	Nombre	Cargo	Firma	Fecha
Elaborado	Omar Cruz Cabrera	Administrador de Redes		2007-02-07
Revisado	Lourdes Hernandez	Auditoria & Control		2011-06-09
Aprobado	Richard Santiago	Director Tecnologías de Información	10-9-2011	2011-06-09

Inicio Vigencia	2007-02-07
Ultima Revisión	2011-06-09
Próxima Revisión	2012-06-09

Se prohíbe la reproducción parcial o total de este documento sin la debida autorización.

Política de la Red de Comunicaciones ASEMNet

La Administración de Servicios Médicos de Puerto Rico (ASEM) es responsable de garantizar seguridad en su red *ASEMNet* y sus sistemas de computadoras en un grado razonable y económicamente factible en contra de acceso no-autorizado y/o abuso, mientras los hacemos accesibles para usuarios autorizados y legítimos. Esta responsabilidad incluye el informar a los usuarios de estándares de conducta esperados y las medidas disciplinarias por no asimilar las mismas. Cualquier atentado de violar las provisiones de esta política puede resultar en acción disciplinaria mediante revocación temporera de cuentas, sin importar el éxito o falla del atentado. Revocaciones permanentes pueden resultar mediante acciones disciplinarias tomadas por una junta de un panel jurídico llamado para investigar abusos en las redes de comunicaciones.

Los usuarios de la red *ASEMNet* son responsables de respetar y asimilar leyes locales, estatales, federales e internacionales. Cualquier atentado de violar esas leyes a través del uso de la red *ASEMNet* puede resultar en litigación en contra del ofensor por las autoridades apropiadas. Si este tipo de evento ha de ocurrir, ASEM cumplirá en su totalidad con las autoridades para proveer cualquier información necesaria para el proceso litigante.

Una vez el usuario recibe una cuenta (userID) a ser usada para acceder la red *ASEMNet* y los sistemas de computadoras en esa red, éste es completamente responsable por todas las acciones tomadas mientras utiliza esa cuenta (userID). Por lo tanto:

1.1 Solicitar una cuenta (userID) intencionalmente falsa es una ofensa con castigo disciplinario.
1.2 Compartir su cuenta (userID) con otra persona está prohibido. Si surge esto, usted será totalmente responsable por las acciones apropiadas por la otra persona.
1.3 Eliminar, examinar, copiar, o modificar archivos y/o data correspondiente a otros usuarios sin el consentimiento previo de estos está prohibido.
1.4 Atentados de evadir o cambiar las cuotas de los recursos está prohibido.
1.5 El continuo impedimento de otros usuarios mediante el acaparamiento de los recursos de los sistemas, luego de recibir notificación para que cese dicha actividad, está prohibido.
1.6 El uso de las facilidades y/o servicios para propósitos de re-venta está prohibido.

Se prohíbe la reproducción parcial o total de este documento sin la debida autorización.

1.7 Cualquier acción no-autorizada que perjudique o destruya un sistema de computadoras, altere el funcionamiento normal, o cause un mal funcionamiento es una violación sin importar la localización del sistema ni la duración.

Cuando envíe correo electrónico, su nombre y su cuenta (userID) están incluidos en el mensaje. Usted es responsable por todo el correo electrónico que se origine desde su cuenta (userID). Por lo tanto:

2.1 Falsificación (o atentado de falsificación) de mensajes de correo electrónico está prohibido.
2.2 Atentados de leer, eliminar, copiar, o modificar el correo electrónico de otros usuarios están prohibidos.
2.3 Atentados de, al enviar correo electrónico, hostigamiento, obscenidades y/o amenazas a otro usuario están prohibidos.
2.4 Atentados de, al enviar correo electrónico, mensajes de basura no-solicitados, o mensajes encadenados están prohibidos.

