BANCO DE DESARROLLO ECONÓMICO PARA PUERTO RICO

GOBIERNO DE PUERTO RICO

ÁREA DE FINANZAS Y OPERACIONES
DIVISIÓN DE SISTEMAS DE INFORMACIÓN

MANUAL DE PROCEDIMIENTOS

BDE-005-SI.01

APROBADO EL 12 DE DICIEMBRE DE 2006
Y ENMENDADO EL 31 DE ENERO DE 2008,
14 DE OCTUBRE DE 2009 Y 30 DE AGOSTO DE 2010

Tabla de Contenido

I. INTRODUCCIÓN

En el Manual de Procedimientos de la División de Sistemas de Información se detallan las tareas y actividades que se llevan a cabo en la División para cumplir con los aspectos operacionales. También se presentan las guías y normas de seguridad de los sistemas, con el propósito de proteger todo tipo de información, particularmente la producida, guardada y transmitida a través de las computadoras.

La División de Sistemas de Información está a cargo del mantenimiento de la página de Internet del Banco. Se presenta el procedimiento para solicitar cambios a la página.

II. DEFINICIONES

A. En general – Las palabras y frases usadas en este Manual de Procedimientos se interpretarán según el contexto y el significado sancionado por el uso común y corriente. El tiempo presente también incluye el futuro; las usadas en el género masculino incluyen el femenino. El número singular incluye el plural y el plural, el singular, salvo en los casos en que tal interpretación resultase absurda.

B. En particular – Las definiciones que aparecen en este inciso, aplican a todo el Manual de Procedimientos. Las palabras y frases que a continuación se mencionan son términos cortos o conceptos de las siguientes definiciones:

1. BDE o Banco – Se refiere al Banco de Desarrollo Económico para Puerto Rico.

2. Disposición de Equipo – Proceso utilizado para eliminar equipo perteneciente al Banco y sus Oficinas Regionales, debido a que es de bajo rendimiento, propiedad dañada, obsoleta o en desuso.

3. Equipo – Incluye, pero no está limitado a computadoras, impresoras, cables, "*hubs*", "*routers*", baterías (UPS), "escaners" y otros equipos o accesorios relacionados.

4. Licencia para programas – Tipo de contrato entre el autor del programa y el usuario, que le permite al usuario utilizar el programa de forma legal. Las licencias contienen un acuerdo donde usualmente está estipulado quiénes pueden utilizar dicho programa, usos permitidos, si se pueden hacer copias del mismo, entre otras estipulaciones.

5. Propiedad dañada, obsoleta o en desuso – Equipo que para poder ser utilizado para el propósito que fue diseñado, necesita amplias modificaciones o reparaciones considerables y cuyo costo supera los beneficios que se obtendrán una vez haya sido reparado.

6. Remoción de contenido – Proceso utilizado para eliminar completamente el contenido de los medios para almacenamiento de datos (discos duros, cintas magnéticas, memorias y otros), de tal manera que dicho contenido no pueda recuperarse en el futuro.

7. Seguridad de información – implica proteger la información del Banco para evitar el manejo indebido de la misma, sea accidental o intencional, por persona o personas no autorizadas a modificar, destruir o exponer la misma.

8. Usuario – Se refiere a los empleados del Banco a los que la División de Sistemas de Información le provee servicios técnicos y de programación de computadoras.

III. PROCEDIMIENTO DE VERIFICACIÓN DEL ACCESO DE ENTRADA AL CENTRO DE CÓMPUTOS

Proceso mediante el cual la División de Sistemas de Información mantiene un control de acceso al Centro de Cómputos. No se permitirá el acceso al Centro de Cómputos a personal no relacionado con la operación diaria del mismo. Sólo se permitirá el acceso ilimitado y sin escolta al personal de Sistemas de Información.

EMPLEADO Y SU RESPONSABILIDAD

- **Gerente de Sistemas de Información**
- **Oficial de Seguridad de Informática**
- **Técnico de Computadoras**

1. El **Técnico de Computadoras o Personal designado** que vaya a atender a un usuario, contratista o visitante solicitará a éste que firme el Registro de Visitantes para tener acceso al Centro de Cómputos.

2. El **Gerente u Oficial de Seguridad de Sistemas de Información** proveerá escolta a empleados del Banco, contratistas o visitantes a quienes se le requiera o tengan la necesidad de entrar al Centro de Cómputos.

3. El **Gerente de Sistemas de Información** firmará en el espacio provisto para certificar la página del registro de Control de Acceso.

IV. PROCEDIMIENTO DE SOLICITUD DE ACCESO AL SISTEMA DE PRÉSTAMOS

Proceso mediante el cual la División de Sistemas de Información delinea y establece los niveles y controles de acceso al Sistema de Préstamos y registro de toda la documentación relacionada.

EMPLEADO Y SU RESPONSABILIDAD

- **Gerente de Sistemas de Información**
- **Gerente o Supervisor de División**
- **Oficial de Seguridad de Informática**
- **Contralor o Firma Autorizada de la División de Contraloría**

1. El **Gerente o Supervisor de División** del Banco llena el Formulario para Solicitar Acceso al Sistema de Préstamos (**BDE.F-034**).

2. Evalúa las tareas del empleado para solicitar el tipo de acceso, según se detalla en la sección de Funciones del Formulario BDE.F-034.

3. Firma el Formulario y obtiene la firma del empleado. En caso de solicitar acceso a monetario, remite el Formulario a Contraloría para obtener la firma del **Contralor o Firma Autorizada de la División de Contraloría.**

4. El **Gerente o Supervisor de División** remite el Formulario al Oficial de Seguridad de Informática de la División de Sistemas de Información.

5. El **Oficial de Seguridad de Informática** recibe el Formulario. Coteja los accesos solicitados por el Supervisor o Gerente y bloquea los espacios para los cuales no se solicita acceso. En caso de acceso a monetario, coteja que esté firmado por el Contralor del Banco o persona autorizada.

6. Revisa los accesos solicitados y refiere el documento al Gerente de Sistemas de Información para su verificación y firma.

7. El **Gerente de Sistemas de Información** recibe y verifica que el Formulario esté debidamente completado por el Oficial de Seguridad y que los niveles de acceso otorgados son los solicitados y estén correctos.

   a. En caso de no estar correcto, entrega el Formulario al Oficial de Seguridad de Informática para que realice las correcciones necesarias.

   b. El **Oficial de Seguridad de Informática** corrige cualquier error referido por el Gerente de Sistemas de Información y se lo devuelve nuevamente para verificación y firma.

