EDICIÓN 2 FECHA: 03 OCTUBRE 2025 RCE-16-PE01 NIVEL DE SEGURIDAD: PUBLICA	**PE01- DIRECCION Y LIDEGAZGO**	
	Política de transferencia de Información	

TABLA DE CONTENIDO

EDICIÓN 2 FECHA: 03 OCTUBRE 2025 RCE-16-PE01 NIVEL DE SEGURIDAD: PUBLICA	**PE01- DIRECCION Y LIDEGAZGO** **Política de transferencia de Información**	

1**. OBJETIVO**

Regular la transferencia de información dentro y fuera de la empresa para prevenir accesos no autorizados o fugas de datos.

2. **ALCANCE**

Aplica a todos los funcionarios, contratistas y terceros que transfieran información corporativa.

3. **LINEAMIENTOS**

- Solo se deben usar canales autorizados para la transferencia de información (correo corporativo, VPN, plataformas seguras).
- La información confidencial enviada por correo debe cifrarse y protegerse con contraseñas seguras.
- Está prohibido compartir información corporativa no autorizadas.
- La transferencia de datos a terceros debe contar con autorización y acuerdos de confidencialidad.
- Se realizarán controles para monitorear el tráfico de información y detectar posibles fugas de datos.
- Se cuenta con Antivirus y Antimalware, estas soluciones realizan análisis periódicos de los sistemas y archivos en busca de posibles códigos maliciosos, y bloquean cualquier intento de infección.
- Análisis en Tiempo Real en todos nuestros sistemas están configurados para realizar un análisis en tiempo real de archivos y aplicaciones en ejecución, lo que permite detectar y prevenir cualquier intento de malware de manera inmediata.
- se ejecutan actualizaciones y Parches de Seguridad, asegurando que todos los sistemas operativos, aplicaciones y software de seguridad reciban actualizaciones de seguridad oportuna
- odas las transferencias de información se registran de manera detallada en un sistema de registro de eventos (logs) para garantizar la trazabilidad y el monitoreo continuo de las mismas. Esto nos permite detectar cualquier transferencia no autorizada o inusual.
- Los datos y documentos generados en la plataforma se almacenan en bases de datos y repositorios en AWS, los cuales cuentan con cifrado en reposo (AES-256) y en tránsito (TLS 1.2/1.3)
- La transferencia de datos realiza a través de una aplicación web, donde la comunicación está cifrada utilizando HTTPS con TLS 1.2/1.3 y autenticación.
-

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

4. **CONTROL DE ACCESOS:**
Aplicamos políticas de control de acceso estrictas, de modo que solo personal autorizado pueda acceder a áreas críticas de la red y los sistemas.

Los usuarios tienen privilegios mínimos para realizar tareas, lo que ayuda a limitar el impacto de un posible ataque de malware.

4.1 Protección contra Phishing y Ataques de Ingeniería Social:
Implementamos filtros de correo electrónico para bloquear mensajes de phishing y otros intentos de ingeniería social, que son métodos comunes para introducir malware en los sistemas

4.2. Análisis de Archivos Descargados:
Los archivos descargados de Internet o recibidos por correo electrónico son analizados automáticamente antes de ser ejecutados para detectar posibles amenazas.

Se limita el acceso a sitios web no seguros y se bloquean aplicaciones de descargas no autorizadas que puedan ser vectores de infección.

4.3. Segmentación de Red y Monitoreo Continuo:
Nuestra red está segmentada para limitar la propagación de posibles infecciones. Si un sistema se ve comprometido, su acceso a otras partes de la red es restringido.

Contamos con un sistema de monitoreo continuo de la red para detectar comportamientos anómalos que podrían indicar la presencia de malware o un ataque en curso.

4.4. Copias de Respaldo (Backup):
Realizamos copias de seguridad regulares de datos importantes y sistemas clave, que se almacenan de forma segura y fuera de línea, para asegurar la recuperación en caso de un ataque de ransomware o cualquier otro tipo de malware que afecte la disponibilidad de los datos.

4.5. Respuesta ante Incidentes:
En caso de que se detecte malware o cualquier otra amenaza, contamos con un procedimiento de respuesta ante incidentes que permite actuar rápidamente para mitigar los efectos, identificar la fuente del ataque, y restaurar los sistemas comprometidos a su estado seguro.
RESPONSABILIDADES

- Coordinador de SGI (sistema de Gestión Integral):
- Funcionarios y colaboradores de la empresa CONEXIONES EMPRESARIALES SAS

1. INCUMPLIMIENTO

El incumplimiento puede derivar en restricciones de acceso, sanciones disciplinarias o acciones legales según la gravedad.

2. DISPONIBILIDAD Y COMUNICACIÓN.

a) Se comunicará a todos los colaboradores y partes interesadas relevantes mediante capacitaciones, boletines y reuniones periódicas.
b) Será revisada y actualizada anualmente o cuando se requiera por cambios normativos o tecnológicos.

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