Política de criptografía

Propietario de la política: VICTOR ACOSTA LOPEZ

Fecha de entrada en vigencia: 09/04/2024

Objetivo

Garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad o integridad de la información. Esta política establece los requisitos para el uso y la protección de claves criptográficas y métodos criptográficos durante todo el ciclo de vida del cifrado.

Alcance

Todos los sistemas de información desarrollados o controlados por D3M3NT SA DE CV que almacenen o transmitan datos confidenciales.

Política

D3M3NT SA DE CV evaluará los riesgos inherentes al procesamiento y almacenamiento de datos, e implementará controles criptográficos para mitigar esos riesgos cuando se considere apropiado. Cuando se utilice el cifrado, se implementará y documentará una criptografía fuerte con procesos y procedimientos asociados de administración de claves. Todo el cifrado se realizará de acuerdo con los estándares de la industria, incluido el estándar NIST SP 800-57.

Los datos confidenciales del cliente o de la empresa deben utilizar cifrados y configuraciones sólidos de conformidad con las recomendaciones del proveedor y las prácticas recomendadas de la industria, incluido NIST cuando se almacenan o transfieren mediante una red pública.

Administración de claves

El acceso a claves y secretos se controlará firmemente de acuerdo con la Política de control de acceso.

La siguiente tabla incluye el uso recomendado de claves criptográficas:

Dominio	**Tipo de clave**	**Algoritmo**	**Longitud de la clave**	**Vencimiento máximo**
Certificado web	RSA o ECC con firma SHA2+	RSA o ECC con firma SHA2+	2048 bits o más/RSA, bits o más/ECC	Hasta 1 año
Cifrado web (TLS)	Cifrado asimétrico	Cifrado de calificación B o superior en SSL Labs	Varía	N/A
Datos confidenciales en reposo	Cifrado simétrico	AES	256 bits	1 año
Contraseñas	Hash unidireccional	Bcrypt, PBKDF2 o scrypt, Argon2	256 bits+10K de longitud Incluir sal+pimienta criptográfica única	N/A
Almacenamiento de puntos de conexión (SSD/HDD)	Cifrado simétrico	AES	128 o 256 bits	N/A

Excepciones

Las solicitudes de excepción a esta política deben enviarse al gerente de TI para su aprobación.

Se requiere una excepción documentada antes de mover, copiar o almacenar los datos confidenciales del cliente o de la empresa en cualquier medio o dispositivo extraíble; todos los dispositivos portátiles y los medios extraíbles que contengan datos confidenciales deben cifrarse utilizando estándares y mecanismos aprobados.

Infracciones y cumplimiento

Cualquier infracción conocida de esta política debe reportarse al gerente de TI. Las infracciones de esta política pueden dar lugar a la retirada o suspensión inmediata de los privilegios del sistema y la red o medidas disciplinarias de acuerdo con los procedimientos de la empresa, incluido el despido.

Versión	Fecha	Descripción	Autor	Aprobado por
1.0	25/05/2023	Primera Revisión	Víctor Acosta	Marco Villanueva
1.1	09/04/2024	Ajuste por Traducción	Víctor Acosta	Marco Villanueva