Gobierno de Puerto Rico
Agencia Estatal para el Manejo de Emergencias y Administración de Desastres

Hon. Luis G. Fortuño
Gobernador

Heriberto N. Sauri, MPH
Director Ejecutivo

Heriberto Sauri Santiago, MPH
Director Ejecutivo

CARTA CIRCULAR CSI-2011-001 NORMAS Y PROCEDIMIENTO PARA LA PREVENCIÓN DE ACCESOS NO AUTORIZADOS AL SISTEMA

FECHA DE EFECTIVIDAD: 04/2011

I. OBJETIVO

La protección de la confidencialidad, integridad y disponibilidad de la información requieren que se establezcan las normas para prevenir de accesos no autorizados al sistema de información de la AEMEAD. Esta protección se requiere tanto a nivel físico como lógico de la información.

II. ALCANCE

Este procedimiento es aplicable a todas las dependencias de la AEMEAD.

III. REFERENCIA

La Política Núm. TIG-008, Uso de Sistemas de Información, de la Internet y del Correo Electrónico establece las normas generales aplicables al uso de los sistemas de de información.

La Orden Ejecutiva Núm.001-A Serie 2008-2009, "Para establecer la Política Pública de Uso en los Sistemas de Información y de la Agencia Estatal para el Manejo de Emergencias y Administración de Desastres (AEMEAD) y las Normas y Procedimientos para el Acceso de Areas Restringidas al Centro de Información de Datos y Cuadro Telefónico de la Oficina Central y Once Oficinas de Zonas", establece medidas de seguridad restringiendo el acceso físico para proteger información, equipo e infraestructura.

PO Box 194140
San Juan, PR 00919-4140 USA
(787) 724-0124 (787) 725-4244 fax
info@aemead.pr.gov
www.manejodeemergencias.pr.gov

Normas para el Acceso Físico

La Carta Circular 77-05 del 8 de diciembre del 2004 en su política TIG-003 SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN, en su artículo J, Controles Físicos, establece que: "El acceso a las facilidades de sistemas de información deberá estar controlado para que solamente el personal autorizado pueda utilizarlas".

Para dar cumplimiento a esta disposición general, se establece que además de las disposiciones de la Orden Ejecutiva Num.001-A Serie 2008-2009, el acceso a las facilidades de sistemas de información de la AEMEAD estará controlado para que solamente el personal autorizado por el CSI pueda tener acceso físico al centro de cómputo.

El área de servidores y comunicaciones estará vigilada por sistemas de seguridad que serán monitoreados 24 horas al día 7 días a la semana, por el personal de seguridad. Esta área contará con 4 medidas de seguridad: las cámaras de seguridad, el lector de tarjetas (*card reader*), la cerradura convencional y la llave de seguridad. Solamente tendrán los juegos de llaves necesarias para el acceso físico al Centro de Cómputo el Director, el Administrador y el personal del CSI.

Cuando alguno de estos funcionarios se desvincule de la Agencia, los códigos de seguridad de las tarjetas (*card reader*) serán cambiados y la llave de seguridad deberá ser reconfigurada.

Solamente el personal del CSI está autorizado para permitir el acceso al Centro de Cómputo. Todo visitante al Centro de Cómputo deberá firmar el registro de visitantes al mismo, registrando la fecha, hora y motivo del acceso.

Siempre que un empleado del CSI necesite retirarse del CSI verificará si queda otro de sus empleados y en caso contrario, la puerta de acceso al CSI deberá quedar cerrada con la llave de seguridad.

Normas para el Acceso Lógico

La Política TIG-003 en el artículo E.3 establece que "La información y los programas de aplicación utilizadas en las operaciones de la agencia deberán tener controles de acceso para su utilización de tal manera que solamente el personal autorizado pueda ver los datos que necesita ver, o usar las aplicaciones (o la parte de las aplicaciones) que necesita utilizar. Estos controles deberán incluir mecanismos de autenticación y autorización".

