

Estado Libre Asociado de Puerto Rico
Oficina del Contralor

5/2/09
Copia a todos
los directos del
Gobernador.
M.

Manuel Díaz Saldaña
Contralor

Carta Circular
OC-09-15

Año Fiscal 2008-2009
23 de enero de 2009

Gobernador, Presidente del Senado de Puerto Rico, Presidenta de la Cámara de Representantes, secretarios de Gobierno, directores de organismos de las tres ramas del Gobierno del Estado Libre Asociado de Puerto Rico, alcaldes, presidentes de corporaciones municipales, directores ejecutivos de consorcios y auditores internos

Asunto: Sugerencias para establecer un programa para la divulgación al personal de las normas y los procedimientos de seguridad de la información

Estimados señores y señoras:

La información es considerada actualmente como uno de los activos más valiosos e importantes con que cuentan las organizaciones para cumplir cabalmente con su misión y para la consecución de las metas establecidas. Los procedimientos creados para la seguridad de la información buscan proteger los activos de informática de una pluralidad de posibles amenazas. Dichas amenazas se extienden desde aquellas creadas por personas inescrupulosas destinadas a explotar las vulnerabilidades de los sistemas, hasta aquellas de fuerza mayor, como son los desastres naturales. Mediante estos procedimientos podemos asegurar, entre otros, la continuidad de los servicios, minimizar la pérdida de información, mitigar los posibles daños a las operaciones, maximizar los beneficios de la inversión y poder garantizar el servicio a los ciudadanos en todo momento. Para lograr que efectivamente la información esté protegida, es necesario la implantación de controles adecuados tales como: políticas internas, reglamentos y procedimientos, la aplicación de mejores prácticas, y el establecimiento de una estructura organizacional dirigida a la protección de los activos de informática.

Reconociendo la necesidad de que cada entidad gubernamental, establezca un programa para la divulgación de normas y procedimientos de seguridad de información, y de cumplir con las guías establecidas en la **Ley Núm. 151 del 22 de junio de 2004, Ley de Gobierno Electrónico**, según enmendada, más adelante se incluyen unas sugerencias para la implantación del mismo.

Un programa bien diseñado para la divulgación de las normas y los procedimientos de seguridad debe estar, primeramente, encaminado a crear conciencia de los riesgos a los cuales están expuestos los sistemas de información, y luego a desarrollar actitudes prácticas en los empleados y en los funcionarios de una organización con el fin de promover la protección tanto de los activos físicos como los de la información. Estos en conjunto, nos sirven para estar alertas y reconocer las posibles situaciones donde existe el potencial de hurto, daño o uso indebido, ya sea deliberado o de forma accidental, de la información almacenada en los sistemas electrónicos de la organización. La concienciación de los riesgos y las salvaguardas disponibles son las primeras líneas de defensa que se utilizan en la seguridad de los sistemas de información y de las redes de comunicación gubernamentales.

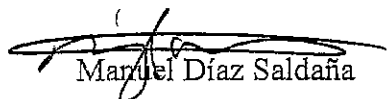
En nuestras auditorías realizamos pruebas para determinar si se han establecido normas y procedimientos para salvaguardar la información y que se haya implantado un programa para la divulgación de las normas y los procedimientos de seguridad de información a todos los empleados y los funcionarios de las entidades gubernamentales.

En el **Anejo** les ofrecemos varios elementos y aspectos que deben ser tomados en consideración antes de implantar un programa para la divulgación de normas y procedimientos entre los empleados y los funcionarios, que ayude a la protección de la información.

Estamos a sus órdenes para ofrecerles cualquier información adicional que estimen necesaria. Al respecto, pueden comunicarse con la Sra. Lourdes Díaz Valcárcel, Directora de la División de Auditorías de Tecnología de Información, al (787) 294-0286.

Contamos con su cooperación para mejorar la fiscalización y la administración de la propiedad y de los fondos públicos.

