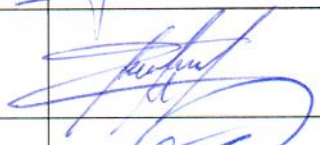
EPN-DGIP-CSIRT-04-PR

PROCEDIMIENTO DE GESTIÓN DE VULNERABILIDADES

ELABORADO	Dirección de Gestión de la Información y Procesos	Ing. Daniela Córdova	
		Ing. David Quinchaguano	
		Ing. Javier Erazo	
REVISADO	Dirección de Gestión de la Información y Procesos	Ing. Juan Carlos Proaño	
		Ing. Pablo Ortiz	
APROBADO	Director DGIP	Ing. Roberto Andrade, MSc.	

Contenido

1. OBJETIVO

Describir las actividades básicas a realizar para la búsqueda y gestión de vulnerabilidades de seguridad en la infraestructura tecnológica y red de datos de la Escuela Politécnica Nacional - EPN.

2. ALCANCE

Este procedimiento se implementa en forma semestral y bajo demanda, a fin de precautelar la información y los activos informáticos de la Institución, durante procesos de paso a producción de nuevos servicios o implementación de nueva arquitectura informática, con el fin de que estos riesgos sean identificados y valorados.

3. MARCO LEGAL

Las Normas de Control Interno Para las Entidades, Organismos del Sector Público indican:

> ***"410-12 ADMINISTRACIÓN DE SOPORTE DE TECNOLOGÍA DE INFORMACIÓN***
>
> *La unidad de tecnología de información definirá, aprobará y difundirá procedimientos de operación que faciliten una adecuada administración del soporte tecnológico y garanticen la seguridad, integridad, confiabilidad y disponibilidad de los recursos y datos, tanto como la oportunidad los servicios tecnológicos."*

De acuerdo al Instructivo General de Seguridad y uso adecuado de las tecnologías de la información y comunicación se tiene que:

> ***"DEL ÁMBITO DE USO DE LOS ACTIVOS DE INFORMACIÓN:***
>
> *Art. 13.- Auditoría y Evaluación de vulnerabilidades:*
>
> *Los auditores internos y/o externos de la Escuela Politécnica Nacional realizarán inspecciones de seguridad del tráfico sin previo aviso, para capturar evidencia de técnicas maliciosas realizadas sobre los activos de información de la EPN.*
> *(...)*
>
> *La EPN, por medio de la DGIP, se reserva el derecho de utilizar, monitorear e investigar el uso inadecuado de sus activos de información, siempre y cuando se tenga evidencia que establezca sospechas acerca del mal uso de la información generada y/o almacenada en éstos.*
>
> *La evidencia admisible que la DGIP puede utilizar debe ser aquella que pueda ser capturada de forma accidental y/o como resultado de actividades de monitoreo o auditoría interna.*
>
> *La DGIP puede iniciar una investigación interna sujeta a directrices y procedimientos, por el mal uso de activos de información, siempre y cuando se establezcan fundamentos basados en la evidencia recolectada, que establezcan que cualquier empleado, trabajador, personal académico, estudiante, haya infringido las normas institucionales, las políticas internas, los reglamentos institucionales, el Estatuto institucional, y/o las leyes de la República del Ecuador.*
>
> *(...)*
>
> *Los que gestionan los activos de información institucional deberán colaborar con los auditores internos, auditores externos, personal de la DGIP, responsables del proceso de evaluación del riesgo."*

4. DEFINICIONES

Seguridad de la información: La preservación de la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio.

Evento de seguridad de la información: Es la ocurrencia detectada en un estado de un sistema, servicio o red que indica una posible violación de la Política de Seguridad de la Información, un fallo de las salvaguardas o una situación desconocida hasta el momento y que puede ser relevante para la seguridad.

Incidente de seguridad de la información: Un único evento o una serie de eventos de seguridad de la información inesperados o no deseados, que tienen una probabilidad significativa de comprometer las operaciones empresariales y de amenazar la seguridad de la información.

Confidencialidad[1]: La propiedad por la que la información no se pone a disposición o se revela a individuos, entidades o procesos no autorizados.