El CSI efectuará la administración de los permisos de acceso a los recursos del sistema utilizando los mecanismos de autenticación y autorización que éste provee, para lo que seguirá

PO Box 194140
San Juan, PR 00919-4140 USA
(787) 724-0124 (787) 725-4244 fax
info@aemead.pr.gov
www.manejodeemergencias.pr.gov

1) Enfatizar en los requerimientos de seguridad de cada una de las aplicaciones.
2) Hacer compulsorio el que los usuarios conozcan las políticas, reglamentaciones y mejores prácticas de protección del acceso a los datos y servicios.
3) Definir los perfiles de acceso de usuarios estándar, comunes a cada categoría de puestos de trabajo.
4) Administrar los derechos de acceso en el ambiente de la red, teniendo en cuenta todos los tipos de conexiones disponibles.
5) Imponer sanciones por el mal uso del sistema.

La Oficina de Recursos Humanos incluirá las funciones relativas a la seguridad de la información en las descripciones de puestos de los empleados, informará a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información haciendo entrega de las políticas para seguridad de la información y el uso de correspondencia electrónica y coordinará las tareas de concienciación de usuarios sobre la seguridad del sistema.

Para el control de acceso al sistema, el CSI realizará lo siguiente:

A. Manejo de Cuentas de Usuario

El manejo de cuentas de usuario comprende el proceso de solicitar el ingreso del usuario al sistema, crear la cuenta según solicitado, informar al usuario como se identificará en el sistema para poder tener acceso al mismo, el efectuar las modificaciones que sean necesarias si hubiera una reasignación de sus funciones en el sistema y finalmente el cierre de la cuenta. También conlleva el dar seguimiento a su actividad en el sistema.

1) Para poder tener acceso al sistema de la AEMEAD todo usuario deberá ser previamente autorizado por el CSI para lo que requerirá que el supervisor del área llene la forma MANEJO DE CUENTAS DE USUARIO (Anejo 1) y la envié al CSI.
2) El CSI revisará la solicitud y de encontrarla correcta, procederá a crear la cuenta dándole acceso como usuario (*user*) al sistema, grupo y aplicaciones. En caso contrario, se comunicará con el supervisor informando sobre las correcciones necesarias.
3) El CSI le informará al supervisor sobre la creación de la cuenta y se comunicará con el usuario a quien le hará entrega de la forma INSTRUCCIONES PARA ACCESO AL SISTEMA (ver Anejo 2). Le indicará las aplicaciones a las que tiene acceso, le dará las instrucciones de cómo acceder al mismo y qué hacer en caso de requerir ayuda y le hará entrega del documento NORMAS Y REGLAMENTO DEL USO DE INTERNET Y CORREO ELECTRONICO DE AEMEAD (ver Anejo 3).

PO Box 194140
San Juan, PR 00919-4140 USA
(787) 724-0124 (787) 725-4244 fax
info@aemead.pr.gov
www.manejodeemergencias.pr.gov

El CSI revisará periódicamente los registros (*logs*) de las aplicaciones para detectar fallas en las aplicaciones o posibles violaciones de seguridad y otras situaciones que permitan identificar tendencias y necesiten remediarse.

C. *Parámetros de Seguridad de los Servidores para Control de Acceso a los Recursos de la Red*

Con el fin de controlar el acceso a los recursos de la red, el Oficial Principal de Informática fijará los siguientes parámetros de seguridad para los servidores de la AEMEAD:

1) Tiempo mínimo para Cambio de Contraseña (*Minimum Password Age*). El sistema requerirá un mínimo de 5 días para que el usuario pueda cambiar nuevamente la contraseña. Si por una situación excepcional necesita cambiarla antes de ese tiempo, deberá comunicarse con el CSI para que le autorice el cambio.
2) Forzar historial de contraseñas (*Enforce Password History*). La reutilización de contraseñas deja abierta la posibilidad de que alguien más pueda hacer uso de ella. El sistema requerirá un mínimo de seis contraseñas diferentes antes de volver a utilizar la misma.
3) Tiempo máximo para uso de Contraseña *(Maximum Password Age)*. Este parámetro determina el número de días que se podrá usar la contraseña antes de que el sistema le pida al usuario cambiarla. El sistema requerirá un máximo de 180 días.
4) Cantidad de caracteres requeridos para la contraseña (*Min password len*). El sistema requerirá un mínimo de ocho (8) caracteres.
5) Las contraseñas deben cumplir requerimientos de complejidad *(Password must meet complexity requirements*). Las contraseñas deberán ser una combinación de letras y números y no deberán contener parte de la identificación del usuario.
6) Intentos de acceso sin éxito a los recursos de la red (*Lockout after __ bad logon attempts*). El sistema deberá deshabilitar automáticamente las cuentas de acceso después de cinco (5) intentos fallidos de acceso a la red. En estos casos los usuarios tendrán que comunicarse con el CSI para habilitar nuevamente la cuenta.