Como usuario de la red *ASEMNet*, usted puede estar permitido de acceder otras redes (y/o sistemas de computadoras conectados a esas redes). Por lo tanto:

3.1 El uso de sistemas y/o redes atentando a lograr acceso no-autorizado a sistemas remotos está prohibido.
3.2 El uso de sistemas y/o redes para conectarse a otros sistemas, evadiendo las limitaciones físicas del sistema remoto/local, está prohibido.
3.3 Descifrar las contraseñas del sistema o de los usuarios está prohibido.
3.4 El copiar archivos del sistema está prohibido.
3.5 El copiar materiales con derechos de autor, tales como programas/aplicaciones de terceros, sin el permiso escrito del autor o la licencia apropiada, está prohibido.
3.6 Atentados intencionales de quebrantar redes de computadoras o programas son ofensas con castigo disciplinario.
3.7 Cualquier atentado de asegurar un nivel alto de privilegio en sistemas de redes de computadoras son ofensas con castigo disciplinario.
3.8 Introducir voluntariosamente "viruses" de computadoras u otros programas destructivos en la red de computadoras *ASEMNet* o en redes de computadoras externas está prohibido.

Traducido y adaptado de Network Computing Policy
Wes Morgan y Arlene H. Rinaldi
asemnet\security\ncp.doc
last revision: 1/04

Se prohíbe la reproducción parcial o total de este documento sin la debida autorización.

Tecnologías de Información Gubernamental
Oficina de Gerencia y Presupuesto

TIG-008 Uso de Sistemas de Información, de la Internet y del Correo Electrónico

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.

ALCANCE
Esta política será aplicable a todos los organismos o instrumentalidades y entidades de la Rama Ejecutiva del Estado Libre Asociado de Puerto Rico, tales como departamento, juntas, comisiones, administraciones, oficinas, subdivisiones y corporaciones públicas, conforme a lo dispuesto en la Ley Núm. 151 del 18 de junio de 2004.

ACTUALIZACIÓN DE LA POLÍTICA
La Oficina de Tecnologías de Información Gubernamental de la Oficina de Gerencia y Presupuesto es responsable por la actualización de esta política.

POLÍTICA
La política pública del Estado Libre Asociado de Puerto Rico es facilitar y agilizar los procesos operacionales de los numerosos organismos de la Rama Ejecutiva, aumentar la eficiencia y efectividad en la prestación de los servicios gubernamentales al público y viabilizar la interconexión tecnológica entre los organismos y agencias. La automatización de los procesos operacionales requiere regular el uso apropiado de sus componentes y equipos e implantar las medidas necesarias para garantizar la confidencialidad de la información. Conforme a lo anterior, resulta necesario establecer las políticas necesarias para garantizar el uso adecuado, efectivo y seguro de los sistemas de información y las herramientas de trabajo que éstos proveen.

Esta política tiene el objetivo de fijar las normas fundamentales que deben regir los controles básicos a ser establecidos por las agencias de manera que se garantice el uso adecuado de los recursos relativos a los sistemas de información. Las agencias deben

Se prohibe la reproducción parcial o total de este documento sin la debida autorización.

promulgar políticas conforme al contenido de la presente política y velar por el cumplimiento de las mismas por parte de todo usuario de los sistemas de información del Estado Libre Asociado de Puerto Rico, incluyendo empleados, contratistas y otros autorizados a tal uso.

Normas generales aplicables al uso de los sistemas de información:

1. Cada entidad gubernamental será responsable de crear una política interna que regule el uso de los sistemas de información de la entidad, y de las herramientas de Internet y correo electrónico. En ésta se indicarán los usos permitidos, los no permitidos y las sanciones o medidas disciplinarias que se aplicarían a los usuarios que incumplieran con la misma. Asimismo, será responsabilidad de cada entidad particular notificar debidamente a los empleados del contenido de la misma. Los usuarios a su vez, firmarán un documento indicando que conocen la política y que cumplirán con ella.

2. Los sistemas de información de las entidades gubernamentales, incluyendo los programas, aplicaciones y archivos electrónicos, son propiedad del Estado Libre Asociado de Puerto Rico, por lo que deben constar en el inventario de las respectivas agencias y sólo pueden utilizarse para fines estrictamente oficiales y legales.

3. Cada entidad gubernamental debe colocar un aviso que indique al usuario o a quien acceda a su sistema de información que está accediendo a un sistema de información propiedad de esa entidad del Estado Libre Asociado de Puerto Rico y que se compromete a utilizarlo conforme a las normas establecidas.