Disponibilidad[2]: La propiedad de ser accesible y utilizable por una entidad autorizada.

Integridad[3]: La propiedad de salvaguardar la exactitud y completitud de los activos.

Áreas involucradas: Son todas las Unidades Académicas y Administrativas de la EPN.

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.

5. RESPONSABILIDAD Y AUTORIDAD

Responsables de elaborar este documento:

Centro de Respuesta a Incidentes Informáticos CSIRT-EPN

Responsables de revisar este documento:

Líder de Redes e Infraestructura, Líder de Operaciones

Responsables de aprobar este documento:

Director de la DGIP

Responsables de aplicar este procedimiento:

Personal de la DGIP

---

[1] (Conforme Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27001:2011)

6. DIRECTRICES

Vulnerabilidad de Seguridad

Todo evento que permite que un atacante comprometa la integridad, disponibilidad o confidencialidad de los sistemas de información e infraestructura tecnológica de la Institución. Se encuentran las debilidades o vulnerabilidad desde los siguientes puntos de vista.

- Vulnerabilidades de software: errores de aplicaciones, errores de sistemas operativos, rutinas de acceso no autorizados, servicios no autorizados, etc.
- Vulnerabilidades de hardware: inapropiada operación, fallas en mantenimiento, inadecuada seguridad física, falta de protección contra desastres naturales, etc.
- Vulnerabilidades de datos: inadecuados controles de acceso a personal no autorizado, etc.
- Vulnerabilidades administrativas: ausencia de políticas de seguridad, ausencia de cultura de seguridad, ausencia de procedimientos, falta de educación y entrenamiento en seguridad, etc.
- Vulnerabilidades de comunicaciones: inadecuados controles de acceso a la red, inadecuados mecanismos para prevenir fallas en comunicaciones, etc.
- Vulnerabilidades de personal (empleados): inadecuados controles de acceso físico, inadecuados controles de acceso lógico.

Valoración del impacto y frecuencia de ocurrencia

Se realiza una revisión de la información que previamente se ha recolectado en eventos anteriores, la frecuencia está registrada en la bitácora de seguridad, logs y reportes de incidentes. El impacto se determina en forma cuantitativa tomando diversos criterios como: por ejemplo, afectación a los sistemas o a los dispositivos, afectación en los usuarios por pérdida del servicio.

Mesa de servicio

En caso que la Mesa de Servicio de TIC de la DGIP reciba una notificación para realizar un análisis de vulnerabilidades, incidente o requerimiento de seguridad, esta deberá asignarlo a la cola de Seguridades DGIP, creada en la herramienta OTRS para su gestión, o reportarlo al personal de la DGIP con funciones de Seguridad de la Información, a la dirección de correo electrónico: gestion.incidentes@epn.edu.ec.

Seguridad de la Información

Todo evento de seguridad de la información es notificado a los funcionario de la DGIP que tienen actividades acerca de Seguridad de la Información, a la dirección de correo electrónico: gestion.incidentes@epn.edu.ec.

El personal de la DGIP, con actividades inmersas en Seguridad de la Información clasifica el evento reportado, de manera que sean gestionados mediante los procedimientos definidos para el efecto.

