A Todo el Personal – Cuerpo de Emergencias Médicas Estatal

Política sobre el Uso de los Sistemas de Información

12/29/2009

Archivo:	Cuerpo de Emergencias Médicas Estatal Versión 1.1
Fecha de Revisión:	29/Diciembre/2009
Preparado por:	Omar Rodríguez Silva / Director de Informática
Revisado por:	
Contacto:	Omar Rodríguez Silva / E-mail: orodriguez@cem.gobierno.pr

Aspectos Generales

Para propósito de este reglamento se definen los siguientes términos:

Definiciones:

a) Contraseña – Una contraseña que resiste los intentos de descubrirla. Debe contener un mínimo de ocho caracteres alfanuméricos (letras, números y símbolos) en cualquier proporción y arreglo, según lo permita el equipo o tecnología en cuestión.

b) CEM – Cuerpo de Emergencias Médicas.

c) Usuarios o Personal – Todo el personal administrativo y operacional que utiliza os programas o aplicaciones de la agencia.

d) Red – Conjunto de Computadoras, estaciones de trabajo o equipos de comunicación del CEM que permite a los usuarios acceder a los servicios compartidos de los sistemas de información.

e) Servidor – una estación principal o equipo; que su programación provee servicios compartidos a usuarios en la red.

f) Sistemas de Información (CEM) – Se refiere:

- Todo el equipo de computadora o estaciones de la oficina.
- Los servicios asociados a la programación que ejecutan, tanto personal interno como externo de la agencia.
- El sistema de correo electrónico mejor conocido como (e-mail).
- La intranet y el acceso a los documentos y programas que existen en ésta.
- El acceso a Internet y a los documentos, páginas WEB y programas que existen en ésta.

Uso de los Sistemas de Información

- **Restricción de Uso**

  Los sistemas de información o aplicaciones del Cuerpo de Emergencias Médicas son propiedad de ésta. Por lo tanto dichos sistemas sólo podrán utilizarse para propósitos lícitos, prudentes, responsables y dentro de las funciones o poderes de esta agencia.

- **No privacidad**

Las operaciones realizadas a través de Internet o por el correo electrónico pueden generar responsabilidad por parte del CEM, por lo que los usuarios que tengan acceso a Internet por medio de los recursos provistos del CEM no tienen expectativa de privacidad alguna con relación al uso y a los accesos realizados a través de Internet. El CEM se reserva el derecho a intervenir, auditar y revisar sin previo aviso los accesos realizados por los usuarios a través de los sistemas de información de ésta, el acceso a Internet y el contenido de lo accedido.
El uso de un código de acceso (password) no impedirá que se audite el sistema y no significa que el usuario albergue expectativa de intimidad alguna con relación a la información almacenada en la computadora que tenga asignada o en cualquier otra.

Normas de Uso

El Cuerpo de Emergencias Médicas Estatal (CEM) adoptará las normas de uso de los sistemas de información y las revisará periódicamente en caso de que surjan nuevas necesidades, únicas y particulares de la agencia. Estas normas aplican a todo el personal administrativo y operacional del Cuerpo de Emergencias Médicas de Puerto Rico y todos los usuarios de Sistemas de Información sin distinción de personas.

A tono con esto, la Agencia ha adoptado las siguientes normas sobre el uso de la tecnología de información en el (CEM):

- La información contenida en la computadora, los servicios asociados tanto internos como externos, los mensajes de correspondencia electrónica (E-mails), la información de la Intranet o Internet y los documentos y programas existentes, no podrán reproducirse o utilizarse para fines ajenos a las funciones y poderes del (CEM)

- Se prohíbe terminantemente utilizar programas o recursos para los cuales no exista una licencia o autorización de uso válida a nombre del (CEM).

- Se prohíbe terminantemente copiar programas o aplicaciones del (CEM) para instalarlos en otras computadoras, sin la autorización por escrito del Director Ejecutivo o Director de Informática de la agencia.

- Se prohíbe el uso de los sistemas de computadoras y comunicaciones del (CEM) para propósitos personales, de recreo, para manejo de un negocio o asunto privado del usuario o para la utilización y envío de mensajes en cadena. De igual forma, el usuario no podrá utilizar los recursos electrónicos del (CEM) para tener acceso a compras, juegos, concursos, encuestas, páginas de entretenimiento o cualquier otro tipo ajeno a las funciones operaciones y administrativas del (CEM).

- Se prohíbe acceder a, o utilizar propiedad intelectual (copyright information) que viole los derechos del autor.

