



Escuela Politécnica Nacional

Dirección de Gestión de la Información y Procesos

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



EPN-DGIP-CSIRT-17-DI

DIRECTRIZ DE REQUERIMIENTOS DE SEGURIDAD Y USO ACEPTABLE DE ESTACIONES DE TRABAJO DE USUARIO FINAL DE LA EPN

Elaborado por:		Ing. Javier Erazo	
Revisado por:	Dirección de Gestión de la Información y Procesos	Ing. Liliana Córdova Ing. Juan Carlos Proaño	
Aprobado por	Director DGIP	Ing. Juan Pablo Ponce	



ESCUELA POLITÉCNICA NACIONAL
DIRECTRIZ DE REQUERIMIENTOS DE SEGURIDAD Y USO ACEPTABLE DE ESTACIONES DE TRABAJO DE USUARIO FINAL DE LA EPN



EPN-DGIP-CSIRT-17-DI

HOJA DEL ESTADO DEL DOCUMENTO

TÍTULO DEL DOCUMENTO: Directriz de Requerimientos de Seguridad y uso aceptable de Estaciones de Trabajo de Usuario Final de la EPN

ESTADO DEL DOCUMENTO: Por aprobar

1. QUIEN EDITA	2. QUIEN REVISA	3. FECHA	4. RAZONES DE CAMBIO/QUIEN CAMBIA
Ing. Javier Erazo	Ing. Liliana Córdova	08/05/2020	Creación del documento



ESCUELA POLITÉCNICA NACIONAL

DIRECTRIZ DE REQUERIMIENTOS DE SEGURIDAD Y USO ACEPTABLE DE ESTACIONES DE TRABAJO DE USUARIO FINAL DE LA EPN



1. OBJETO

Describir los lineamientos de seguridad que deben ser aplicados para toda estación de trabajo previo la entrega al usuario final de la Escuela Politécnica Nacional, con la finalidad de asegurar y mitigar el riesgo ante posibles brechas de seguridad proveniente de estos activos de información de TI.

2. ALCANCE

Aplica para toda estación de trabajo, ya sea equipo de escritorio (PCs) o equipos móviles (laptops), que la DGIP y otras unidades de la EPN (Centro de Educación Continua – CEC, Instituto Geofísico – IGEPN) que gestionan servicios de TI, configuran para el uso del Personal Académico, Personal de Apoyo Académico, servidores y trabajadores, para el desarrollo de sus actividades en función del cargo que desempeñan en la Institución.

3. RESPONSABILIDAD Y AUTORIDAD

El responsable de elaborar, revisar esta directriz es:	Centro de Respuesta a Incidentes de Seguridad – CSIRT-EPN
El responsable de revisar y aprobar esta directriz es:	Director de Gestión de la Información y Procesos – DGIP
Los responsables para hacer cumplir esta directriz son:	Autoridades de las Unidades Académicas y Administrativas de la EPN, y autoridades de las unidades desconcentradas
Los responsables de cumplir esta directriz son:	Personal académico, personal de apoyo académico, servidores y trabajadores de la EPN

4. MARCO LEGAL

Ítem	Norma	Fecha	Título de la Norma	Artículos
1	Constitución de la República del Ecuador	2008, última reforma 2020	Título segundo, derechos	16 - 17.2 - 18 - 66.19 - 92 - 229 - 233
2	Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación	2016	Título quinto, capítulo segundo, acceso y soberanía del conocimiento en entornos digitales e informáticos	39





ESCUELA POLITÉCNICA NACIONAL

DIRECTRIZ DE REQUERIMIENTOS DE SEGURIDAD Y USO ACEPTABLE DE ESTACIONES DE TRABAJO DE USUARIO FINAL DE LA EPN



Item	Norma	Fecha	Título de la Norma	Artículos
3	Ley Orgánica de Telecomunicaciones	2015, última reforma 2019	Título tercero, capítulo primero, Secreto de las comunicaciones	76
4	Ley Orgánica de Educación Superior	2010, última reforma 2020	Título décimo primero, De las Faltas y Sanciones	207
5	Ley Orgánica de Servicio Público, LOSEP	2010, última reforma 2019	Título tercero, capítulo cuarto, del régimen disciplinario	43
6	Reglamento General a la Ley Orgánica de Servicio Público	2011, última reforma 2019	Título segundo, capítulo quinto, sección segunda De las sanciones	80 – 89
7	Normas de Control Interno de la Contraloría General del Estado	2009, última reforma 2019	410 Tecnología de la Información	Norma 410 - 10 Seguridad de Tecnología de Información
8	Estatuto Escuela Politécnica Nacional	2013, última reforma octubre 2019	Título quinto, de la Disciplina y Sanciones	94 – 99
9	Reglamento Interno de Trabajo Escuela Politécnica Nacional	2015	Capítulo VIII del Régimen Disciplinario	51 - 57
10	Reglamento Interno de Administración del Talento Humano de la Escuela Politécnica Nacional	2018	Capítulo XI Régimen Disciplinario Capítulo XII De la Competencia, procedimiento y recursos	59 – 71 72 – 73
11	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. Del ámbito de la Seguridad de los activos de información.	2, incisos 1-3 4, incisos 1,3 8, incisos 2-3
12	Directrices para uso de antivirus	2015	6.6 Uso antivirus para usuario final	1
13	Directrices de Seguridad de la red de computadoras	2016	5.5 Directriz de Seguridad de Sistemas Informáticos “ <i>Los sistemas informáticos deben autenticarse contra el Directorio Activo Institucional</i> ”.	1