Debido a la naturaleza de las funciones de la Agencia, no se aplicará la restricción de tiempo de acceso a la red (*Do not force logoff when logon hours expire*) para todas las cuentas conforme a las responsabilidades y las necesidades de servicios de cada usuario.

D. Aplicación de Políticas de Auditoría

Con el fin de monitorear la actividad en el sistema y detectar usos incorrectos y posibles ataques al sistema, los servidores de la red deberán tener definidas las políticas de auditoría (*Audit Policy*) para que el sistema produzca un registro cuando ocurran los siguientes eventos:

PO Box 194140
San Juan, PR 00919-4140 USA
(787) 724-0124 (787) 725-4244 fax
info@aemead.pr.gov
www.manejodeemergencias.pr.gov

VII. DEFINICIONES

Aplicaciones – Son sistemas compuestos por programación y bases de datos diseñados para automatizar funciones especificas de la Agencia. Ejemplo: sistemas de nóminas, sistema financiero.

Autenticación – Es el proceso por el cual una persona presenta información que lo identifica ante un sistema de información y el sistema compara la información contra su base de datos para validarla.

Autorización – Es el proceso por el cual se adjudican privilegios especificos a una persona para el uso de recursos en los sistemas de información.

Dominio – En un sistema, un proveedor de servicio (en nuestro caso la AEMEAD) que es un repositorio de la seguridad del mismo, permitiendo fácilmente la autenticación y autorización de usuarios con credenciales.

Servidor - Computadora central en un sistema de red que se encarga de prestar un servicio a otros computadoras (estaciones de trabajo) que se conectan a ella.

Usuario - Empleado de la agencia, contratista o voluntario que tiene acceso autorizado a los sistemas de la Agencia.

VIII. ANEJOS

1. MANEJO DE CUENTAS DE USUARIO
2. INSTRUCCIONES PARA ACCESO AL SISTEMA
3. NORMAS Y REGLAMENTO DEL USO DE INTERNET Y CORREO ELECTRONICO DE AEMEAD

PO Box 194140
San Juan, PR 00919-4140 USA
(787) 724-0124 (787) 725-4244 fax
info@aemead.pr.gov
www.manejodeemergencias.pr.gov

ANEJO 2

Centro de Sistemas de Información de la AEMEAD

INSTRUCCIONES PARA ACCESO AL SISTEMA

Fecha: _____

[Nombre del usuario]
[Dependencia]

Bienvenido a nuestro Sistema de Información

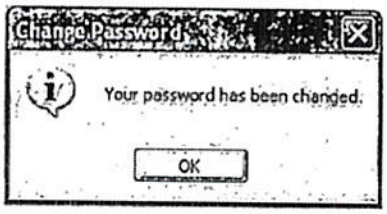
Su identificación de usuario (User Id) es _____
Y su contraseña (Password) temporera es: gobierno
Su correo electrónico es: _____

Al ser usuario de nuestro sistema está comprometido a velar por la seguridad y buen uso del mismo. Tan pronto como entre al sistema éste le pedirá cambiar su contraseña (password) para poder activar su cuenta. Deberá tener en cuenta las siguientes instrucciones:

