Escuela Politécnica Nacional

Dirección de Gestión de la Información y Procesos

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

EPN-DGIP-CSIRT-07-DI

DIRECTRICES PARA SEGURIDAD DE LAS COMUNICACIONES UNIFICADAS DE LA EPN

Elaborado por:	Centro de Respuesta a Incidentes de Seguridad	Ing. Javier Erazo	
Revisado por:	Centro de Respuesta a Incidentes de Seguridad	Ing. Liliana Córdova	
	Dirección de Gestión de la Información y Procesos	Ing. Juan Carlos Bastidas	
		Ing. Juan Carlos Proaño	

Aprobado por:	Director DGIP	Ing. Roberto Andrade, MSc.	

HOJA DEL ESTADO DEL DOCUMENTO

TÍTULO DEL DOCUMENTO: Directrices para Seguridad de las Comunicaciones Unificadas 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	Ing. Liliana Córdova Ing. Juan Carlos Bastidas Ing. Juan Carlos Proaño	27/junio/2018	Creación documento

1. OBJETO

El objetivo de esta directriz es proporcionar los lineamientos de seguridad que deben ser implementados en el Servicio de Telefonía IP de la Escuela Politécnica Nacional – EPN, que ayuden a combatir la amenaza de ataques a seguridad de VoIP que pueden ocurrir durante una conexión.

2. ALCANCE

Esta directriz cubre las comunicaciones de voz sobre IP realizadas mediante equipos telefónicos IP en las diferentes dependencias académicas y administrativas de la EPN dentro del Campus Politécnico, mismas que deben contar con el cifrado de la información.

3. RESPONSABILIDAD Y AUTORIDAD

El responsable de elaborar esta directriz es:

Centro de Respuesta a Incidentes de Seguridad – CSIRT-EPN

Los responsables de revisar esta directriz son:

Centro de Respuesta a Incidentes de Seguridad – CSIRT-EPN
Líder de Servicios Computacionales

El responsable de aprobar esta directriz es:

Director de la DGIP

La autoridad para hacer cumplir esta directriz es:

Director de la DGIP

Los responsables de cumplir esta directriz son:

Responsable del servicio de Comunicaciones Unificadas; Personal de la DGIP.

4. MARCO LEGAL

Normas de Control Interno de la Contraloría General del Estado

"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 de los servicios tecnológicos."

Instructivo General de Seguridad y uso adecuado de las tecnologías de la información y comunicación de la EPN

"DEL ÁMBITO DE USO DE LOS ACTIVOS DE INFORMACIÓN:

Art. 9.- Confidencialidad de la información y uso de credenciales de acceso a los activos de información institucionales:

Los usuarios desarrolladores de software y administradores de sistemas deben usar algoritmos de cifrados autorizados según las directrices y procedimientos de la DGIP.

La DGIP definirá un proceso continuo de identificación y clasificación de información institucional.

La DGIP definirá y difundirá las directrices y procedimientos que garanticen la confidencialidad de la información personal de los empleados, trabajadores, personal académico y estudiantes de la EPN.

(...)
Es responsabilidad de los empleados, trabajadores, personal académico y estudiantes, acatar las directrices, y procedimientos de la DGIP para mantener la confidencialidad de los activos de información y credenciales de acceso, que les han sido asignados.

NORMA TÉCNICA ECUATORIANA NTE INEN-ISO/IEC 27001:2006

"A.10.8 Intercambio de Información

A10.8.3: Medios físico en tránsito: Los medios que contienen información se deben proteger contra el acceso no autorizado, el uso inadecuado o la corrupción durante el transporte más allá de los límites físicos de la organización.

A.10.8.5 Sistemas información del negocio: Se deben establecer, desarrollar e implementar políticas y procedimientos para proteger la información asociada con la interconexión de los sistemas de información del negocio.

A.10.10 Monitoreo

A.10.10.2 Monitoreo del uso del sistema: Se deben establecer procedimientos para el monitoreo del uso de los servicios de procesamiento de información, y los resultados de las actividades de monitoreo se deben revisar con regularidad."