8. Si todo está correcto, el **Gerente de Sistemas de Información** firma el Formulario y lo refiere al Oficial de Seguridad de Informática para que registre la información en el módulo de Seguridad del Sistema de Préstamo.

9. El **Oficial de Seguridad de Informática** registra los códigos de acceso en el módulo de Seguridad del Sistema de Préstamo.

10. Le notifica al usuario sus códigos de acceso y le requiere la firma en el Acuerdo de Confidencialidad, Seguridad de Información y Protección de Equipo (**BDE-F.035**).

11. Una vez firmado, archiva toda la documentación en el expediente correspondiente. La documentación se puede archivar digitalizada para referencia futura.

V. PROCEDIMIENTO DE VERIFICACIÓN DEL INFORME DE EXCEPCIONES

Proceso mediante el cual la División de Sistemas de Información revisa y evita los accesos ilegales al Sistema de Préstamos y de Contabilidad.

FUNCIONARIO Y SU RESPONSABILIDAD

- **Oficial de Seguridad de Informática**
- **Gerente de Sistemas de Información**

1. El **Oficial de Seguridad de Informática** revisa y analiza cada una de las transacciones del Informe Diario de las Excepciones. Este Informe (SCM/8220-004) debe ser impreso diariamente antes de las 9:00AM.

2. Para determinar si hubo algún intento de acceso no autorizado al Sistema de Préstamos o Contabilidad, verifica lo siguiente:
   a. ¿Cuál fue la situación?
   b. ¿Cuál fue el Terminal?
   c. Fecha
   d. Hora
   e. Informa y verifica con el usuario sobre los intentos inválidos desde su Terminal.
   f. ¿Quién trató de acceder al Sistema?
   g. ¿Cuántas veces?
   h. Cualquier otra información

3. Recopila toda la información pertinente, al intento de acceso.

4. Firma y anota la fecha de la revisión en el Informe de Excepciones.

5. Prepara un informe de los intentos de acceso no autorizado al Sistema de Préstamos o Contabilidad.

6. Somete el Informe a través del correo electrónico al **Gerente de Sistemas de Información.**

7. Recibe y verifica el Informe.

8. De ser necesario, informa a otras fuentes sobre el intento ilegal de acceso. Esta comunicación podrá ser notificada por correo electrónico al Supervisor Inmediato, al Vicepresidente Ejecutivo y/o Recursos Humanos con una recomendación.

9. Entrega al **Oficial de Seguridad de Informática** la documentación para que la archive para referencia futura e información.

VI. PROCEDIMIENTO PARA GUARDAR DOCUMENTOS EN EL SERVIDOR DE LA RED

En el Servidor de la Red se graban todos los documentos de *WORD, EXCEL, POWER POINT* y todos los mensajes del Correo Electrónico. Se guardan en el directorio **F:**, que se conoce como el disco "*USERS*".

Cada usuario cuenta con un "*user-id*" que se utiliza con el "*password*". En el directorio "*F – Users*" hay un cartapacio por cada usuario y solamente el dueño de cada cartapacio o cuenta lo puede acceder. Los documentos que cada empleado guarda en su cuenta de usuario en el directorio *USERS* están más protegidos que los que se graban en el disco duro de la computadora, por lo que es más difícil que se pierdan.

EMPLEADO Y SU RESPONSABILIDAD

- **Usuarios de Sistemas de Información**
- **Oficial de Seguridad de Informática**

1. Proceso para guardar los documentos en el directorio "*F-USERS*".

   a. El Usuario que interese guardar un documento debe seleccionar la opción FILE en la parte superior izquierda del Programa de WORD, EXCEL o POWER POINT que esté utilizando.

   b. Luego, marcar "*Save As*". En la parte de arriba de la pantalla aparece "*Save In*" y el nombre del documento que se está utilizando. El usuario debe seleccionar el directorio donde usted desea guardar el documento: 🗁DOCUMENTOS WORD, EXCEL o POWER POINT, según donde se esté trabajando en ese momento.

   c. Marcar el botón de "*Save*" en la parte inferior derecha. Cotejar que el nombre del documento sea el apropiado para ser identificado.

d. Sistemas de Información sólo puede garantizar la confidencialidad de los documentos mientras el usuario los grabe bajo su cuenta. Si el usuario graba en el directorio "*USERS*", fuera de su cuenta, los documentos **no** tienen ningún privilegio de seguridad, pues todos tienen acceso a los mismos.

2. Mantenimiento del directorio "*F-USERS*".

a. Los usuarios deben separar un tiempo para cotejar todos los documentos que tienen grabados en su directorio del disco F:.

b. Hacer una buena limpieza, eliminando todos aquellos documentos que no añaden ningún valor mantenerlos en disco. Cuando se eliminan archivos, se deben asegurar de seleccionar la opción de "*empty recycle bin*", para que los archivos sean eliminados por completo. Ejemplo: los memorandos anunciando reuniones o situaciones ya pasadas, cartas que ya fueron procesadas y enviadas a su destinatario y de la cual se mantiene copia en los expedientes. Lo mismo ocurre con las presentaciones y las hojas de Excel.

c. Cotejar los mensajes en su correo electrónico ("*Outlook*"): en "*INBOX*", en el "*SENT ITEMS*" y en el "*DELETED ITEMS*", ya que cada uno de estos mensajes está grabado en el servidor y ocupa espacio. Debe seleccionar aquellos que no interesen para ser borrados. Cuando se elimine un mensaje, se debe también eliminar del "*DELETED ITEMS*".

d. Se recomienda hacer el proceso de limpieza de los directorios periódicamente para hacer buen uso del espacio de los discos del servidor. Si existe duda de cómo realizar el proceso, se deben comunicar con Sistemas de Información.

VII. PROCEDIMIENTO DE SOLICITUD, RECIBO, ALMACENAMIENTO E INVENTARIO DE APLICACIONES

Proceso mediante el cual, la División de Sistemas de Información mantiene control sobre el inventario de las aplicaciones ("*software*") y las licencias correspondientes. Es responsabilidad de la División de Sistemas de Información realizar inventarios, por lo menos dos (2) veces al año, de los programas o aplicaciones que posee el Banco.

