Ministerio de
Planificación Estratégica y Modernización

Gobierno de JUJUY
Cerca de la gente

PROTOCOLO
PROVINCIAL DE CIBERSEGURIDAD

Estándar de IT: Estándar de Cifrado

12
CAPÍTULO

Estándar de TI: Estándar de Cifrado

1.0 Propósito y Beneficios

El cifrado es una operación criptográfica que se utiliza para mejorar la seguridad y proteger los datos electrónicos (“datos”) transformando información legible (“texto sin formato”) en información ininteligible (“texto cifrado”). El cifrado es una herramienta eficaz para mitigar la amenaza del acceso no autorizado a los datos.

2.0 Alcance

Esta norma se aplica a todos los sistemas, que incluyen sitios web y servicios web, para los cuales la Repartición tiene responsabilidad administrativa, incluidos aquellos administrados y alojados por terceros en nombre del Gobierno de la Provincia de Jujuy.

3.0 Declaración de Información

La necesidad de cifrar la información se basa en su clasificación, los resultados de la evaluación de riesgos y el caso de uso.

Se debe prestar atención a las regulaciones y restricciones nacionales (por ejemplo, controles de exportación) que pueden aplicarse al uso de técnicas criptográficas en diferentes partes del mundo.

Sin perjuicio de las normas nacionales que resultaren aplicables, los productos de cifrado para la confidencialidad de los datos en reposo y en tránsito deben incorporar algoritmos aprobados por entidades nacionales y/o internacionales para el cifrado de datos. Los algoritmos de cifrado aprobados se encuentran en el Apéndice A.

Los algoritmos hash transforman un mensaje digital en una representación corta para usar en firmas digitales y otras aplicaciones para validar la integridad del mensaje.

Aunque las funciones hash como SHA 1 proporcionan una cierta cantidad de seguridad, no cumplen con todos los requisitos de seguridad para funciones hash con clave como HMAC SHA 1. Consulte FIPS 180-4 para obtener más infor-

mación sobre los diferentes tipos de algoritmos hash de aplicaciones así como **Apéndice A**.

Los algoritmos hash se pueden utilizar para múltiples propósitos, incluidos, entre otros, firmas digitales, códigos de autenticación de mensajes, funciones de derivación de claves y funciones pseudoaleatorias.

Las funciones hash aprobadas están contenidas en **Apéndice A.**

Está prohibido el uso de algoritmos de cifrado/funciones hash patentados, obsoletos y criptográficamente rotos.

La información electrónica utilizada para autenticar la identidad de un individuo o proceso (es decir, PIN, contraseña, frase de contraseña) debe cifrarse cuando se almacena, transporta o transmite. Esto no incluye la distribución de un PIN, contraseña, frase de contraseña, código token, etc. de un solo uso, siempre que no se distribuya junto con ninguna otra información de autenticación (por ejemplo, ID de usuario).

El plan de seguridad de un sistema debe incluir documentación que muestre una revisión adecuada de las metodologías y productos de cifrado. Esto demostrará la debida diligencia al elegir un método o producto que haya recibido una revisión positiva sustancial por parte de analistas externos acreditados.

3.1 DATOS EN TRÁNSITO

Se requiere cifrado para los datos en tránsito en las siguientes situaciones:

1. Cuando se transmite información electrónica de identificación personal (PII) (incluidos, entre otros, correo electrónico, protocolo de transferencia de archivos (FTP), mensajería instantánea, fax electrónico, voz sobre protocolo de Internet (VoIP), etc.).
2. Cuando el cifrado de datos en tránsito esté prescrito por ley o reglamento.
3. Al conectarse a las redes internas a través de una red inalámbrica.
4. Al acceder de forma remota a las redes o dispositivos internos de una Repartición a través de una red compartida (por ejemplo, Internet) o personal (por ejemplo, Bluetooth, infrarrojos). Esto no se aplica al acceso remoto a través de una conexión dedicada punto a punto administrada por una Repartición.
5. Cuando los datos se transmiten con el sitio web público y/o los servicios web de una entidad, se les exige utilizar el Protocolo seguro de transferencia de hipertexto (HTTPS) en lugar del Protocolo de transferencia de hipertexto (HTTP) cuando sea técnicamente posible.

