2005-02

1. NÚMERO DE DIRECTRIZ: AD-2005-02

2. FECHA DE VIGENCIA: 1 de julio de 2005

3. ASUNTO: Directriz para la protección de los recursos informáticos de la ACP de ataques por código malicioso.

4. EXPOSICIÓN DE MOTIVO: Esta directriz tiene como propósito establecer los criterios necesarios para prevenir y proteger los recursos informáticos de la ACP de ataques por código malicioso.

5. DEFINICIONES:

a. Código malicioso: programa de computadora con intención de afectar negativamente la operación de los recursos informáticos. Ejemplo: virus, gusanos, programas troyanos y spyware.

b. Programa antivirus: programa de computadora con capacidad de detectar, limpiar y eliminar códigos maliciosos.

c. "Hardware": dispositivo electrónico con capacidad de procesamiento o almacenamiento de datos. Ejemplo: estaciones de trabajo, servidores, agendas electrónicas, teléfonos celulares, dispositivos de almacenamiento externos.

d. Red informática de la ACP: todos los programas ("software") y equipos o componentes ("hardware") de computadora o informáticos que son utilizados por la ACP para apoyar o realizar las operaciones del Canal, así como la adquisición, almacenamiento, manipulación, administración, movimiento, control, exhibición, conmutación, intercambio, transmisión o recepción de voz y/o datos que realiza la ACP.

6. DIRECTRIZ:

a. Todo "hardware" con programa antivirus disponible, que esté conectado a la red informática de la ACP, debe tener correctamente instalado, configurado, actualizado y activado el programa corporativo de antivirus.

b. Sólo se puede utilizar el programa antivirus autorizado por la ACP.

c. El programa antivirus debe actualizarse periódicamente en todo "hardware" que tenga instalado dicho programa, siguiendo los procedimientos establecidos.

d. Todo archivo que sea cargado desde algún "hardware" hacia la red informática de la ACP debe ser analizado con el programa antivirus antes de su uso.

e. En desarrollo de esta directriz, el Departamento de Informática y Tecnología (IM) establecerá e implementará las normas, guías y procedimientos para la administración, mantenimiento y utilización del programa antivirus.

f. Se prohíben las siguientes acciones:

(1) Conectar estaciones de trabajo, servidores o cualquier otro "hardware" a la red de ACP sin la debida protección antivirus.

(2) Desactivar la protección antivirus en los equipos de la ACP.

(3) Mantener conectados a la red de la ACP estaciones de trabajo, servidores o cualquier otro “hardware” infectados por algún código malicioso.

(4) Descargar o propagar cualquier código malicioso en la red de la ACP.

g. A continuación se detallan las responsabilidades para el cumplimiento de esta directriz.

(1) Director de Informática y Tecnología:

Revisará y propondrá al Administrador modificaciones a esta directriz.

(2) Oficina de Seguridad de Sistemas de Informática:

(a) Coordinará la estrategia corporativa de protección contra código malicioso.

(b) Realizará auditorías para verificar la efectividad de los procesos de actualización antivirus realizados por la División de Atención al Cliente y reportará el resultado de las investigaciones realizadas a los niveles jerárquicos correspondientes.

(c) Publicará en el Intranet de la ACP las actualizaciones, programas antivirus, actualizaciones de programas antivirus, alertas de virus y cualquier información relativa a código malicioso que considere necesario.

(d) Anunciará a todos los usuarios de la ACP, a través de los canales establecidos, las nuevas actualizaciones y versiones de programas, alertas de virus y cualquier otra información relativa a código malicioso.

(e) Elaborará y establecerá las normas, guías y procedimientos para la instalación, configuración y actualización del programa antivirus.

(3) División de Atención al Cliente:

(a) Elaborará e implementará los procedimientos necesarios para la distribución de las actualizaciones de los programas antivirus en los sistemas informáticos bajo su responsabilidad.

(b) Distribuirá las actualizaciones de los programas a todas las estaciones de trabajo de los usuarios en el periodo establecido.

(c) Resolverá las condiciones de error o problemas que impidan la actualización sistemática de los programas antivirus en las estaciones de los usuarios.

(d) Mantendrá actualizado y configurado el programa antivirus en los sistemas informáticos bajo su responsabilidad.

(e) Mantendrá los registros de las instalaciones y actualizaciones del programa antivirus en los sistemas informáticos bajo su responsabilidad.

(f) Suministrará los archivos, bitácoras o pistas de auditoría a la Oficina de Seguridad de Sistemas de Informática cada vez que se solicite.

(4) División de Ingeniería de Sistemas:

Asegurará la publicación y disponibilidad de los programas, actualizaciones, alertas de virus y cualquier información relativa al antivirus en el Intranet de la ACP, en coordinación con la Oficina de Seguridad de Sistemas de Informática.

(5) Directores, gerentes y supervisores:

Informarán sobre esta directriz y las normas para la protección contra código malicioso a los usuarios de los departamentos y oficinas que dirigen.

(6) Coordinadores de automatización de oficina y administradores de redes de área local:

(a) Cumplirán con los procedimientos establecidos por el Departamento de Informática y Tecnología para la instalación, configuración, operación y actualización del programa antivirus.

(b) Mantendrán los registros de las instalaciones y actualizaciones del programa antivirus en los sistemas informáticos bajo su responsabilidad.

(c) Reportarán cualquier infección o brote de código malicioso a la Oficina de Seguridad de Sistemas de Informática.

(d) Verificarán que sus respectivos servidores tengan las versiones actualizadas de los programas antivirus.

(7) Usuarios:

(a) Verificarán que sus respectivas estaciones de trabajo tengan las versiones actualizadas de los programas antivirus anunciadas por el Departamento de Informática y Tecnología.

(b) Reportarán cualquier infección o brote de código malicioso o condición de error en su programa antivirus a su administrador de red, coordinador de automatización de oficina o la instancia administrativa correspondiente.

h. El incumplimiento de las instrucciones contenidas en esta directriz y la realización de las actividades expresamente prohibidas en ella, constituyen faltas sancionables, por las que sus ejecutores pueden quedar sujetos a la aplicación de acciones disciplinarias o medidas adversas, según lo dispuesto en la Lista de Faltas y Sanciones del Reglamento de Administración de Personal. La aplicación de las sanciones se hará sin perjuicio de la responsabilidad civil o penal del infractor proveniente del mismo hecho.

7. FECHA DE EXPIRACIÓN: Indefinida.

Alberto Alemán Zubieta
Administrador