5. DEFINICIONES

Activo: 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.[1]
Amenaza: Causa potencial de un incidente no deseado, el cual puede resultar en daños al sistema o a la organización.[2]
Control: Medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras. Salvaguardia – contramedida.
Vulnerabilidad: Debilidad de un activo o control que puede ser aprovechado por una amenaza. [3]

6. POLÍTICA

6.1. Consideraciones Generales

- La EPN cuenta con un Servicio de Telefonía IP compuesto por: 8 líneas analógicas, 1 troncal E1, 1 troncal SIP, una Central Telefónica desplegada en Software y terminales IP distribuidos en las diferentes localidades de la

[1] Fuente: Instructivo General de Seguridad y uso adecuado de las Tecnologías de la Información y Comunicación.
[2] Fuente: Norma Técnica Ecuatoriana ISO/IEC 27000
[3] Fuente: Norma Técnica Ecuatoriana ISO/IEC 27000

institución, el cual permite la comunicación de voz por medio de llamadas entrantes, salientes e internas.

- La DGIP administra el Servicio de Telefonía IP que incluye:
    - Gestión de las aplicaciones, plataforma e infraestructura del servicio de telefonía IP, para mantenerlo actualizado y disponible permanentemente.
    - Gestión de la capacidad de componentes, para la adquisición de terminales telefónicas.
    - Gestión de las configuraciones, para desplegar un buzón telefónico asociado a una extensión telefónica configurada en un teléfono IP y en la central telefónica.
    - Soporte al usuario final, para el funcionamiento del terminal telefónico IP, en la instalación en su puesto de trabajo, la verificación de la disponibilidad del servicio y la solución de problemas.
    - Gestión de incidentes y problemas, para restablecer el servicio de Telefonía IP, en el menor tiempo posible, en casos de interrupción.

- El registro de custodia de los equipos telefónicos es responsabilidad de la Dirección Administrativa de la Institución.

- Es responsabilidad de la DGIP, que la comunicación entre los equipos telefónicos IP dentro del Campus Politécnico viaje en forma cifrada, asegurando de esta manera la confidencialidad de la información en caso de existir una intercepción de una llamada, producto de que se materialice un ataque de hombre en el medio.

- El estándar utilizado en la telefonía IP es SIP desarrollado por la IETF (RFC3261). La voz sobre IP será codificada para los formatos: G.711, G.729 y G.722.

6.2. Directrices

- La DGIP debe asegurar el canal de comunicación dentro del Campus Politécnico mediante el uso de protocolos seguros de encriptación.
- La DGIP debe habilitar el cifrado en las extensiones telefónicas y terminales IP asignadas al usuario.
- La DGIP debe asegurar que todos los terminales IP distribuidas en el Campus Politécnico cuenten con el cifrado habilitado.

- La DGIP deberá mantener el directorio telefónico actualizado y conciliado con la nómina de Talento Humano, de las extensiones telefónicas configuradas y asignadas en la EPN.

6.3. Monitoreo del uso

- El CSIRT-EPN realiza revisiones continuas de seguridad para verificar que el Sistema de Telefonía IP en su conjunto permitan la comunicación cifrada.

- Los controles a monitorear son los detallados en el Anexo 1.

7. CUMPLIMIENTO

Es obligatorio el cumplimiento de estas directrices para la comunicación en forma segura en el Servicio de Telefonía IP dentro del Campus Politécnico.

8. ANEXOS

Anexo 1: Monitoreo de Seguridad del Sistema de Comunicaciones Unificadas

Anexo 1

Monitoreo de Seguridad del Sistema de Comunicaciones Unificadas

Control	Descripción	Fecha	Estado	Responsable Seguridad
Seguridad Física y Ambiental	Evitar el acceso físico no autorizado, daño e interferencia con la información y los locales de la organización.			
Asegurar la operación correcta y segura de los medios de procesamiento	Control de acceso a los servidores de telefonía (en forma segura).			
Gestión de vulnerabilidades servidores de comunicaciones unificadas	Implementar las recomendaciones de los informes de vulnerabilidades del sistema de comunicaciones unificadas, estas correcciones sean oportunas.			
Respaldos de Información	Asegurar que se realicen respaldos de información.			
Directorio telefónico actualizado y conciliado	Asegurar que se mantiene el directorio telefónico actualizado y conciliado con la nómina de Talento Humano, de las extensiones telefónicas asignadas en la EPN. El directorio telefónico deberá estar conciliado con el directorio activo institucional de acuerdo al procedimiento definido para el efecto.			
Asegurar el plan de continuidad	Asegurar que los planes de continuidad sean actualizados y conocidos por todos.			
Repasar los planes de contingencia	Asegurar que la reanudación del sistema por falla sea oportuna a defectos. Asegurar que el plan de contingencia esté actualizado.			