POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Código: PO-TIC-02
Versión: 1.0
Clasificación: Uso Interno
Propietario: Seguridad de la Información / Gerencia de Tecnología
Fecha: 11/11/2025

---

1. PROPÓSITO

Establecer los lineamientos oficiales de Seguridad de la Información de la organización, garantizando la confidencialidad, integridad, disponibilidad, legalidad, privacidad y trazabilidad de la información, mediante la adopción, operación y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).

Esta política constituye el marco rector del SGSI y reemplaza cualquier lineamiento de seguridad que pueda estar incluido en políticas generales de tecnología. Todos los temas de seguridad se gobiernan exclusivamente desde este documento y el Manual del SGSI (MA-TIC-01).

---

2. ALCANCE

Esta política aplica a:

- Todos los colaboradores, contratistas, proveedores y terceros que accedan, procesen o administren información de la organización.
- Toda la información en cualquier formato, medio, ubicación o sistema.
- Arquitectura tecnológica, infraestructura on-premise y en la nube, aplicaciones, bases de datos, redes, dispositivos, plataformas y servicios digitales.
- Procesos de negocio, procesos de soporte y operaciones tecnológicas relacionadas con el tratamiento o protección de la información.

Nota: PO-TIC-01 establece las directrices generales de Tecnología, pero cualquier instrucción o requisito que afecte la seguridad de la información se rige únicamente por lo establecido en PO-TIC-02.

---

3. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

La política se fundamenta en los siguientes principios:

3.1 Confidencialidad

La información estará disponible solo para personas, sistemas o procesos autorizados.

3.2 Integridad

La información se mantendrá exacta, completa y libre de modificaciones no autorizadas.

3.3 Disponibilidad

Los activos estarán accesibles cuando se requieran para soportar las operaciones del negocio.

3.4 Legalidad y Cumplimiento

La organización cumplirá la legislación aplicable, incluyendo protección de datos personales, delitos informáticos y normas sectoriales.

3.5 Gestión del Riesgo

La seguridad se gestionará con base en evaluación y tratamiento del riesgo.

3.6 Mejora Continua

El SGSI operará bajo el ciclo PHVA (Planear – Hacer – Verificar – Actuar).

3.7 Responsabilidad Compartida

La seguridad es responsabilidad de todos los usuarios.

3.8 No Ocultamiento de Incidentes

Todo incidente debe reportarse inmediatamente por los canales establecidos.

---

4. GOBIERNO DE SEGURIDAD DE LA INFORMACIÓN

El SGSI contará con una estructura de gobernanza que incluye:

- Dirección General
- Dirección Jurídica
- Gerencia de Tecnología
- Seguridad de la Información
- Comité de Ciberseguridad
- Auditoría Interna
- Equipos técnicos y funcionales

Todos ellos cumplirán funciones descritas en MA-TIC-01 y procedimientos PR-TIC.

---

5. MARCO NORMATIVO

El SGSI se alinea con:

- ISO/IEC 27001:2022
- ISO/IEC 27002:2022
- SOC 2 Trust Services Criteria
- Ley 1581 de 2012 (Datos Personales) y normas complementarias
- Ley 1273 de 2009 (Delitos Informáticos)
- Normativa corporativa interna (MA-TIC-01, PR-TIC-03, PR-TIC-02, PR-TIC-01)

Esta política se alinea con la Política Estratégica de Tecnología (PO-TIC-00) y la Política Integral de Tecnología (PO-TIC-01), sin perjuicio de que en materia de seguridad PO-TIC-02 prevalece sobre cualquier lineamiento tecnológico.

---

6. DOMINIOS DE LA SEGURIDAD DE LA INFORMACIÓN

6.1 Gestión de Activos

- Clasificación, inventario, custodia y ciclo de vida de la información y activos tecnológicos.

6.2 Control de Accesos

- Identidad digital, autenticación, autorización y principios de mínimo privilegio.
- Revocación oportuna de accesos.

6.3 Seguridad en el Ciclo de Vida de Desarrollo (SDLC)

- Revisión de vulnerabilidades, pruebas de seguridad, segregación de ambientes y control de cambios.

6.4 Gestión de Incidentes de Seguridad

- Obligatoria para todos los usuarios.
- El proceso oficial se rige por **PR-TIC-03**.

6.5 Seguridad en Infraestructura y Operaciones

- Protección de redes, monitoreo, hardening, registro de eventos, controles de seguridad y gestión de vulnerabilidades.

6.6 Seguridad en Nube

- Configuraciones seguras, protección de identidades, cifrado, monitoreo y gestión de proveedores.

6.7 Gestión de Backups y Recuperación

- Se rige por **PR-TIC-01** y los lineamientos del DRP (PL-TIC-01 y PL-TIC-02).

6.8 Seguridad Física

- Controles de acceso físico, protección de equipos y ambientes críticos.

6.9 Privacidad y Protección de Datos Personales

- Cumplimiento de normativa colombiana e internacional aplicable.
- Procesos de notificación de incidentes a la SIC cuando corresponda.

6.10 Continuidad y Resiliencia

- Integración formal con el DRP y procesos de continuidad.

---

7. ROLES Y RESPONSABILIDADES

Dirección General

- Aprueba la política y asigna recursos.

Dirección Jurídica

- Define lineamientos legales y regulatorios.

Gerencia de Tecnología

- Implementa controles técnicos y garantiza la operación segura.

Seguridad de la Información

- Administra el SGSI.
- Define controles, supervisa su cumplimiento y gestiona riesgos.

Comité de Ciberseguridad

- Supervisa incidentes críticos.
- Revisa riesgos, auditorías y decisiones de seguridad.

Colaboradores y Terceros

- Cumplen esta política y los procedimientos derivados.

---

8. CUMPLIMIENTO Y SANCIONES

El incumplimiento de esta política podrá generar:

- Acciones disciplinarias.
- Suspensión de accesos.
- Investigaciones internas.
- Terminación de contratos con terceros.

La organización realizará auditorías periódicas para validar su cumplimiento.

---

9. MEJORA CONTINUA

Esta política será revisada anualmente o cuando existan:

- Cambios significativos en infraestructura o procesos.
- Incidentes relevantes.
- Cambios regulatorios.
- Requerimientos de auditorías o certificaciones.

---

10. CONTROL DE CAMBIOS

Versión	Fecha	Descripción	Autor	Aprobó
1.0	11/11/2025	Emisión inicial	Jefe de Tecnología y Ciberseguridad	Gerencia de Tecnología

---