EPN-DGIP-CSIRT-21-DI

DIRECTRICES PARA USO DE ANTIVIRUS

Elaborado por:	Dirección de Gestión de la Información y Procesos	Ing. Javier Erazo	JAVIER ERNESTO ERAZO HIDALGO Firmado digitalmente por JAVIER ERNESTO ERAZO HIDALGO Fecha: 2021.10.21 08:47:33 -05'00'
Revisado por:		Ing. Liliana Córdova	LILIANA DE LOURDES CORDOVA RAMOS Firmado digitalmente por LILIANA DE LOURDES CORDOVA RAMOS Fecha: 2021.10.20 20:33:35 -05'00'
Aprobado por	Director DGIP	Ing. Juan Pablo Ponce	Firmado digitalmente por JUAN PABLO PONCE VASQUEZ DN: CN=JUAN PABLO PONCE VASQUEZ, SERIALNUMBER=1201211611 29, OU=ENTIDAD DE CERTIFICACION DE INFORMACION, O=SECURITY DATA S.A. 2, C=EC Fecha: 2021.10.21 10:35: 54-05'00'

EPN-DGIP-CSIRT-21-DI

HOJA DEL ESTADO DEL DOCUMENTO

TÍTULO DEL DOCUMENTO: Directrices para uso de antivirus **ESTADO DEL DOCUMENTO:** Aprobado			
1. QUIEN EDITA	**2. QUIEN REVISA**	**3. FECHA**	**4. RAZONES DE CAMBIO/QUIEN CAMBIA**
Ing. Liliana Córdova	Ing. Sandra Sarango	14-septiembre-2015	Creación del documento
Ing. Javier Erazo	Ing. Liliana Córdova	20-octubre-2021	Actualización nuevo formato, marco legal, cumplimiento, definiciones, consolas principales y secundaria, política de uso de la información.

1. OBJETO

El objeto del presente documento es establecer los requisitos y directrices que deben cumplirse para asegurar un eficaz descubrimiento y prevención de virus, garantizando y protegiendo los activos informáticos de propiedad de la EPN.

2. ALCANCE

Esta directriz se aplica a todos los equipos conectados a la red institucional.

Esto incluye, pero no se limita a, las computadoras de escritorio, computadoras portátiles, servidores de archivos/ftp/tftp/proxy y cualquier computador de un laboratorio generador de tráfico en la red.

3. RESPONSABILIDAD Y AUTORIDAD

El responsable de elaborar esta directriz es:	**Centro de Respuesta a Incidentes de Seguridad – CSIRT-EPN**
El responsable de revisar esta directriz es:	**Centro de Respuesta a Incidentes de Seguridad – CSIRT-EPN**
El responsable de 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:	**Comunidad Politécnica.** **Usuarios de equipos y/o dispositivos que requieran conectarse a la Red Institucional.**

4. MARCO LEGAL

Ítem	Norma	Fecha	Título de la Norma	Artículos
1	NTC-ISO-IEC 27001:2013	2013	Tecnología de la Información – Técnicas de Seguridad – Sistemas de Gestión de la Seguridad de la Información – Requisitos.	Anexo A A.12.2 Protección contra códigos maliciosos A.12.2.1. Controles contra códigos maliciosos
2	Ley Orgánica de Educación Superior	2010, última reforma 2020	Título décimo primero, De las Faltas y Sanciones	207

Ítem	Norma	Fecha	Título de la Norma	Artículos
3	Ley Orgánica de Servicio Público, LOSEP	2010, última reforma 2019	Titulo tercero capítulo cuarto, del régimen disciplinario	43
4	Reglamento General a la Ley Orgánica de Servicio Público	2011, última reforma 2019	Título segundo capítulo quinto, sección segunda De las sanciones	80-89
5	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
6	Estatuto Escuela Politécnica Nacional	2013, última reforma octubre 2019	Título V de la Disciplina y Sanciones	94 - 99
7	Reglamento Interno de Trabajo Escuela Politécnica Nacional	2015	Capítulo VIII del Régimen Disciplinario	51 - 57
8	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
9	Política de uso de la información, activos de información institucional y seguridad informática	2021	Del uso de la información y los activos de información institucional	9, 13

Tabla 1. Base legal

5. DEFINICIONES

Antivirus: El software antivirus es una aplicación o un conjunto de programas que encuentra y elimina virus de ordenadores y redes [1].

