Directiva 005-2004-PCM/SG

Directiva de seguridad ante la presencia de virus informático en la Presidencia del Consejo de Ministros

2004

I

HOJA DE INFORMACION GENERAL

CONTROL DOCUMENTAL:

PROCEDIMIENTO:	Directiva de seguridad ante la presencia de virus informático en la Presidencia del Consejo de Ministros
PROYECTO:	Directiva de seguridad ante la presencia de virus informático en la Presidencia del Consejo de Ministros
ENTIDAD:	Presidencia del Consejo de Ministros
VERSIÓN:	1.0
FECHA EDICIÓN:	04/06/2004
DOCUMENTOS RELACIONADOS:	
NOMBRE DE ARCHIVO:	P01-PCM-DIR_SEG_VIRUS-001 **Directiva 005-2004-PCM/SG**
RESUMEN:	Documento que presenta la directiva para la seguridad ante la presencia de virus informático en la Presidencia del Consejo de Ministros

DERECHOS DE USO:

La presente documentación es de uso para la Administración Pública del Estado Peruano.

ESTADO FORMAL:

Preparado por:	Revisado por:	Aprobado por:
Nombre: Cecilia Loayza Miller, Oficina de Desarrollo y Sistemas con el apoyo ONGEI Cargo: PCM Entidad: PCM Fecha: Junio 2004	Nombre: Rafael Parra Erkel Cargo: Jefe (e) Oficina de Desarrollo y Sistemas Jefe de la Oficina Nacional de Gobierno Electrónico e Informática Entidad: PCM Fecha: Junio 2004	Nombre: Jaime Reyes Miranda Cargo: Secretario General Entidad: PCM Fecha: Junio 2004

CONTROL DE VERSIONES

FUENTE DE CAMBIO	FECHA DE SOLICITUD DEL CAMBIO	VERSIÓN	PARTES QUE CAMBIAN	DESCRIPCIÓN DEL CAMBIO	FECHA DE CAMBIO
P01-PCM-DIR_SEG_VIRUS-001		1.00	N/A		

1

INDICE

"Directiva 005-2004-PCM/SG
Directiva de seguridad ante la presencia de virus informático en la Presidencia del Consejo de Ministros"

1. OBJETIVO

Informar a los usuarios de los Sistemas de Información y de redes de la Presidencia del Consejo de Ministros sobre las normas y mecanismos que deben cumplir y utilizar para proteger los componentes de dichos sistemas ante posibles ataques de virus.

Establecer las Políticas y Normas de Seguridad Informática antivirus y definir los responsables de su desarrollo, implantación y gestión.

Analizar los riesgos existentes relacionados a la presencia de virus informático y establecer las acciones necesarias para su reducción o eliminación.

2. BASE LEGAL

a. Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros (aprobado por D.S. Nº 067-2003-PCM).
b. Manual de Organización y Funciones de la Presidencia del Consejo de Ministros.

3. ALCANCE

La observancia de la presente Directiva es obligación de todos los que prestan servicios en la Presidencia del Consejo de Ministros y en sus Comisiones adscritas, entendiéndose a ellos además como los usuarios.

4. DE LA OFICINA DE DESARROLLO Y SISTEMAS

Se entiende a la Oficina de Desarrollo y Sistemas, como el órgano de la Presidencia del Consejo de Ministros que administra, opera y supervisa los sistemas informáticos y de redes de la institución, o al órgano que haga sus veces.

5. VIGENCIA

La presente Directiva tendrá vigencia a partir del día siguiente de su aprobación por la Secretaría General.

6. CONCEPTOS GENERALES

a) ENLACE DE COMUNICACIONES
Es cualquier medio o tecnología que da la capacidad de transmitir datos.

b) CONEXIÓN EXTERNA
- Un acceso remoto a los Sistemas y Activos de Información internos, por usuarios o por terceros, desde terminales que no están controlados por la Institución;
- Un acceso remoto a Sistemas o Activos de Información externos, por usuarios, desde terminales controlados por la Institución;
- Una conexión entre un servicio interno y un servicio ajeno a la Institución.

c) INTERNET
Es una gran comunidad de computadoras conectadas entre sí por medio de líneas de comunicaciones especiales.

d) CORREO ELECTRÓNICO
El correo electrónico, o e-mail, es el medio por el cual se pueden intercambiar mensajes utilizando un dispositivo electrónico.

e) DIRECCIÓN IP (IP ADDRESS)
La dirección lógica en la red que indica una posición geográfica.

f) ROUTER
Es un procesador de redes interconectadas que encamina paquetes de datos entre dos o más redes.

g) SERVIDOR FTP ANÓNIMO (ANONYMOUS FTP SERVER)
Un sistema de Internet que permite el acceso público a archivos disponibles y su transferencia mediante FTP.

h) SISTEMA FIREWALL
Un Sistema Firewall consta de un conjunto de mecanismos, filtros de protocolo y dispositivos de control de accesos que manejan de forma segura la conexión entre redes.
Este sistema protege las comunicaciones entre un usuario y una red externa, de la forma más transparente posible para el usuario, facilitándole al máximo los servicios que dicha red ofrece.

La mayoría de los sistemas firewall están diseñados para asegurar el tráfico con la red Internet, debido a que representa la mayor fuente de información y de medios de comunicación con terceros, incluyendo:

clientes, suministradores y cualquier otro tipo de personas que comparten interes es comunes.

