Introducción:

El manejo y administración de información en toda organización constituye una de las funciones más relevantes de un departamento de sistemas de información, y por lo tanto, la seguridad de la misma es considerada como un elemento crítico en el desempeño de esta función. Tomando en cuenta la naturaleza de negocio del Banco Gubernamental de Fomento para Puerto Rico (Banco) la seguridad de los recursos e infraestructura de sistemas de información cobra mayor trascendencia, por lo que es primordial el implantar medidas y controles de seguridad que minimicen los riesgos y accesos no autorizados.

El Departamento de Sistemas de Información (Departamento) juega un papel protagónico y es responsable de administrar los recursos del Banco y asegurar el uso correcto de los mismos. Por tal razón, el Departamento deberá ejecutar medidas y controles de seguridad como administrador de los recursos de los sistemas de información para mitigar los riesgos y salvaguardar la integridad de la información del Banco.

Propósito y Alcance:

Esta política tiene como propósito primordial definir y establecer las directrices y parámetros mínimos de seguridad por parte del Departamento en el manejo y administración de la información de los sistemas. El alcance de la política aplica a toda administración, manejo y procesamiento de información que pertenezca al Banco.

Aspectos Fundamentales:

1. El Departamento de Sistemas de Información es responsable de implantar, y promover el cumplimiento de los controles y medidas de seguridad necesarias para minimizar los riesgos de accesos no autorizados, pérdidas de información y asegurar el funcionamiento adecuado de la infraestructura y la integridad de la información contenida en ella.

2. Es política del Banco el mantener la confidencialidad de los estándares técnicos de los sistemas de información con el propósito de salvaguardar la integridad de las medidas de seguridad establecidas en los mismos.

3. El Departamento tendrá la responsabilidad sobre todos los datos, aplicaciones, equipo e infraestructura de los sistemas de información del Banco. Esto excluye a los sistemas adquiridos y administrados independientemente por otros departamentos del Banco.

Seguridad en el Centro de Cómputos:

4. El Centro de Cómputos deberá ser un área de acceso restringido. Solamente personal debidamente autorizado tendrá acceso al Departamento de Sistemas de Información. Aquellas personas que necesiten operar, supervisar o proveer mantenimiento a las facilidades o equipos del Centro de Cómputos, tendrán acceso por medio de una llave magnética que cuya configuración de acceso es por el Oficial de Seguridad Física. Personas que no tengan acceso mediante la llave magnética que debe firmar una hoja de entrada y salida cada vez que ingresen o salgan del área.

El Centro ...

Seguridad en el Centro de Cómputos (cont.):

5. El Centro de Cómputos deberá contar con un sistema alterno de generación de energía, el cual deberá estar conectado a la toma principal de corriente del edificio. Sistemas de baterías o "UPS" son requeridos para evitar cualquier interrupción del servicio eléctrico. Además, es necesario tener una planta de generación de energía disponible para poder proveer energía a los sistemas de aire acondicionado, luces y demás, en caso de emergencia.

6. El Centro de Cómputos deberá tener sus propias unidades de aire acondicionado, independientemente de si existe en el edificio un sistema de aire acondicionado central.

7. Todo material utilizado en construcciones en las facilidades del Centro de Cómputos deberá ser a prueba de fuego. Además, el Centro de Cómputos deberá ser habilitado con sistemas automáticos de detección y extinción de fuego que disminuyan las posibilidades de un incendio.

8. No se hará pública la localización del Centro de Cómputos por medio de carteles ni señales con el propósito de mantener un perfil bajo de la ubicación del Centro de Cómputos.

9. El Centro de Cómputos no deberá estar localizado en un área inundable.

10. Diariamente, se harán copias de resguardo ("backup") de todos los datos contenidos en los sistemas de información, incluyendo los servidores y el computador principal ("mainframe"), según el "Procedimiento de Manejo de Copias de Resguardo en la Red" MSI-301-03 y el "Procedimiento de Manejo de Copias de Resguardo en el Computador Central" MSI-301-02.

11. Es política del Banco realizar pruebas anuales del Plan de Recuperación de Desastres ("Disaster Recovery Plan", "DRP"), para asegurar la ejecución eficiente del mismo en caso de alguna emergencia. Estas pruebas deberán llevarse a cabo siguiendo las directrices establecidas en el "Procedimiento de Pruebas del Plan de Recuperación de Desastres" MSI-410-02.

Seguridad en Aplicaciones de Sistemas:

12. El Departamento de Sistemas de Información es responsable de segregar y mantener los siguientes ambientes de sistemas de información:

- **Ambiente de Desarrollo**. Ambiente donde se programarían o se daría mantenimiento a aplicaciones desarrolladas internamente.

