



Manual : Procedimientos Administrativos
Sección : Asuntos Generales
Asunto : Política de Seguridad de los Sistema de Información

Aprobado por : Junta de Directores del BGF
mediante la Resolución Núm. 7915

Fecha : 1 noviembre 2002

Introducción:

La seguridad de los recursos de computadoras y redes de intercomunicación es un elemento vital para la continuidad de las operaciones de toda organización, exigiendo un esfuerzo mayor en el caso del Banco, dada la naturaleza de negocio que lleva a cabo, así como su carácter de entidad gubernamental. La retención y transacciones de índole confidencial entre entidades dentro y fuera del Banco usando los sistemas de información constituyen elementos de alto riesgo que deben ser controlados adecuadamente. Para manejar ese riesgo es necesario implantar medidas de seguridad alrededor de los sistemas de información que ayuden en la prevención de "filtraciones" o divulgación no autorizada de información del Banco.

El monitoreo continuo y la detección temprana forman parte de un plan completo de seguridad de los sistemas de información del Banco. No obstante, el mayor riesgo de una organización proviene dentro de sí misma, por lo cual se deben implantar diversos controles y medidas para minimizar los riesgos de seguridad. En fin, la política de seguridad del Departamento de Sistemas de Información afecta la estructura completa del Banco, por lo cual debe ser comprensiva y abarcadora en su implantación.

Propósito y Alcance:

Esta política establece medidas de seguridad del Banco Gubernamental de Fomento para Puerto Rico y sus subsidiarias y afiliadas en lo que respecta al uso y manejo de los recursos de sistemas de información. Aplica a todos los empleados a nivel de usuario de los sistemas de información (incluyendo temporeros o por contrato), contratistas y otros autorizados a utilizar los recursos de computadoras o redes de intercomunicación con el Banco, así como a aquellos que están conectados por medio electrónico con el Banco.

Todos los usuarios de los recursos de computadoras o redes de intercomunicación deben familiarizarse con esta política y cumplirla. Las violaciones a las normas que dispone la misma pueden conllevar la revocación de los privilegios de utilizar el sistema, y la imposición de medidas disciplinarias, así como otras sanciones que apliquen de acuerdo a las disposiciones del *Manual de Normas Generales del Trabajo* del Banco. Cualquier pregunta respecto a ésta política debe dirigirse a la División de Servicios al Usuario de Sistemas de Información.

Aspectos Fundamentales:

- El privilegio de uso de los recursos asignados por el Departamento de Sistemas de Información se otorga con el estricto propósito de agilizar las labores y responsabilidades de trabajo de los empleados y no constituye un derecho. Por tal razón, todos los usuarios de sistemas de información deben observar y mantener un uso apropiado de los sistemas y equipos asignados.
- Toda información que pudiera afectar adversamente las operaciones del Banco debe ser manejada con suma cautela, evitando en todo momento la interceptación por terceros. De surgir alguna duda sobre la seguridad de dicha información, este personal debe consultar al oficial asignado a seguridad de datos.

El Banco...

Sección : Asuntos Generales**Asunto** : Política de Seguridad de los Sistema de Información**Aspectos Fundamentales (Cont.):**

- El Banco podrá monitorear toda información electrónica sensitiva, incluyendo la denominada personal o confidencial, según establecido por cada unidad, mediante el uso de herramientas disponibles. La transmisión de información sensitiva tiene posibilidad de ser interceptada por un tercero poniendo en riesgo la integridad de la misma, por lo cual se debe minimizar el uso de correo electrónico para dicha correspondencia.
- En el caso que sea necesario transmitir o difundir información sensitiva del Banco usando los sistemas de información, ésta tiene que estar codificada ("encrypted") mediante un mecanismo aprobado y provisto por el Departamento de Sistemas de Información.
- Cualquier distribución de información que pudiera afectar adversamente las operaciones o reputación del Banco, debe contar con la aprobación previa y escrita del Director de Comunicaciones. Además, todo usuario es responsable de manejar adecuadamente toda información confidencial que la misma le haya sido proporcionada.
- Ningún usuario está autorizado a realizar movimientos de equipo de sistemas de información dentro ni fuera de los predios del Banco, aunque el equipo en cuestión fuese el asignado a su persona. Todo movimiento de equipo de sistemas de información deberá regirse por el "Procedimiento de Control de Inventario y Transferencia de Equipo Mobiliario o Propiedad Mueble" MPA-0320-03. De igual forma, ningún usuario está autorizado a desmantelar, disponer, modificar, o alterar ningún equipo de sistemas de información.
- No se permitirá la remoción de equipo o información contenida en medios electrónicos de los predios del Banco sin previa autorización por escrito del Departamento de Sistemas de Información.
- Ningún usuario deberá intentar acceso a información a la que no está debidamente autorizado.
- Es responsabilidad de cada Director de Departamento fomentar que todo usuario autorizado cumpla con estas políticas. En caso de observarse alguna violación a esta política, deberá notificarlo al Departamento de Sistemas de Información para su verificación.