	ESCUELA POLITÉCNICA NACIONAL DIRECTRIZ DE REQUERIMIENTOS DE SEGURIDAD Y USO ACEPTABLE DE ESTACIONES DE TRABAJO DE USUARIO FINAL DE LA EPN	
-----------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------

Item	Norma	Fecha	Título de la Norma	Artículos
14	Directriz de asignación del identificador único o cuenta de usuario	2018	6. Política 6.1 Disposiciones generales	1-3
15	Estándar para la creación de cuentas de usuario para el acceso a servicios y aplicaciones de Tecnología de Información – TI, de la EPN	2017	6. Generalidades	2-3

Tabla 1. Base legal

5. DEFINICIONES

Activo: Cualquier cosa que tiene valor para la organización [1].

Cuenta de usuario personal: Cuenta creada para el uso de una función, una actividad o un área específica y está asociada a un usuario normal [2].

Directorio Activo - Active Directory (AD): Término utilizado por Microsoft para referirse a la implementación de servicio de directorio en una red distribuida de computadores. Utiliza distintos protocolos (principalmente LDAP, DNS, DHCP, kerberos, etc.). Su estructura jerárquica permite mantener una serie de objetos relacionados con componentes de una red, como usuarios, grupos de usuarios, permisos y asignación de recursos y políticas de acceso [3].

Privilegio mínimo: El principio de que se debe diseñar una arquitectura de seguridad, para que cada entidad del sistema reciba los recursos mínimos del sistema y autorizaciones que la entidad necesita para hacer su trabajo [4].

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

6. DIRECTRIZ

6.1. Disposiciones generales

La DGIP y otras dependencias de la EPN que gestionan servicios de TI, previo la asignación de estaciones de trabajo (equipos de escritorio o laptops) al usuario final, configurarán los siguientes parámetros de seguridad:

- Configurar el software base necesario para que el equipo quede registrado en el inventario institucional de TI.



ESCUELA POLITÉCNICA NACIONAL

DIRECTRIZ DE REQUERIMIENTOS DE SEGURIDAD Y USO ACEPTABLE DE ESTACIONES DE TRABAJO DE USUARIO FINAL DE LA EPN



- Nombre de equipo configurado de acuerdo al estándar gestionado por la DGIP u otras dependencias de la EPN que gestionan servicios de TI.
- Equipo unido al Directorio Activo.
- Equipo con Software base autorizado por la institución, a nivel de Sistema Operativo, aplicaciones de ofimática y utilitarios instalados.

Se considera como software base autorizado:

- Última versión estable de Sistema Operativo Windows licenciado por la institución, con los últimos parches de seguridad instalados.
- Última versión estable de Sistema Operativo Linux.
- Última versión estable de la Herramienta de Ofimática licenciado por la institución.
- Aplicativo para grabación de CD o DVD, si aplica.
- Aplicativo para compresión y descompresión de archivos.
- Aplicativo para visualización de archivos PDF.
- Antivirus institucional.
- Agente de antivirus institucional.
- Agente de Inventario.

6.2. Normas

6.2.1. Del proceso configuración y entrega al usuario final

La DGIP y otras unidades de la EPN que gestionan servicios de TI, al momento de la entrega del equipo deberán configurar un perfil de sistema con la cuenta del usuario (identificador único) previamente creada en el Directorio Activo y entregada al usuario final, asegurando de que se le conceda el acceso al usuario final bajo el principio de *privilegio mínimo*.

6.2.2. De la instalación de software adicional

En el caso de requerir la instalación de software adicional, el cual previamente se ha verificado que forma parte del software licenciado ofertado por la institución, el usuario solicitará la licencia, enviando un correo electrónico a la dirección: asistencia.tecnica@epn.edu.ec.

Para la instalación de software con versiones de prueba o distribuciones abiertas, distribuidas por el propio fabricante, el usuario solicitará autorización para su



ESCUELA POLITÉCNICA NACIONAL

DIRECTRIZ DE REQUERIMIENTOS DE SEGURIDAD Y USO ACEPTABLE DE ESTACIONES DE TRABAJO DE USUARIO FINAL DE LA EPN



instalación, enviando un correo electrónico a la dirección: asistencia.tecnica@epn.edu.ec.