7. OPERATIVIDAD

7.1. Políticas de Seguridad para Administradores de Seguridad de Correo Electrónico y Red

- Los administradores de seguridad de la información, de redes o quienes hagan sus funciones, deberán desarrollar políticas de Prevención de Ataque, incluyendo en estas lineamientos para poder salvaguardar la información ante nuevos virus (por ejemplo, políticas de bloqueo de virus y filtrado de contenido).

- Los administradores de seguridad de la información, de redes o quienes hagan sus funciones, deberán elaborar reportes predefinidos, para su fácil compresión y manejo de los datos, como por ejemplo:
  i. Los 10 virus más encontrados en los sistemas .
  ii. Los 10 usuarios con mayor contaminación.
  iii. Puntos de entrada de los virus en su sistema (e-mail, Web. documentos, usuarios, equipos, etc.).

- Los administradores de seguridad de la información, de redes o quienes hagan sus funciones, deberán configurar los ruteadores y paredes de fuego (firewall) de la manera más segura posible para que permitan la detección de códigos contaminados introducidos por SMTP, HTTP y FTP, así como códigos en Java, VB Script y Active X. De esta manera, el sistema del usuario quedará protegido al entrar a Internet (a una página Web o al bajar información de la misma).

- Los administradores de seguridad de la información, de redes o quienes hagan sus funciones, deberán realizar un cronograma de limpieza de virus en la institución de manera permanente.

- Los administradores de seguridad de la información, de redes o quienes hagan sus funciones, deberán tener herramientas que les permitan analizar cada e-mail entrante y saliente por el contenido que se desea bloquear en su cabecera, cuerpo o attachment. La herramienta deberá permitan filtrar

potencialmente los contenidos maliciosos al proporcionar algunos filtros significativos que detectan el contenido de correos electrónicos como puede ser el remitente, al asunto, el cuerpo del mensaje y el anexo.

- Los administradores de seguridad de la información, de redes o quienes hagan sus funciones, ante la violación de cualquier política definida, deberá configurar acciones de procesamiento tales como eliminar el e-mail o eliminar el attachment. Deberá notificar de las acciones tomadas al emisor, receptor y al administrador.
  - Bloqueo de e-mail´s por el campo FROM o DE.
  - Bloqueo de e-mail´s por el campo SUBJECT o ASUNTO.
  - Bloqueo de e-mail´s por el campo CC o Con Copia.
  - Bloqueo de e-mail´s por el campo DOMAIN o DOMINIO.
  - Bloqueo de e-mail´s por el campo TO o PARA.
  - Bloqueo de e-mail´s por tipos de extensión del adjunto.
  - Bloqueo de e-mail´s por tipos el nombre del adjunto.
  - Bloqueo de e-mail´s por tamaño del adjunto.
  - Bloqueo de código o scripts HTML.
  - Análisis de contenidos en archivos de la gama MS Office.
  - Notificaciones al emisor.
  - Notificaciones al receptor.
  - Notificaciones a un grupo de administradores.

- Los administradores de seguridad de la información, de redes o quienes hagan sus funciones, deberán mantener actualizada la protección antivirus en toda la institución sin intervención del usuario final, mediante actualizaciones automáticas y calendarizadas.

- Los administradores de seguridad de la información, de redes o quienes hagan sus funciones, deberán mantener el control de las alertas recibidas de las estaciones de trabajo y servidores.

- Los administradores de seguridad de la información, de redes o quienes hagan sus funciones, deberán realizar actualización automática del producto antivirus una vez al día y en caso de alerta, cada 3 horas.

7.2. Políticas de Seguridad para Usuarios de Correo Electrónico y Red

a) Educación a los usuarios

La Oficina de Desarrollo y Sistemas es la encargada de la educación de los usuarios sobre cómo protegerse frente a los virus informáticos y cómo actuar si un virus informático infecta sus equipos.

Los administradores de seguridad de la información, de redes o quienes hagan sus funciones deberán planificar anualmente sesiones de formación de Seguridad para los usuarios.

b) Utilización de software antivirus

Los administradores de seguridad de la información, de redes o quienes hagan sus funciones deberán formar a los usuarios para la utilización y configuración del antivirus de manera correcta.

El uso extendido de un software antivirus de alta calidad, junto con medidas de prevención lógicas, como la restricción de la instalación de software, la protección contra escritura de sistemas y disquetes de software así como la modificación de las configuraciones del sistema para evitar el inicio del sistema desde la unidad de disquetes, evitarán la irrupción de muchos virus.

c) Informe de incidentes

Cuando un usuario crea que su equipo puede estar infectado deberá tener una idea clara de cómo proceder, para lo cual debió ser capacitado previamente (Educación a los usuarios).

El usuario debe ser consciente de la urgencia de informar el incidente a la Oficina de Desarrollo y Sistemas.

8. SANCIONES

Cualquier acción que contravenga a la presente Directiva, ameritará la aplicación de la sanción correspondiente, de parte de la Secretaría de Administración u el órgano correspondiente conforme a Ley.

9. DISPOSICIONES FINALES

Déjese sin efecto las disposiciones internas, en tanto se opongan a la presente Directiva.