

	<b>POLÍTICA DE CONTROLES CRIPTOGRÁFICOS</b>	<b>VERSIÓN:</b> 02
		<b>Fecha:</b> 02/05/2025
	<b>GESTIÓN DE TECNOLOGÍA</b>	<b>POL-GT-002</b>
		<b>Página</b> 1 de 2
	<b>ETIQUETA</b>	<b>RESTRINGIDO</b>

ELABORÓ	REVISÓ	APROBÓ
Samuel Andrés Córdoba <b>CISO</b>	Johely Lorena López A. <b>Gerente Administrativa y Financiera</b>	Pedro Pabón <b>Gerente General</b>

## 1. OBJETIVO GENERAL

Garantizar el uso seguro, eficiente y conforme de controles criptográficos para proteger la información sensible y cumplir con los requisitos legales, regulatorios y contractuales.

## 2. OBJETIVOS ESPECÍFICOS

- Proteger la confidencialidad, integridad y disponibilidad de la información.
- Asegurar el cumplimiento de normativas, estándares y leyes aplicables.
- Establecer directrices para la implementación, gestión y uso de criptografía.

## 3. ALCANCE

Esta política aplica a todos los empleados, contratistas, socios y terceros que utilicen o gestionen activos de información de la organización.

## 4. POLÍTICA DE CONTROLES CRIPTOGRÁFICOS

### 4.1. Selección de Métodos Criptográficos

Se deben utilizar algoritmos criptográficos aprobados por estándares internacionales como NIST o ISO. Se deben evitar algoritmos obsoletos o inseguros (tales como MD5, DES, TLS 1.0).

### 4.2. Uso de Criptografía en las Comunicaciones

- Implementar cifrado para proteger los datos en tránsito utilizando TLS 1.2 o superior.
- Respecto a las redes inalámbricas se debe emplear siempre WPA2 con el cifrado AES (Advanced Encryption Standard). Evitar configuraciones que permitan el uso de TKIP.
- Para las redes inalámbricas utilizar contraseñas largas, complejas y únicas (al menos 12 caracteres combinando letras, números y símbolos).
- Para transferir información sensible relacionada con códigos, datos o contraseñas se debe emplear el aplicativo ClavesSeguras2, diseñado por la organización para tal fin.

### 4.3. Protección de Datos en Reposo

- Se utiliza cifrado de disco completo a través de la herramienta dispuesta por Microsoft
- Asegurar que las bases de datos almacenen datos sensibles de forma cifrada.

	<b>POLÍTICA DE CONTROLES CRIPTOGRÁFICOS</b>	<b>VERSIÓN:</b> 02
		<b>Fecha:</b> 02/05/2025
	<b>GESTIÓN DE TECNOLOGÍA</b>	<b>POL-GT-002</b>
		<b>Página</b> 2 de 2
	<b>ETIQUETA</b>	<b>RESTRINGIDO</b>

#### 4.4. Firma Digital y Autenticación

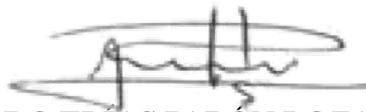
- Implementar firmas digitales para garantizar la autenticidad de documentos y transacciones.
- Utilizar mecanismos de autenticación multifactor (MFA) con tecnologías criptográficas para aquellos servicios que lo permiten.

#### 5. VIGENCIA

Esta Política es aplicable para todos los funcionarios, contratistas y terceros a partir de momento de su publicación, será revisada anualmente y actualizada según corresponda y comunicada por los medios establecidos por la Organización a todos los trabajadores y partes interesadas.

#### 6. CONSECUENCIA DE INCUMPLIMIENTO

Cualquier violación o incumplimiento a la presente política es calificada como grave y constituye justa causa para dar por terminado el contrato laboral o contractual vigente.



**PEDRO ELÍAS PABÓN LOZANO**  
Gerente General

#### CONTROL DE CAMBIOS

VERSIÓN	OBSERVACIÓN	FECHA
1.0	Creación del documento.	24/10/2024
2.0	Se hace referencia al aplicativo ClavesSeguras2 diseñada por la organización.	02/05/2025