Comunidad politécnica: Son todas las autoridades, miembros del personal académico, personal de apoyo académico, servidores, trabajadores y estudiantes de la EPN.

Control: medios de gestión del riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas de gestión o de naturaleza jurídica [2].

Consola de antivirus principal: La consola de "panel único" le permite ver y administrar la seguridad en todo su entorno corporativo; es decir, las máquinas físicas y virtuales, y los dispositivos móviles [3].

Consola de antivirus secundaria: utilizada en la creación de una jerarquía de servidores de administración, cuando es agregada como parte de una consola principal [4].

CSIRT-EPN: Centro de Respuesta a Incidentes de Seguridad Informática de la Escuela Politécnica Nacional.

FTP (File Transfer Protocol): Protocolo de transferencia de archivos.

Objetivo de control: declaración que describe qué se espera lograr como resultado de implementar controles [2].

Servidor: Una entidad del sistema que proporciona un servicio en respuesta a solicitudes de otras entidades del sistema llamadas clientes [5].

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

Usuarios de la información (usuarios internos): Se considera usuario de la información a todo miembro de la Comunidad Politécnica, que haga uso de los sistemas y de la información, bajo un acceso con usuario y contraseña asignado por la Institución, con el objeto de cumplir sus actividades.

6. DIRECTRIZ

6.1. USO DE ANTIVIRUS EN EQUIPOS (SERVIDORES) INSTITUCIONALES

Todos los servidores desplegados en la red de la EPN, DEBEN tener instalado un antivirus que ofrezca escaneo en tiempo real para la protección de archivos y aplicaciones que se ejecutan en el sistema destino, y en especial si se ajustan a una o varias de las condiciones siguientes:

- El sistema es un servidor de archivos.
- El acceso de parte de NBT/Microsoft está disponible en este servidor para los usuarios sin derechos administrativos.

- El acceso HTTP/FTP está abierto al Internet.

Todos los servidores desplegados en la red de la EPN, deben tener instalada una solución de antivirus, quedando a criterio del administrador del servidor si utiliza o no el antivirus institucional u otro software antivirus, siempre y cuando se contemple lo indicado en el numeral 13. Instalación de Software, párrafo 2, de la Política de uso de la Información, activos de información institucional y seguridad informática que indica: *"No está permitida la instalación de software o aplicaciones piratas o de dudosa procedencia"*, sin embargo si el antivirus escogido no es el institucional el personal responsable del equipo asume la responsabilidad de la solución del problema de virus; la DGIP podrá desconectar los dispositivos tecnológicos de la red, cuando encuentre en éstos virus o software malicioso, producto de la omisión o falta de uso de un antivirus.

El análisis del servidor en busca de virus se recomienda al menos una vez a la semana, frecuencia que puede ser coordinada en el momento de la instalación, sin embargo, es obligación del administrador del servidor revisar que el equipo esté actualizado y que se realicen los análisis establecidos.

En caso de que se desee desinstalar la solución de antivirus institucional, es obligación del administrador del servidor informar al personal de la DGIP para que se pueda reutilizar dicha licencia.

Si el rendimiento del servidor es bajo a raíz de la instalación del antivirus, es obligación del administrador del servidor informar al personal de la DGIP, de manera que se realicen configuraciones alternativas o se pueda recurrir a versiones especiales del antivirus que permitan un mejor rendimiento.

6.2. CONSOLAS DEL ANTIVIRUS INSTITUCIONAL

Las actualizaciones de firma de virus se realizan de forma automática, desde la Consola de antivirus principal o secundaria, a la cual el equipo esté ligado.

6.2.1. Consolas principales y secundarias

En caso de que sea requerida la instalación de consolas principales o secundarias, los administradores de dichas consolas deben cumplir con las siguientes condiciones:

- Cada consola principal o secundaria, utilizará exclusivamente el número de licencias asignadas en la instalación, si se desea un número mayor de licencias, el administrador de la consola debe solicitar autorización a la DGIP.

- Previo a formatear el servidor donde está instalada la consola principal o secundaria, debe comunicarse con el personal técnico de la DGIP y respaldar la configuración de la consola a su cargo.

- Es obligación de los administradores:

    - Revisar que se realicen los respaldos de la configuración de la consola principal o secundaria.
    - Revisar que se realicen las actualizaciones de la consola principal o secundaria.
    - Revisar que exista una conexión activa entre la consola secundaria y la consola principal.
    - Revisar que exista una conexión activa entre la consola principal o secundaria y las estaciones de trabajo registradas a la misma, según sea el caso.