6.2.3. De las prohibiciones

No está permitido:

- El formateo del equipo entregado.
- Dar la baja al equipo del Directorio Activo.
- Desinstalación de uno o varios aplicativos del software base autorizado.
- Dañar(derramar agua, café u otras sustancias que pueden afectar el funcionamiento del equipo o sus componentes), reconfigurar (extraer, aumentar memoria, aumentar disco, cambiar Sistema Operativo) al equipo.
- Mover en forma definitiva el activo institucional como el escáner, pc de escritorio, impresora, monitor, dentro de la institución a otra área, sin la autorización y conocimiento de la DGIP y el departamento de bienes.
- La salida de bienes y/o equipos fuera de la institución sin autorización del responsable de la Unidad Académica, Administrativa y/o autoridades de las unidades desconcentradas, sin seguir el debido “Procedimiento para salida de equipos-EPN”, inserto en la Circular Nro. EPN-DA-2020-0005-C de 16 de marzo de 2020.
- El uso del equipo para fines comerciales, no institucionales o para beneficio personal.
- La instalación de software pirata.
- Reconfigurar o conectar dispositivos de comunicación (router, switch, acces point) a la red (cableada o inalámbrica) institucional sin la aprobación de la DGIP.
- Introducir Malware en forma deliberada o imprudente.
- Interrumpir o eludir cualquier control de seguridad de la información.

6.2.4. Uso aceptable del activo institucional

Los activos de información se proporcionan para su uso en el desarrollo de la misión de la Escuela Politécnica Nacional, para apoyar la enseñanza, el aprendizaje, la investigación o en relación con el cargo que desempeña en la institución.

El uso del activo de información para actividades personales, debe mantenerse al mínimo, siempre que no infrinja la política de seguridad institucional, leyes gubernamentales y directrices institucionales.



ESCUELA POLITÉCNICA NACIONAL

DIRECTRIZ DE REQUERIMIENTOS DE SEGURIDAD Y USO ACEPTABLE DE ESTACIONES DE TRABAJO DE USUARIO FINAL DE LA EPN



El uso personal del activo institucional está sujeto a las siguientes limitaciones:

- El activo está disponible para uso del usuario a quien le fue asignado.
- Se debe dar prioridad al uso de los recursos para el propósito principal de la institución.
- El uso personal no debe ser para un propósito comercial.
- Tras la terminación de un contrato, jubilación, o retiro de la Escuela Politécnica Nacional, del personal académico, personal de apoyo académico, servidores y trabajadores que tiene a su cargo un activo institucional tecnológico, previo a su devolución a la Unidad de Bienes, debe:
 - Realizar un respaldo (en un dispositivo de almacenamiento como CDs, DVDs, flash, disco duro, etc.) de toda la información que ha generado producto de su relación laboral con la institución y entregarlo al Responsable de la unidad administrativa, académica o unidad desconcentrada en la cual prestó sus servicios.
 - Solicitar a la DGIP se realice la verificación técnica respectiva, para que se emita un informe.
- Las credenciales entregadas al usuario les conceden derechos de acceso a los Sistemas de información para los que han sido autorizados.

6.3. Revisión de seguridad

La DGIP y otras unidades de la EPN (CEC, IGEPN, en otras) que gestionan servicios de TI, son los responsables de asegurar que todo equipo entregado al usuario final cuente con los parámetros de seguridad indicados en las secciones 6.1 y 6.2.1 de esta directriz.

El CSIRT-EPN realizará revisiones aleatorias en los equipos de usuario final, en Unidades de la EPN para verificar que:

- Los equipos de usuario final cuenten con los parámetros de seguridad indicados en la directriz.
- El equipo cuente con las configuraciones y software base autorizado.
- El usuario cumpla con las políticas, normas y directrices de seguridad.

7. CUMPLIMIENTO

Si el uso del activo institucional entra en conflicto con la política de seguridad, directrices institucionales, procedimientos institucionales, incluida la presente directriz, los privilegios de acceso serán removidos.



ESCUELA POLITÉCNICA NACIONAL

DIRECTRIZ DE REQUERIMIENTOS DE SEGURIDAD Y USO ACEPTABLE DE ESTACIONES DE TRABAJO DE USUARIO FINAL DE LA EPN



En caso de infringir esta directriz, los órganos competentes de la Escuela Politécnica Nacional, aplicarán las sanciones disciplinarias correspondientes de conformidad al artículo 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, artículo 46 del Código del Trabajo conjuntamente con el Reglamento Interno de Administración del Talento Humano, el Reglamento Interno de Trabajo de la Escuela Politécnica Nacional y su Estatuto aplicables para el personal académico, personal de apoyo académico, servidores, trabajadores y estudiantes.

8. REFERENCIAS

[1] ISO27000.

[2] Directriz de Asignación del Identificador Único o cuenta de Usuario.

[3] https://www.ecured.cu/Active_Directory.

[4] IETF RFC 4949 Ver 2. Internet Security Glossary, <https://www.rfc-editor.org/rfc/pdf/rfc/rfc4949.txt.pdf>