- Se prohíbe el envío o recibo de mensajes de correo electrónico (e-mails) o de cualquier tipo entre el personal del (CEM) y otras personas que no pertenezcan a la misma, en los cuales se divulguen, comenten o expresen hechos, opiniones o cualquier tipo de información relacionada con situaciones, controversias, problemas, malentendidos, funcionamiento, políticas, personas o cualquier otra situación o asunto interno del (CEM) aunque la información divulgada no sea de naturaleza confidencial.

- Se prohíbe el envío de documentos electrónicos o mensajes por medio del correo electrónico (e-mail) que contengan información confidencial del (CEM).

- Todos los archivos que se creen en el folder de (My documents) en las computadoras o estaciones de trabajo deben guardarse en el directorio asignado a cada usuario con el propósito de que puedan protegerse mediante los mecanismos de respaldo o mejor conocido como (back-ups) existentes.

- Se prohíbe modificar los privilegios de acceso a las redes de interconexión internas o externas para obtener acceso no autorizado a dichos recursos.

- Se prohíbe la modificación de los parámetros o configuración de los equipos de computadoras del (CEM) para darle capacidad de recibir llamadas telefónicas o cualquier otro tipo de acceso o conexión remota que permita instrucciones no autorizadas a la Red del (CEM).

- Se prohíbe terminantemente la utilización de la computadora o del sistema de correspondencia electrónica para enviar, recibir o crear mensajes o documentos de contenido discriminatorio por razón de raza, color, sexo, nacimiento, impedimento físico, edad, origen, condición social, preferencia sexual, ideas políticas o religiosas o por razón de matrimonio.

- Se prohíbe el manejo o transmisión de material obsceno, profano u ofensivo a través del sistema de computadoras o del sistema de comunicación electrónica del (CEM). Esto incluye entre otros: acceso a materiales eróticos, bromas de cualquier forma o cualquier comentario o chiste que pueda violar la política de discrimen del (CEM) o su política de hostigamiento sexual.

- Se prohíbe el uso de protector de pantallas (screen savers) con fotos de personas (amigos o familiares), artistas, modelos, deportistas, fotos de calendario o cualquier otra imagen que no haya sido autorizada por el Director Ejecutivo o el Director de Informática del (CEM).

- Se prohíbe el envío a otras personas de copia de un mensaje de correspondencia electrónica recibido sin el conocimiento o consentimiento del remitente original.

- Se prohíbe que los usuarios se suscriban a listas de correo electrónico o que participen en grupos de noticias (newsgroups) que divulguen información o mensajes ajenos a las funciones y deberes del (CEM).

- Se prohíbe el uso de programas para platicar (chats) sin la autorización del (CEM) y sobretodo utilizando el dominio de la agencia.

- Se prohíbe utilizar para fines no autorizados estaciones de trabajo, equipo de tecnología que tengan número de propiedad y que pertenezcan al (CEM)

- El Cuerpo de Emergencias Médicas (CEM) se reserva la facultad de comenzar los procesos administrativos, civiles o criminales pertinentes a los actos cometidos, aunque los mismos no están expresamente prohibidos en estas normas, si dichos actos, directa o indirectamente, ponen en riesgo la seguridad, integridad y confiabilidad de la información, el equipo y los sistemas de de información de la agencia.

Divulgación de las Normas de Uso

El Departamento de Informática del Cuerpo de Emergencias Médicas Estatal divulgará y entregará a los usuarios las normas de uso de los sistemas de información de la agencia.

Seguridad en los Sistemas de Información (CEM)

a) Control de acceso – el acceso a la red, así como la información grabada en esta, se restringirá, mediante un sistema de control de acceso y horarios y solamente a usuarios debidamente autorizados. Los usuarios sólo accederán aquellos datos, equipos y sistemas que precisen para realizar sus funciones y operaciones diarias.

b) Servicio Internet – El (CEM) provee el servicio para acceder a Internet al personal que lo necesita y lo requiere para llevar a cabo sus funciones. Este se provee mediante un proveedor de servicio mejor conocido como (Internet Service Provider).El acceso a este servicio será restringido a los usuarios debidamente autorizados por el Director de Informática conjunto con la seguridad y el bloqueo de las páginas WEB que contengan contenido adulto y que sea para compras y ventas.

b) Computadoras Portátiles – El (CEM) y el departamento de Informática provee Computadoras portátiles (Laptops) al personal que las necesite para llevar a cabo sus funciones. Los usuarios de las mismas deberán proteger la información almacenada en los equipos bajo su custodia contra pérdida, robo y acceso no autorizado. También protegerlas contra cantazos, vandalismo y negligencia.