1) Tan pronto como encienda su estación de trabajo aparecerá una pantalla con información de Normas Sobre el Uso de los Sistemas Electrónicos. Deberá leer detenidamente las mismas y tenerlas en cuenta en el desarrollo de sus labores en esta Agencia. Para continuar, deberá dar *click* donde dice **Si, Acepto**.
2) El sistema le desplegará entonces una pantalla para su identificación y autenticación en el sistema. Deberá tener en cuenta lo siguiente:
3) Su contraseña deberá tener por lo menos 8 caracteres y deberá ser una combinación de letras y números y no deberá incluir parte de su identificación de usuario.
4) Esa contraseña la podrá utilizar por un período de 180 días y 15 días antes de esa fecha cuando entre al sistema le informará que su contraseña *(password)* está por expirar y deberá cambiarla. Además, en cualquier momento que advierta que su contraseña puede haber sido descubierta, deberá cambiarla. Sin embargo, deberá tener en cuenta que no la podrá cambiar de nuevo antes de 10 días. Si por una situación excepcional necesitara hacerlo, deberá comunicarse con esta oficina. De no cambiar la contraseña dentro del período especificado el sistema inactivará automáticamente la cuenta y necesitará entonces comunicarse con el CSI para habilitar la cuenta nuevamente.
5) Para cambiar su contraseña, presione simultáneamente las teclas Ctrl, Alt y Delete con lo que le aparecerá una pantalla similar a la siguiente:

PO Box 194140
San Juan, PR 00919-4140 USA
(787) 724-0124 (787) 725-4244 fax
info@aemead.pr.gov
www.manejodeemergencias.pr.gov

nueva contraseña que va a utilizar. En el encasillado **Confirm New Password:** vuelva a escribir ese misma contraseña. Para terminar, haga *click* en **OK**. El sistema verificará que la información que usted ha escrito sea correcta y le desplegará entonces el siguiente mensaje:



Si no le aparece este mensaje y en su lugar aparece un mensaje de error, verifique que: 1) el teclado esté para escribir letras minúsculas, 2) ha entrado las contraseñas correctas. Tenga en cuenta que el sistema le pide escribir la nueva contraseña dos veces, 3) la contraseña tiene como mínimo 8 caracteres y son una combinación de letras y números, 4) no ha utilizado esa misma contraseña durante los últimos 6 meses.

Las instrucciones aquí dadas son las de autenticación para la entrada al sistema de la red de la AEMEAD. Para la utilización de una aplicación en particular, requerirá otro juego de usuario y contraseña que el supervisor de su área deberá solicitar y coordinar con el CSI.

Adjunto encontrará el Reglamento de Uso y Manejo de Sistemas. Se hace énfasis que todo usuario que detecte una situación que pudiera comprometer la seguridad del sistema deberá comunicarlo inmediatamente al Centro de Sistemas de Información.

Para cualquier información adicional que necesite, comuníquese con nosotros a las extensiones: 1170 o 1048.

Centro de Sistemas de Información

PO Box 194140
San Juan, PR 00919-4140 USA
(787) 724-0124 (787) 725-4244 fax
info@aemead.pr.gov
www.manejodeemergencias.pr.gov

ANEJO 3

NORMAS Y REGLAMENTO DEL USO DE INTERNET Y CORREO ELECTRONICO DE AEMEAD

TIG-008

Uso de Sistemas de Información, de la Internet y del Correo Electrónico

FECHA DE EFECTIVIDAD: 15 de diciembre de 2004

FECHA DE REVISIÓN: 12 de septiembre de 2007

TEMA: uso de sistemas de información, de la Internet y del Correo Electrónico

DESCRIPCIÓN

Esta política define y detalla el uso aceptable de la información que se maneja a través de los sistemas de información gubernamentales y las herramientas de Internet y Correo Electrónico, para así proteger al usuario y al gobierno de situaciones que pongan en peligro los sistemas y la información que contienen.

BASE LEGAL

Ley Núm. 151 del 22 de junio de 2004, conocida como Ley de Gobierno Electrónico, establece que la Oficina de Gerencia y Presupuesto tendrá la facultad para instrumentar, establecer y emitir la política pública a seguir y las guías que regirán la adquisición e implantación de los sistemas, equipos y programas de información tecnológica para los organismos gubernamentales con el objetivo primordial de lograr la interconexión de los organismos para facilitar y agilizar los servicios al pueblo. Asimismo, esta Ley establece que la Oficina de Gerencia y Presupuesto podrá establecer políticas a nivel gubernamental. Dicha Ley es aplicable a todas las agencias, organismos e instrumentalidades, tales como departamentos, juntas, comisiones, administraciones, oficinas y corporaciones públicas bajo el control de la Rama Ejecutiva, las cuales tienen el deber de cumplir con las políticas de manejo de información y los estándares tecnológicos relativos a la Informática emitidos por la Oficina de Gerencia y Presupuesto.