4. Los sistemas de información y las herramientas asociadas, como el correo electrónico y la Internet, sólo podrán ser utilizados por personal debidamente autorizado. Será responsabilidad de cada entidad gubernamental definir las tareas que conllevan acceso a tal herramienta. El uso de tales recursos constituye un privilegio otorgado con el propósito de agilizar los trabajos de la entidad gubernamental y no es un derecho.

5. 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.

6. Es responsabilidad de cada entidad gubernamental tomar las medidas necesarias para salvaguardar la confidencialidad de los datos personales de los empleados o de los ciudadanos contenidos en sus sistemas de información, conforme a la legislación aplicable.

7. 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.

8. El titular de los derechos relativos a las creaciones de funcionarios

Se prohíbe la reproducción parcial o total de este documento sin la debida autorización.

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.

9. 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.

10. 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.

11. Cada entidad gubernamental será responsable de establecer las normas mediante las cuales se asignan las cuentas acceso, incluyendo las medidas de seguridad aplicables tales como: claves secretas (contraseñas), controles de acceso a los servidores y sistemas para auditar su uso, la integridad y la seguridad de los datos y comunicaciones que se envían. (Ver Política de Seguridad TIG-003). Los usuarios de los sistemas deberán cumplir con todas las normas de uso y las relativas a la seguridad de la información emitidas por la entidad gubernamental. Cada usuario será individualmente responsable por el manejo adecuado de los códigos de acceso o contraseñas asignadas.

12. 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.

13. 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 legislación local y federal vigente y a las normas aplicables que rigen la conducta de los empleados.

14. Cada entidad gubernamental será responsable de verificar que el Internet y el correo electrónico estén funcionando adecuadamente. También se asegurarán que la información contenida en dichos sistemas esté protegida de accesos no autorizados. La agencia utilizará sistemas de protección contra virus y sistemas de protección contra accesos no autorizados ubicados en Servidores de Seguridad de Computadoras y Redes (*firewall*). (Ver Política de Seguridad TIG-003).

15. Las normas aquí establecidas deben interpretarse como complementarias a las normas legales de ordinario aplicables. Las entidades gubernamentales del Estado Libre Asociado se reservan la facultad de comenzar los procesos

Se prohíbe la reproducción parcial o total de este documento sin la debida autorización.

administrativos, civiles o criminales pertinentes a los actos cometidos, aunque los mismos no estén expresamente prohibidos en este documento, si dichos actos, directa o indirectamente, ponen en riesgo la seguridad, integridad y confiabilidad de la información, el equipo y los sistemas de información de la agencia. Tanto estas normas como las emitidas al amparo de esta política en las respectivas entidades gubernamentales, serán revisadas y actualizadas periódicamente, por lo que es responsabilidad de la agencia notificar al usuario el contenido de las mismas. Cualquier violación a las normas puede conllevar la revocación de cualquier privilegio de uso de los sistemas de información y deberá ser notificada al Director del Departamento de Sistemas de Información, al Director del Departamento de Recursos Humanos y al supervisor del empleado.

Normas aplicable al uso de Internet:

1. Los sistemas de comunicación y acceso a la Internet son propiedad de la entidad gubernamental y deberán ser utilizados exclusivamente como una herramienta de trabajo conforme a las normas que rigen el comportamiento del personal de la entidad y nunca con fines no oficiales o para actividades personales o con fines de lucro.
2. Las operaciones realizadas a través de la Internet pueden generar responsabilidad por parte de las entidades gubernamentales del Estado Libre Asociado, por lo que los usuarios que tengan acceso al Internet a través de la entidad gubernamental no tienen expectativa de privacidad alguna con relación al uso y los accesos realizados a través de la Internet. La agencia se reserva el derecho a intervenir y auditar los accesos realizados por los usuarios a través de su sistema de información, el acceso a la Internet y el contenido de lo accedido.
3. La entidad gubernamental que provee acceso a la Internet no se responsabiliza por la validez, calidad, contenido o corrección de la Información contenida en la Internet.
4. Cada entidad gubernamental será responsable por velar que la conexión a la Internet se lleve a cabo conforme a la Política de Seguridad de la información y podrá monitorear el funcionamiento correcto de las mismas.
5. La publicación de información de la entidad gubernamental a través de la Internet deberá ser debidamente autorizada por el jefe de la agencia o la persona a quien éste delegue.