Contraseñas

El Cuerpo de Emergencias Médicas Estatal (CEM) utiliza sistemas de control de acceso y mecanismos técnicos para que el ambiente de las redes sean confiables a cualquier interferencia. Estos requieren como mínimo una clave de acceso y una contraseña personal para autenticar el usuario.
Las contraseñas personales (password) constituyen un elemento fundamental de la seguridad de acceso a los sistemas y la información que almacenan. Estas

contraseñas (password) deben ser estrictamente confidenciales, privadas y que no se presten a ser descubiertas por un tercero. Por consiguiente cada usuario debe ser responsable de:

- Usuarios con acceso a la red; tienen que utilizar una contraseña alfanumérica de ocho caracteres combinando signos, letras mayúsculas y minúsculas. También bien importante recalcar que en la contraseña no puede utilizar su nombre ni apellido ni tampoco una contraseña repetida y también tampoco deben contener información relacionada directamente con el personal. Esta contraseña creada por el usuario estará en función alrededor de 90 días como por ejemplo:
    a) Nombre propio del usuario o familiares
    b) Nombre de Mascotas
    c) Fechas de nacimiento o cualquier otra fecha significativa para el usuario.
    d) Número de seguro social, número de licencia de conducir, número de empleado o de la tablilla del vehículo de motor del usuario.
    e) Combinaciones que hagan referencia al mes o ciclo corriente.

- Mantener la confidencialidad de sus contraseñas si son más de una. En caso de que la misma sea conocida de manera fortuita o mediante fraude, el usuario vendrá obligado a notificar inmediatamente al Administrador de la Red (LAN Administrator) o al Director de Informática y proceder con el cambio de contraseña.

- El Director de Informática deberá establecer las medidas de seguridad necesarias para asegurar la confidencialidad, disponibilidad e integridad de los archivos del sistema operativo que contengan dichas contraseñas. Las contraseñas se asignarán y se cambiarán mediante el método y la periodicidad que establezca el Director de Informática. El Departamento de Informática mantendrá para utilidad de los usuarios las guías necesarias que éstos puedan utilizar de referencia para activar o cambiar tales contraseñas.

- Se instaló en cada estación de trabajo como en los servidores; la pantalla del Programa de Advertencias de la página del Contralor de Puerto Rico. http://www.ocpr.gov.pr/. Este es un screen que aparece cuando la persona entra su User Name y su password y hace Log-on a la estación. Este screen te habla sobre el buen uso de los sistemas, e-mails, seguridad, política antidiscrimen, aceptación y procedimientos disciplinarios. El usuario tiene que indicar que acepto el mismo para que continúe sus labores en la red.

- A través del Isa Server; se bloquearon páginas de Internet que no responden a ninguna operación de la agencia como (Facebook, My space, Clasificados online, Twitter, Hi-5, You tube etc). Como también a páginas con contenido adulto.

Tabla de Contenidos

Normas y Procedimientos de Seguridad y Uso de los Sistemas de Información

12/18/09

Resumen

Archivo:	Cuerpo de Emergencias Médicas Estatal Versión 1.1
Fecha de Revisión:	21/Octubre/2009
Preparado por:	Omar Rodríguez Silva / Director de Informática
Revisado por:	Lic. Carlos Salgado Schwarz Asesor Legal
Contacto:	Omar Rodríguez Silva / E-mail: orodriguez@cem.gobierno.pr

Introducción

El Cuerpo de Emergencias Médicas Estatal (CEM) provee a su personal administrativo y operacional el equipo de computadoras y los servicios tanto de sistemas como de soporte computadorizados necesarios para el cumplimiento de los deberes ministeriales.

Como parte de la misión de esta agencia y el departamento de Informática de promover el uso eficiente y efectivo de los recursos; es importante establecer normas de seguridad aplicables a estos equipos, servicios y planes de contingencia. De igual modo es importante establecer normas para el uso de éstos.

Objetivo

El propósito de este reglamento es disponer de las normas de seguridad y del buen uso de los sistemas de información; además de los equipos que pertenecen al departamento de Informática del Cuerpo de Emergencias Médicas Estatal (CEM).