FUNCIONARIO Y SU RESPONSABILIDAD

- **Gerente de Sistemas de Información**
- **Oficial de Seguridad de Informática**
- **Técnico de Computadoras**
- **Vicepresidente Ejecutivo de Finanzas y Operaciones**

1. El **Gerente de Sistemas de Información** analiza la necesidad de aplicaciones y programas para las operaciones del Banco y solicita los mismos, a través del Programa de Compras.

2. Recibe, de la División de Servicios Administrativos, los programas y aplicaciones solicitados y verifica que sean los correctos.

3. Refiere al **Oficial de Seguridad de Informática** las licencias adquiridas para mantener al día el registro de las mismas.

4. El **Gerente de Sistemas de Información** refiere al **Técnico de Computadoras** los programas y aplicaciones para que los instale a los usuarios asignados, de manera que se controle el número de licencias.

5. Para mantener el control y la seguridad, el **Técnico de Computadoras** entrega los programas y aplicaciones al **Oficial de Seguridad en Informática.**

6. El **Oficial de Seguridad en Informática** almacena los originales de los programas y aplicaciones en el armario designado para ese propósito. Éste debe ser seguro y a prueba de fuego.

7. El inventario que se realiza dos veces al año es revisado por el **Gerente de Sistemas de Información** y aprobado por el **Vicepresidente Ejecutivo de Finanzas y Operaciones.**

VIII. PROCEDIMIENTO PARA LA REMOCIÓN Y DISPOSICIÓN DE LICENCIAS Y DE EQUIPO DE COMPUTADORAS

Este proceso describe los mecanismos que utiliza el Banco para eliminar completamente de las computadoras y equipos que se vayan a disponer, el contenido de los medios para almacenamiento de datos (discos duros, cintas magnéticas, memorias y otros), de tal manera, que dicho contenido no pueda ser recuperado en el futuro. Se presenta además, el proceso para disponer de las licencias, computadoras y equipos relacionados del Banco, cuando tengan bajo rendimiento, estén dañados, obsoletos o en desuso.

FUNCIONARIO Y SU RESPONSABILIDAD

- **Gerente de Sistemas de Información**
- **Técnico de Computadoras**

1. Cuando un empleado del Banco tiene problemas con la computadora o equipos relacionados, se comunica con la División de Sistemas de Información para que la revise. El **Técnico de Computadoras** la examina y realiza lo siguiente:

    a. Reinstala programas, añade memoria, sustituye alguna pieza que se encuentre dañada o algún otro tipo de reparación menor. En caso de equipos dañados, coteja si tiene garantía para solicitarla.

    b. Si la computadora se encuentra en buen estado, pero se determina que no tiene la capacidad para las operaciones que se manejan, recomienda que se sustituya por otra de mayor capacidad. En estos casos, la computadora se guarda en el almacén para ser utilizada cuando sea necesario.

    c. Si la computadora se encuentra en buen estado, pero se determina que no se le dará uso alguno, procede a disponer de la propiedad, informando al Gerente de Sistemas de Información, quien notifica, por escrito, a la División de Administración de Propiedades.

d. Si determina que la computadora está dañada y no se puede reparar, por ser un equipo inservible u obsoleto, procede a disponer de la propiedad, informando al **Gerente de Sistemas de Información**, quien notifica, por escrito, al Encargado de la Propiedad de la División de Servicios Administrativos.

2. En los casos de computadoras que sean para disposición, antes de ser entregadas a la División de Administración de Propiedades, el **Técnico de Computadoras**, borra o remueve la información contenida en los discos, de manera que dicha información no pueda recuperarse en el futuro, utilizando diferentes métodos para la remoción de datos. En estos casos, formatea el disco, luego reescribe el disco y finalmente borra nuevamente la información que se reescribe.

   a. Mantiene, por escrito, la información de todo el equipo al que se le removió su contenido, incluyendo:

      i. Fecha de remoción del contenido
      ii. Número de Serie del equipo
      iii. Marca y Modelo
      iv. Método de remoción o destrucción utilizado
      v. Nombre de la persona encargada del proceso de remoción
      vi. Firma de la persona que realizó el proceso de remoción

   b. Entrega las licencias que contenía el equipo al **Gerente de Sistemas de Información**. En el caso de licencias globales adquiridas a través de la Oficina de Gerencia y Presupuesto y pertenecientes a dicha agencia, éstas se devolverán una vez se finalice el proceso de remoción de contenido del equipo. Si los programas instalados en el equipo se van a utilizar en otro equipo, no procede el proceso de devolución.

3. Si se trata de otros equipos, tales como monitores, módems, impresoras y escaners, el **Técnico de Computadoras** lo incluye en la lista de equipos para disposición y lo informa al **Gerente de Sistemas de Información** para que lo notifique, por escrito, al Encargado de la Propiedad de la División de Servicios Administrativos.

4. En los casos de programas ("*softwares*") obsoletos que se decide no utilizarlos, se procede a disponer del mismo. Si contiene número de propiedad, le notifica, por escrito, al Encargado de la Propiedad de la División de Servicios Administrativos.

5. En todos los casos que haya movimiento de equipo que contenga número de propiedad, le notifica a la División de Servicios Administrativos el nombre de la persona a quien se le asigna. De igual forma, le notifica cuando se recomienda la disposición de algún equipo que contenga número de propiedad.

IX. PROCEDIMIENTO DE MONITOREO DE LA RED

Proceso mediante el cual, la División de Sistemas de Información monitorea la red en búsqueda de accesos indebidos y errores ocurridos en los servidores para que ésta funcione a cabalidad.

FUNCIONARIO Y SU RESPONSABILIDAD

- **Gerente de Sistemas de Información**
- **Oficial de Seguridad de Informática**
- **Vicepresidente de Recursos Humanos**

A. Búsqueda de Incidentes en la Red

Todos los días, el **Oficial de Seguridad de Informática** verifica el "*Event Viewer*" de los servidores. De detectarse errores en ellos, los identifica y prosigue a corregir los mismos. Después que se corrigen, anota en la bitácora los errores y la acción correspondiente para corregirlos.

B. Programa Proventia

1. Diariamente, luego de revisar el "*Event Viewer*", el **Oficial de Seguridad de Informática**, entra en el programa Proventia para verificar los eventos que ocurrieron en las pasadas horas. Examina todos los eventos: los eventos de afuera hacia los servidores, así como los de adentro o usuarios a los servidores. Además, identifica cuáles son falsos positivos y cuáles son positivos.