PO Box 194140
San Juan, PR 00919-4140 USA
(787) 724-0124 (787) 725-4244 fax
info@aemead.pr.gov
www.manejodeemergencias.pr.gov

2. La información desarrollada, transmitida o almacenada en los sistemas de información de las agencias es propiedad de la entidad gubernamental y del Estado Libre Asociado de Puerto Rico, por lo que le aplican todas las disposiciones legales aplicables a los documentos públicos. La divulgación de tal información sin autorización está estrictamente prohibida. La alteración fraudulenta de cualquier documento en formato electrónico conllevará las sanciones aplicables a la alteración fraudulenta de documentos públicos.

3. Los documentos generados o contenidos en los sistemas de información de las entidades gubernamentales serán parte de los expedientes oficiales de la entidad. La destrucción de tales documentos electrónicos estará sujeta a las sanciones aplicables a la destrucción de documentos públicos.

4. El titular de los derechos relativos a las creaciones de funcionarios gubernamentales o por encargo de éstos es el Estado Libre Asociado de Puerto Rico. Los usuarios de los sistemas de información están obligados a respetar los derechos de propiedad intelectual de los autores de las obras, programas, aplicaciones u otros, manejadas o accedidas a través de dicho sistema.

5. Los programas y recursos utilizados en los sistemas de información de las entidades gubernamentales deben tener su correspondiente licencia vigente o autorización de uso para poder ser utilizadas. Dichos programas sólo podrán ser instalados por personal autorizado a tales efectos. Además, no podrán instalarse programas sin la previa autorización del Departamento de Sistemas de Información, aunque sean programas libres de costos.

6. Los programas y aplicaciones contenidos en los sistemas de información no podrán reproducirse sin autorización o ser utilizados para fines ajenos a las funciones o poderes de la entidad gubernamental.

7. La correspondiente asignación de códigos de acceso no impedirá que el uso de los sistemas de información sea auditado por el personal autorizado por la agencia a tales fines, con el propósito de garantizar el uso apropiado de los recursos de la entidad gubernamental. Asimismo, los usuarios no deben tener expectativa de privacidad alguna con relación a la información almacenada en su computadora o que sea emitida o comunicada a través de los sistemas de información del Estado Libre Asociado de Puerto Rico.

8. El acceso a información o a una cuenta ajena sin autorización, obtenido mediante la modificación de privilegios de acceso o la interceptación de información en cualquier otra manera está prohibido, por lo que tal conducta se castigará conforme a la

PO Box 194140
San Juan, PR 00919-4140 USA
(787) 724-0124 (787) 725-4244 fax
info@aemead.pr.gov
www.manejodeemergencias.pr.gov

de privacidad alguna con relación a la información contenida en dichas cuentas. Las cuentas están sujetas a auditorias y revisiones sin previo aviso por el personal autorizado por la entidad gubernamental a tales efectos.

3- El correo electrónico podrá utilizarse únicamente para propósitos oficiales relativos a las funciones de la agencia. Se prohíbe el uso del mismo para asuntos no oficiales o actividades personales con fines de lucro o en menoscabo de la imagen de la entidad gubernamental o sus empleados. Los usuarios deberán velar por el cumplimiento de las normas aplicables al comportamiento los empleados de la entidad al momento de utilizar el correo electrónico.

CUMPLIMIENTO DE LA POLÍTICA

El no cumplir con las políticas relacionadas a los sistemas de información podría conllevar sanciones y/o la suspensión de los servicios recibidos.

Revisado: Lcda. Alfrida M. Tomey Imbert – Subdirectora Ejecutiva

Ernesto A. Pujols Molina – Oficial Principal de Informática

Lcda. Ileana Reyes Lora – Directora Recursos Humanos

Javier Rodríguez Castillo – Director Administración

PO Box 194140
San Juan, PR 00919-4140 USA
(787) 724-0124 (787) 725-4244 fax
info@aemead.pr.gov
www.manejodeemergencias.pr.gov