Los sitios web públicos deben utilizar HTTP Strict Transport Security (HSTS), redirigiendo automáticamente las solicitudes HTTP a sitios web HTTPS cuando sea técnicamente posible. La compatibilidad mínima del navegador se enumera en el Apéndice B.

Los métodos de cifrado adecuados para los datos en tránsito incluyen, entre otros, Transport Layer Security (TLS) 1.2 o posterior, Secure Shell (SSH) 2.0 o posterior, Wi-Fi Protected Access (WPA) versión 2 o posterior (con WiFi Protected Access). Configuración deshabilitada) y redes privadas virtuales (VPN) cifradas. Los componentes deben configurarse para admitir los conjuntos de cifrado más potentes posibles. Los cifrados que no cumplan con este estándar deben desactivarse.

3.2 LOS DATOS EN REPOSO

Se requiere cifrado para los datos en reposo, de la siguiente manera:

1. Para los sistemas enumerados a continuación:
    a. Escritorios que acceden o contienen información de identificación personal (PII);
    b. Almacenes de datos (incluidos, entre otros, bases de datos y archivos compartidos) que contienen PII;
    c. Todos los dispositivos móviles, ya sea emitidos por la Repartición o de terceros, que accedan o contengan cualquier información de la Provincia; y
    d. Todos los dispositivos de almacenamiento portátiles que contengan cualquier información de la Provincia.
2. Cuando la información PII electrónica se transporta o almacena fuera de las instalaciones del Gobierno de la Provincia.

Se requiere cifrado de disco completo para todas las computadoras portátiles emitidas por alguna Repartición que acceden o contienen información del Gobierno de la Provincia. Los productos de cifrado de disco completo deben utilizar autenticación previa al arranque que utiliza el Módulo de plataforma segura (TPM) del dispositivo o el arranque seguro de la interfaz de firmware extensible unificada (UEFI).

Para mitigar los ataques contra las claves de cifrado, cuando se encuentren fuera de las instalaciones de la Repartición, las computadoras portátiles y las computadoras portátiles de terceros que accedan o contengan PII deben apagarse (es decir, apagarse o hibernarse) cuando estén desatendidas.

La entidad debe contar con un proceso o procedimiento para confirmar que los dispositivos y medios se hayan cifrado exitosamente utilizando al menos uno de los siguientes, enumerados en orden preferido:

1. aplicación automatizada de políticas;
2. sistema de inventario automatizado; o
3. mantenimiento de registros manuales.

3.3 GESTIÓN DE CLAVES

La entidad debe garantizar que se establezca un entorno seguro para proteger las claves criptográficas utilizadas para cifrar y descifrar la información. Las claves deben distribuirse y almacenarse de forma segura.

El acceso a las claves debe restringirse únicamente a las personas que tengan una necesidad gubernamental de acceder a las claves.

Las claves no cifradas no deben almacenarse con los datos que cifran. Las claves estarán protegidas con un token de autenticación que se ajuste al nivel de seguridad identificado.

El compromiso de una clave criptográfica haría que toda la información cifrada con esa clave se considere no cifrada. Si se descubre un compromiso, se debe generar y utilizar una nueva clave para continuar con la protección de la información cifrada. Se deben evaluar circunstancias específicas para determinar si se requiere una notificación de incumplimiento.

Las claves de cifrado y sus productos de software asociados deben conservarse durante la vida útil de los datos archivados que se cifraron con ese producto.

4.0 Cumplimiento

Los empleados que incumplan esta política pueden estar sujetos a medidas disciplinarias, así como sanciones penales, civiles y/o administrativas si correspondieren. Los no empleados, incluidos, entre otros, los contratistas, pueden estar sujetos a la rescisión de acuerdos contractuales, a la denegación de acceso a los recursos de TI y a otras acciones, así como a sanciones tanto civiles como penales.