Alcance

Este reglamento aplica a los sistemas de información del Cuerpo de Emergencias Médicas Estatal (CEM) y a todos los usuarios tanto personal administrativo y operacional que utilicen los mismos. El acceso a las redes y al ambiente de las tecnologías de información del Cuerpo de Emergencias Médicas es para uso exclusivamente de usuarios del sistema y que pertenecen a la agencia. Se utilizaran mecanismos técnicos para el ambiente de seguridad de las redes y que sean confiables a cualquier interferencia.

Prohibición de Discrimen

A tenor con las normas constitucionales y estatutarias que prohíben el discrimen por razón de género, al aplicar este Reglamento todo término utilizado para referirse a una persona o puesto se refiere a ambos sexos (género) sin importar raza, religión etc.

Disposición General

Cuando se determine dar acceso a los sistemas de información del (CEM) a consultores o proveedores de ésta; las normas para el uso de los mismos dispondrán mediante las cláusulas a tales efectos en los respectivos contratos.

Aspectos Generales

Para propósito de este reglamento se definen los siguientes términos:

Definiciones:

a) Contraseña – Una contraseña que resiste los intentos de descubrirla. Debe contener un mínimo de ocho caracteres alfanuméricos (letras, números y símbolos) en cualquier proporción y arreglo, según lo permita el equipo o tecnología en cuestión.

b) CEM – Cuerpo de Emergencias Médicas.

c) Usuarios o Personal – Todo el personal administrativo y operacional que utiliza os programas o aplicaciones de la agencia.

d) Red – Conjunto de Computadoras, estaciones de trabajo o equipos de comunicación del CEM que permite a los usuarios acceder a los servicios compartidos de los sistemas de información.

e) Servidor – una estación principal o equipo; que su programación provee servicios compartidos a usuarios en la red.

f) Sistemas de Información (CEM) – Se refiere:

- Todo el equipo de computadora o estaciones de la oficina.
- Los servicios asociados a la programación que ejecutan, tanto personal interno como externo de la agencia.
- El sistema de correo electrónico mejor conocido como (e-mail).
- La intranet y el acceso a los documentos y programas que existen en ésta.
- El acceso a Internet y a los documentos, páginas WEB y programas que existen en ésta.

Uso de los Sistemas de Información

- **Restricción de Uso**

  Los sistemas de información o aplicaciones del Cuerpo de Emergencias Médicas son propiedad de ésta. Por lo tanto dichos sistemas sólo podrán utilizarse para propósitos lícitos, prudentes, responsables y dentro de las funciones o poderes de esta agencia.

- **No privacidad**

  Las operaciones realizadas a través de Internet o por el correo electrónico pueden generar responsabilidad por parte del CEM, por lo que los usuarios

que tengan acceso a Internet por medio de los recursos provistos del CEM no tienen expectativa de privacidad alguna con relación al uso y a los accesos realizados a través de Internet. El CEM se reserva el derecho a intervenir, auditar y revisar sin previo aviso los accesos realizados por los usuarios a través de los sistemas de información de ésta, el acceso a Internet y el contenido de lo accedido.
El uso de un código de acceso (password) no impedirá que se audite el sistema y no significa que el usuario albergue expectativa de intimidad alguna con relación a la información almacenada en la computadora que tenga asignada o en cualquier otra.

Normas de Uso

El Cuerpo de Emergencias Médicas Estatal (CEM) adoptará las normas de uso de los sistemas de información y las revisará periódicamente en caso de que surjan nuevas necesidades, únicas y particulares de la agencia. Estas normas aplican a todo el personal administrativo y operacional del Cuerpo de Emergencias Médicas de Puerto Rico y todos los usuarios de Sistemas de Información sin distinción de personas.

A tono con esto, la Agencia ha adoptado las siguientes normas sobre el uso de la tecnología de información en el (CEM):

- La información contenida en la computadora, los servicios asociados tanto internos como externos, los mensajes de correspondencia electrónica (E-mails), la información de la Intranet o Internet y los documentos y programas existentes, no podrán reproducirse o utilizarse para fines ajenos a las funciones y poderes del (CEM)

- Se prohíbe terminantemente utilizar programas o recursos para los cuales no exista una licencia o autorización de uso válida a nombre del (CEM).

- Se prohíbe terminantemente copiar programas o aplicaciones del (CEM) para instalarlos en otras computadoras, sin la autorización por escrito del Director Ejecutivo o Director de Informática de la agencia.

- Se prohíbe el uso de los sistemas de computadoras y comunicaciones del (CEM) para propósitos personales, de recreo, para manejo de un negocio o asunto privado del usuario o para la utilización y envío de mensajes en cadena. De igual forma, el usuario no podrá utilizar los recursos electrónicos del (CEM) para tener acceso a compras, juegos, concursos, encuestas, páginas de entretenimiento o cualquier otro tipo ajeno a las funciones operaciones y administrativas del (CEM).