2. Si el **Oficial de Seguridad de Informática** encuentra vulnerabilidad en algún evento, procede a corregir el mismo, bloqueando el ataque. Verifica la función de Proventia que bloquea el ataque y le da "*enable*" a esa función.

3. Si el ataque fuese por algún usuario o empleado del BDE, tratando de entrar malintencionadamente a un servidor o si logra acceder a información restringida o confidencial para dicho usuario, el **Oficial de Seguridad de Informática** cancelará toda clase de acceso al sistema

y programas utilizados por éste inmediatamente. Informa la situación, de inmediato, al **Gerente de Sistemas de Información**.

4. El **Gerente de Sistemas de Información** referirá la situación al **Vicepresidente de Recursos Humanos** para la acción o medidas disciplinarias que apliquen.

5. El **Oficial de Seguridad de Informática** imprimirá diariamente un reporte de los eventos ocurridos. Analiza el reporte y lo refiere al **Gerente de Sistemas de Información** para su verificación y firma.

6. Luego, se archiva el reporte en la carpeta "Reporte Incidente Proventia" que se ubica en la oficina del **Oficial de Seguridad de Informática**.

C. Parchos de Seguridad

1. La primera semana de cada mes, el **Oficial de Seguridad de Informática** verifica los nuevos parchos de seguridad que publica Microsoft por internet para determinar cuáles aplican a los servidores.

2. De determinar e identificar que es necesario algún parcho, evalúa cuál es el servidor que lo necesita, lo instala y le da "*restart*" para que actualice la información instalada. Si es un servidor que está en producción, procede a instalar el parcho y luego, fuera de horas laborables, le da "*restart*".

D. Programa "*Websense*"

El Programa "*Websense*" tiene el propósito de restringir los accesos al internet que por política del BDE no se pueden acceder. Este programa provee para hacer reportes que identifican los sitios del internet que están accediendo los usuarios internos.

1. Una vez a la semana, el **Oficial de Seguridad de Informática**, escoge al azar, de diez (10) a quince (15) usuarios y verifica los sitios que están accediendo.

2. Si el **Oficial de Seguridad de Informática** se percata de que un usuario está entrando a un sitio que no se puede entrar, la razón es que el sitio no está categorizado por el "*Websense*". En estos casos, el **Oficial de Seguridad de Informática** entrará al "*Websense*" y categoriza la dirección para que el sitio quede restringido.

3. Si por alguna razón, un usuario tiene acceso a páginas no autorizadas, utilizando programas o equipo autorizados o no autorizados, el **Oficial de Seguridad de Informática** le suspenderá de inmediato el acceso al internet. Informa la situación, de inmediato, al **Gerente de Sistemas de Información**.

4. El **Gerente de Sistemas de Información** referirá la situación al **Vicepresidente de Recursos Humanos** para la acción o medidas disciplinarias que apliquen.

X. PROCEDIMIENTO DE RESGUARDO DE SERVIDORES

Proceso mediante el cual, la División de Sistemas de Información realiza diariamente un "*back-up*" completo de todo directorio de importancia.[1] Se utiliza una cinta para cada día (lunes a viernes).

FUNCIONARIO Y SU RESPONSABILIDAD

- **Técnico de Computadoras**
- **Oficial de Seguridad de Informática**

A. Proceso de Resguardo (*Back-up*)

1. El **Técnico de Computadoras** realiza el proceso de "*back-up*", el cual conlleva la realización de cinco (5) "*back-ups*" diarios a los siguientes servidores.

   a. Exchange
      BDE02Mail (Exchange)

   b. "*Program* y *Program1*" (Resguardos de los datos de las aplicaciones y el sistema operativo en los servidores)

      i. Program
         - BDE_PDC
         - BDE01RRAS
         - BDE02DC
         - BDE01ISA
         - BDE01RH
         - BDESQL01

      ii. Program1
         - BDEPRIME
         - BDE01RRAS

[1] Los directorios de importancia son los que cuentan con data de los programas, documentos de usuarios, correo electrónico, base de datos, sistemas operativos y programas.

- BDE01DC
- BDE01RH

c. SQL

- BDESQL01
- BDE01RH
- BDE01RRAS
- BDEPRIME

d. Folder de Usuarios

- BDE_PDC

e. Folder comunes

- BDEDIRECTOR

2. El proceso de "*back-up*" comienza a las 7:00 AM.

3. El primer "*back-up*" que se lleva a cabo es el de "*Program*" o "*program1*", dependiendo del "*back-up*" que toca ese día y comienza a las 7:00 AM.

4. El segundo "*back-up*" es el de "SQL_Oracle" y comienza a las 6:00 PM.

5. El tercer "*back-up*" es el de "*Exchange*" y comienza a las 6:00 PM.

6. El cuarto "*back-up*" es el de "*Users*" y comienza a las 6:00 PM.

7. El quinto "*back-up*" es el de Director y comienza a las 6:00 PM.

8. Los "*back-ups*" diarios se guardan bisemanal.

   La cinta correspondiente a los lunes se utilizará nuevamente a las dos (2) semanas siguientes.

B. Activar Programas de Resguardo ("Back-up")

El **Técnico de Computadoras** realizará lo siguiente:

1. Programa "*Back-up Exec*" (BDE01ISA, BDE02MAIL)

   Activar el programa de "*back-up*".
   a. *Start Menu*
   b. *Program*
   c. *Veritas Back-up Exec*

2. Programa *Back-up* de Windows 2003 (BDEDIRECTOR)

   Activar el programa de "*back-up*" de Windows.
   a. Start Menu
   b. Accessories
   c. System Tools
   d. Back-up

C. Ejecutar los Resguardos (Back-ups)

El **Técnico de Computadoras** realizará lo siguiente:

1. Programa "*Back-up Exec*" (BDE01ISA, BDE02MAIL)

   a. Una vez activado el programa de "*Back-up*", oprime la pestaña de "*DEVICE*". Se coloca el cursor encima de "*Compaq*" (BDE01ISA) y se oprime el botón derecho del "*mouse*". Selecciona "*ERASE*", elige "*Quick*" y luego escoge "*Yes*". (Este proceso se lleva a cabo para borrar la data de la cinta.)

   b. Luego, busca el "*back-up*" que se va a ejecutar y lo marca con el cursor. Oprime el botón derecho del "*mouse*" y selecciona "*Run Now*".

   c. Una vez completado el primer "*back-up*" procede a dejar listos los "*back-up*" de SQL que se realizan en el servidor de "BDE01ISA". El de Exchange se realiza en el servidor "BDE02mail". Ambos utilizan el programa de "*back-up exec*".