7. DIAGRAMA GENERAL DE FLUJO DEL PROCEDIMIENTO

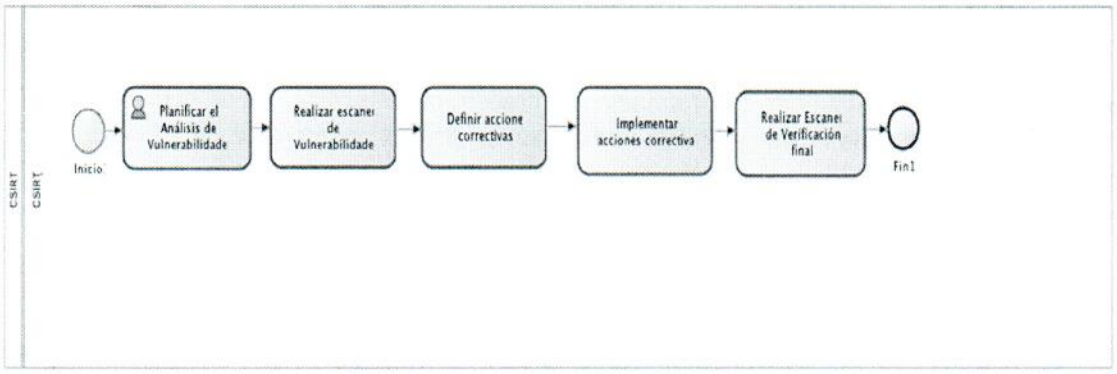


Imagen 1. Diagrama general del flujo del procedimiento

8. DESCRIPCIÓN DEL PROCEDIMIENTO PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Planificar y Preparar el esquema de análisis de vulnerabilidades.
Realizar escaneo y analizar vulnerabilidades.
Definir las acciones a seguir.
Implementar acciones correctivas.
Realizar escaneo de verificación final.

8.1 Planificar y Preparar el esquema de análisis de vulnerabilidades

El personal de la DGIP, con actividades inmersas en Seguridad de la Información realiza una reunión inicial para planificar el análisis de vulnerabilidades semestral, en la que se plantea un esquema y se identifican los elementos a los que se realizará el análisis.

Si el análisis debe realizarse bajo demanda, la reunión inicial es para planificar las acciones a realizarse en torno al pedido realizado.

En esta reunión:

- Definir el alcance del análisis: Definir los activos que van a ser analizados y el alcance del análisis (aplicaciones, sistemas operativos, software y librerías, base de datos, entre otros)

- Definir variables del análisis:
  Posicionamiento: Externo, Interno
  Visibilidad: Blackbox, Graybox y Whitebox
  Perfil Adoptado: Usuario sin privilegios, Usuario con privilegios

- Definir información de vulnerabilidades: Se presenta un ejemplo en la siguiente tabla:

ID	SERVICIO	ACTIVO	LOCALIZACION	TIPO	VULNERABILIDAD/DEBILIDAD	DESCRIPCION	CRITICIDAD	IP/URL AFECTADA	PUERTO	REMEDIACION	TIEMPO PARA CIERRE
#TAA - Activo	SII-EPN	10.10.10.10	UIO	Fallos conocidos en versiones de software	Vulnerabilidad MS15-034	Vulnerabilidad en la pila del protocolo HTTP. Un atacante puede ejecutar código malicioso o causar una denegación del servicio	Alta	10.10.10.10	80 443	Instalar el parche MS15-034	1 semana

Tabla 1. Ejemplo de presentación vulnerabilidades

- Priorizar las vulnerabilidades según grado de afectación
- Definir tiempo de cierre de acuerdo a la prioridad
- Planificar las actividades con cada dueño de los activos: Coordinar con los dueños de los activos la fecha y hora del análisis en base a las acciones que van a ser realizadas y a los requisitos expuestos por los administradores (ventana de mantenimiento, consideraciones especiales para servicios en producción, entre otros).

En caso de análisis con posicionamiento externo, se realiza la notificación a los administradores de los equipos de seguridad perimetral para revisar el correcto funcionamiento de las configuraciones sobre los mismos.

8.2 Realizar escaneo y analizar las vulnerabilidades

- Crear expediente digital
- Realizar Investigación (Control Operativo, Control Administrativo, Control Técnico)
- Elaborar Informe
- Registrar en Bitácora y en base de conocimiento
- Revisar la base de conocimiento

El personal de la DGIP, con actividades inmersas en Seguridad de la Información cuenta con un check list de vulnerabilidades que deben realizarse en cada revisión. De este análisis se obtendrá un informe que evidencia los hallazgos, así como también la valoración de cada uno de los riesgos identificados, con acciones concretas a realizarse.

8.2.1 Crear expediente digital

El área Seguridad de la Información, crea el expediente en el repositorio destinado para el efecto, en el cual se almacena toda la información de los análisis de vulnerabilidades generados.

8.2.2 Investigación

Se realizan al menos las siguientes acciones:

- Control operativo: estos controles hacen referencia a los procedimientos que sirven para asegurar los requerimientos de seguridad. Ejemplo: planes de contingencia, manejo de incidentes, realización de backups, etc.