- **Ambiente de Prueba**. Ambiente donde se probarían cambios o nuevos desarrollos de aplicaciones, simulando condiciones reales.

- **Ambiente de Producción**. Ambiente donde residirían las aplicaciones debidamente probadas. En este ambiente se ejecutan las operaciones diarias del Banco.

Toda aplicación ...

Seguridad en Aplicaciones de Sistemas (cont.):

13. Toda aplicación adquirida o desarrollada internamente que pase al ambiente de producción del Banco deberá ser validada previamente tomando en cuenta el alcance y los componentes de la aplicación. Dicha validación deberá ser debidamente documentada de acuerdo a la "Política de Desarrollo de Aplicaciones" MSI-101-01.

14. Todo desarrollo o adquisición de aplicaciones que apoyen funciones sensitivas y/o principales para el Banco deben ser comprobadas y validadas adecuadamente contra violaciones a la seguridad en el sistema. Estas deberán poseer un control de acceso que requiera la identificación de usuario y contraseña, independiente al control de acceso al "network" del Banco. Dicha validación deberá incluir los procesos de actualización de la aplicación en forma de "patches" para prevenir problemas conocidos o publicados en la seguridad de la aplicación.

15. Toda restauración de datos y/o aplicaciones en el sistema, dentro del ambiente de producción, deberá ser aprobada por el Director del Departamento y notificada al Asesor Principal de Informática y al Oficial de Seguridad de Acceso a Sistemas de Información antes de ejecutar la misma, siguiendo los lineamientos establecidos en el "Procedimiento de Manejo de Copias de Resguardo en la Red" MSI-301-03 y en el "Procedimiento de Manejo de Copias de Resguardo en el Computador Central" MSI-301-02, según apliquen. Además, previo a este proceso, se hará una copia transitoria de los datos o la aplicación vigente con el propósito de investigación o restauración posterior de la misma si la restauración en proceso no es exitosa.

16. La depuración de archivos ("purge") tanto de documentos oficiales y bases de datos que residan en los servidores y en aplicaciones se llevará a cabo mensualmente, según se establece en el "Procedimiento de Depuración de Archivos en la Red" MSI-301-06 y en el "Procedimiento de Depuración de Datos en Aplicaciones" MSI-301-07. Esto excluye al espacio en el "network" que se le asigna a cada usuario, ya que es su responsabilidad el manejo de dicho recurso.

17. El Departamento deberá revisar periódicamente la nueva tecnología disponible y mantenerse informado de nuevos mecanismos de control, así como de tecnología que es utilizada por "hackers" para violentar la seguridad de los controles.

Seguridad en Bases de Datos:

18. La administración, seguridad e integridad de toda base de datos recae bajo responsabilidad de la División de Administración de Datos, siguiendo las guías establecidas en el "Procedimiento de Mantenimiento de Base de Datos" MSI-220-07, el "Procedimiento de Control y Acceso de la Base de Datos" MSI-220-06, y el "Procedimiento de Seguridad en la Base de Datos" MSI-220-05.

19. En la medida que sea posible y siempre que la base de datos contenga información confidencial, deberá mantenerse la base de datos en un servidor dedicado ("Data Server") distinto al que contiene la aplicación que permite su manejo ("Application Server").

El diseño ...

Seguridad en Bases de Datos (cont.):

20. El diseño de cualquier base de datos que resida en el ambiente de producción de los sistemas del Banco deberá estar de acuerdo a los estándares vigentes establecidos, al "Procedimiento de Diseño de Base Datos" MSI-220-01, y poseer toda documentación necesaria.

Seguridad en PC's y Estaciones de Trabajo:

21. Los programas de antivirus en todas las estaciones de trabajo deberán ser actualizados con las definiciones nuevas de antivirus según sean provistos por el vendedor del programa, de acuerdo a los lineamientos establecidos en el "Procedimiento de Actualización de Programas Antivirus" MSI-311-01. (Corroborar con los procedimientos)

22. Todo movimiento de equipo de sistemas de información deberá ser autorizado por la División de Apoyo Técnico del Departamento y será notificado a la División de Servicios Administrativos y Seguridad del Banco, según el "Procedimiento de Control de Inventario de Equipo" MSI-313-01.

23. El Departamento es responsable de evaluar y eliminar toda información contenida en cualquier equipo de sistemas que se requiere disponer. Además, deberán identificar cualquier tipo de información que requiera ser salvaguardada.

Instrucciones Especiales:

Esta política deroga las políticas MPA-0490-03 y MPA-0490-03A que fueron aprobadas el 22 de mayo de 1995, y la política MPA-0490-01 que fue aprobada el 31 de octubre de 1994.

oOo