecto a la gestión de identidades, para garantizar que los colaboradores sean autenticados con las fuentes autoritativas correctas y tengan acceso a los recursos específicos donde están autorizados (Segregación de funciones), con la finalidad de mantener la confidencialidad, integridad y disponibilidad de la información de la empresa.

F A L A B E L L A • • • • •	Política General de Seguridad de la Información	PL-01
Fecha Revisión: 09/09/2025	Versión: 3.7	Página

- Los negocios de **Falabella** deben elaborar, gestionar y probar todos sus procedimientos de continuidad de negocio y velar por el cumplimiento de controles de seguridad de la información en los procesos de continuidad del negocio, ante eventos de desastres o que afecten la disponibilidad o correcto funcionamiento.
- Todos los colaboradores de los negocios de **Falabella** son responsables por la custodia y protección de la información que manejan en el desempeño de sus funciones.
- Esta política debe ser aplicada, difundida y conocida por todo el personal de los negocios de **Falabella** y su incumplimiento constituye una falta grave, la que será sancionada como tal de acuerdo con los procedimientos de sanciones que correspondan. Por lo mismo, los negocios deben realizar los respectivos procesos de sensibilización y capacitación que sean necesarios.
- **Falabella** reconoce como parte integrante de esta política de seguridad de la información y de las políticas anteriormente mencionadas, a todas las normas, procedimientos, estándares y líneas base que se desprenden de éstas.

FALABELLA	Política General de Seguridad de la Información	PL-01
Fecha Revisión: 09/09/2025	Versión: 3.7	Página

CLASIFICACIÓN	FECHA APROBACIÓN	N° DE PROCEDIMIENTO
Uso Interno	09/09/2025	PL-01

CONTROL DE VERSIONES					
Fecha	Versión	Modificaciones	Redactor	Revisor	Aprobador
16/05/2013	1.0	Creación de política.	CISO Corporativo.	CISO Corporativo.	CCSI.
29/08/2014	2.0	Actualización de política.	Normatividad y Compliance.	Normatividad y Compliance.	CISO Corporativo
26/08/2015	2.1	Cambio menor de la política.	Normatividad y Compliance.	Normatividad y Compliance.	CISO Corporativo
28/11/2015	2.2	Cambio menor de la política.	Normatividad y Compliance.	Normatividad y Compliance.	CISO Corporativo
15/07/2016	2.3	Cambio menor de la política.	Normatividad y Compliance.	Normatividad y Compliance.	CISO Corporativo
30/12/2016	2.4	Actualización de política.	Normatividad y Compliance.	Normatividad y Compliance.	CISO Corporativo
31/08/2017	2.5	Cambio menor de la política.	Normatividad y Compliance.	Normatividad y Compliance.	CISO Corporativo
07/11/2017	2.6	Actualización anual de la política.	Normatividad y Compliance.	Normatividad y Compliance.	CISO Corporativo
30/11/2018	2.7	Actualización anual de la política.	Normatividad y Compliance.	Normatividad y Compliance.	CISO Corporativo
30/03/2019	2.8	Cambio menor de la política.	Normatividad y Compliance.	Normatividad y Compliance.	CISO Corporativo
30/04/2019	3.0	Cambios en la política, Hecho Esencial 02/19 S.A.C.I. Falabella – Punto 2, párrafos i) - iii).	Riesgo SI y Compliance	Riesgo SI y Compliance	CISO Corporativo
24/09/2020	3.1	Actualización de Política: Se agrega Política de Gestión de Cloud	Políticas y Métricas	Políticas y Métricas	CISO Corporativo

FALABELLA	Política General de Seguridad de la Información	PL-01
Fecha Revisión: 09/09/2025	Versión: 3.7	Página

22/06/2021	3.2	Actualización de cargos y nombres de los firmantes	Gobierno SI	Gobierno SI	CISO Corporativo
21/06/2022	3.3	Incorporación de las políticas específicas: • Gestión de Seguridad de la Información de FTC. • Gestión de Identidades y cambios menores.	Gobierno SI	Gobierno SI	CISO Corporativo
23/09/2022	3.4	• Incorporación de la aprobación de Políticas de SI en los Directorios de cada Negocio. • Incorporación del rol de DPO. Definición de eventos periódicos y no periódicos.	Subgerencia de Riesgo y Gobierno SI	Subgerencia de Riesgo y Gobierno SI	CISO Corporativo
04/10/2023	3.5	Cambios menores a la Política.	Cyber Risk & Compliance	Cyber Risk & Compliance	CISO Corporativo
09/09/2024	3.6	Cambios menores a la Política.	Gobierno y Protección de Datos	Gobierno y Protección de Datos	CISO Corporativo
09/09/2025	3.7	Actualización anual y cambio a formato corporativo	Gobierno y Protección de Datos	Gerencia de Riesgo y Gobierno de SI	CISO Corporativo