ESTADO LIBRE ASOCIADO DE
PUERTO RICO
Banco Gubernamental de Fomento
para Puerto Rico

POLÍTICA DE MANEJO DE LA SEGURIDAD

DE SISTEMAS DE INFORMACIÓN

2016

BGF
BANCO GUBERNAMENTAL DE FOMENTO PARA PUERTO RICO

I. Introducción:

El manejo y administración de información en toda organización constituye una de las funciones más relevantes del Departamento de Sistemas de Información (Departamento) 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 transcendencia, por lo que es primordial implantar medidas y controles de seguridad que minimicen los riesgos y accesos no autorizados.

El Departamento juega un papel protagónico y es responsable de administrar los recursos de los sistemas de información 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.

II. Propósito y Alcance:

La presente 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. Esta política aplica a toda administración, manejo y procesamiento de información que pertenezca al Banco. También aplica a todo empleado y contratista que usa y maneja los sistemas de información del Banco. La violación a las disposiciones de esta política puede conllevar la revocación de los privilegios de utilizar los sistemas del Banco y/o aplicación de medidas disciplinarias, según apliquen.

III. Términos/Acrónimos:

- Información Sensitiva – data que podría tener un impacto significativo en las operaciones del negocio, estatus financiero o imagen pública si es diseminada sin autorización.

- Cifrada ("Encrypted") - acción de proteger información para que no pueda ser leída sin una clave.

IV. Política:

Aspectos Fundamentales

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

2. El Departamento tendrá la responsabilidad sobre todos los datos, aplicaciones, equipo e infraestructura de los sistemas de información del Banco.

Seguridad en el Centro de Cómputos

1. El Centro de Cómputos deberá ser un área de acceso restringido. Solamente personal debidamente autorizado tendrá acceso al Departamento.

   a) El personal autorizado que necesite operar, supervisar o proveer mantenimiento a las facilidades o equipos del Centro de Cómputos, tendrá acceso por medio de una llave magnética, cuya configuración de acceso será otorgada por el Oficial de Seguridad Física.
   b) El personal no autorizado al Centro de Cómputos, deberá firmar en la hoja de registro indicando la hora de entrada y salida, cada vez que ingrese o salga del área, según establece el procedimiento "Control de Acceso al Centro de Cómputos" MSI-400-04.

2. 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. Como parte de este sistema alterno, se requiere la disponibilidad de sistemas de baterías o "UPS", 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 acondicionamiento de aire, luces y demás, en caso de emergencia.

3. El Centro de Cómputos contará con sistemas de monitorización para medir y regular la temperatura y humedad, fuente de energía, supresión contra incendio detector o medidor de vibraciones, y los Sistemas de Alimentación Ininterrumpida.

4. El Centro de Cómputos deberá tener sus propias unidades de acondicionamiento de aire, independientes al sistema de acondicionamiento de aire del edificio donde está localizado.

5. Todo material utilizado en construcciones en las facilidades del Centro de Cómputos deberá ser resistente al 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.

Seguridad en el Centro de Cómputos (cont.)

6. 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 mismo.

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

Respaldos

1. Diariamente, se harán copias de resguardo ("backup") de todos los datos contenidos en los sistemas de información incluyendo los servidores, según se establece en el procedimiento "Manejo de Copias de Respaldo" MSI-301-03.

Plan de Recuperación de Desastres

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

Manejo de Aplicaciones

1. El Departamento es responsable de segregar y mantener los siguientes ambientes de sistemas de información, para asegurar que sólo se lleva a producción las versiones de programas que hayan sido probadas apropiadamente:

   a) **Ambiente de Desarrollo** – Ambiente donde se programarían o se daría mantenimiento a aplicaciones desarrolladas internamente.
   b) **Ambiente de Prueba** – Ambiente donde se probarían cambios o nuevos desarrollos de aplicaciones, simulando condiciones reales. Este ambiente debe estar separado de los ambientes de desarrollo y producción.
   c) **Ambiente de Producción** – Ambiente donde residirían las aplicaciones debidamente probadas y donde se ejecutan las operaciones diarias del Banco. Dicho ambiente está bajo la custodia de la División de Operaciones Técnicas.

