Escuela Politécnica Nacional

Dirección de Gestión de la Información y Procesos

CENTRO DE RESPUESTA A INCIDENTES DE SEGURIDAD (CSIRT-EPN)

EPN-DGIP-CSIRT-09-DI

DIRECTRIZ DE CIFRADO ACEPTABLE DE LA EPN

Elaborado por:	Dirección de Gestión de la Información y Procesos	Ing. Liliana Córdova	Firmado electrónicamente por: LILIANA DE LOURDES CORDOVA RAMOS
Revisado por:		Ing. Javier Erazo	Firmado electrónicamente por: JAVIER ERNESTO ERAZO HIDALGO
		Ing. Daniela Córdova	Firmado electrónicamente por: MARIA DANIELA CORDOVA PINTADO
	Director CEC	Dr. Oswaldo Viteri	Firmado electrónicamente por: HECTOR OSWALDO VITERI SALAZAR
	Director IG-EPN	Dr. Mario Ruiz	Firmado electrónicamente por: MARIO CALIXTO RUIZ ROMERO
Aprobado por:	Director DGIP	Ing. Juan Pablo Ponce	JUAN PABLO PONCE VASQUEZ Firmado digitalmente por JUAN PABLO PONCE VASQUEZ DN: CN=JUAN PABLO PONCE VASQUEZ, SERIALNUMBER=120121161129, OU=ENTIDAD DE CERTIFICACION DE INFORMACION, O=SECURITY DATA S.A. 2, C=EC Razón: Soy el autor de este documento Ubicación: Fecha: 2023.11.22 11:08:51-05'00' Foxit PDF Reader Versión: 2023.2.0

ESCUELA POLITÉCNICA NACIONAL

DIRECTRIZ DE CIFRADO ACEPTABLE

EPN-DGIP-CSIRT-09-DI

HOJA DEL ESTADO DEL DOCUMENTO

TÍTULO DEL DOCUMENTO: Directriz de cifrado aceptable de la EPN

ESTADO DEL DOCUMENTO: En proceso de actualización.

1. QUIEN EDITA	2. QUIEN REVISA	3. FECHA	4. RAZONES DE CAMBIO/QUIEN CAMBIA
Ing. Javier Erazo	CSIRT	27/sep/2018	Cambio a Directriz Inserción Marco Legal
Ing. Liliana Córdova	CSIRT	14/06/2023	Actualización algoritmos de cifrado y longitud de la clave de cifrado.
Ing. Liliana Córdova	CSIRT	15/11/2023	Actualización de algoritmos de cifrado. Revisión algoritmos de cifrado. Revisión marco legal.

ESCUELA POLITÉCNICA NACIONAL

DIRECTRIZ DE CIFRADO ACEPTABLE

1. OBJETO

Normar el uso de cifrado de información y de contraseñas en los servicios de la Escuela Politécnica Nacional (EPN) para la protección de datos.

2. ALCANCE

Debe ser aplicada por todos los usuarios de las dependencias de la EPN que gestionan información confidencial.

3. RESPONSABILIDAD Y AUTORIDAD

El responsable de elaborar esta directriz es:	**Personal del Centro de Respuesta a Incidentes de Seguridad Informática de la EPN–CSIRT-EPN**
El responsable de revisar esta directriz es:	**Personal de la Dirección de Gestión de la Información y Procesos – DGIP** **Instituto Geofísico – IG-EPN** **Centro de Educación Continua – CEC**
El responsable de aprobar esta directriz es:	**Rector o Rectora**
Los responsables para hacer cumplir esta directriz son:	**Director de la DGIP** **Autoridades Académicas y Administrativas de la EPN.** **Autoridades de las unidades desconcentradas**
Los responsables de cumplir esta directriz son:	**Administradores de sistemas, administradores de bases de datos, personal académico, personal de apoyo académico, servidores, trabajadores y estudiantes de la EPN**

4. MARCO LEGAL

Ítem	Norma	Fecha	Título de la Norma	Artículos
1	Constitución de la República	2008	Sección tercera Comunicación e Información	Art. 66 numeral 19
2	Ley orgánica de transparencia y acceso a la información pública	2004	Principio de publicidad de la información pública. Información confidencial Difusión de la información pública	Art. 1 Art. 2 Art. 6 Art. 7
3	Ley de comercio electrónico, firmas electrónicas y mensajes de datos (LCE)	2002	Confidencialidad y reserva Protección de datos	Art. 5 Art. 9 Art. 21
4	Ley de protección de datos personales	Mayo, 2021	Términos y definiciones, dato personal, consentimiento, dato genético. Datos sensibles Capítulo II Principios, literal j) Seguridad de datos personales	Art. 4 Art. 10
5	Estatuto de la Escuela Politécnica Nacional	Codificado octubre, 2019	Funciones del Rector Funciones y atribuciones del Vicerrector de Docencia Funciones y atribuciones del Vicerrector de Investigación, Innovación y Vinculación.	Art. 42 Art. 45 Art. 47
6	Política de uso de la información, activos de información institucional y seguridad informática	2021	Definiciones, Protección de datos Respaldos de información Control de acceso Información confidencial	Numeral. 4 Numeral 6 Numeral 10 Numeral 14