Normas aplicable al uso del correo electrónico:

1- El sistema de correo electrónico es propiedad de la entidad gubernamental y es parte íntegra de sus sistemas de información, por lo que la misma se reserva el derecho absoluto de intervenir, auditar e investigar para constatar el uso adecuado del mismo.

2- Las operaciones realizadas por medio del correo electrónico pueden generar

Se prohíbe la reproducción parcial o total de este documento sin la debida autorización.

responsabilidad por parte de las agencias del Estado Libre Asociado, por lo que los usuarios de las cuentas de correo electrónico no tienen expectativa 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.

4- Las entidades gubernamentales deberán establecer claramente una norma con relación a enviar por medio del correo electrónico documentos que contengan información confidencial de la agencia o que contengan información en los cuales se comenten asuntos internos de la agencia que no deben ser divulgados, conforme a las normas que rigen la conducta de los empleados. De ser necesario enviar tal información sensitiva, la misma deberá ser cifrada (*encrypted*) para evitar su divulgación. De sospecharse la interceptación o divulgación de tal información, se deberá informar al Departamento de Sistemas de Información inmediatamente, de manera que puedan tomar las medidas cautelares que procedan.

5- Cada agencia será responsable de establecer las normas mediante las cuales se asignan las cuentas de correo electrónico, incluyendo las medidas de seguridad aplicables, como son los códigos de acceso y las contraseñas, los controles de acceso al servidor, los sistemas para auditar el uso del sistema, la integridad y seguridad de los datos y las comunicaciones enviadas.

6- Las entidades gubernamentales deberán establecer claramente una prohibición con relación a obtener acceso no autorizado a las cuentas de correo electrónico, a leer, interceptar o revisar cualquier documento electrónico sin el consentimiento del remitente y del destinatario de la comunicación.

7- Durante horas laborables, los usuarios no podrán utilizar o acceder a cuentas de correo electrónico distintas a las cuentas oficiales de la agencia, a menos que estén autorizados a tal uso.

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.

EXENCIONES

Esta política aplica a todas las entidades gubernamentales detalladas en el alcance de esta política.

DEFINICIONES

Se prohíbe la reproducción parcial o total de este documento sin la debida autorización.

Agencia - Todos los organismos o instrumentalidades y entidades de la Rama Ejecutiva del Estado Libre Asociado de Puerto Rico, tales como departamentos, juntas, comisiones, administraciones, oficinas, subdivisiones y corporaciones públicas que estén bajo el control de dicha Rama.

Antivirus - Programa que protege a los sistemas de los ataques de virus conocidos.

Cifrar (encrypt) - Proceso en el cual los datos se convierten a un formato que no puede descifrarse fácilmente por personas no autorizadas a acceder los mismos.

Contraseña - Secuencia de caracteres que se utiliza para comprobar que el usuario que está requiriendo acceso a un sistema es realmente ese usuario.

Firewall (Servidor de Seguridad de Computadoras y Redes) - Conjunto de programas que protege los recursos de una red de accesos no autorizados.

Lenguaje discriminatorio - Expresiones que podrían percibirse como ofensivas, ya sea por razones de raza, sexo, origen, nacionalidad, orientación sexual, edad, impedimento, religión o ideales políticos.

Usuario - Empleado del gobierno o contratista que tiene acceso autorizado a los sistemas.

Virus- Programa de computadora cuyo fin es hacerle daño a la computadora donde reside.

ANEJOS
Ninguno

REFERENCIAS
Política de Seguridad (TIG-003)

Se prohíbe la reproducción parcial o total de este documento sin la debida autorización.

TIG-003 Seguridad de los Sistemas de Información

Esta política consiste de directrices generales que permitirán a las agencias establecer controles adecuados en sus sistemas electrónicos de información para garantizar la confidencialidad, la integridad y la disponibilidad de la información que manejan.