- Se prohíbe acceder a, o utilizar propiedad intelectual (copyright information) que viole los derechos del autor.

- Se prohíbe el envío o recibo de mensajes de correo electrónico (e-mails) o de cualquier tipo entre el personal del (CEM) y otras personas que no pertenezcan

a la misma, en los cuales se divulguen, comenten o expresen hechos, opiniones o cualquier tipo de información relacionada con situaciones, controversias, problemas, malentendidos, funcionamiento, políticas, personas o cualquier otra situación o asunto interno del (CEM) aunque la información divulgada no sea de naturaleza confidencial.

- Se prohíbe el envío de documentos electrónicos o mensajes por medio del correo electrónico (e-mail) que contengan información confidencial del (CEM).

- Todos los archivos que se creen en el folder de (My documents) en las computadoras o estaciones de trabajo deben guardarse en el directorio asignado a cada usuario con el propósito de que puedan protegerse mediante los mecanismos de respaldo o mejor conocido como (back-ups) existentes.

- Se prohíbe modificar los privilegios de acceso a las redes de interconexión internas o externas para obtener acceso no autorizado a dichos recursos.

- Se prohíbe la modificación de los parámetros o configuración de los equipos de computadoras del (CEM) para darle capacidad de recibir llamadas telefónicas o cualquier otro tipo de acceso o conexión remota que permita instrucciones no autorizadas a la Red del (CEM).

- Se prohíbe terminantemente la utilización de la computadora o del sistema de correspondencia electrónica para enviar, recibir o crear mensajes o documentos de contenido discriminatorio por razón de raza, color, sexo, nacimiento, impedimento físico, edad, origen, condición social, preferencia sexual, ideas políticas o religiosas o por razón de matrimonio.

- Se prohíbe el manejo o transmisión de material obsceno, profano u ofensivo a través del sistema de computadoras o del sistema de comunicación electrónica del (CEM). Esto incluye entre otros: acceso a materiales eróticos, bromas de cualquier forma o cualquier comentario o chiste que pueda violar la política de discrimen del (CEM) o su política de hostigamiento sexual.

- Se prohíbe el uso de protector de pantallas (screen savers) con fotos de personas (amigos o familiares), artistas, modelos, deportistas, fotos de calendario o cualquier otra imagen que no haya sido autorizada por el Director Ejecutivo o el Director de Informática del (CEM).

- Se prohíbe el envío a otras personas de copia de un mensaje de correspondencia electrónica recibido sin el conocimiento o consentimiento del remitente original.

- Se prohíbe que los usuarios se suscriban a listas de correo electrónico o que participen en grupos de noticias (newsgroups) que divulguen información o mensajes ajenos a las funciones y deberes del (CEM).

- Se prohíbe el uso de programas para platicar (chats) sin la autorización del (CEM) y sobretodo utilizando el dominio de la agencia.

- Se prohíbe utilizar para fines no autorizados estaciones de trabajo, equipo de tecnología que tengan número de propiedad y que pertenezcan al (CEM)

- El Cuerpo de Emergencias Médicas (CEM) se reserva la facultad de comenzar los procesos administrativos, civiles o criminales pertinentes a los actos cometidos, aunque los mismos no están expresamente prohibidos en estas normas, si dichos actos, directa o indirectamente, ponen en riesgo la seguridad, integridad y confiabilidad de la información, el equipo y los sistemas de de información de la agencia.

Divulgación de las Normas de Uso

El Departamento de Informática del Cuerpo de Emergencias Médicas Estatal divulgará y entregará a los usuarios las normas de uso de los sistemas de información de la agencia.

Seguridad en los Sistemas de Información (CEM)

a) Control de acceso – el acceso a la red, así como la información grabada en esta, se restringirá, mediante un sistema de control de acceso y horarios y solamente a usuarios debidamente autorizados. Los usuarios sólo accederán aquellos datos, equipos y sistemas que precisen para realizar sus funciones y operaciones diarias.

b) Servicio Internet – El (CEM) provee el servicio para acceder a Internet al personal que lo necesita y lo requiere para llevar a cabo sus funciones. Este se provee mediante un proveedor de servicio mejor conocido como (Internet Service Provider).El acceso a este servicio será restringido a los usuarios debidamente autorizados por el Director de Informática conjunto con la seguridad y el bloqueo de las páginas WEB que contengan contenido adulto y que sea para compras y ventas.

b) Computadoras Portátiles – El (CEM) y el departamento de Informática provee Computadoras portátiles (Laptops) al personal que las necesite para llevar a cabo sus funciones. Los usuarios de las mismas deberán proteger la información almacenada en los equipos bajo su custodia contra pérdida, robo y acceso no autorizado. También protegerlas contra cantazos, vandalismo y negligencia.