- Análisis de riesgos
- Separación de deberes
- Identificación del personal clave
- Conocimiento y entrenamiento de personal
- Efectiva administración de usuarios
- Registro de intrusos
- Planes de contingencia
- Controles de acceso físico
- Seguridad física contra incendios

- Control administrativo: estos controles hacen referencia a la recolección de documentos como: políticas y normatividad general referente a la seguridad del sistema
  - Existe una política específica del sistema para el manejo de seguridad.
  - Existen políticas para el manejo de redes, sistemas operativos, aplicaciones, etc.
  - Existen políticas para el manejo de Internet
    - Tipo de información que puede ser transmitida
    - Tipos de sistemas que pueden ser conectados a la red
    - Uso de firewalls y gateways seguros
    - Requerimientos para autenticación de usuarios
  - Existen políticas para el manejo de otras redes externas
  - Existe un ente encargado de dar solución a incidentes de seguridad
  - Las funciones de seguridad están integradas en las funciones del personal

- Control Técnico: estos controles hacen referencia a cualquier dispositivo de hardware o software que aseguran el cumplimiento de los requerimientos de seguridad. Ejemplo: control de acceso y autorización, firewalls, mecanismos de auditoria de eventos, etc.
  - Identificación y autenticación
  - Manejo de llaves
  - Control de acceso lógico
  - Protección a puertos
  - Firewalls, gateways seguros
  - Autenticación basada en hosts
  - Auditoria
  - Detección de intrusos
  - Reconstrucción de eventos
  - Logs, revisión
  - Criptografía
  - Firmas electrónicas
  - Certificados

8.2.3 Registrar en bitácora y en base de conocimientos

El personal de la DGIP, con actividades de Seguridad de la Información registra en la bitácora y las medidas implementadas para su contención en la base de conocimientos.

8.2.4 Elaborar informe

Luego de realizado el análisis de vulnerabilidades semestral o bajo pedido, sl personal de la DGIP, con actividades de Seguridad de la Información emite un informe detallado con todos los hallazgos, riesgos, impacto y sugerencias para mitigar estos riesgos y vulnerabilidades.

8.2.5 Revisar la base de conocimientos

- Revisar la base de conocimientos cuando se genere un nuevo evento de vulnerabilidades.
- Implementar acciones de remediación
- El área de Seguridad de la Información, envía el informe de las vulnerabilidades halladas con el respectivo riesgo que este ocasiona si el mismo no es resuelto.
- Cada dueño de los activos en conjunto con los miembros del área de Seguridad de la Información, definen las acciones y generan un cronograma para la remediación.
- En caso de que existieran vulnerabilidades que no puedan cerrarse dentro de un periodo de tiempo establecido, se firma un acta aceptando los riesgos que esto conlleva y se realiza un nuevo control a los seis meses.

8.3 Definir las acciones a seguir

Una vez realizado el análisis de vulnerabilidades, se definen las acciones a seguir a fin de realizar la remediación de cualquier tipo de vulnerabilidades identificada y calificada, para lo cual se realizarán los siguientes pasos:

- Reunión inicial con el equipo del CSIRT y áreas involucradas.
- Revisión del informe generado
- Asignación de tareas a cada responsable
- Implementación de soluciones propuestas
- Escaneo de verificación de acciones de remediación

8.4 Implementar acciones correctivas

El personal de la DGIP, con actividades de Seguridad de la Información verifica que el equipo de trabajo propuesto para remediar cualquier tipo de vulnerabilidad identificada y valorada, efectivamente aplique la solución y emita el respectivo comunicado de que se ha procedido a solventar los hallazgos.

8.5 Realizar escaneo de verificación final

Finalmente, el personal de la DGIP, con actividades de Seguridad de la Información realiza un nuevo proceso de verificación tanto en los sistemas de Información como en la Infraestructura para verificar que se han solucionado las vulnerabilidades encontradas dentro de la etapa de análisis. Con esto finalmente se cerciora de que la Infraestructura de Información de la Institución se encuentra debidamente protegida.