Cordialmente,


Manuel Díaz Saldaña

Anejo

ASPECTOS A CONSIDERAR AL ESTABLECER UN PROGRAMA PARA DAR A CONOCER LAS NORMAS, LOS PROCEDIMIENTOS Y LAS MEDIDAS DE SEGURIDAD DE LA INFORMACIÓN

1. El factor humano

Una de las principales amenazas que enfrenta toda organización para proteger su información es el factor humano. A pesar de todos los esfuerzos que realiza una entidad gubernamental en la implantación de la seguridad de la información, éstos pueden ser pasados por alto por errores tales como, una configuración errónea, una mal interpretación o acciones mal intencionadas. Esto debido, entre otras razones, a que no hubo una divulgación adecuada, ni hubo adiestramientos efectivos para los empleados y los funcionarios sobre la responsabilidad en el trabajo para conservar la seguridad de la información.

Los estudios demuestran que el 75 por ciento de los incidentes de seguridad son causados por errores o por desconocimiento humano¹. Una agencia o entidad gubernamental, debe tener en cuenta que sus sistemas, las redes de interconexión y sus aplicaciones no estarán seguros hasta que todos sus empleados hayan sido debidamente adiestrados e informados sobre la importancia de la seguridad, sus roles y sus responsabilidades en la implantación de las medidas y de una infraestructura de seguridad en la entidad gubernamental.

2. El compromiso de la gerencia

El compromiso de la alta gerencia con respecto a la implementación de las iniciativas de la seguridad de la información es otro de los elementos críticos para el éxito de un programa de seguridad. Esto conlleva la integración de la seguridad en las operaciones estratégicas y administrativas de la agencia o entidad. Los administradores y directores ejecutivos son los responsables de:

- Establecer normas y procedimientos de acuerdo con las metas y las prioridades, por cada área, conforme a la Misión de la entidad gubernamental.
- Preparar un programa de seguridad de la información en la entidad gubernamental. Éste, deberá incluir, entre otros, la divulgación de normas de uso y protección de los sistemas computadorizados y de la información.
- Asegurar que la entidad gubernamental cuente con los recursos humanos, tecnológicos y económicos necesarios para apoyar y mantener el programa de seguridad de información.

¹ "The Human Factor", Maris, K. (2005).

3. **La Ley de Gobierno Electrónico y la Carta Circular Núm. 77-05²**

La **Ley Núm. 151 del 22 de junio de 2004, Ley de Gobierno Electrónico (Ley Núm. 151)**, según enmendada, establece que, entre las funciones de la Oficina de Gerencia y Presupuesto (OGP) se encuentra el desarrollar una estructura que garantice la efectividad de los controles relacionados con la seguridad de los sistemas de información que apoyan las operaciones y los activos gubernamentales. Además, entre sus facultades se encuentran, el poder establecer las políticas de seguridad en el ámbito gubernamental sobre el acceso, uso, clasificación y custodia de los sistemas de información, y las políticas dirigidas a garantizar la privacidad y protección de la información personal con relación al uso de la Internet.

Mediante la **Ley Núm. 151**, las entidades gubernamentales son las responsables de impartir las instrucciones necesarias para asegurar el cumplimiento de la **Ley** y de las normas que se emitan de conformidad con la misma. De esta manera, se asegura que las políticas gerenciales de manejo de información y las guías que bajo dicha **Ley** emita la OGP, sean divulgadas al personal correspondiente de manera rápida y efectiva. Además, para asegurar que la estructura de las respectivas áreas de sistemas de información de cada agencia, están diseñadas de manera que sean las encargadas o responsables de implementar las políticas de manejo de información y las guías sobre el particular que emita la OGP.

Entre los derechos de los ciudadanos del Estado Libre Asociado de Puerto Rico, está el que los servicios gubernamentales que se ofrezcan por medios electrónicos sean brindados de manera armonizada con las disposiciones aplicables relativas a la protección de la privacidad, a la seguridad de la información, a las políticas de disponibilidad de información y a las garantías de acceso a las personas con impedimentos.

Por otra parte, en la **Política Núm. TIG-003, Seguridad de los Sistemas de Información³**, se establece, entre otras cosas, que las entidades gubernamentales son responsables de:

- Proveer adiestramientos a toda la gerencia y a los supervisores de la entidad gubernamental para que estén al tanto de los controles de seguridad y los beneficios correspondientes.
- Asegurarse de que el personal de sistemas de información y de telecomunicaciones esté adiestrado y con conocimientos actualizados sobre los aspectos de seguridad de sus áreas.
- Crear mecanismos de capacitación para que todos los empleados conozcan los procedimientos de seguridad que le apliquen.