2. Programa "*Back-up Windows 2003*"

   a. Una vez activado el programa de "*Windows Back-up*", el **Técnico de Computadoras** busca la opción de "*Back-up Media or file Name*" y selecciona "*new*".

   b. Selecciona los archivos que se van a resguardar.

   c. Selecciona la opción de "*Start Back-up*". La diferencia entre el "*Backup exec*" y el "*back-up*" de Windows es que en el de Windows no hay que borrar la cinta manual. El "*back-up*" de Windows la borra automáticamente.

3. El **Oficial de Seguridad de Informática** verifica diariamente que los "*Back-ups*" hayan sido tomados y almacenados.

E. Retención de Cintas

1. Luego de realizado el resguardo, el **Técnico de Computadora** anotará toda cinta utilizada en el registro provisto para ese propósito.

   a. Toda cinta se utilizará nuevamente a las dos (2) semanas en su rotación correspondiente.

      Existen dos (2) juegos de cintas diarias de "*back-up*" semanal.

   b. Se utilizará el segundo juego de cinta semanal, luego de haber utilizado el primero.

      Esto significa que las cintas se estarán rotando continuamente cada semana.

   c. A fin de mes, se tomará un "*full back-up*" que tendrá un periodo de retención de un año. Estas cintas se llamarán **Fin de Mes** con la fecha del mes correspondiente.

2. Los "*back-up*" realizados los fines de mes se trasladarán a "*International Safe Deposit*" y se guardarán en la gaveta designada del BDE, hasta que se vaya a utilizar el próximo año.

3. El **Oficial de Seguridad de Informática** verifica diariamente que los "*back-ups*" hayan sido tomados y almacenados.

XI. PROCEDIMIENTO DE CORRIDA EN EL CENTRO DE CÓMPUTOS ("*OFF-LINE*")

Proceso mediante el cual la División de Sistemas de Información actualiza la información de la actividad financiera del día anterior del sistema financiero.

FUNCIONARIO Y SU RESPONSABILIDAD

- **Técnico de Computadoras**
- **Supervisor de Desarrollo de Aplicaciones**
- **Supervisor de Operaciones**

A. Corrida de "*off-line*"

El **Técnico de Computadoras** comienza el proceso de corrida ("*off-line*") del día anterior a las 6:30 AM. Realiza los siguientes pasos:

1. Create Printer **PRBKUP** Tape

   a. Antes de comenzar el proceso, borra el contenido de la cinta que se va a utilizar.

   b. Para borrar la cinta se escribe el siguiente comando "**SN MT80 ddmmyy**.

2. Procede a escribir el comando "START (ITI)BDS/PREUPDATE" para remover los archivos de trabajo BDS y FMS.

3. Luego del comando anterior, el sistema pregunta tres (3) veces la fecha del día de la corrida para los programas LAS/3000, CIS/300 y FMS/3000. Ejemplo:

JOB	TASK	PR1	ELAPSED	1WAITING	ENTRY
3555/3558		85	7:41		(ITI)*ITI/LAS/3000

El **Técnico de Computadoras** corrobora si las fechas que aparecen escritas en la pantalla de "*complete entries*" son las correctas. Si son correctas escribe "**MX AX Y**" para cada una de las preguntas. Este número de MX sale en la pantalla de"*waiting*" bajo el nombre de "*task*". El número de "*task*" siempre va a sustituir el MX.

Si la fecha no está correcta, en vez de escribir "*YES*" se le escribe "NO". Esto hará que el sistema provea para escribir la fecha correcta y vuelva a preguntar si la fecha es correcta.

4. "*Disable*" a todos los programas de ITI

   a. Se escribe el comando **START (ITI)PRM/DISABLE**. Cuando el sistema termina de bajar todos los programas sale en la pantalla de "*complete*" **BDS/DISABLE**.

   b. Luego que los programas están "*disable*" se entra las siguientes instrucciones:

      i. **USER=ITI/ITI;RUN ITI/IES/3210** y el **Técnico de Computadoras** contesta al "*waiting*" **MX AX S/ALL END**

      ii. **USER=ITI/ITI;RUN ITI/IES/3010;SW1** y el **Técnico de Computadoras** contesta al "*waiting*" **MX AX GROUP=01 END.** Pregunta si la fecha de la corrida está correcta. Si lo está, le contesta **MX AX Y.** Si la fecha no está correcta, en vez de escribir "*YES*" se le escribe "NO". Esto hará que el sistema provea para escribir la fecha correcta y vuelva a preguntar si la fecha es correcta. Esta pregunta lo va hacer para la institución 1 y 3.

      iii. Estos comandos se ejecutan semanalmente.

         1. **REMOVE SUMLOG/= ON SPARE1**
         2. **REMOVE *BD/= ON SPARE1**
         3. **REMOVE (ITI)BDSRCV/= ON SPARE1**
         4. **PS DEL ALL**

      iv. "*Run Offline*" (comienza el "*offline*")

1. **START (ITI)BDS/PRMUPDATE** cuando se indica este comando, el sistema pregunta que si quiere comenzar el proceso de nuevo "*restart*" y el **Técnico de Computadoras** contesta **MX AX N.**

2. Automáticamente después de dar la instrucción anterior salen tres (3) "*waiting*".
   a. "Clear APS Audit File", se contesta **MX AX Y**
   b. "Clear APS Log File", se contesta **MX AX Y**
   c. Luego pide que entre la fecha de hoy y se contesta **MX AX MM/DD/YY** donde M significa mes, D día y Y year.
   d. Luego de entrar la fecha, el sistema pregunta si es correcta. Si es correcta se entra **MX AX Y**. Si la fecha no está correcta, en vez de escribir "*YES*" se le escribe "NO". Esto hará que el sistema provea para escribir la fecha correcta y vuelva a preguntar si la fecha es correcta.

3. Una vez terminado los "*back-ups*" del "*offline*" y sale la cinta, se procede a contestar el "*waiting*" que durante la corrida aparece en la ventana de "*waiting*" **MX AX OK.** Luego el sistema pregunta si la fecha es correcta, se contesta **MX AX Y**. Si la fecha no está correcta, en vez de escribir "*YES*" se le escribe "NO". Esto hará que el sistema provea para escribir la fecha correcta y vuelva a preguntar si la fecha es correcta.

