EDICIÓN 2 FECHA: 3 OCTUBRE 2025 RCE-18-PE01 NIVEL DE SEGURIDAD: PUBLICA	**PROCESO APOYO - DIRECCION Y LIDEGAZGO** **Políticas De Seguridad De La Información**	

TABLA DE CONTENIDO

REALIZO:	REVISO:	APROBO:
Equipo SGI Coordinador SGI	LAIDY SEGURA Director Nacional de operaciones	Luis Alejandro Rodríguez Ariza Gerente General

1. POLITICA DE SEGURIDAD DE LA INFORMACIÓN

Conexiones Empresariales S.A.S. establece esta Política de Seguridad de la Información con el compromiso de proteger la confidencialidad, integridad y disponibilidad de la información, asegurando la continuidad del negocio y el cumplimiento de los requisitos normativos y contractuales aplicables.

Nuestro enfoque es brindar trato con excelencia y responsabilidad a la información que ingresa a nuestra compañía, adoptando medidas de formación y conciencia a todos nuestros colaboradores.

2. ALCANCE

Esta política aplica a todos los colaboradores, proveedores, aliados estratégicos y terceros que tengan acceso a los sistemas de información, datos, infraestructura tecnológica y activos de información de la organización.

3. PRINCIPIOS Y COMPROMISOS

a) Adecuación al Propósito de la Organización

Esta política está alineada con la misión y visión de Conexiones Empresariales, asegurando la protección de la información en los servicios de mensajería y logística a nivel nacional.

b) Objetivos de Seguridad de la Información

- Proteger los datos y activos de información contra accesos no autorizados, alteraciones, pérdidas o divulgaciones indebidas.
- Garantizar la seguridad en el desarrollo de software y en la integración con terceros.
- Aplicar controles de seguridad en dispositivos móviles, entornos de escritorio limpio y control de accesos.

- Implementar medidas para la seguridad de la cadena de suministro con terceros.
- Fomentar una cultura organizacional de seguridad de la información.

c) Cumplimiento de Requisitos Aplicables

Conexiones Empresariales se compromete a cumplir con:

- La norma ISO/IEC 27001 y regulaciones nacionales aplicables en protección de datos.
- Requisitos contractuales y normativos con clientes y entidades reguladoras.
- Lineamientos de seguridad en la gestión de proveedores y servicios de terceros.

d) Compromiso con la Mejora Continua

La Alta Dirección garantiza la actualización constante del SGSI a través de:

- Evaluaciones periódicas de riesgos y auditorías internas.
- Revisión y actualización de controles de seguridad según amenazas emergentes.
- Formación y concienciación continua del personal en seguridad de la información.

4. POLÍTICAS ESPECIFICAS

4.1 Política de Dispositivos Móviles

- Los dispositivos móviles que accedan a información corporativa deberán contar con autenticación robusta y cifrado de datos.
- Está prohibido el uso de redes WiFi públicas no autorizadas para acceder a información corporativa.
- Se deberán implementar soluciones de administración de dispositivos móviles (MDM) para aplicar controles de seguridad.

4.2 Política de Escritorio Limpio y Pantalla Limpia

- Los colaboradores deben asegurar que ningún documento sensible quede expuesto en escritorios o espacios de trabajo compartidos.
- Las pantallas de los equipos deben bloquearse automáticamente tras un tiempo definido de inactividad.
- Se debe evitar el almacenamiento de información confidencial en dispositivos personales no autorizados.

4.3 Política de Desarrollo Seguro

- Todo software desarrollado internamente o adquirido deberá cumplir con principios de seguridad desde el diseño (Security by Design).
- Se realizarán pruebas de seguridad (pentesting, revisión de código) antes de desplegar cualquier aplicación en producción.
- Se implementará control de versiones y gestión de cambios en desarrollos internos.

4.4 Seguridad en la Cadena de Suministro con Terceras Partes

- Se establecerán cláusulas de seguridad de la información en los contratos con proveedores.
- Los terceros deberán cumplir con los estándares de seguridad exigidos por Conexiones Empresariales.
- Se realizarán auditorías y revisiones periódicas a los servicios de terceros para validar su cumplimiento.

4.5 Control de Accesos

- Se aplicará el principio de mínimos privilegios, otorgando acceso solo a la información necesaria para cada rol.
- Se implementará autenticación multifactor (MFA) en accesos críticos.
- Se revisarán periódicamente los permisos de acceso y se revocarán cuando ya no sean necesarios.

5. INCUMPLIMIENTO

El incumplimiento de esta política, así como de los procedimientos y controles establecidos en el SGSI, puede derivar en acciones disciplinarias y/o legales, según la gravedad de la falta y en conformidad con la normativa interna y la legislación vigente.

Las consecuencias del incumplimiento incluyen, pero no se limitan a:

a) Sanciones administrativas internas, que pueden incluir advertencias, suspensión o terminación del contrato laboral.
b) Acciones legales en caso de negligencia grave o incumplimientos que afecten a clientes, aliados estratégicos o a la organización.
c) Limitación o revocación de accesos a los sistemas de información para prevenir riesgos adicionales.
d) Reportes a entidades reguladoras, en caso de incumplimientos que comprometan la seguridad de los datos personales o normativas aplicables.

Cada colaborador y tercero que interactúe con los activos de información de la empresa es responsable de conocer y cumplir con esta política, así como de reportar cualquier sospecha de incumplimiento a través de los canales internos de seguridad de la información.

6. DISPONIBILIDAD Y COMUNICACIÓN

a) Esta política se encuentra disponible como información documentada en el sistema de gestión de documentos de la organización.
b) Se comunicará a todos los colaboradores y partes interesadas relevantes mediante capacitaciones, boletines y reuniones periódicas.
c) Será revisada y actualizada anualmente o cuando se requiera por cambios normativos o tecnológicos.