POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. Objetivo

Establecer los lineamientos para garantizar la **confidencialidad, integridad y disponibilidad** de la información, en todos los procesos de la compañía, protegiendo los activos de información y asegurando el cumplimiento de requisitos legales, contractuales y normativos relacionados con la **seguridad de la información**.

2. Alcance

Esta política es de obligatorio cumplimiento para todos los colaboradores, contratistas, proveedores, aliados estratégicos y cualquier tercero que, en ejercicio de una relación laboral, comercial o contractual, tenga acceso a los sistemas de información, datos personales o activos digitales de la compañía. Incluye información física, digital, almacenada, transmitida o procesada en cualquier medio, y aplica a dispositivos móviles, redes, correo corporativo, bases de datos, sistemas GPS, software logístico, servidores y archivos físicos.

Principios de confidencialidad:

- **Confidencialidad:** Solo las personas autorizadas pueden acceder a la información.
- **Integridad:** La información debe mantenerse completa, exacta y protegida contra modificaciones no autorizadas.
- **Disponibilidad:** La información debe estar disponible cuando se requiera para las operaciones del negocio.
- **Trazabilidad:** Toda acción o acceso sobre la información deberá ser trazable y registrable.
- **Responsabilidad proactiva (Accountability):** Se deben implementar medidas preventivas y correctivas que evidencien el cumplimiento normativo.

3. Lineamientos Generales

- Todo usuario debe utilizar credenciales únicas y mantener la confidencialidad de sus contraseñas.
- Se prohíbe el acceso no autorizado a los sistemas de información.

- La información sensible debe ser protegida mediante cifrado y medidas de seguridad adecuadas.
- El acceso a internet estará restringido a fines laborales conforme al reglamento interno.

4. Uso de los Sistemas de Información

- Los sistemas deben ser utilizados exclusivamente para fines laborales.
- Se prohíbe la instalación de software no autorizado.
- El acceso a internet debe estar regulado para evitar riesgos de seguridad.

5. Seguridad en Red Interna

Las redes tienen como propósito principal servir en la transformación e intercambio de información dentro de la entidad, por lo tanto:

- El Área de sistemas no es responsable por el contenido de datos ni por el tráfico que en ella circule, la responsabilidad recae directamente sobre el usuario que los genere o solicite.
- Nadie puede ver, copiar, alterar o destruir la información que reside en los equipos sin el consentimiento explícito del responsable del equipo.
- No se permite el uso de los servicios de la red cuando no cumplan con las labores propias de la entidad.
- Las cuentas de ingreso a los sistemas y los recursos de cómputo son propiedad de la entidad y se usarán exclusivamente para actividades relacionadas con la labor asignada.
- Todas las cuentas de acceso a los sistemas y recursos de las tecnologías de información son personales e intransferibles. Se permite su uso única y exclusivamente durante la vigencia de derechos del usuario.
- No se permitirá el uso de analizadores para monitorear o censar redes ajenas a Las Empresas y no se deberán realizar análisis de la Red desde equipos externos a la entidad.
- No deben ser reemplazados ni modificados sin la intervención del responsable del área de sistemas de la Entidad; los Firewalls, antivirus y en general, todos los programas o aplicativos destinados a la prevención de intrusos no deseados y de elementos dañinos para los equipos.

6. Configuración e Instalación de los Servidores

El área de sistemas tiene la responsabilidad de verificar la instalación, configuración e implementación de seguridad, en los servidores conectados a la red. Durante la configuración de los servidores se deben genera las normas para el uso de los recursos del sistema y de la red, principalmente la restricción de directorios, permisos y programas a ser ejecutados por los usuarios.

7. Protección de Datos

- Se implementarán copias de seguridad diariamente.
- La empresa garantizará el cumplimiento de normativas de protección de datos personales.
- Se aplicarán protocolos de respuesta ante incidentes de seguridad.

8. Sanciones

El incumplimiento de esta política podrá derivar en sanciones disciplinarias: se considera falta grave por parte del trabajador la elaboración de cualquier tipo de copia no autorizada de cualquier documento o archivo contenido en papeles, cintas magnetofónicas, videos, discos de computadora, etc.; su sustracción sin la autorización de su inmediato superior, o el revelar la información o por cualquier clase de medio.

Se aplicarán controles de seguridad a los datos personales conforme a la legislación vigente (Ley 1581 de 2012).

9. Responsable de la política

El **Oficial de Protección de Datos Personales (DPO)** de CONEXIONES S.A.S. será el encargado de velar por la implementación, actualización y cumplimiento de esta política, así como de liderar campañas de concientización, auditorías internas y respuesta ante vulneraciones.
Contacto: protecciondatos@conexiones.net.co

10. Vigencia

Esta política rige a partir del **01 de agosto de 2025** y permanecerá vigente mientras existan datos o información bajo tratamiento por parte de la compañía. Será revisada y actualizada anualmente o cuando se presenten cambios regulatorios o tecnológicos significativos.

Aprobado por:
GERENCIA GENERAL – CONEXIONES S.A.S.