B. Pasos a Seguir en caso de Emergencia o cuando se Presenten Problemas durante la Corrida

1. En caso de surgir algún error en la corrida, el **Técnico de Computadoras** debe contactar inmediatamente al **Gerente de Sistemas de Información** y al **Supervisor de Desarrollo de Aplicaciones** para notificarle el problema.

2. Sigue las instrucciones impartidas por éstos para verificar si el problema puede ser resuelto.

3. De no poder corregir el problema vía telefónica con el **Gerente de Sistemas de Información** o con el **Supervisor de Desarrollo de Aplicaciones**, uno de éstos o ambos, deberán personarse al Centro de Cómputos para resolver el problema y/o comunicarse con Asistencia Técnica de ITI, a los números de emergencia.

   Números de Asistencia Técnica de ITI:
   1-402-421-4242 ó 1-402-421-4228

4. De surgir una situación extrema que no se pueda resolver, el **Gerente de Sistemas de Información** deberá enviar una notificación, a través del correo electrónico, a todas las divisiones afectadas, indicando que ha surgido un error en la corrida y la hora estimada en que el sistema debe estar activo.

   La notificación a través del correo electrónico debe enviarse solamente si se estima que se va a afectar la hora en que el Sistema deba estar activo. La notificación puede hacerse por teléfono si se considera pertinente.

XII. PROCEDIMIENTO DE INSPECCIÓN DEL SISTEMA DE EXTINTORES DEL CENTRO DE CÓMPUTOS

Proceso mediante el cual la División de Sistemas de Información revisa cada seis (6) meses los distintos sistemas de extintores de incendios del Centro de Cómputos del Banco para asegurar que los mismos estén vigentes.

FUNCIONARIO Y SU RESPONSABILIDAD

- **Gerente de Sistemas de Información**
- **Supervisor de Operaciones**
- **Gerente de Servicios Administrativos**

1. Cada seis (6) meses, el **Supervisor de Operaciones**, revisa que los extintores de incendio localizados en el Centro de Cómputos no estén expirados.

2. Si encuentra algún extintor expirado o cercano a la fecha de expiración, el **Supervisor de Operaciones**, o en su ausencia, el **Gerente de Sistemas de Información**, notificará al **Gerente de Servicios Administrativos**, mediante correo electrónico o llamada telefónica para que realice el contacto con el suplidor de los extintores para que los verifiquen y pongan al día.

3. El FM200 es otro sistema de detector de incendio ubicado dentro del Centro de Cómputos. Todos los meses, el suplidor realiza una inspección de este sistema y pruebas necesarias para su buen funcionamiento. Se mantiene un récord de las visitas realizadas por el suplidor. El récord de visitas se mantendrá bajo la custodia del **Supervisor de Operaciones**.

4. En el caso de que transcurra más de un mes y no se haya realizado la inspección del FM200, el **Supervisor de Operaciones** notificará al suplidor para que realice la inspección. El Supervisor de Operaciones mantendrá récord de las gestiones realizadas.

5. El **Supervisor de Operaciones** completará el Formulario de Verificación de los Sistemas de Incendio (**BDE-SI-F.138**), el cual se utiliza para cotejar cada una de las unidades del Centro de Cómputos y se lo entrega al **Gerente de Sistemas de Información** para obtener su firma. El **Supervisor de Operaciones** mantendrá un récord de dicho Formulario.

XIII. PROCEDIMIENTO DE RECUPERACIÓN ANTE INCIDENTES DE SEGURIDAD

Procedimiento mediante el cual, la División de Sistemas de Información restablece la información afectada por algún incidente en la seguridad.

FUNCIONARIO Y SU RESPONSABILIDAD

- **Gerente de Sistemas de Información**
- **Oficial de Seguridad de Informática**

1. El **Oficial de Seguridad de Informática** desconecta la red o apaga el equipo para evitar que el atacante pueda seguir accediendo al equipo, evitando que recupere la información que haya podido obtener sobre otras redes, intente borrar sus huellas o inutilice (borrado o formateo) el equipo atacado.

2. Investigar, examinando los datos disponibles, toda la información posible sobre el ataque: vulnerabilidad empleada por el atacante, "*logs*" que muestren los ataques, escaneo y conexiones del atacante, programas instalados, "*logs*" y las herramientas que el atacante ha instalado, etc. Con estos datos recopilados se deben realizar pruebas a otros equipos que se han podido ver involucrados.

3. En los casos que lo amerite se procederá a eliminar toda la información de la computadora o inicializar el disco duro, "*format*" para restaurar el equipo. Vuelve a configurar el equipo utilizando los resguardos, según sean necesario o reinstalando el Sistema Operativo si es preciso, y aplicando los parches y configuraciones adecuadas para evitar que el intruso se vuelva a conectar.

4. Realiza las pruebas que sean necesarias para asegurar que el Sistema Operativo no esté corrupto o se hayan eliminado archivos.

5. De existir daños en el Sistema Operativo, aplicarán los parchos necesarios para un óptimo rendimiento del mismo.

6. En caso de que existan cuentas de usuarios en el equipo, es conveniente que avise a todos los usuarios y que éstos cambien sus cuentas, ya que el atacante puede haberse copiado las claves y proceder después en su equipo a buscar claves débiles para volver a entrar.

7. Dependiendo de los daños causados, procederá a cambiar las cuentas de los usuarios existentes y los equipos de computadora afectados.

XIV. PROCEDIMIENTO DE APAGAR Y ENCENDER LOS SERVIDORES Y BATERÍAS DEL CENTRO DE CÓMPUTOS

Proceso mediante el cual la División de Sistemas de Información apaga y enciende los servidores y las baterías, en caso de ser necesario, por alguna emergencia, tales como: problemas eléctricos, huracanes, mantenimiento a la subestación, entre otros.

FUNCIONARIO Y SU RESPONSABILIDAD

- **Gerente de Sistemas o Personal asignado**
- **Supervisor de Operaciones**
- **Técnico de Computadoras**

A. Proceso para Apagar el "*Mainframe*" o Sistema de Préstamos

El **Supervisor de Operaciones o Personal asignado**, después de correr el "*offline*", baja el Sistema de Préstamos. Para bajar el Sistema de Préstamos, realiza lo siguiente:

1. Escribe la siguiente instrucción en letras mayúsculas:

   USER=ITI/ITI;START
   BDEUTL/WFLRUN/CTLPROGRAMS("DISABLE").