Claves de Acceso:

- Es obligación de cada empleado del Banco que tenga acceso a los recursos del sistema de información mantener las claves de acceso ("password") en estricta confidencialidad y asegurarse de no escribirla en ningún sitio visible. El incumplimiento con esta política podría conllevar a la cancelación de los privilegios de este acceso, así como otras sanciones o medidas que apliquen, según establecidas por el Departamento de Recursos Humanos y Relaciones Laborales, en el "Manual de Normas Generales del Trabajo".
- Todos los usuarios tendrán tres (3) oportunidades consecutivas para entrar la clave de acceso en el sistema, posterior a ello todo acceso a la cuenta será suspendido. Es responsabilidad del usuario informarle a la División de Servicio al Usuario del Departamento de Sistemas de Información el estado de su cuenta para prevenir acceso no autorizado al sistema.

Todo acceso...

Sección : Asuntos Generales**Asunto** : Política de Seguridad de los Sistema de Información**Claves de Acceso: (Cont.)**

- Todo acceso a los sistemas financieros y legales del Banco estará estrictamente monitoreado. Solamente personas autorizadas podrán tener acceso a los sistemas legales y los de transacciones financieras. El incumplimiento de esta política podrá conllevar la suspensión de empleo, así como otras sanciones o medidas que apliquen, según establecidas por el Departamento de Recursos Humanos y Relaciones Laborales, en el “Manual de Normas Generales del Trabajo”.
- Si un usuario olvida su contraseña o sospecha la divulgación de ésta, deberá informar la situación al Departamento de Sistemas de Información.

Seguridad en las aplicaciones de Sistemas:

- Los usuarios no están autorizados a instalar aplicaciones en cualquier equipo de propiedad del Banco sin que medie autorización por escrito del Departamento de Sistemas de Información.
- El acceso remoto a las instalaciones de los sistemas de información estará estrictamente prohibido, excepto para administradores y usuarios que estén previamente autorizados. Este acceso conlleva los mismos privilegios que se le otorgan al administrador o usuario localmente en el Banco. No se permitirá el acceso remoto y local simultáneo a una misma cuenta.
- El acceso a la Internet y correo electrónico es un privilegio que se le otorga a los empleados e individuos que específicamente lo necesitan para cumplir con sus responsabilidades de trabajo (ver “Política de Control y Uso de la Internet” MPA-0140-02 y “Política de Control y Uso del Sistema de Correo Electrónico” MPA-0140-03).
- Cualquier acceso remoto a los sistemas de información del Banco deberá ser adecuadamente restringido por una conexión segura y privada. No se permitirá el acceso remoto cuando se sospeche algún atentado al sistema por medio de dichas conexiones.
- Los empleados del Banco no deberán divulgar o publicar información que pueda afectar las operaciones, negocios, relaciones con los clientes o imagen pública de la institución, salvo que cuenten con la aprobación previa del Director de Comunicaciones.

Seguridad en PC's y Estaciones de Trabajo:

- La seguridad en computadoras personales, durante horas laborales, debe ser vigilada por cada empleado que tenga asignado ese equipo, de manera que ninguna otra persona pueda usar dicho equipo. Además, se requiere bloqueo automático después de quince (15) minutos de inactividad.
- La seguridad en computadoras portátiles debe ser vigilada por cada empleado que tenga asignado ese equipo, tal que nadie más pueda usar el mismo. Se requiere bloqueo automático después de quince (15) minutos de inactividad. Además, por ser unidad portátil, se debe utilizar un mecanismo para asegurar el equipo físicamente en el lugar de trabajo.

Todo usuario...

Sección : Asuntos Generales

Asunto : Política de Seguridad de los Sistema de Información

**Seguridad en PC's y Estaciones
de Trabajo: (Cont.)**

- Todo usuario deberá tomar las precauciones necesarias en cuanto a verificación de presencia de virus, y de ser necesario, se prevendrá el esparcimiento de virus a través del "Network". Es responsabilidad del usuario notificar a la División de Servicios al Usuario del Departamento de Sistemas de Información la detección de un virus.
- En caso de sospechas sobre introducción de virus o daños intencionales a las computadoras, se iniciará una investigación por parte del Banco. La persona responsable de tales actos estará sujeta a medidas disciplinarias.

oOo