TECNOLOGIAS DE INFORMACION GUBERNAMENTAL
OFICINA DE GERENCIA Y PRESUPUESTO

POLITICA NÚM. TIG-003

FECHA DE EFECTIVIDAD: 15 de diciembre de 2004
FECHA DE REVISIÓN: 12 de septiembre de 2007

TEMA: SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

DESCRIPCIÓN
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. 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 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.

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.

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 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 2004