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.

ALCANCE
Estas políticas aplican a todas las agencias adscritas a la Rama Ejecutiva del Estado Libre Asociado de Puerto Rico.

ACTUALIZACIÓN DE LA POLÍTICA
El Área de Tecnologías de Información Gubernamental de la Oficina de Gerencia y Presupuesto es responsable por la actualización de estas políticas.

POLÍTICA
Toda agencia adscrita a la Rama Ejecutiva del Estado Libre Asociado de Puerto Rico deberá seguir las siguientes políticas de seguridad en sus sistemas de información. Los usuarios de los Servicios de la Red Interagencial que no sean agencias (i.e. municipios) están sujetos al cumplimiento de las secciones E, J y K de esta política para poder hacer uso de los Servicios de la Red Interagencial. Es responsabilidad de cada organismo el desarrollo y publicación de políticas y procedimientos aplicables para cumplir la política aquí delineada.

A. Análisis de Riesgos

1. Cada agencia deberá implantar controles que minimicen los riesgos de que los sistemas de información dejen de funcionar correctamente y de que la información sea accedida de forma no autorizada y/o maliciosa. Para ello deberá llevar a cabo análisis de riesgos:

a. Será necesario un inventario de activos de sistemas de información que incluya el equipo, los programas (ver sección de Definiciones) y los datos. Todos los activos deberán ser clasificados de acuerdo al nivel de importancia para la continuidad de las operaciones. En particular, los datos electrónicos deberán ser clasificados de acuerdo a su nivel de confidencialidad. Esto permitirá establecer qué es lo que se va a proteger.
b. Deberán identificarse las posibles amenazas contra los sistemas de información (i.e. robos, desastres naturales, fallas, virus, acceso indebido a los datos, etc.) junto con un análisis del impacto en las operaciones y la probabilidad de que ocurran esas amenazas.

Se prohíbe la reproducción parcial o total de este documento sin la debida autorización.

Esto permitirá establecer con qué se van a proteger los activos identificados anteriormente.

B. Continuidad de Negocios

1. El análisis de riesgo mencionado antes debe servir de base para desarrollar un Plan de Continuidad de Negocios que incluya un Plan para Recuperación de Desastres y un Plan para la Continuidad de las Operaciones.
2. Deberán existir procedimientos para tener y mantener una copia de resguardo (backup) recurrente de la información y de los programas de aplicación y de sistema (ver sección de Definiciones) esenciales e importantes para las operaciones.
3. Las facilidades de sistemas de información deberán estar colocadas en un área donde sea menor la probabilidad de daños por fuego, inundaciones, explosiones, disturbios civiles y otras formas de desastres.

C. Políticas de Seguridad Adicionales

1. Las políticas de seguridad de este documento son solo el fundamento para unas políticas más detalladas desarrolladas por cada agencia. Será responsabilidad de cada agencia el desarrollar políticas específicas de seguridad tomando en cuenta las características propias de los ambientes de tecnología de la agencia, particularmente sus sistemas de misión crítica. Las políticas desarrolladas por la Oficina de Gerencia y Presupuesto para su uso interno podrán ser utilizadas como modelos iniciales en el desarrollo de las políticas específicas de cada agencia.
2. Las políticas escritas en este documento no podrán ser invalidadas por las políticas particulares desarrolladas en cada agencia.

D. Leyes y Reglamentos

1. Las políticas y procedimientos de seguridad deberán estar de acuerdo a la legislación y los reglamentos vigentes.

E. Controles Generales

1. Las agencias deberán instalar controles automáticos para la prevención y detección de programas no deseados (i.e. virus, spyware, adware y updates automáticos).
2. La seguridad de la información deberá ser parte integral del diseño de cualquier programa de aplicación que se adquiera o desarrolle la agencia para facilitar las operaciones de la agencia y/o mejorar el servicio a los ciudadanos.
3. 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 (ver la sección de Definiciones).
4. Todos los mecanismos de autenticación deberán incluir una contraseña combinada de números y letras, no menor de seis (6) caracteres.
5. Los privilegios de acceso de los usuarios deberán ser reevaluados regularmente.
6. Deberán existir procesos que permitan monitorear las actividades de los usuarios en