2. Verificará en la consola que todos los programas de ITI estén abajo. Para esto, puede verificar escribiendo "AA USER=ITI". Aparecerán todos los programas que estén activos bajo ITI. Si hay alguno activo, procederá a bajarlos manualmente de la forma siguiente:

   - Escribir "número de System Coms" SM DISABLE PROGRAM "nombre del programa" (ej.: PRM0152) y luego transmitirá

   Si no baja de esta forma, procederá a cancelarlo de la siguiente manera:

   - Quitar el "*lock*" al programa que va a cancelar;
   - Escribir el número de "*task*" del programa que tiene al lado izquierdo (ej.: 4659 PRM0152) y la instrucción LP;

- Cancelarlo con el número de "*task*" del programa que tiene al lado izquierdo (ej.: 4659 PRM0152) y la instrucción DS;
- Transmitir para que lo cancele.

3. Proceder a bajar el sistema de "*Mainframe*" escribiendo la siguiente instrucción:
   - *POWER OFF SYSTEM* y transmitirá.

4. Luego de bajar el Sistema, esperar alrededor de diez (10) minutos y proceder a apagar el servidor oprimiendo "*shutdown*" a "*Windows Servers*".

B. Proceso para Apagar los Servidores y Baterías

El **Supervisor de Operaciones** apaga todos los servidores, incluyendo el servidor que maneja los mensajes del celular "*Blackberry*".

1. Los últimos servidores que se apagan son el BDE01DC y por último, el BDE02DC.

2. Apaga los "*switches*" y las baterías de los servidores (pequeños).

3. Mover el "*switch*" de "*enable*" a "*disable*" al FM-200 y oprime "*SILENCE*". Éste se encuentra a la derecha de la puerta que da acceso al Centro de Cómputos.

4. Apaga el aire acondicionado del Centro de Cómputos <u>antes</u> de apagar las baterías.

5. Apaga las baterías grandes del Centro de Cómputos.

   a. <u>UPS #2 FE</u>

      i. Apretar en el panel de control **ctrl 1**

      ii. Oprimir "*enter*" dos veces.

b. UPS #1 APC

i. Buscar con la tecla de las flechas la opción "CONTROL", seleccionarla y luego oprimir la tecla de "ENTER".

ii. Bajar con la tecla de las flechas hasta la opción "TURN OFF UPS OUTPUT" y luego oprimir la tecla de "ENTER".

C. Proceso para Encender las Baterías

El **Supervisor de Operaciones** realiza el siguiente proceso para encender las baterías:

1. Enciende las baterías grandes.

   a. UPS #2 FE

   Aprieta en el panel de control, ctrl 2, luego oprime dos (2) veces "*enter*".

   b. UPS #1 APC

   Busca con la tecla de las flechas la opción "*TURN ON UPS*" y luego confirma seleccionando "*YES*".

2. Enciende el aire acondicionado del centro de cómputos.

3. Mover el "*switch*" de "*disable*" a "*enable*" al FM-200 y oprime "*reset*".

4. Enciende las baterías pequeñas y los "*switches*".

5. Enciende los servidores.

   a. Enciende primero el BDE02DC y luego que ya esté arriba, enciende el BDE01DC.

   b. Luego el BDE01MAIL

   c. Luego enciende los servidores, incluyendo el servidor que maneja los mensajes de celular "*Blackberry*".

6. Cuando todos los servidores estén encendidos, prende el "MAINFRAME", BDEPROD y BDETEST y luego continua con las siguientes instrucciones para ambos servidores.

   a. Se incluye el "*user*" y el "*password*" del Administrador.

   b. Cuando suba la pantalla de Windows, entra al programa **Console MCP**.

   c. Al entrar, selecciona el **Partition 1** y oprime Load.

   d. Luego, sale de ese programa y busca el **ODT unit1** para subir a la pantalla del Sistema de Préstamos.

   e. Cuando suba, en los mensajes de "*Waiting*" va a salir un "*waiting*" de "*Software Program*" y le contestas # de "*task OK*" y "*trasmit*".

   f. Si sale otro "*waiting*" relacionado a "*Time and Date*", hay que darle el # de "*task DS*" y "*trasmit*".

   g. Luego, se le da el mismo # de "*task*" DS y "*trasmit*".

   h. Los otros "*waiting*" se van cuando se entra al programa de "*Infoconnet*" en la máquina que esté dentro del Centro de Cómputos.

   i. Por último, se corre la instrucción para subir el Sistema de Préstamos

      USER=ITI/ITI;STARTBDEUTL/WFLRUN/CTLPROGRAMS("ENABLE").

D. Cotejo de Equipos y Programas

El **Supervisor de Operaciones** debe verificar que todos los equipos estén encendidos:

Baterías
"Switches"
"*Routers*" (CISCO)
"*Firewall*" (NetScreen 50 y Provential)
Cuadro Telefónico
"*Modems*" (DSL Bloomberg)
Servidores
"*Hub*"
Monitores
Sistema de Cámaras de Seguridad

El **Supervisor de Operaciones** debe cotejar que funcionen las siguientes aplicaciones:

- Intranet
- Premier II
- Correo electrónico interno
- Correo electrónico desde fuera del BDE hacia el BDE y viceversa
- Internet
- Moody's
- Sistema de Compras
- Sistema de Originación
- Sistema Blackberry
- ITS – Ponches de Nómina
- RAS
- Proventia "*Mail Filter*" que esté bloqueando
- "*Websense*" que esté bloqueando

XV. PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN

A. Propósito

El propósito del Plan de Contingencia es establecer procedimientos que guíen al grupo de trabajo de la División de Sistemas de Información para la prevención y recuperación efectiva de los Sistemas, minimizando el impacto que puedan sufrir las funciones críticas del Banco, luego de un desastre o situación de emergencia.

B. Guías Generales

1. Se le notificará a todos los empleados de la División de Sistemas de Información cuando sea necesario activar el Plan de Contingencia.

2. El grupo de emergencia tendrá disponible el equipo necesario para llevar a cabo la operación en un lugar alterno.

3. Se llevarán a cabo las operaciones diarias en el Banco o en un lugar alterno, de acuerdo a arreglos especiales coordinados con anticipación.