Contraseñas

El Cuerpo de Emergencias Médicas Estatal (CEM) utiliza sistemas de control de acceso y mecanismos técnicos para que el ambiente de las redes sean confiables a cualquier interferencia. Estos requieren como mínimo una clave de acceso y una contraseña personal para autenticar el usuario.
Las contraseñas personales (password) constituyen un elemento fundamental de la seguridad de acceso a los sistemas y la información que almacenan. Estas contraseñas (password) deben ser estrictamente confidenciales, privadas y que no se presten a ser descubiertas por un tercero. Por consiguiente cada usuario debe ser responsable de:

- Usuarios con acceso a la red; tienen que utilizar una contraseña alfanumérica de ocho caracteres combinando signos, letras mayúsculas y minúsculas. También bien importante recalcar que en la contraseña no puede utilizar su nombre ni apellido ni tampoco una contraseña repetida y también tampoco deben contener información relacionada directamente con el personal. Esta contraseña creada por el usuario estará en función alrededor de 90 días como por ejemplo:
    a) Nombre propio del usuario o familiares
    b) Nombre de Mascotas
    c) Fechas de nacimiento o cualquier otra fecha significativa para el usuario.
    d) Número de seguro social, número de licencia de conducir, número de empleado o de la tablilla del vehículo de motor del usuario.
    e) Combinaciones que hagan referencia al mes o ciclo corriente.

- Mantener la confidencialidad de sus contraseñas si son más de una. En caso de que la misma sea conocida de manera fortuita o mediante fraude, el usuario vendrá obligado a notificar inmediatamente al Administrador de la Red (LAN Administrator) o al Director de Informática y proceder con el cambio de contraseña.

- El Director de Informática deberá establecer las medidas de seguridad necesarias para asegurar la confidencialidad, disponibilidad e integridad de los archivos del sistema operativo que contengan dichas contraseñas. Las contraseñas se asignarán y se cambiarán mediante el método y la periodicidad que establezca el Director de Informática. El Departamento de Informática mantendrá para utilidad de los usuarios las guías necesarias que éstos puedan utilizar de referencia para activar o cambiar tales contraseñas.

- Se instaló en cada estación de trabajo como en los servidores; la pantalla del Programa de Advertencias de la página del Contralor de Puerto Rico. http://www.ocpr.gov.pr/. Este es un screen que aparece cuando la persona entra su User Name y su password y hace Log-on a la estación. Este screen te habla sobre el buen uso de los sistemas, e-mails, seguridad, política antidiscrimen, aceptación y procedimientos disciplinarios. El usuario tiene que indicar que acepto el mismo para que continúe sus labores en la red.

- A través del Isa Server; se bloquearon páginas de Internet que no responden a ninguna operación de la agencia como (Facebook, My space, Clasificados online, Twitter, Hi-5, You tube etc). Como también a páginas con contenido adulto.

Respaldo de la Información

a) Servidores de la Red – El Departamento de Informática realizará diariamente el respaldo (back-up) de la información almacenada en los servidores y la operación de la red diaria en medios removibles seguros. Dichos medios se están guardando en una caja fuerte resistente a fuegos y vandalismos en algún piso de la agencia. Pronto tomaremos medidas para enviarlas fuera de

la agencia a un Safe Deposit en algún punto del área metropolitana donde se mantendrán conforme con los ciclos aprobados por el Director de Informática.

b) Computadoras Portátiles (Laptops) – El usuario de computadoras portátiles deberá respaldar la información almacenada en estás en medios removibles (USB Drive, CD's, back-ups) mediante el método y la periodicidad que establezca el Director de Informática.

c) Plan de Recuperación de Desastres – El Director de Informática recomendará la aprobación del Director Ejecutivo un Plan de Recuperación de Desastres (Disaster Recovery Plan) que servirá como guía para asegurar la restauración de los servicios computadorizados definidos como críticos, luego de situaciones en que estos se hayan perdido o destruido. Además, éste se asegurará de que se implanten las acciones necesarias para actualizar el Plan cuando sea necesario y que el mismo se conserve actualizado en un lugar seguro fuera de los predios de la Agencia (CEM).

