Escuela Politécnica Nacional

Dirección de Gestión de la Información y Procesos

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

EPN-DGIP-CSIRT-02-PR

PROCEDIMIENTO PARA LA GESTIÓN DE REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA EPN

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

EPN-DGIP-CSIRT-02-PR

Contenido

1. OBJETIVO

Describir las actividades a realizar, para la gestión de requerimientos de seguridad de la información, que se pueden originar durante el uso o acceso a los sistemas, aplicaciones y/o servicios de la Escuela Politécnica Nacional – EPN.

2. ALCANCE

Este procedimiento es implementado para toda la Comunidad Politécnica y usuarios externos relacionados.

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. 2.- Propiedad y uso de los activos de información institucional:*
> *Los activos de información institucionales son: el software, hardware, aplicaciones, sistemas informáticos institucionales y la información generada y/o contenida en éstos, siempre y cuando sean parte del inventario institucional.*
>
> *Es propiedad de la EPN, toda la información contenida en los activos de información institucionales, excluyendo la información personal de los empleados, trabajadores, personal académico y estudiantes.*
>
> *Es responsabilidad de los empleados, trabajadores, personal académico y estudiantes, el uso adecuado de la información generada y/o contenida en los activos de información institucionales.*
>
> *Los activos de información definidos como propiedad de la EPN se utilizarán exclusivamente al servicio de los intereses de la Institución y de sus dependencias.*
>
> *(...)*
>
> *La DGIP notificará a las autoridades institucionales acerca de acciones sospechosas o ilegales que atenten contra la Constitución, leyes de la República, el Estatuto, normas internas y/o la imagen Institucional; y solicitará autorización al rectorado, para acceder a información confidencial y/o personal que se encuentre almacenada en activos de información de propiedad de la EPN y que esté ligada a dichas acciones."*

La Normativa de control de acceso a servicios de TI de la EPN indica:

> **"DIRECTRICES**
> *Art. 1.- De los sistemas de información, aplicaciones, recursos, servicios de procesamiento y redes de comunicaciones de la EPN - Servicios de TI.*
>
> *(...)*

La utilización de todos los servicios de TI, no deberá permitirse para otros fines que no sean los definidos por la Institución."

4. DEFINICIONES

Seguridad de la información[1]: 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[2]: 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[3]: 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.

Requerimiento: Pedido o solicitud que requiere atención o revisión por parte Seguridades de la DGIP

5. RESPONSABILIDAD Y AUTORIDAD

Responsables de elaborar este documento: Seguridades de la Información y Seguridad Informática

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

6. DIRECTRICES

Requerimientos de seguridad de la información

Todo pedido o solicitud que requiere atención o revisión de Seguridades de la DGIP será considerado un requerimiento de seguridad de la información, entre los cuales se pueden considerar y no limitarlos a:

- Revisión de seguridad, previo el paso a producción de nuevo servicio, aplicación.
- Revisión de seguridad, por pedido de entrega de información.
- Generación de acuerdos de confidencialidad.
- Pedido de análisis de vulnerabilidades a un activo de soporte (componente de hardware, software, servicio o aplicación).
- Pedido de análisis de requerimientos de seguridad para ser incluidos en la adquisición o desarrollo de un nuevo servicio o aplicación.

Mesa de Servicio de TIC de la DGIP

En caso que la Mesa de Servicio de TIC de la DGIP reciba una notificación de un evento, incidente o requerimiento de seguridad, esta deberá asignarlo a la cola de Seguridades DGIP, creada en la herramienta

---

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

OTRS para su gestión, y/o reportarlo a Seguridad de la Información, a la dirección de correo electrónico: gestion.incidentes@epn.edu.ec.

Seguridad de la Información

Seguridad de la Información será el único punto de contacto para la notificación de eventos, incidentes o requerimientos de seguridad de la información.

Seguridad de la Información realizará la clasificación de los eventos de seguridad reportados, de manera que sean gestionados mediante los procedimientos definidos para el efecto.

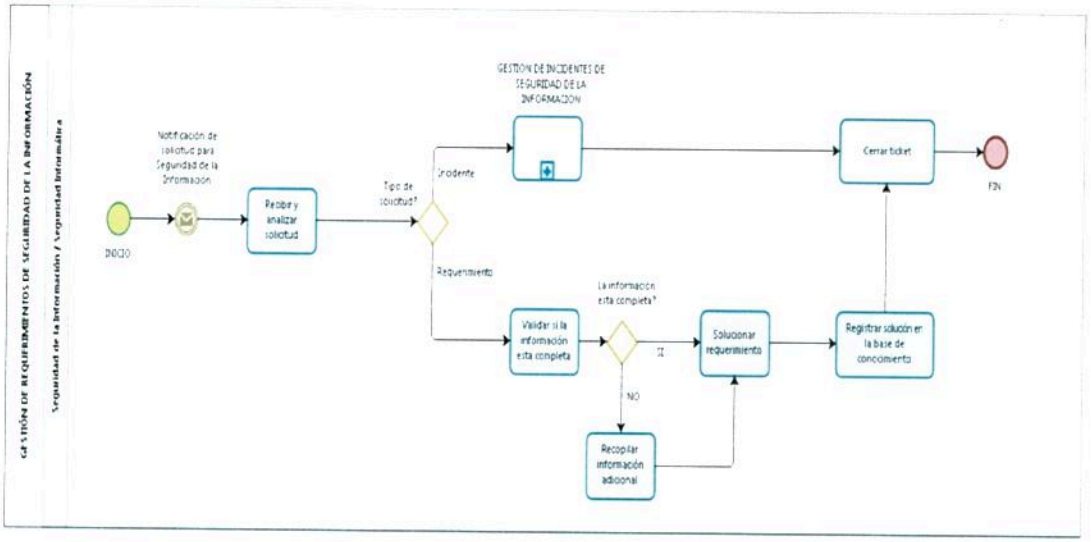
Seguridad Informática

Seguridad Informática gestionará con los administradores de los servicios y aplicaciones de TI, la solución de los requerimientos de seguridad.

Personal DGIP

Todo evento, incidente o requerimiento de seguridad de la información deberá ser notificado a Seguridad de la Información, a la dirección de correo electrónico: gestion.incidentes@epn.edu.ec.

7. DIAGRAMA DE FLUJO DEL PROCEDIMIENTO



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

8.1 Recibir y analizar solicitud

Seguridad de la Información, recibirá y revisará la solicitud, si la solicitud es catalogada como un incidente de seguridad, será gestionado mediante el procedimiento de Gestión de Incidentes de Seguridad de la Información.

8.2 Validar que la información está completa

Si la solicitud es catalogada como un requerimiento, se valida que la información este completa.

8.3 Recopilar información adicional

En el caso de que la información no está completa se recopila la información adicional.

8.4 Solucionar requerimiento

Seguridad de la Información juntamente con Seguridad Informática gestionarán la atención del requerimiento.

8.5 Registrar solución en la base de conocimiento

El responsable del requerimiento registrará la solución del requerimiento en la base de conocimientos.

8.6 Cerrar ticket

El responsable del requerimiento cerrará el ticket asignado con las principales actividades ejecutadas para la solución del mismo.

9. TABLA DE CONTROL DE CAMBIOS

VERSIÓN	ÍTEM	ASPECTO CAMBIADO	RAZONES	PERSONA QUE SOLICITÓ EL CAMBIO