DGIP-CSIRT-006

DIRECTRICES DE SEGURIDAD DE LOS EQUIPOS DE TELECOMUNICACIONES

Elaborado por:	Dirección de Gestión de la Información y Procesos	Ing. David Quinchaguano	
Revisado por:	Dirección de Gestión de la Información y Procesos	Ing. Juan Carlos Proaño, MSc. Ing. Liliana Córdova Msc.	

Aprobado por:	Dirección de Gestión de la Información y Procesos	Ing. Roberto Andrade, MSc.	

HOJA DEL ESTADO DEL DOCUMENTO

TITULO DEL DOCUMENTO: Directrices de seguridad de los equipos de telecomunicaciones			
ESTADO DEL DOCUMENTO: Para aprobación			
1. QUIEN EDITA	**2. QUIEN REVISA**	**3. FECHA**	**4. RAZONES DE CAMBIO/QUIEN CAMBIA**
Ing. David Quinchaguano Duque	Ing. Liliana Córdova, Ing. Juan Carlos Proaño, Ing. Kléber Serrano		Creación documento

1. OBJETO

Este documento describe los requerimientos mínimos de seguridad en la configuración de todos los equipos de telecomunicaciones (Routers, switches, Access points) conectados a la red de la EPN, así como su aseguramiento físico.

2. ALCANCE

Esta directriz cubre todos los equipos de telecomunicaciones que proporcionan una conexión del usuario a la red de datos institucional y el Internet. Los equipos de comunicaciones que conformen las áreas DMZ deben ser configurados de acuerdo a la política de la zona desmilitarizada DMZ de la EPN.

3. RESPONSABILIDAD Y AUTORIDAD

El responsable de elaborar esta directriz es:

Responsable de Seguridad

El responsable de revisar esta directriz es el:

Líder del CSIRT

Líder de Área de Redes e Infraestructura

El responsable de aprobar esta directriz es:

Director de la DGIP

La autoridad para hacer cumplir esta directriz es:

Director de la DGIP
Líder del Área de Redes e Infraestructura

Los responsables de cumplir esta directriz son:

Personal DGIP

4. MARCO LEGAL

Instructivo general de seguridad y uso adecuado de las tecnologías de la información y comunicación

DEL AMBITO DE LA SEGURIDAD DE LOS ACTIVOS DE INFORMACIÓN

"Art. 10.- Seguridades de redes LAN internas, servidores y laboratorios:

Toda conexión de comunicaciones externa a cualquier dependencia de la EPN en caso de ser requerida, debe ser aprobada por la DGIP.

Es responsabilidad de la DGIP mantener un filtro de todo el tráfico entre el Internet y la Red de Datos Institucional.

Las personas responsables de la administración de servidores internos y laboratorios de la EPN deben respetar las directrices y procedimientos de configuración general y seguridades establecidas por la DGIP, las excepciones a este literal deben ser aprobadas por el Dgip.

La DGIP se reserva el derecho de interrumpir el servicio brindado por unidades no institucionales (laboratorios en asociaciones, copiadoras, entre otros) cuando la actividad de éstos, impacte negativamente o sean un riesgo de seguridad para la red interna institucional."

RFC 1918

"En este documento se describe la asignación de direcciones para redes privadas. La asignación permite la conectividad de capa de red completa entre todos los hosts dentro de una empresa, así como entre todos los hosts públicos de diferentes empresas."

https://tools.ietf.org/html/rfc1918

5. DIRECTRIZ

Art. 1- Consideraciones Generales

- La Escuela Politécnica Nacional por medio de su infraestructura de datos provee a la comunidad politécnica e invitados el servicio de Internet e Intranet a través de sus equipos.
- La DGIP se encargará de validar la configuración de los equipos de comunicaciones de acuerdo a las políticas aprobadas.
- La DGIP gestionará las credenciales de acceso a los equipos de comunicaciones.
- La DGIP se reserva el derecho de permitir la conexión o interconexión de equipos ajenos a la institución.

Art. 2- Requisitos para la conexión de equipos de comunicaciones

A. Instalaciones físicas

Los equipos de comunicaciones deben ser instalados en un lugar de fácil acceso para el personal de TI, el lugar debe ofrecer las seguridades necesarias para que personal ajeno no tenga acceso a los mismos.

Es deseable tener un control de acceso y una bitácora de cambios, en el lugar de operación de los equipos.

B. Configuración

La DGIP es la encargada de gestionar la configuración de los equipos de comunicaciones institucionales de acuerdo a las siguientes consideraciones:

1. El nombre del equipo se configurará de acuerdo a la ubicación del mismo, señalando también el tipo de equipo y su función en la red.
2. La contraseña de acceso a los equipos debe ser guardada de manera segura y con un método de cifrado.
3. Cambiar las contraseñas de los equipos siguiendo las directrices institucionales para el manejo de contraseñas.
4. Se debe deshabilitar lo siguiente:
   a. Envío de broadcast entre subredes, a excepción del tráfico DHCP.

   b. El ingreso de paquetes con direcciones inválidas como las referenciadas en RFC 1918.

c. Servicios TCP y UDP que no hayan sido plenamente justificados siguiendo el procedimiento establecido para el efecto.

d. Todas las fuentes de enrutamiento que no sean aprobadas por la DGIP.

e. Todos los servicios Web que estén corriendo en los equipos de comunicaciones, a excepción del servicio web de gestión del equipo, que deberá ser utilizado solo por la red de gestión Institucional.

5. Usar cadenas estandarizadas SNMP.
6. Las reglas de acceso deben ser añadidas según las necesidades de la institución.
7. El router debe estar incluido en el sistema de administración corporativo de la institución con un punto de contacto designado.
8. Cada equipo de comunicación debe tener las siguientes instrucciones mostradas en un punto claramente visible: "EL ACCESO SIN AUTORIZACIÓN A ESTE DISPOSITIVO DE RED ESTÁ PROHIBIDO".

   Se debe tener permisos explícitos para acceder o configurar este dispositivo. Todas las actividades realizadas sobre este dispositivo deben ser registradas y las violaciones de esta política puede dar como resultado una acción disciplinaria; las violaciones serán reportadas para la respectiva aplicación de la ley.

9. Telnet nunca debe ser usado sobre la red para administrar los equipos de comunicación, a menos que exista un túnel de seguridad que proteja todo el canal de comunicación. Se utilizará para el efecto protocolos cifrados para la administración del equipo.

DEL AMBITO DE LAS SANCIONES

La DGIP debe notificar el incumplimiento de lo establecido en la presente política, a la autoridad correspondiente para los fines legales respectivos.

DISPOSICIONES GENERALES

PRIMERA.- En todo lo no previsto en este instructivo, de acuerdo a la naturaleza de control y administración de bienes y normativa que la regula, se aplicarán según corresponda las

leyes y reglamentos vigentes y demás instrumentos jurídicos que tengan relación con los mismos.

SEGUNDA.- De la ejecución del presente instructivo, que entrará en vigencia a partir de su suscripción, encárguese al Director de la Dirección de Gestión de la Información y Procesos.

DEROGATORIA

Se derogan las normas de igual o menor jerarquía emitidas con anterioridad, que se opongan al presente Instructivo.

Dado en la ciudad de Quito, D.M. a los 17 días del mes de junio del 2016.