d) Protección contra Programación dañina – El personal de Informática tomara las medidas necesarias para minimizar el riesgo de que una programación dañina o virus logra penetrar las defensas establecidas en la Red, el personal de Informática actuará con diligencia para limitar, evitar o prevenir el daño. Además, se asegurará de fortalecer contra ataques similares. Cada usuario deberá mantener al día su computadora en su computadora los mecanismos de defensa (Antivirus) contra programación dañina (malware); mediante el método de periodicidad que establezca el Departamento de Informática. Aunque hay unas políticas en la consola de Antivirus que explore, diagnostique y actualice todas las estaciones de trabajo y los servidores.

e) Disposición de Información sensitiva y de programas – El Departamento de Informática establecerá los procedimientos necesarios para asegurar la disposición adecuada de los archivos y programas, antes de transferir o dar de baja cualquier equipo de computadora y los medios de almacenamiento de información. Esto es una manera preventiva de que la información cometida en los mismos no pueda ser accedida por personas no autorizadas.

f) Seguridad Física – El (CEM) deberá proteger los equipos de tecnología, comunicaciones y los medios de almacenamiento de datos contra daño físico, robo, pérdida y acceso no autorizado.

g) Cuarto de servidores y equipo de comunicación – se mantendrán los cuartos de los servidores (Data Center o Server Room) y de equipos de comunicación cerrados con control de acceso mediante tarjeta (Card Reader) y llave en todo momento. Sólo personal autorizado de Informática tiene accesos a los mismos. Entre otras medidas de seguridad; los cuartos de los servidores se vigilarán mediante un sistema de cámaras de seguridad. Toda persona ajena al (CEM) ya sea (contratista, consultores, etc.) que requiera tener acceso a dichos cuartos y equipos será escoltado por personal de dicho Departamento y firmar un libro de registros (Record Book) mientras esté en los mismos.

Además, el personal de Informática se asegurará que en los referidos cuartos:

- La temperatura se mantenga de acuerdo con lo especificado por los fabricantes de los equipos en el (Server Room). En caso de variación se tomarán las medidas necesarias para atender la situación.

- Esté equipados con alarmas y extintores de fuego y que éstos han sido inspeccionados según las especificaciones.

- Tengan luces de emergencias y planta eléctrica, incluyendo los pasillos.

- Estén identificados los lugares de salidas de emergencias y las cámaras de seguridad.

- Estén limpios y libres de materiales inflamables.

- Tengan organizados y debidamente identificados los cables de la red y las áreas de Informática.

h) Medios removibles – El usuario deberá proteger los medios removibles (USB Drive, CD's y Floppy Disk) que contienen información confidencial del (CEM) contra robo, pérdida, daño físico y acceso no autorizado. El personal de Informática mantendrá losmedios removibles que contienen información de la agencia y las licencias guardadas en caja fuerte con acceso restringido.

i) Computadoras Portátiles (Lap-Top) – El usuario tomará las medidas necesarias para minimizar los riesgos de daño físico, robo, pérdida o falta de autorización para acceder al equipo que se le asigna.

Orientación y Capacitación

Todo el personal o usuario de estaciones de trabajo de la agencia (CEM) vendrá obligado a observar las normas, las medidas y los estándares de seguridad que afecten sus funciones. El Departamento de Informática periódicamente mediante correo electrónico, informará sobre cambios en las normas, los estándares y los cambios o enmiendas sobre las normas de seguridad y de uso de los sistemas de información.