Tabla 1. Base legal aplicable a la presente directriz

5. DEFINICIONES

- **AES (Advanced Encryption Standard):** Algoritmo de cifrado simétrico estándar. [1]
- **Anonimizar:** Expresar un dato relativo a entidades o personas, eliminando la referencia a su identidad. [2]
- **Comunidad politécnica:** Son todas las autoridades, miembros del personal académico, personal de apoyo académico, servidores, trabajadores y estudiantes de la EPN. [3]
- **Confidencialidad:** Propiedad que implica que la información no está disponible o no es divulgada a personas, entidades o procesos no autorizados [4].
- **ChaCha20**: Algoritmo de cifrado de flujo. Utilizado en aplicaciones de cifrado en línea y para cifrar datos en bases de datos.
- **Dato personal**: Dato que identifica o hace identificable a una persona natural, directa o indirectamente. [5]
- **Diffie-Hellman (DH):** Protocolo, cuyo algoritmo permite el intercambio de claves compartidas en comunicaciones seguras. [1]
- **ECC (Elliptic Curve Cryptography):** Sistema de cifrado asimétrico basado en curvas elípticas. Proporciona un nivel de seguridad similar al de (Rivest-Shamir-Adleman) RSA pero con claves más cortas. [1]
- **Elliptic Curve Diffie-Hellman (ECDH):** Variante del protocolo Diffie-Hellman que utiliza criptografía de curva elíptica para el intercambio de claves. [1]
- **Encrypt: Cifrado. -** Transformación criptográfica de datos (denominada "texto sin formato") en una forma diferente (llamada "texto cifrado") que oculta el significado original de los datos y evita que la forma original de estos sea usada. El proceso inverso correspondiente es el “descifrado", que representa una transformación que restaura los datos cifrados a su forma original. [1]
- **Información pública:** es la información que ha sido declarada de conocimiento público por alguien con la autoridad para hacerlo y que se puede distribuir libremente a cualquiera sin ningún posible daño a los intereses y propiedad intelectual de la Escuela Politécnica Nacional.
- **Información confidencial**: *“Se considera información confidencial aquella información pública personal que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales, especialmente aquellos señalados en los artículos 23 y 24 de la Constitución de la República.”* [6]

  La información que afecte a la intimidad de la persona o cuyo uso indebido genere discriminación, revele su origen étnico, su vida afectiva y familiar, creencias religiosas, filiación o pensamiento político, condición migratoria, su vida sexual o

reproductiva, su orientación sexual, identidad de género, datos biométricos, cuyo uso público atente contra los derechos humanos consagrados en la Constitución de la República e Instrumentos Internacionales, se considera información confidencial.

- **Internet Key Exchange (IKE):** Protocolo utilizado para establecer y negociar parámetros de seguridad en conexiones VPN (Virtual Private Network). IKE se basa en varios algoritmos criptográficos, incluido Diffie-Hellman, para establecer claves compartidas de manera segura. [1]
- **Protección de datos:** "*El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información, requerirán la autorización del titular o el mandato de la ley*." [7]
- **RSA (Rivest-Shamir-Adleman**): Algoritmo de cifrado asimétrico para ocultar fuentes, utilizado para el intercambio de claves y la firma digital. [1]

6. DIRECTRICES

6.1. Algoritmos permitidos

AES, RSA, Twofish ,Serpent y Elliptic Curve Cryptography (ECC), deben ser usados como base para las tecnologías de cifrado. Adicionalmente también se recomienda el uso de ChaCha20.

6.2. Longitud de clave de algoritmos

La longitud de la clave de un sistema de cifrado simétrico se procurará que sea de al menos 512 bits.

Las claves de los sistemas de cifrado asimétricos deben ser de una longitud que proporcione una firmeza equivalente a la del cifrado simétrico.

Los requerimientos de la longitud de la clave de la Escuela Politécnica Nacional serán revisados periódicamente y actualizados como la tecnología lo permita.

6.3. Autenticación y acuerdo de clave

Para el intercambio de claves se deben usar los siguientes protocolos criptográficos: Diffie-Hellman, IKE, o Elliptic curve Diffie-HeIIman (ECDH).

6.4. Generación de claves

Las claves criptográficas deben generarse y almacenarse de manera segura, para evitar pérdida, robo o que sean comprometidas.

6.5. Monitoreo del uso

El CSIRT-EPN podrá realizar revisiones a las diferentes áreas de la DGIP, administradores de sistemas de información y personal que gestiona información confidencial para verificar que se utilizan algoritmos de cifrado para guardar la confidencialidad y proteger la información institucional.

El uso de los algoritmos de cifrado no autorizados por la DGIP se encuentra prohibido, a menos que sea revisado por expertos calificados o sea incluido en la directriz.

7. CUMPLIMIENTO

En caso de infringir esta directriz, los órganos competentes de la Escuela Politécnica Nacional, aplicarán las sanciones disciplinarias correspondientes de conformidad al artículo 207 de la Ley Orgánica de Educación Superior, artículo 43 de la Ley Orgánica del Servicio Público, artículo 80 del Reglamento a la Ley Orgánica del Servicio Público, artículo 46 del Código del Trabajo conjuntamente con el Reglamento Interno de Administración del Talento Humano, el Reglamento Interno de Trabajo de la Escuela Politécnica Nacional y su Estatuto, además de lo indicado en el numeral 6.2 de la Directriz general cumplimiento de regulaciones de seguridad de la información e infracciones, aplicable para autoridades, personal académico, personal de apoyo académico, servidores, trabajadores y estudiantes.

8. REFERENCIAS

[1] IETF RFC 4949 Ver 2. Internet Security Glossary, páginas 251, 119, 102, 117, 251 y 256, https://www.rfc-editor.org/rfc/pdfrfc/rfc4949.txt.pdf
[2] https://dle.rae.es/anonimizar.
[3] Política de uso de la información, activos de información institucional y seguridad informática, Definiciones.
[4] NTE INEN-ISO/IEC 27000:2012, página; 2 y 3, sección 2, Términos y definiciones.
[5] Ley Orgánica de Protección de Datos Personales, Art. 4 Términos y definiciones.
[6] Ley Orgánica de acceso y Transparencia a la información Pública, Art. 6.
[7] Constitución de la República., Art. 66 numeral 19.