6.3. ANTIVIRUS DEL SERVIDOR DE CORREO

Para servidores de correo desplegados en la infraestructura de la institución, se debe tener instalado una aplicación antivirus tanto externa como interna que analice todo el correo con destino hacia y desde el servidor de correo. La ejecución local de la aplicación antivirus puede ser desactivada durante la obtención de copias de seguridad o respaldos.

6.4. ANTISPYWARE

Todos los servidores deberán tener una aplicación antispyware instalada, que ofrezca protección en tiempo real al sistema objeto del ataque si se cumple una o más de las siguientes condiciones:

- Cualquier sistema en el que usuarios no técnicos o no administrativos tienen acceso remoto a la red y cualquier acceso de salida permitido al Internet.

- Cualquier sistema en el que usuarios no técnicos o no administrativos tienen la capacidad de instalar software.

6.5. ANTISPAM

Todos los servidores de correo desplegados en la infraestructura de la institución deberán tener una aplicación antispam instalada, que ofrezca protección en tiempo real.

La DGIP establece controles para evitar la recepción de correo no deseado, envío y difusión de SPAM en el correo electrónico, y otras actividades que afectan el servicio de correo electrónico.

6.6. USO ANTIVIRUS EN ESTACIONES DE TRABAJO DE USUARIOS INTERNOS

A continuación se presentan procesos para prevenir problemas de virus:

- Siempre correr la versión corporativa estándar del software antivirus que la EPN haya adquirido y ejecutar la versión más actual; descargar e instalar las actualizaciones para el antivirus apenas éstas estén disponibles.

- Nunca abrir archivos o macros adjuntos a un correo electrónico desde una fuente desconocida, sospechosa o no confiable. Borrar estos archivos adjuntos inmediatamente, luego vaciar la papelera de reciclaje.

- Borrar el SPAM, cadenas y demás tipos de correo basura.

- Nunca descargar archivos desde fuentes sospechosas o desconocidas.

- Evitar la compartición de un disco dando acceso de lectura/escritura a menos que haya un requerimiento absoluto de la institución para hacerlo.

- Siempre analizar los dispositivos removibles (memorias flash, discos duros externos, dispositivos móviles, entre otros en busca de virus antes de usarlos.

- Respaldar la información crítica y configuraciones del sistema sobre una base regular y guardar la información en un lugar seguro.

- Si existen conflictos con el software antivirus con algún aplicativo que el miembro de la comunidad politécnica utilice, este debe ser reportado a la DGIP para verificar el inconveniente y realizar las pruebas de laboratorio necesarias.

- Nuevos virus son descubiertos casi todos los días, es obligación del usuario revisar que el antivirus de su equipo esté actualizado, de presentarse alguna novedad debe solicitar ayuda a la DGIP.

6.7. EXCEPCIONES

Una excepción a lo anterior por lo general se concederá con el debido respaldo documentado.

7. CUMPLIMIENTO

La DGIP deberá notificar el incumplimiento de lo establecido en la presente Directriz al Rector y a los Vicerrectores, para establecer las medidas correctivas o disciplinarias a las que hubiere lugar, de conformidad con el artículo 207 de la Ley Orgánica de Educación Superior, artículo 43 de la Ley Orgánica del Servicio Público, artículo 80 del Reglamento General a la Ley Orgánica del Servicio Público, artículo 46 del Código de Trabajo, conjuntamente con el Reglamento Interno de Trabajo de la Escuela Politécnica Nacional y su Estatuto, además de lo indicado en el numeral 6.2 de la Directriz General Cumplimiento de Regulaciones de Seguridad de la Información e Infracciones, aplicable para autoridades, personal académico, personal de apoyo académico, servidores, trabajadores y estudiantes.

8. REFERENCIAS

[1] https://softwarelab.org/es/que-es-un-antivirus/

[2] NTE INEN-ISO/IEC 27000:2012, página 2, sección 2, Términos y definiciones.

[3] https://latam.kaspersky.com/small-to-medium-business-security/security-center

[4] https://support.kaspersky.com/ksc/11/es-MX/178059.htm

[5] IETF RFC 4949 Ver. 2. Internet Security Glossary, página 279 https://www.rfc-editor.org/rfc/pdfrfc/rfc4949.txt.pdf