Sanciones

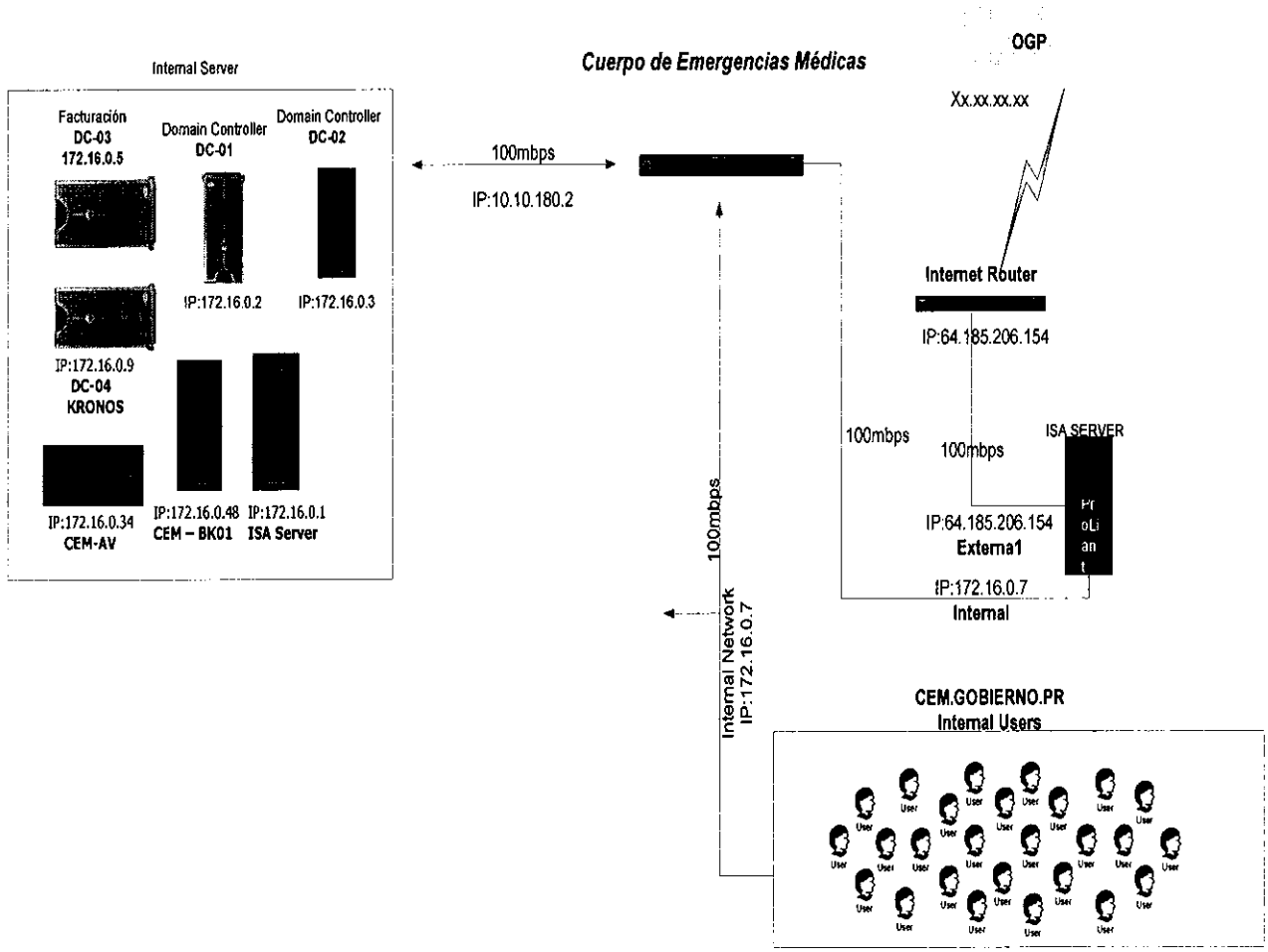
Se tomarán las medidas correctivas, disciplinarias, civiles o criminales que correspondan contra los usuarios que violen estas normas o abusen del acceso a los sistemas de información del (CEM). En el caso de las medidas disciplinarias están peden ser bien severas como amonestaciones escritas o si es un caso grave o reincidente la destitución.

Server Room

En cuanto a los servidores del CEM se hicieron los siguientes cambios:

- Migración de Exchange Server de la Agencia a las facilidades de OGP.
- OGP es responsable diariamente el backup del Exchange o HMC de la agencia.
- Se creó un servidor de Back-UPS con el programa Veritas Backups 10.0; el cual no había ninguno en función ni operando.

- A continuación un Diagrama de la Red y el dominio del CEM y sus conexiones.



Antivirus

En cuanto a herramientas de seguridad como los antivirus se coordinó con OGP; para obtener la licencia de la nueva versión de Symantec Endpoint Protection 11.0.

- Se utilizó un servidor para la nueva instalación e implementación del Antivirus

*En el Departamento de Informática hay 4 empleados a tiempo completo incluyendo a este servidor.

Sr. William Rosado – Analista/Programador
Sra. Georgina Carrasquillo – Help Desk Technician
Sra. Carmen Sánchez – Coordinadora de Comunicaciones
Sr. Omar Rodríguez – Director de Informática

Revisado por:

Lcdo. Carlos G. Salgado
Asesor Legal

Fecha 12/18/09

Aprobado por:

Dr. Jose E. Alicea Melero
Director Ejecutivo

Fecha 12/18/09