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	
Revisado por:		Ing. Javier Erazo	
Aprobado por:	Director DGIP	Ing. Roberto Andrade, MSc.	

Centro de Respuesta a Incidentes Informáticos
CSIRT EPN

EPN-DGIP-CSIRT-09-DI

HOJA DEL ESTADO DEL DOCUMENTO

TÍTULO DEL DOCUMENTO: Directriz de Cifrado Aceptable de la EPN. **ESTADO DEL DOCUMENTO:** Aprobada			
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

1. OBJETO

Brindar una orientación a los usuarios responsables de gestionar información institucional, para el uso del cifrado con algoritmos que han obtenido un reconocimiento público y que han demostrado que trabajan eficazmente; y aseguran el cumplimiento de regulaciones internacionales.

2. ALCANCE

Aplica a todas las dependencias y a todos los funcionarios de la Escuela Politécnica Nacional, para cifrar información identificada como sensible o crítica

3. RESPONSABILIDAD Y AUTORIDAD

El responsable de elaborar esta directriz es:

Centro de Respuesta a Incidentes de Seguridad – CSIRT-EPN

El responsable de revisar esta directriz es:

Centro de Respuesta a Incidentes de Seguridad – CSIRT-EPN

El responsable de aprobar esta directriz es:

Director de la DGIP

Los responsables para hacer cumplir esta directriz son:

Autoridades de las Unidades Académicas y Administrativas de la EPN

Los responsables de cumplir esta directriz son:

Personal de la Institución desarrolladores de software y/o administradores de sistemas, administradores de bases de datos.

4. MARCO LEGAL

Ítem	Norma	Fecha	Título de la Norma	Artículos
1	Normas de Control Interno de la Contraloría General del Estado	2014	410-12 Administración de soporte de tecnología de información	1
2	Instructivo General de Seguridad y uso adecuado de las tecnologías de la información y comunicación de la EPN	2013	Del ámbito de uso de los activos de información	2
3	Instructivo General de Seguridad y uso adecuado de las tecnologías de la información y comunicación de la EPN	2013	Del ámbito de la seguridad de los activos de información. Confidencialidad de la información y uso de credenciales de acceso a los activos de información institucionales	9
4	Directrices de clasificación y acceso a la información	2016	Directriz, Antecedentes	1-11

Tabla 1. Base legal

5. DEFINICIONES

Propietario de la información: Responsable de las diferentes Unidades Académicas y Administrativas de la EPN, quien decide sobre el uso y acceso a cada uno de los activos de la información, que utilizan para el soporte de sus procesos en el ámbito de sus competencias.

Usuarios de la información (usuarios internos): Se considera usuario de la información a todo miembro de la Comunidad Politécnica, que haga uso de los sistemas y de la información, bajo un acceso con usuario y contraseña asignado por la Institución, con el objeto de cumplir sus actividades.

Información crítica: Es indispensable para la operación de la Institución.

Información sensible: Debe de ser conocida por las personas autorizadas.

6. DIRECTRICES

Art. 1.- Algoritmos permitidos

Algoritmos que han mostrado un trabajo eficaz como AES, RSA, Twofish, Serpent y Elliptic Curve Cryptography (ECC), deben ser usados como base para las tecnologías de cifrado.

Art. 2.- Longitud de clave de algoritmos

La longitud de la clave de un sistema de cifrado simétrico debe ser de por lo menos 128 bits.

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

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

Art. 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-Hellman (ECDH).

Art. 4.- Generación de claves

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

Art. 5.- Monitoreo del uso

El área de Seguridad de la Información realiza revisiones periódicas a las áreas de desarrollo de software y administradores de sistemas de información para verificar que se utilizan algoritmos de cifrado para 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 y sea aprobado por la Dirección de Gestión de la Información y Procesos.

7. CUMPLIMIENTO

En caso de infringir esta directriz, los órganos competentes de la Escuela Politécnica Nacional, aplicarán las sanciones disciplinarias correspondientes de conformidad al Art. 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 y el Estatuto de la Escuela Politécnica Nacional aplicables para el personal académico, servidores, trabajadores y estudiantes.