EPN-DGIP-CSIRT-18-DI

DIRECTRIZ PARA REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN

Elaborado por:	Dirección de Gestión de la Información y Procesos	Ing. Javier Erazo	JAVIER ERNESTO ERAZO HIDALGO Firmado digitalmente por JAVIER ERNESTO ERAZO HIDALGO Fecha: 2020.10.28 15:31:43 -05'00'
Revisado por:		Ing. Juan Carlos Proaño	JUAN CARLOS PROANO CARGUA Digitally signed by JUAN CARLOS PROANO CARGUA DN: c=EC, o=BANCO CENTRAL DEL ECUADOR, ou=ENTIDAD DE CERTIFICACION DE INFORMACION-ECIBCE, l=QUITO, serialNumber=0000429540, cn=JUAN CARLOS PROANO CARGUA Date: 2020.10.28 20:11:29 -05'00'
		Ing. Liliana Córdova	LILIANA DE LOURDES CORDOVA RAMOS Firmado digitalmente por LILIANA DE LOURDES CORDOVA RAMOS Fecha: 2020.11.13 09:05:12 -05'00'
Revisado por	Director DGIP	Ing. Juan Pablo Ponce	Firmado electrónicamente por: JUAN PABLO PONCE

EPN-DGIP-CSIRT-18-DI

HOJA DEL ESTADO DEL DOCUMENTO

TÍTULO DEL DOCUMENTO: Directriz para revisión independiente de la Seguridad de la Información **ESTADO DEL DOCUMENTO:** Por aprobar			
1. QUIEN EDITA	**2. QUIEN REVISA**	**3. FECHA**	**4. RAZONES DE CAMBIO/QUIEN CAMBIA**

1. OBJETO

Describir los lineamientos que regirán la revisión independiente de la seguridad de la información, que debe ser realizado en cuanto a la gestión de la seguridad de la información y su implementación en la institución, para asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos de la organización.

2. ALCANCE

Aplica para todos los objetivos de control, controles, políticas, directrices, procesos y procedimientos de seguridad de información que la institución mantiene vigente.

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 Gestión de la Información y Procesos – DGIP**
Los responsables para hacer cumplir esta directriz son:	**Autoridades de las Unidades Académicas y Administrativas de la EPN, y autoridades de las unidades desconcentradas**
Los responsables de cumplir esta directriz son:	**Personal académico, personal de apoyo académico, servidores y trabajadores de la EPN**

4. MARCO LEGAL

Ítem	Norma	Fecha	Título de la Norma	Artículos
1	NTC-ISO-IEC 27001:2013	2013	Tecnología de la Información – Técnicas de Seguridad – Sistemas de Gestión de la Seguridad de la Información – Requisitos.	Anexo A A.18.2 Revisión de seguridad de la información A.18.2.1. Revisión independiente de la seguridad de la información
2	Ley Orgánica de Educación Superior	2010, última reforma 2020	Título décimo primero, De las Faltas y Sanciones	207

Ítem	Norma	Fecha	Título de la Norma	Artículos
3	Ley Orgánica de Servicio Público, LOSEP	2010, última reforma 2019	Titulo tercero capítulo cuarto, del régimen disciplinario	43
4	Reglamento General a la Ley Orgánica de Servicio Público	2011, última reforma 2019	Título segundo capítulo quinto, sección segunda De las sanciones	80-89
5	Normas de Control Interno de la Contraloría General del Estado	2009, última reforma 2019	410 Tecnología de la Información	Norma 410-10 Seguridad de Tecnología de Información
6	Estatuto Escuela Politécnica Nacional	2013, última reforma octubre 2019	Título V de la Disciplina y Sanciones	94 - 99
7	Reglamento Interno de Trabajo Escuela Politécnica Nacional	2015	Capítulo VIII del Régimen Disciplinario	51 - 57
8	Reglamento Interno de Administración del Talento Humano de la Escuela Politécnica Nacional	2018	Capítulo XI Régimen Disciplinario Capítulo XII De la Competencia, procedimiento y recursos	59 – 71 72 – 73
9	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.	13, incisos 1, 8

Tabla 1. Base legal

5. DEFINICIONES

CSIRT-EPN: Centro de Respuesta a Incidentes de Seguridad Informática de la Escuela Politécnica Nacional.

Unidades: Segmento de la organización de la EPN académico, administrativo, de investigación y/o vinculación, se incluye al CEC y al Geofísico.

Control: medios de gestión del riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas de gestión o de naturaleza jurídica [1].

Objetivo de control: declaración que describe qué se espera lograr como resultado de implementar controles [1].

6. DIRECTRIZ

6.1. Disposiciones generales

El CSIRT-EPN, realiza revisiones periódicas de seguridad, con el objetivo de verificar que se están cumpliendo las políticas, directrices, procesos y procedimientos, que se encuentran implementados y vigentes en la institución.

"Los directores deben revisar con regularidad el cumplimiento del procesamiento de la información y procedimientos dentro de su área de responsabilidad, con las políticas y normas de seguridad de la información [2]".

Las revisiones de seguridad se realizarán a intervalos planificados o cuando existan cambios significativos en la normativa de seguridad interna.

6.2. Normas

6.2.1. De la revisión independiente

El CSIRT-EPN, remitirá a la autoridad respectiva de la unidad administrativa o académica de investigación y/o vinculación de la institución:

- La normativa de seguridad (políticas, directrices, procesos o procedimientos) vigente, que serán objeto de la revisión.
- El cronograma y metodología de trabajo a utilizar durante la revisión.

6.2.2. Resultados de la revisión

Los resultados y recomendaciones de la revisión serán remitidos a la autoridad respectiva de la unidad administrativa o académica de investigación y/o vinculación de la institución.

La autoridad respectiva de la unidad administrativa o académica de investigación y/o vinculación de la institución, remitirá al CSIRT-EPN el cronograma para la aplicación de las medidas correctivas que sean necesarias.

El CSIRT-EPN, una vez cumplido los tiempos establecidos en el cronograma y de acuerdo a la criticidad de las recomendaciones realizadas, ejecutará una segunda revisión a la normativa de seguridad, a fin de verificar que se ha implementado las medidas correctivas necesarias.

6.2.3. Metas de la revisión

Proteger la privacidad: Adecuado uso de la información personal.

Enfoque basado en el riesgo: La metodología de la revisión tiene el enfoque basado en el riesgo, donde la EPN asigna los recursos para proteger la información institucional y los recursos de TI en función de las amenazas y su probabilidad de causar un resultado adverso, la revisión de seguridad considera este enfoque.

Mantener la confidencialidad: Revisar si el manejo de la información asegura de que no se divulgue de formas incompatibles con el uso autorizado y su propósito original.

Proteger la integridad: Revisión para asegurar que la información esté protegida contra la modificación o destrucción indebida de la información, revisar si la información es auténtica.

Asegurar la disponibilidad: Revisar que existe una adecuada gestión de la información y los recursos de TI, para garantizar que sean accesibles y puedan satisfacer las necesidades operativas.

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 59 del Reglamento Interno de Administración del Talento Humano de la Escuela Politécnica Nacional, artículo 46 del Código del Trabajo conjuntamente con el Reglamento Interno de Trabajo de la Escuela Politécnica Nacional y su Estatuto aplicables para el personal académico, personal de apoyo académico, servidores, trabajadores y estudiantes.

8. REFERENCIAS

[1] NTE INEN-ISO/IEC 27000.
[2] NTE INEN-ISO/IEC 27001.