5.0 Historial de revisiones

Fecha	Descripción de Cambio	Crítico
29/072024	Documento inicial, primera revisión	Alejandro Castro Pablo Zalazar

6.0 Documentos relacionados

Publicación 140-2 del Estándar Federal de Procesamiento de Información (FIPS) del NIST

Publicación 198-1 del Estándar Federal de Procesamiento de Información (FIPS) del NIST

Publicación 180-4 del Estándar Federal de Procesamiento de Información (FIPS) del NIST

Publicación especial del NIST 800-107, revisión 1, recomendación para aplicaciones que utilizan algoritmos hash aprobados

APÉNDICE A

Los algoritmos **Secure Hash Algorithms (SHA)** son una familia de funciones hash criptográficas diseñadas por el **National Institute of Standards and Technology (NIST)** para proporcionar integridad y autenticidad en la transmisión y almacenamiento de datos. Estas funciones generan un valor hash fijo a partir de datos de entrada, actuando como una "huella digital" del mensaje o documento.

Principales Algoritmos SHA:

1. **SHA-1:** Genera un hash de 160 bits. Fue ampliamente utilizado en aplicaciones de seguridad como SSL/TLS, firmas digitales y certificados digitales.
2. **SHA-224, SHA-256, SHA-384 y SHA-512:** Forman parte de la familia SHA-2, con hashes de 224, 256, 384 y 512 bits, respectivamente. Estos algoritmos mejoran la seguridad frente a colisiones y ataques de preimagen.

Deprecación de SHA-1 por NIST:

SHA-1 fue desarrollado en 1993 como parte de la primera generación de algoritmos de hash seguro. Aunque inicialmente fue seguro, con el tiempo se descubrieron vulnerabilidades criptográficas significativas que lo hicieron susceptible a ataques de colisión.

Deprecación de SHA-1:

- **Fecha de deprecación:** En 2011, NIST declaró que **SHA-1** debía ser reemplazado por SHA-2 para todas las aplicaciones nuevas y que su uso debía ser descontinuado gradualmente. A partir de **2017**, NIST retiró formalmente el soporte para SHA-1 en la mayoría de las aplicaciones.
- **Fecha de retiro**: NIST anuncia el retiro de SHA-1 y recomienda que se migre a SHA-2 o SHA-3 tan pronto como sea posible. La fecha límite es el 31 de diciembre, 2030.

Tipo de HASH	Longitud del HASH	Características	Casos de Uso
MD5	128 bits	• Rápido.	• Comprobación de integridad de archivos (no recomendado para seguridad).
		• Vulnerable a colisiones y ataques de preimagen.	
SHA-1	160 bits	• Mayor longitud que MD5.	• Firmas digitales (obsoleto).
		• Vulnerable a colisiones.	• Certificados SSL/TLS (descontinuado).
SHA-224	224 bits	• Parte de la familia SHA-2.	• Usado en sistemas con limitaciones de almacenamiento.
		• Menor tamaño que SHA-256, pero similar en seguridad.	• Certificados digitales.
SHA-256	256 bits	• Alta seguridad.	• Firmas digitales.
		• Amplio uso en criptografía moderna.	• Certificados SSL/TLS.
			• Criptomonedas como Bitcoin.
SHA-384	384 bits	• Mayor seguridad debido a la longitud del hash.	• Usado en sistemas que requieren alta seguridad.
		• Parte de SHA-2.	• Protección de datos críticos.
SHA-512	512 bits	• Máxima seguridad en la familia SHA-2.	• Certificados digitales.
		• Adecuado para datos altamente sensibles.	• Seguridad en comunicaciones críticas.
			• Protección de grandes volúmenes de datos.

SHA-3	Variable (224, 256, 384, 512 bits)	• Diferente diseño a SHA-2. • Alta resistencia a ataques avanzados.	• Aplicaciones que requieren resistencia cuántica. • Reemplazo potencial para SHA-2 en el futuro.

Algoritmo	Longitud mínima de clave	Caso de uso
AES	128	Cifrado de datos
RSA	2048	Firmas digitales Cifrado de clave pública
ECDSA	256	Firma digital Cifrado de clave pública
sha	256	hash
HMAC SHA 1	112	Código de autenticación de mensaje hash con clave