Se prohíbe la reproducción parcial o total de este documento sin la debida autorización.

aquellos activos sensitivos que lo ameriten.
7. Si se va a disponer de equipo que contiene información sensitiva deberá hacerse de forma segura con un método que no permita acceder los datos una vez el equipo esté fuera de las facilidades de la Agencia.
8. Las agencias deberán tener los controles necesarios para evitar que de forma intencionada o accidental se inicien ataques desde sus redes internas hacia otros sistemas de información externos.

F. Personal

1. Cada agencia será responsable de tener el personal necesario ya sea interno o contratado para diseñar y mantener la seguridad de sus sistemas de información.
2. Las agencias establecerán controles en el reclutamiento del personal de sistemas de información, especialmente para el área de seguridad, de tal manera que se verifique su conocimiento en el área técnica y su reputación en el área profesional y firmarán acuerdos por escrito de no divulgación antes de exponerlo a datos confidenciales u otros activos sensitivos.
3. Deberán establecerse controles para el manejo de la terminación de empleados en la Agencia de tal manera que estas circunstancias no afecten la seguridad de la información ni de los sistemas. Para esto deberán establecerse procedimientos que incluyan una comunicación efectiva entre el área de Recursos Humanos, el área en que trabaja el empleado y el área de Sistemas de Información.

G. Manejo de Incidentes

1. Las agencias deberán desarrollar procedimientos para detectar, reportar y responder a incidentes de seguridad incluyendo límites para esos incidentes en términos de tiempo máximo y tiempo mínimo de respuesta.
2. Todos los empleados y contratistas deberán conocer los procedimientos para informar los diferentes tipos de incidentes.

H. Manejo de Cambios

1. La agencia es responsable de diseñar procedimientos que permitan que los cambios a la seguridad de los sistemas sean realizados y documentados adecuadamente y que esta documentación a su vez sea asegurada.

I. Adiestramientos

1. La agencia es responsable de proveer adiestramientos a toda la gerencia y los supervisores de la agencia para que estén al tanto de los controles de seguridad y los beneficios correspondientes.
2. El personal de sistemas de información y telecomunicaciones deberá estar adiestrado y con conocimientos actualizados sobre los aspectos de seguridad de sus áreas.
3. La agencia es responsable de crear mecanismos de capacitación para todos los empleados conozcan los procedimientos de seguridad que le apliquen.

Se prohibe la reproducción parcial o total de este documento sin la debida autorización.

J. Controles Físicos

1. El acceso a las facilidades de sistemas de información deberá estar controlado para que solamente el personal autorizado pueda utilizarlas.
2. Cualquier equipo usado fuera de la agencia deberá estar autorizado por la gerencia y deberá haber procedimientos para controlar su utilización.

K. Internet

1. La comunicación con Internet desde adentro de la agencia deberá estar controlada por un firewall (Servidor de Seguridad de Computadoras y Redes). Las agencias deberán desarrollar las políticas de uso de Internet y de correo electrónico y utilizar el firewall (Servidor de Seguridad de Computadoras y Redes) como uno de los mecanismos de control de esas políticas.
2. Si existe la necesidad de acceder a la red interna desde afuera de las facilidades de la Agencia (por ejemplo, para que un empleado realice un trabajo en un programa de aplicación desde Internet), deberán existir los controles de autenticación, autorización, confidencialidad, integridad y monitoreo necesarios para proteger los sistemas y la información.
3. Si se determina que hay datos sensitivos pasando a través de redes que no son seguras (como Internet o redes inalámbricas), se deberán tener los controles necesarios para garantizar la confidencialidad, como por ejemplo, el uso de encripción.
4. Toda agencia que desarrolle un programa de aplicación para brindar servicios de la agencia a los ciudadanos a través de Internet deberá asegurarse de que toma en cuenta los siguientes elementos de costos en su estudio de viabilidad para la implantación del programa:

a. Un diseño de seguridad.
b. La integración de mejores prácticas de seguridad en programación para evitar el acceso no autorizado y/o malicioso a través de Internet.
c. Un firewall (Servidor de Seguridad de Computadoras y Redes) que permita controlar el acceso al programa desde Internet.
d. Asegurar que si el servicio que está disponible maneja datos sensitivos sea instalado en una red alterna. En este caso el programa deberá funcionar en una red alterna y segura que permita el acceso desde Internet y a la misma vez permita un acceso controlado a la red interna para el intercambio controlado y monitoreado de datos.
e. Cerciorarse que si el servicio ofrecido a través de Internet maneja datos sensitivos existe implantado un sistema de detección de intrusos, de no ser así debe considerarse un elemento de costo (ver sección de Definiciones).

L. Servicios Suministrados por Contratistas

1. Es necesario mantener la seguridad de los sistemas de información aún cuando el manejo y el control de parte o de todos los procesos ha sido delegado a un tercero.
2. Los contratos hechos con terceros deberán incluir la salvaguarda de los activos sensitivos, especialmente cuando los servicios contratados incluyen el manejo de estos activos fuera de las facilidades de la Agencia.

Se prohíbe la reproducción parcial o total de este documento sin la debida autorización.

3. Si el servicio suministrado por terceros incluye que parte de los procesos corren en las facilidades de los contratistas deberán establecerse controles de mutuo acuerdo para proteger la información y estos acuerdos deberán ser parte del contrato.

EXENCIONES
Ninguna

DEFINICIONES
Adware - Es un programa que se instala inadvertidamente en una computadora y que su principal propósito es desplegar ante el usuario anuncios y propaganda pero también puede tener un comportamiento como el spyware.

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 específicos a una persona para el uso de recursos en los sistemas de información.

Confidencialidad - Es la característica que se le da a una información para que pueda ser vista solamente por personas autorizadas.

Datos sensitivos - Datos que contienen información financiera, de los ciudadanos, de los recursos humanos u otra información crítica para la operación de la agencia.

Encripción - Es el proceso por el cual unos datos se transforman en información no entendible por aquellos que no están autorizados a verlos.

Firewall (Servidor de Seguridad de Computadoras y Redes) - Aplicación, equipo o conjunto de ambos que protege los recursos de la red de accesos no autorizados. En el caso de las aplicaciones son programas que reside en una computadora o en un equipo especializado y que permiten controlar el tráfico de información entre varias redes. Tradicionalmente protegen la red interna de una entidad del acceso indebido de usuarios que vienen de Internet.

Integridad - Es el proceso que permite proteger información de alteraciones indebidas.

Programa - Conjunto de instrucciones que permite que una computadora lleve a cabo una función. Puede haber programas de sistema que controlan el funcionamiento de las computadoras y de las redes de informática y también programas de aplicación que facilitan y/o automatizan las operaciones de una entidad para que no tengan que ser llevadas a cabo de forma manual.

Sistema de Detección de Intrusos - Es un programa que reside en una computadora o en un equipo especializado y que permite detectar ataques o intentos indebidos de acceso

Se prohíbe la reproducción parcial o total de este documento sin la debida autorización.

hacia un sistema de información.

Seguridad de Informática - Protección de los sistemas de información en contra del acceso o modificación física o electrónica de la información; protección en contra de la negación de servicios a usuarios autorizados o de la disponibilidad de servicios a usuarios no autorizados; las políticas, normas, medidas, proceso y herramientas necesarias para detectar, documentar, prevenir y contrarrestar los ataques a la información o servicios antes descritos; los procesos y herramientas necesarias para la restauración de la información o los sistemas afectados por las brechas en la seguridad; disponibilidad y protección de los recursos requeridos para establecer dicha seguridad.

Spyware - Es un programa que se instala inadvertidamente en una computadora y que propaga sin autorización información sobre el usuario de la computadora y sus hábitos de utilización de Internet.

ANEJOS
Ninguno

REFERENCIAS
Ley de Gobierno Electrónico, Núm. 151 de 22 de junio de 2000

Se prohíbe la reproducción parcial o total de este documento sin la debida autorización.