Política del Sistema de Gestión Integral y Seguridad de la Información

Actividad	Nombre	Puesto	Firma
Aprobó:	Beatriz Espejo	VP Audit & Risk Representante Legal.	

Contenido

1. Objetivo del documento

Proporcionar orientación y apoyo a la gestión de seguridad de la información de acuerdo con los requisitos del negocio, leyes y normas para asegurar la confidencialidad, integridad y disponibilidad de la información.

2. Políticas

1. El Audit & Certifications Analyst debe asegurar que la política del Sistema Integral y Seguridad de la Información sea programada para revisión al menos cada 6 meses o antes en caso de que se requiera. Los cambios en el documento deben ser especificados en el con control de cambios.

2. El Head Engineering (Security & ITS) debe coordinar la definición:
   - Del presupuesto de Seguridad de la Información
   - Estrategia de Seguridad de la Información

2.1 Aspectos contractuales de seguridad de la información para proveedores

El VP Legal & Compliance debe asegurar que en todos los contratos cuyo objeto sea la prestación de servicios a título personal bajo cualquier modalidad jurídica que deban desarrollarse en la Organización, establezca los controles de seguridad de la información, protección de datos personales y transferencia de información para asegurar la confidencialidad de patente, marcas, derechos de autor, transferencia de derechos y obligaciones contenidas en los contratos suscritos, siempre restringiendo al mínimo necesario los permisos a otorgar.

2.2 Política del Sistema de Gestión Integral y Seguridad de la Información

Estamos comprometidos con calidad de nuestros servicios, seguridad de la información y protección de datos personales de nuestros clientes, colaboradores y proveedores:

- Ofreciendo soluciones digitales para resolver los retos operacionales, regulatorios y de cumplimiento de las empresas en Iberoamérica.
- Integrando los recursos necesarios para construir procesos de negocio y arquitectura tecnológica en un entorno seguro y de cumplimiento a través de la estandarización de actividades, implementación de controles de seguridad de la información, prevención y detección de soborno en la organización, buscando tener un impacto social y ambiental favorable a la comunidad.
- Preservando la confidencialidad, integridad y disponibilidad de los activos y sistemas de información, trabajando en el cumplimiento de los objetivos del SGI, mantenimiento y mejora continua de nuestro sistema de gestión con apego al marco legal vigente y requisitos aplicables.

2.3 Lineamientos para asegurar la confidencialidad, integridad y disponibilidad de la información ubicada en la infraestructura del proveedor de servicios en la nube.

3. El VP Engineering (Infrastructure) y Head Engineering (Security & ITS) deben especificar y coordinar la gestión de seguridad de la información para el uso de servicios en la nube, así como la revisión de acuerdos para asegurar que este cumple con los controles de seguridad definidos.
   - Soluciones basadas en las normas de la industria de arquitectura y Software.
   - Controles de acceso
   - Monitoreo y protección contra malware
   - Países o regiones para operar aceptados por el grupo
   - Comunicación y atención de incidentes d seguridad de la información
   - Niveles de servicio y escalación de incidentes
   - Pruebas digitales
   - Cambios de infraestructura

2.4 Normatividad vigente respecto a Seguridad de la Información

Las políticas y procedimientos con los cuales opera la Organización se encuentran basados en la normatividad y legislación vigente de seguridad de la información:

- ISO 27001 Tecnología de la Información, "Sistemas de Gestión de Seguridad de la Información".
- ISO 27701 Técnicas de seguridad Extensión ISO 27001, 27002 para la gestión de la protección de datos personales.
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) y su Reglamento

3. Definiciones

Término	Descripción
Seguridad de la información	Conjunto de medidas preventivas y reactivas que permiten resguardar y proteger la información buscando mantener la confidencialidad, disponibilidad e integridad de datos y de la misma.

4. Medidas disciplinarias

La Organización se reserva el derecho de aplicar las sanciones que considere pertinentes en caso de incumplimiento por parte de los colaboradores a los lineamientos establecidos en este documento, así mismo es facultad del Responsable de área solicitar al Comité para exponer el caso y determinar las sanciones disciplinarias, las cuales pueden ser desde llamadas de atención hasta la rescisión de contrato de acuerdo con la regulación vigente o las acciones legales aplicables dependiendo de la criticidad de la falta.

5. Marco de referencia

Marco de referencia	Versión	Cláusula o control
ISO 27001	2022	5.2 Política 6.2 Objetivos de seguridad de la información A.5.1 Directrices de gestión de seguridad de la información
ISO 27701	2019	5.3.2 Política 5.4.2 Objetivos de seguridad de la información y la planeación para lograrlos 6.2.1.1 Políticas de seguridad de la información 6.2.1.2 Revisión de las políticas para seguridad de la información
Matriz de controles SAT	2018	1 Política de seguridad de la información 2 Revisión de Política de Seguridad de la Información 3 Compromiso de la Dirección

6. Control de cambios al documento

Versión	Descripción del cambio	Responsable del cambio
5	Se actualiza en el documento el cargo VP IT & Security	E[redacted] Octubre 2025
6	Se actualizan los puestos: • VP Audit & Risk • VP Infrastructure por VP Engineering (Infrastructure)	Beatriz Espejo Marzo 2026