EDICIÓN 3 FECHA: 13 OCTUBRE 2025 RCE-09-PE01 NIVEL DE INFORMACION: PUBLICA	**PA - 05 PROCESO APOYO - DIRECCION Y LIDEGAZGO**	
	Política de criptografía	

TABLA DE CONTENIDO

1. OBJETIVO **2**

2. ALCANCE **2**

3. PRINCIPIOS GENERALES **2**

3.1. Uso de Criptografía: 2

3.2. Requisitos Técnicos: 3

3.3. Uso de Herramientas de Criptografía: 3

3.4. Capacitación y Concientización: 4

3.5. Cumplimiento Legal y Regulatorio: 4

4. RESPONSABILIDADES **4**

5. REVISION Y ACTUALIZACIONES **4**

1. OBJETIVO

El propósito de esta política es establecer los lineamientos y controles necesarios para la utilización adecuada de la criptografía dentro de CONEXIONES EMPRESARIALES SAS para proteger la confidencialidad, integridad y disponibilidad de la información, y asegurar que los datos sensibles y/o confidenciales estén protegidos contra accesos no autorizados, modificaciones o pérdidas durante su almacenamiento, transmisión o procesamiento.

2. ALCANCE

Esta política es aplicable a todos los sistemas de información, redes, equipos, aplicaciones y datos gestionados por CONEXIONES EMPRESARIALES SAS, y debe ser cumplida por todos los empleados, contratistas, socios y proveedores que tengan acceso a los sistemas y datos protegidos por criptografía dentro de la organización.

3. PRINCIPIOS GENERALES

- Confidencialidad: La criptografía debe ser utilizada para proteger la confidencialidad de la información durante su transmisión y almacenamiento.
- Integridad: Se debe garantizar que los datos no sean alterados de manera no autorizada, mediante el uso de algoritmos de hash y técnicas de verificación de integridad.
- Autenticación: Se utilizarán mecanismos criptográficos para verificar la identidad de los usuarios, dispositivos y sistemas, y para prevenir suplantaciones de identidad.
- No Repudio: La criptografía debe ser utilizada para garantizar que las partes no puedan negar la autenticidad de sus acciones o transacciones en el sistema.

3.1. Uso de Criptografía:

- **Encriptación de Datos Sensibles**: Todos los datos sensibles (personales, financieros, confidenciales, etc.) que sean transmitidos por medios electrónicos o almacenados en dispositivos deben ser encriptados utilizando algoritmos de alta seguridad, tales como **AES-256** para datos en reposo y **TLS/SSL** para datos en tránsito.
- **Gestión de Claves Criptográficas**: La gestión de claves criptográficas es fundamental para garantizar la seguridad de los datos. Las claves deben ser generadas, distribuidas, almacenadas y revocadas siguiendo las mejores prácticas de seguridad. Solo el personal autorizado debe tener acceso a las claves privadas, y las claves deben ser almacenadas en dispositivos seguros como **Hardware Security Modules (HSM)** o sistemas de gestión de claves.

- **Autenticación Multifactor (MFA)**: Se debe implementar la **autenticación multifactor** utilizando algoritmos criptográficos como parte del proceso de verificación de identidad para acceder a sistemas que contengan información sensible.
- **Firma Digital**: Todos los documentos y comunicaciones electrónicas que requieran un nivel adicional de seguridad, como contratos, acuerdos o comunicaciones críticas, deberán estar firmados digitalmente utilizando un certificado válido.

3.2. Requisitos Técnicos:

- **Protocolos de Seguridad**: Los protocolos de seguridad como **TLS (Transport Layer Security)**, **IPsec** y **VPNs** deben ser implementados para proteger la comunicación de datos dentro de la red interna y hacia/desde la red pública.
- **Cifrado de Dispositivos Portátiles**: Todos los dispositivos portátiles (como laptops, teléfonos móviles y USB) que contengan datos sensibles deben estar cifrados utilizando estándares de cifrado robustos.
- **Revocación de Claves**: Las claves criptográficas deben ser revocadas de manera inmediata en caso de compromiso de seguridad, cuando el empleado deje la organización o cuando el acceso ya no sea necesario.
- Toda la información almacenada en nuestras bases de datos y repositorios de documentos en AWS está cifrada utilizando AES-256.
- Cifrado en Tránsito: Se utiliza TLS 1.2/1.3 para proteger la comunicación entre los diferentes componentes de la plataforma.
  Gestión de Claves Criptográficas las cuales se aplican el Principio de Mínimos Privilegios (PoLP) en la gestión de claves, asegurando que solo usuarios y servicios autorizados puedan acceder a ellas.

3.3. Uso de Herramientas de Criptografía:

- Las herramientas y soluciones criptográficas aprobadas por **CONEXIONES EMPRESARIALES SAS** deben cumplir con los estándares internacionales de seguridad y ser evaluadas periódicamente. Los empleados no deben utilizar herramientas o algoritmos criptográficos no autorizados.
- Las soluciones criptográficas deben ser revisadas de forma continua para adaptarse a los avances tecnológicos y para garantizar que las mismas no presenten vulnerabilidades conocidas.

3.4. Capacitación y Concientización:

Todos los empleados de **CONEXIONES EMPRESARIALES SAS** deben recibir capacitación periódica sobre el uso adecuado de la criptografía, la gestión de claves y la protección de datos sensibles, asegurándose de que entienden la importancia de la seguridad criptográfica y las implicaciones de su manejo.

3.5. Cumplimiento Legal y Regulatorio:

CONEXIONES EMPRESARIALES SAS cumplirá con todas las leyes y regulaciones relacionadas con la protección de datos personales y la seguridad de la información, como el **Reglamento General de Protección de Datos (GDPR)**, la **Ley de Protección de Datos Personales**, y otras normativas locales e internacionales aplicables.

4. RESPONSABILIDADES

- El equipo de **Tecnologías de la Información (TI)** es responsable de la implementación, gestión y mantenimiento de los sistemas criptográficos y de asegurar que todos los controles sean cumplidos.
- Los empleados deben cumplir con esta política y reportar cualquier incidente de seguridad relacionado con el uso indebido de la criptografía o el compromiso de claves criptográficas.

5. REVISION Y ACTUALIZACIONES

Esta política será revisada al menos anualmente, o antes si fuera necesario, para asegurar que se mantenga actualizada con los avances tecnológicos, cambios regulatorios o mejoras de procesos