2. 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 realizada en el ambiente de pruebas y debidamente documentada de acuerdo a las políticas "Desarrollo de Aplicaciones" MSI-101-01 y "Control de Cambio" MSI-104-01.

3. Todo desarrollo o adquisición de aplicaciones o sistemas debe ser regulado y cumplir con las políticas que rigen los sistemas de información del Banco. Toda nueva aplicación o sistema debe poseer un control de acceso que autentique las credenciales

Manejo de Aplicaciones (cont.)

de cada usuario utilizando la cuenta existente en la red o a través de una cuenta nueva definida en la aplicación.

4. Toda restauración de datos y/o aplicaciones en el sistema, dentro del ambiente de producción, deberá ser aprobada por el CIO/Director del Departamento y el Oficial de Seguridad de Acceso de Sistemas de Información o representante designado, antes de ejecutar la misma, siguiendo los lineamientos establecidos en el procedimiento "Manejo de Copias de Respaldo" MSI-301-03. 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.

5. La destrucción de archivos ("purge") de documentos oficiales y base de datos que residan en los servidores y en aplicaciones, se llevará a cabo anualmente o cuando el nivel de desempeño de los sistemas así lo requiera, según se establece en los procedimientos "Depuración de Archivos en la Red" MSI-301-06 y "Depuración de Datos en Aplicaciones" MSI-301-07. Esto excluye el espacio en el "network" que se le asigna a cada usuario, ya que es su responsabilidad el manejo de dicho recurso.

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

Seguridad en Base de Datos

1. La administración, seguridad e integridad de toda base de datos es responsabilidad de la División de Desarrollo de Sistemas de Información y Administración de Base de Datos, siguiendo las guías establecidas en los procedimientos "Diseño de Bases de Datos" MSI-220-01, "Administración de Bases de Datos" MSI-220-04 y "Seguridad de Bases de Datos" MSI-220-05.

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

3. 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, en el procedimiento "Diseño de Bases de Datos" MSI-220-01 y poseer toda la documentación necesaria actualizada.

Seguridad en PC's y Estaciones de Trabajo

1. Los programas de antivirus en todas las estaciones de trabajo deberán ser actualizados, según sean provistos por el manufacturero del programa, de acuerdo a los lineamientos establecidos en el procedimiento "Actualización de Programa de Antivirus" MSI-311-01.

2. Todo usuario deberá tomar las precauciones necesarias en cuanto a verificación de presencia de virus, y de ser necesario, se prevendrá la propagación del virus a través del "network". Es responsabilidad del usuario notificar a la División de Servicios al Usuario del Departamento la detección de un virus.

3. La seguridad de las computadoras, durante horas laborables, debe ser vigilada por cada usuario que tenga asignado ese equipo, de manera que ninguna otra persona pueda utilizar dicho equipo. Además, se requiere bloqueo automático después de quince (15) minutos de inactividad.

4. La seguridad en computadoras portátiles debe ser vigilada por cada usuario que tenga asignado ese equipo, para evitar el acceso de otras personas al mismo. Además se requiere bloqueo automático después de período de inactividad, según establecido en la política "Manejo de Computadoras Portátiles del Banco" MSI-106-01.

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

6. 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.

Manejo de Errores

1. Los sistemas de información del Banco deberán identificar y manejar condiciones de error de forma inmediata.

Manejo de Errores (cont.)

2. Los mensajes de error de los sistemas deberán ser mostrados solamente al personal autorizado. Información Sensitiva no debería estar listada en las bitácoras de errores o mensajes administrativos asociados.

V. Enmiendas:

Este documento puede ser enmendado cuando sea necesario para mejorar los servicios y operaciones del Banco.

VI. Vigencia:

Esta política está vigente desde la fecha de su aprobación.

VII. Aprobación:

Aprobada por:

Melba Acosta Febo
Presidenta Junta de Directores

20 de abril de 2016
Fecha de Aprobación