² Carta Circular Núm. 77-05, Normas sobre la Adquisición e Implantación de los Sistemas, Equipos y Programas de Información Tecnológica para los Organismos Gubernamentales del 8 de diciembre de 2004. En dicha Carta Circular se hace referencia a las políticas TIG, sobre diversos asuntos de tecnologías de información.

³ Véase la nota alcance 2.



Además, se establece que será responsabilidad de cada entidad gubernamental 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. Ello implica que, como norma de sana administración, se deben establecer por escrito normas, procedimientos y políticas de control interno eficaces que reglamenten las operaciones computadorizadas y estén aprobadas por la alta gerencia. Mediante las mismas, se logran definir los niveles de control que deben existir en las distintas áreas.

El establecimiento de normas y procedimientos facilita la labor de adiestramiento del personal de nueva selección o de poca experiencia en determinadas áreas de trabajo. Las políticas de seguridad deben asegurar el cumplimiento con las leyes y los reglamentos, y con la integridad, confidencialidad y disponibilidad de los datos. Además, deben estar actualizadas para reflejar los objetivos de la agencia y los estándares y las prácticas generalmente aceptadas en el área de la seguridad. Éstas, deben ser distribuidas a los empleados, contratistas, suplidores y visitantes correspondientes⁴.

De manera similar, en la **Política Núm. TIG-008, Uso de Sistemas de Información, de la Internet y del Correo Electrónico de la Carta Circular Núm. 77-05**, se establece, entre otras cosas, que 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 electrónico⁵. En la misma se indicarán los usos permitidos y las sanciones o medidas disciplinarias que se aplicarán a los usuarios que incumplieron con la misma.

4. Programa para dar a conocer las normas, los procedimientos y las medidas de seguridad de la información

Un programa para la divulgación de normas y procedimientos de seguridad bien diseñado, debe estar primeramente encaminado, a **crear conciencia** del uso apropiado y de los riesgos a los cuales están expuestos los sistemas de información y los usuarios. Esto, con el propósito de desarrollar actitudes prácticas en los usuarios y en los funcionarios de una organización con el fin de promover la protección tanto de los activos físicos como de la información. La concienciación permite estar alerta y reconocer las posibles situaciones donde existe el potencial de hurto, de daño o de uso indebido, ya sea deliberado o de forma accidental, de la información almacenada en los sistemas electrónicos de la organización. **Es por tanto, la primera línea de defensa que se utiliza en la seguridad de los sistemas de información y de las redes de interconexión gubernamentales.**

⁴ La Política Núm. TIG-003, establece que será responsabilidad de cada entidad gubernamental 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.

⁵ La TIG-008 fue revisada por la OGP en septiembre de 2007.

Es necesario que todos los empleados, contratistas, suplidores y visitantes que utilicen los sistemas de información de la agencia o entidad gubernamental participen en el proceso de concienciación. La concienciación se logra mediante el uso de técnicas tales como: consignas o lemas, recordatorios mediante el uso del correo electrónico, pantallas de advertencias, vídeos o carteles, auditorías internas de seguridad, y orientaciones periódicas. Un programa de concienciación debe ayudar a contestar las siguientes preguntas:

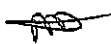
- **¿Podrán identificar los empleados, la comisión de una violación de la seguridad y las consecuencias de tal acción?**
- **De ocurrir una violación de seguridad y poderse identificar la misma, ¿conocerán qué hacer y a quién deben llamar?**

Este tipo de programa debe realizarse de manera periódica y continua. Las orientaciones deberán ofrecerse por lo menos una vez al año. Se trata de lograr que los participantes entiendan como funciona la seguridad en su ambiente de trabajo, a la vez de que se conozca el propósito de tales normas y procedimientos.

