CENTRO NACIONAL DE SEGURIDAD DIGITAL

Política de uso de técnicas criptográficas

Versión 1.0

APROBACIONES

Elaborado por:	Revisado por:	Aprobado por:
<Nombre>	<Nombre>	<Nombre>
<Cargo>	<Cargo>	<Cargo>
<Firma>	<Firma>	<Firma>

HISTORIAL DE REVISIONES

Versión	Fecha	Revisión
1.0	Diciembre 2021	Versión Inicial

Contenido

1. INTRODUCCIÓN 5

1.1 AUTORIDAD 5
1.2 PROPÓSITO 5
1.3 ALCANCE 5

2. POLÍTICA 6

3. CUMPLIMIENTO DE POLÍTICAS 7

1. Introducción

1.1 Autoridad

El Centro Nacional de Seguridad Digital fue creado el 9 de enero del 2020, mediante Decreto de Urgencia N° 007-2020, es el encargado de gestionar, dirigir, articular y supervisar la operación, educación, promoción, colaboración y cooperación de la Seguridad Digital a nivel nacional como componente integrante de la seguridad nacional, a fin de fortalecer la confianza digital. También es responsable de identificar, proteger, detectar, responder, recuperar y recopilar información sobre incidentes de seguridad digital en el ámbito nacional para gestionarlos.

El Centro Nacional de Seguridad Digital se encuentra a cargo de la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital.

1.2 Propósito

El propósito de esta política es asegurar el uso efectivo de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.

1.3 Alcance

Esta política se aplica a todos los empleados y afiliados de la organización.

2. Política

2.1 Se deben tomar las medidas técnicas y organizativas adecuadas contra procesamiento no autorizado o ilegal de datos personales y contra pérdida accidental o destrucción o daño de datos personales

2.2 Los datos deben estar protegidos física o técnicamente cuando los datos se mantienen dentro de un centro de datos, se recomiendan que estén cifrados.

2.3 Cuando los datos se guardan en la estación de trabajo o servidor fuera de una computadora deben estar físicamente asegurada el área y los datos o el disco deberá estar cifrado.

2.4 Cuando los datos están en posesión de un proveedor, deben estar cifrados.

2.5 Mientras se transfieren datos de un dispositivo a otro, a través de una red, ya sea a través de Internet o mediante una conexión inalámbrica, los datos deben estar cifrados.

2.6 Se debe utilizar al menos WPA3 con protocolo de seguridad para conexiones inalámbricas.

2.7 Se deben utilizar el protocolo https para todas las pagina internas y externas de la organización.

2.8 Cuando los datos se transfieren en medios extraíbles, los medios deben estar cifrados. La clave de descifrado debe pasarse al destinatario por separado.

2.9 Cuando las aplicaciones o bases de datos se alojan fuera del centro de datos deben estar cifradas.

2.10 Para el descifrado se debe tener una contraseña compleja de al menos 20 caracteres.

2.11 Todas las computadoras portátiles y tabletas deben estar cifradas.

2.12 Los dispositivos con Windows 10 deben estar cifrados.

2.13 Se debería crear una autoridad de certificación (CA) interna que solo permita dispositivos conocidos para acceder a los sistemas.

2.14 Los servicios de acceso a Internet deben admitir conexiones cifradas al tener un certificado firmado Secure Socket Layer (SSL) aprobado.

2.15 Cuando se accede a los servicios a través de un túnel VPN, el túnel debe estar cifrado.

2.16 La generación de claves no debe ser predecible y generada al azar.

2.17 El acceso a los códigos clave debe estar restringido a las personas clave.

2.18 Solo se deben usar algoritmos criptográficos confiables y verificados.

2.19 Asegúrese de que la longitud de las claves sea proporcional a la información que se protege.

3. Cumplimiento de políticas

3.1.1 Medición de cumplimiento

Se verificará el cumplimiento de esta política a través de varios métodos, incluidos, entre otros, recorridos periódicos, monitoreo de video, informes de herramientas comerciales, auditorías internas y externas y comentarios al propietario de la póliza.

3.1.2 Excepciones

Cualquier excepción a la política debe ser aprobada con anticipación.

3.1.3 Incumplimiento

Un empleado que haya violado esta política puede estar sujeto a medidas disciplinarias.