Escuela Politécnica Nacional

Dirección de Gestión de la Información y Procesos

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

DIRECTRIZ DE MONITOREO AUTORIZADO DE LA EPN

Elaborado por:	Dirección de Gestión de la Información y Procesos	Ing. Liliana Córdova	
Revisado por:		Ing. Javier Erazo	JAVIER ERNESTO ERAZO HIDALGO Firmado digitalmente por JAVIER ERNESTO ERAZO HIDALGO Fecha: 2019.11.19 13:54:58 -05'00'
		Ing. Edison Jiménez	EDISON PATRICIO JIMENEZ RIVERA Firmado digitalmente por EDISON PATRICIO JIMENEZ RIVERA Fecha: 2019.11.25 10:14:56 -05'00'
Aprobado por:	Director DGIP	Ing. Juan Pablo Ponce	

EPN-DGIP-CSIRT-08-DI

HOJA DEL ESTADO DEL DOCUMENTO

TÍTULO DEL DOCUMENTO: Directriz de monitoreo autorizado de la EPN. **ESTADO DEL DOCUMENTO:** Para aprobación			
1. QUIEN EDITA	**2. QUIEN REVISA**	**3. FECHA**	**4. RAZONES DE CAMBIO/QUIEN CAMBIA**
Ing. Javier Erazo	DGIP	11/marzo/2019	Creación del documento
Ing. Liliana Córdova	DGIP	12/noviembre/2019	IG-EPN-CEC

1. OBJETO

Establecer lineamientos necesarios para registrar eventos (logs) y generar evidencia, como parte de una supervisión adecuada en la Escuela Politécnica Nacional – EPN.

2. ALCANCE

Aplica a todo el personal de la Institución, que tengan a su cargo la gestión de activos de información institucionales.

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 que gestionan activos de información institucional.

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. Auditoria y evaluación de vulnerabilidades.	2 13
3	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.

NTP (Network Time Protocol): Protocolo de red para la sincronización de reloj entre sistemas informáticos a través de redes de datos de latencia variable por conmutación de paquetes.

Logs: Bitácoras y registros almacenados secuencial en un archivo o base de datos de todos los eventos o acciones que afectan a un proceso particular (aplicación, actividad de una red informática, etc.).

Necesidad de conocer: Principio de seguridad por el que, para que una persona pueda acceder a una determinada información clasificada, es necesario que ésta sea precisa para poder desarrollar su trabajo, no siendo suficiente su puesto o rango. [CESID:1997]

Miembro asociado: Son aquellos miembros de la Red de Confianza y Grupos de Seguridad que mantienen un Acuerdo de Cooperación con el CSIRT-EPN.

Activos de información críticos: Activos de información institucionales que son vitales para que la EPN cumpla con su misión, visión y cuya pérdida de confidencialidad, integridad y disponibilidad afectan la operación de la Institución.

Vulnerabilidades: Puntos débiles del Software o Hardware que permiten que un atacante comprometa la integridad, disponibilidad o confidencialidad del mismo. Algunas de las vulnerabilidades más severas permiten que los atacantes ejecuten código arbitrario, denominadas vulnerabilidades de seguridad, en un sistema comprometido.

Parche: es un cambio que se aplica a un programa, con la finalidad de corregir errores.

Actualización de seguridad: Una corrección ampliamente extendida para una vulnerabilidad específica del producto, relacionada con la seguridad.

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

6. DIRECTRICES

Art 1.- Registro y seguimiento

Los registros y las supervisiones adecuadas son prácticas necesarias para seguimiento de eventos y generación de evidencia.

Art 2.- Registro de eventos

Las unidades deben cumplir con el registro de eventos (logs) de recursos de TI, al almacenar, procesar o transmitir información institucional.

Las unidades deben obtener la aprobación para borrar, purgar o recortar los registros de eventos (logs) a través del proceso de gestión de cambios.

Art 3.- Protección de la información de registro (logs)

Las unidades deben proteger los registros (logs) de acuerdo con el nivel de protección de la información institucional que contienen y no pueden divulgarlos sin la debida autorización.

Las unidades deben conservar los registros de acuerdo con las obligaciones externas, los contratos, los reglamentos, las retenciones de litigios o las órdenes de conservación.

Para liberar la información que contiene logs institucionales que se capturan por medio del monitoreo, se debe contar con la autorización de la máxima autoridad o por litigio con orden judicial.

Art. 4.- Administración de logs

El CSIRT-EPN como parte de una gestión de Auditoría de seguridad, podrá revisar las cuentas privilegiadas para garantizar que:

- Sólo se produjo la actividad autorizada.
- Las anomalías sean analizadas y las acciones correctivas sean implementadas.

Las unidades deben limitar el acceso a los registros administrativos utilizando el principio de necesidad de conocer.

Art 5.- Sincronización de reloj

Las unidades de la Institución deben sincronizar los relojes de los recursos de TI dentro de la organización con base al estándar de tiempo establecido en el servidor NTP institucional.

Art 6.- Control del software operativo

Las unidades deben obtener la aprobación requerida dentro del proceso de gestión de cambios, para la instalación de software, cambios de configuración y actualizaciones de los sistemas en producción.

Art 7.- Administración de vulnerabilidades técnicas y administración de actualizaciones (parches).

En activos con información crítica, la frecuencia de revisión de actualizaciones (parches) no debe exceder los 90 días. Cuando las vulnerabilidades son críticas y anunciadas por el CSIRT-EPN, el actualizar parches es obligatorio.

Las unidades deben proteger los recursos de TI, que no se pueden aplicar a los estándares actuales con controles compensatorios aprobados, a través del proceso de excepción o eliminar el recurso de TI del acceso a la red.

Las unidades deben garantizar y coordinar con el CSIRT-EPN las siguientes actividades:

- Evaluar las vulnerabilidades sobre los activos institucionales con herramientas de gestión del CSIRT-EPN y otras fuentes que incluyen avisos y / o boletines de terceros asociados.
- Realizar análisis de vulnerabilidades de los activos con información críticas con autenticación.
- Tomar las medidas apropiadas para aplicar parches o aplicar otros controles. El CSIRT-EPN podrá coordinar con las unidades, actividades de actualización de parches de equipos de usuario final, en forma automatizada.
- Documentar las acciones tomadas.

Art 8.- Consideraciones para las auditorías de los sistemas de información

Las auditorías, investigaciones, se deben planificar y controlar para minimizar los efectos adversos en los sistemas de producción y los procesos de negocio.

El CSIRT-EPN se asegurará de que las pruebas de auditoría no alteren los registros de auditoría, ni la información institucional de producción y que las actividades de auditoría, no reduzcan los controles de seguridad por debajo de lo que sea apropiado para la Información institucional o de TI.

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.