



MINISTERIO DE EDUCACIÓN

AÑO DE LAS CUMBRES MUNDIALES EN EL PERU
"DÉCADA DE LA EDUCACIÓN INCLUSIVA"

DIRECTIVA N° 063 -2008/MED-SPE-OFIN

Estándar de Software Antivirus

VERSION 1

Mayo 2008





MINISTERIO DE EDUCACIÓN

Índice

1.	Generalidades	4
1.1.	Objetivos	4
1.2.	Alcance	4
1.3.	Vigencia	4
2.	Normativa asociada	4
3.	Estándares	4
3.1	Niveles de Protección	4
3.2	Tipos de Protección	4
3.3	Características Técnicas mínimas	5
	a) Sistemas Operativos Estaciones de Trabajo	5
	b) Sistemas Operativos Servidores de Red	5
	c) Actualizaciones	5
	d) Consola de Administración	5
4.	Glosario de Términos	5
4.1.	Conceptos	6
4.2.	Siglas y/o Acrónimos	6





MINISTERIO DE EDUCACIÓN

1. Generalidades

1.1. Objetivos

- Establecer la plataforma antivirus a implementar en el Ministerio de Educación.

1.2. Alcance

- El alcance corresponde a todas las Unidades Operativas del Ministerio de Educación, a las Instancias de Gestión Educativa Descentralizadas a nivel nacional y Organismos Públicos Descentralizados del Sector Educación.

1.3. Vigencia

- La vigencia de estos estándares está condicionada a:
- Los cambios de política de la Oficina de Informática del Ministerio de Educación.
- Los cambios en el entorno (mercado, tecnologías, etc.)

2. Normativa asociada

LEY N° 28612	Ley que Norma el uso, adquisición y adecuación del Software en la Administración Pública.
D. S. 013-2003 PCM	Dictan medidas para garantizar la legalidad de la adquisición de programas de software en entidades y dependencias del Sector Público.
NTP ISO/IEC 17799	Código de buenas prácticas para la Gestión de la Seguridad de la Información
RM N° 073-2004-PCM	Guía para la Administración Eficiente de Software Legal en la Administración Pública

3. Estándares

3.1 Niveles de protección

La solución deberá proteger y controlar la seguridad en los siguientes niveles:

- a) Estaciones de trabajo y servidores de red
- b) El perímetro de Internet
 - Gateway de correo (SMTP)
 - Gateway de Internet. (HTTP / HTTPS / FTP)

3.2 Tipo de protección

La solución debe brindar protección multi-amenazas, como mínimo contra:

- Virus.
- Spyware.
- Adware.





MINISTERIO DE EDUCACIÓN

- Control de aplicaciones.
- Amenazas a cliente firewall.
- Spam
- Phishing.
- Contenido inapropiado de correo.
- Sitios web maliciosos.
- Amenazas web a la productividad

3.3 Características Técnicas mínimas.

- Sistema Operativo de Estaciones de Trabajo
La solución deberá soportar las versiones de 32 y 64 bits de los Sistemas Operativos de entorno Windows, a partir de Windows 2000.
- Sistema Operativos de Servidores de Red
La solución deberá soportar las versiones de 32 y 64 bits de los Sistemas Operativos de entorno Windows, a partir de Windows NT Server.
- Actualizaciones
Las actualizaciones del fichero de firmas de virus y del motor de búsqueda en los servidores y estaciones de trabajo deben ser manuales y automáticas (programadas) desde Internet. Debe brindar la capacidad de creación de repositorios distribuidos y programados.
- Consola de Administración
La solución debe contar con una Consola de Administración desde donde se pueda Administrar y controlar la solución antivirus en forma centralizada; asimismo, debe permitir la administración simultánea de equipos y servidores.

La administración deberá estar basada en Políticas y debe contener al menos políticas personalizables para Actualización de Antivirus.

La herramienta deberá ser escalable, el cual permite activar la administración en redes, permitiendo la administración de todos los usuarios desde una sola consola.



4. Glosario de Términos

4.1. Conceptos

VIRUS = Es un programa que se copia automáticamente y que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus son programas que se replican y ejecutan por sí mismos, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus



MINISTERIO DE EDUCACIÓN

pueden destruir, de manera intencionada, los datos almacenados en un ordenador, aunque también existen otros más "benignos", que solo se caracterizan por ser molestos.

PROGRAMAS ESPÍAS = SPYWARE - Los spywares son aplicaciones que recopilan información sobre una persona u organización sin su conocimiento. La función más común que tienen estos programas es la de recopilar información sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas, pero también se han empleado en círculos legales para recopilar información contra sospechosos de delitos, como en el caso de la piratería de software. Además pueden servir para enviar a los usuarios a sitios de internet que tienen la imagen corporativa de otros, con el objetivo de obtener información importante. Dado que el spyware usa normalmente la conexión de una computadora a Internet para transmitir información, consume ancho de banda, con lo cual, puede verse afectada la velocidad de transferencia de datos entre dicha computadora y otra(s) conectada(s) a Internet.

CORTAFUEGOS = FIREWALL - Es un elemento de hardware o software utilizado en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización responsable de la red. La ubicación habitual de un cortafuegos es el punto de conexión de la red interna de la organización con la red exterior, que normalmente es Internet; de este modo se protege la red interna de intentos de acceso no autorizados desde Internet, que puedan aprovechar vulnerabilidades de los sistemas de la red interna.

CORREO BASURA = SPAM - Se llama a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en cantidades masivas que perjudican de una u otra manera al receptor. Se activa mediante el ingreso a paginas de comunidades, grupos o acceder a links en diversas paginas.



PHISHING = Es un término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas, y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria)

4.2. Siglas y/o Acrónimos

SMTP = *Simple Mail Transfer Protocol* - Protocolo simple de transferencia de correo. Protocolo de red basado en texto utilizado para el intercambio de mensajes de correo electrónico entre computadoras o distintos dispositivos (PDA's, teléfonos móviles, etc.)



MINISTERIO DE EDUCACIÓN

HTTP = Es un protocolo orientado a transacciones y sigue el esquema petición-respuesta entre un cliente y un servidor. Al cliente que efectúa la petición (un navegador o un spider) se lo conoce como "user agent" (agente del usuario). A la información transmitida se la llama recurso y se la identifica mediante un URL. Los recursos pueden ser archivos, el resultado de la ejecución de un programa, una consulta a una base de datos, la traducción automática de un documento, etc.

FTP = *File Transfer Protocol* - Protocolo de transferencia de archivos entre sistemas conectados a una red TCP basado en la arquitectura cliente-servidor, de manera que desde un equipo cliente nos podemos conectar a un servidor para descargar archivos desde él o para enviarle nuestros propios archivos independientemente del sistema operativo utilizado en cada equipo.

28 MAYO 2008


MANUEL COK APARCANA
Jefe de la Oficina de Informática