a. La estructura de un programa de divulgación

1) Concienciación

- El personal ejecutivo de la entidad se beneficiaría de una orientación básica sobre la seguridad de los activos y sobre las ganancias o pérdidas asociadas con la seguridad de la información. Para dicho nivel de la gerencia, es importante conocer como integrar la seguridad de la información y sus políticas. Además, conocer como, la falta de seguridad de la información pudiera afectar la imagen de la agencia y las pérdidas asociadas en los casos que ocurren fallas en la misma. El personal ejecutivo de la entidad es el que deberá motivar y ser ejemplo para guiar al resto de la agencia a apoyar la seguridad y tomar conciencia de su importancia. Dentro de ese grupo, se encuentra el personal gerencial, el cual se beneficiaría de una orientación más específica y detallada de las políticas, las normas y los procedimientos, y como aplican a su correspondiente departamento.
- El personal técnico de la entidad deberá recibir un adiestramiento más específico y detallado sobre las configuraciones técnicas de los equipos, el manejo de incidentes y las indicaciones de las posibles amenazas de seguridad, para que puedan ser identificados apropiadamente y a tiempo.
- Los usuarios necesitan entender porque la seguridad es importante para ellos individualmente y para su agencia o entidad gubernamental. Éstos deben entender como actividades no autorizadas ni seguras pudieran afectar sus tareas diarias. Las orientaciones deben incluir ejemplos de actividades autorizadas y las que no lo son con respecto a la seguridad de la información. Los usuarios deben conocer y entender plenamente lo que se espera de ellos según indicado en las normas, en las políticas y en los procedimientos y el efecto de no cumplir con los mismos. Se recomienda que cada empleado firme un documento



indicando que ha sido orientado sobre las normas, las políticas y los procedimientos. Además, que entienda los mismos y las medidas disciplinarias aplicables en el caso de no cumplir con éstos.

- El contenido de las orientaciones debe incluir, entre otros, los siguientes temas:
 - ✓ Normas sobre el uso adecuado de los sistemas de información
 - ✓ Protección de las contraseñas y la producción de respaldos
 - ✓ Programación computadorizada del crimen: *Malware*, *phishing*, entre otros
 - ✓ Manipulación y engaño (*social engineering*)

2) **Adiestramientos en seguridad de tecnología de información**

La diferencia más significativa entre la concienciación y el adiestramiento es que este último busca enseñar destrezas que permiten a una persona realizar una acción específica y pertinente para lograr los objetivos de la seguridad. La concienciación busca enfocar la atención del individuo sobre uno o varios temas relacionados con la seguridad de los sistemas de información. Un ejemplo del adiestramiento, es un curso de seguridad de tecnología de información para los administradores de seguridad que incluya temas como los controles gerenciales, los operacionales y los técnicos que se deben implantar para proteger el sistema de información de la agencia o entidad gubernamental.

b. **Las fases de un programa de divulgación de normas y procedimientos de seguridad**

Las fases son cuatro, según se indica:

- **Diseño del programa para la divulgación y adiestramientos:** La agencia o entidad gubernamental prepara un análisis de necesidades, y desarrolla y aprueba una estrategia de adiestramientos sobre el tema de la seguridad de los sistemas de información.
- **Preparación de los materiales para la divulgación y el adiestramiento:** Se enfoca en la disponibilidad de fuentes de adiestramientos, en el alcance, en el contenido y en el desarrollo de los materiales de adiestramientos. Se debe asegurar que los instructores y los orientadores están capacitados para ofrecer los mismos.
- **Implantación del programa:** Esta fase se realiza mediante una comunicación efectiva y el lanzamiento del programa y los correspondientes adiestramientos. Además, se debe llevar un registro de los participantes de los adiestramientos y monitorear el cumplimiento con los requisitos de horas de adiestramiento por empleado.

~~AD~~

- **Evaluación del programa:** Provee guías para mantener el programa actualizado y para monitorear su efectividad. Para evaluar la efectividad del programa, se pueden utilizar, entre otros, los siguientes métodos: encuestas, evaluaciones y entrevistas a usuarios.

5. **Otra disposición relevante**

Para lograr una sana administración pública de excelencia, es importante mantenerse al día con los avances tecnológicos y utilizarlos para lograr mayor efectividad y eficiencia en las operaciones y en los servicios que se prestan a los clientes y a la ciudadanía en general. Es por eso, que recomendamos utilizar como referencia el folleto informativo - **Las Mejores Prácticas para la Adquisición, Desarrollo, Utilización y Control de la Tecnología de Información**. El mismo fue emitido por esta Oficina mediante la **Carta Circular OC-06-17** del 27 de enero de 2006, disponible en nuestra página de Internet: <http://www.ocpr.gov.pr>.



mz/1000
1/2/2005
1000