C. Pruebas

1. Se realizará un (1) simulacro previo a la temporada de huracanes y cuando exista algún otro riesgo previsible.

2. Luego de activar el "Plan de Contingencia", se evaluará el resultado y se someterán recomendaciones adicionales que mejoren el proceso.

3. Se realizarán dos (2) pruebas al año del Sistema Financiero, o sea, cada seis (6) meses, una en enero y otra en julio.

   Se coordinará con la compañía de recuperación con un mes de anticipación de la prueba. Los números telefónicos de referencia de la compañía de recuperación son los siguientes:

   "*Testing*" – 1-800-541-TEST (8378)
   "*Disaster*" – 1-215-351-1313 (7 días de la semana, las 24 horas)

D. Acuerdos

Se archivarán las copias de los Acuerdos firmados con las agencias o compañías que se utilizarán como lugares alternos. En estos se establecerán los términos y condiciones a seguir en caso de emergencia, hasta que la situación vuelva a la normalidad o sea controlada.

E. Procedimiento de Reducción de Riesgo

FUNCIONARIO Y SU RESPONSABILIDAD

- **Gerente de Sistemas de Información**
- **Supervisor de Desarrollo de Aplicaciones**
- **Desarrollador de Aplicaciones**
- **Oficial de Seguridad de Informática**
- **Supervisor del Área Técnica**
- **Técnico de Computadoras**

1. Una semana antes de la temporada de huracanes o de alguna emergencia que sea previsible:

   a. Los **Técnicos de Computadoras** y/u **Oficial de Seguridad de Informática** verifican que el inventario de materiales esté completo. Este inventario será utilizado para hacer "*back-ups*" e imprimir los informes.

   Cintas de ocho (8) milímetros

   Cintas de cuatro (4) milímetros

   Cartuchos para impresora láser

   Cintas para impresora "*dox-matrix*"

   Suficientes disquetes, CD's y DVD's

   Carpetas ("*binder*") para archivar

   Papel tamaño 14 x 7/8

   Papel tamaño 8½ x 11

   Papel tamaño 8½ x 14

b. Los **Técnicos de Computadoras** o **Personal designado** revisan que en los receptáculos de electricidad anaranjados sólo estén conectados computadoras.

c. Inspeccionan la carga de las baterías de todas las computadoras "*desktops*", "*laptops*" y servidores.

d. Revisan que los UPS del Centro de Cómputos no tengan problemas.

De ser necesario, notifica al **Gerente de Sistemas de Información** para que coordine con la compañía que brinda servicio de mantenimiento al UPS del Centro de Cómputos.

e. De no haber servicio de energía eléctrica ni generador de energía en el edificio del Banco, el **Supervisor del Área Técnica** o el **Oficial de Seguridad de Informática** prepara otro servidor como "*back-up*" para moverlo a otro lugar y trabajar fuera del edificio, de ser necesario.

f. El **Técnico de Computadoras** o **Personal designado** prepara las dos (2) "*laptops*" disponibles con las aplicaciones necesarias.

i. Una con los programas de Inversiones y Office.

ii. Otra con las aplicaciones de Office, Moodys y el Sistema de Préstamos.

g. El **Gerente de Sistemas de Información** identifica, junto al **Vicepresidente Ejecutivo de Finanzas y Operaciones**, un lugar en el Banco donde se puedan instalar computadoras con el Sistema de Préstamos e Inversiones.

Estas computadoras pueden ser llevadas al lugar donde se haya instalado el otro servidor fuera del edificio.

h. El **Supervisor de Desarrollo de Aplicaciones** se comunicará con la compañía de recuperación para trabajar en coordinación los procedimientos sobre el sistema de "*Clear-Path*" y el Sistema

Financiero. Además de crear un ambiente igual al existente en el Banco.

2. Dos (2) días antes de la temporada de huracanes o de alguna emergencia que sea previsible:

   a. Los **Técnicos de Computadoras** o el **Oficial de Seguridad de Informática** imprimen los informes establecidos previamente.

      - Sistema de Préstamos
      - Contabilidad
      - Usuarios
      - Impresoras
      - Usuarios del correo electrónico
      - Según solicitados por División.

   b. Luego de impresos los informes, el **Técnico de Computadoras** o **Personal designado** procede a archivar una copia por división y por aplicación en carpetas debidamente identificadas.

   c. Tan pronto como se finalice el proceso de impresión de los informes, el **Técnico de Computadoras**, procede a realizar el proceso de "*back-up*" de todas las aplicaciones.

   d. El **Oficial de Seguridad de Informática** o los **Técnicos de Computadoras** también realizarán un "*back-up*" a todas las configuraciones de los servidores. Identifican todos los "*back-ups*" con etiquetas engomadas ("*labels*").

   e. El **Supervisor de Desarrollo de Aplicaciones**, los **Desarrolladores de Aplicaciones** y los **Técnicos de Computadoras** realizan un "*back-up*" completo del "*mainframe*" y del Sistema de Préstamos.

3. Almacenamiento

   El **Oficial de Seguridad de Informática** guardará los "*back-up*" de la siguiente manera:

a. Una copia será guardada internamente, en la bóveda ubicada en el Piso 3 en Administración de Colaterales.

b. Otra copia será llevada a la bóveda de "*International Safe Deposit*" en la Ave. Roosevelt, San Juan.

4. Inspección durante dos (2) días luego de ocurrida la emergencia.

a. El **personal de Sistemas de Información** verifica que los equipos del Centro de Cómputos hayan rotado las fechas correctamente y estén funcionando.

b. El **Gerente de Sistemas de Información** imparte instrucciones para que los usuarios revisen las fechas de sus computadoras y cualquier otro problema que puedan detectar.

c. El **Supervisor del Área Técnica** y los **Técnicos de Computadoras** revisan que las aplicaciones se estén trabajando correctamente y sin problemas y que las fechas estén correctas.

d. De no funcionar o presentar algún error el equipo o las aplicaciones, evaluarán la situación para identificar el problema y tomar la acción correspondiente.

e. Esta acción puede ser reparación, sustitución del equipo o reinstalación de la aplicación, según sea el caso.

f. De no existir servicio de electricidad, el **Gerente de Sistemas de Información** coordina con el Gerente de Servicios Administrativos o con el Administrador del Edificio la disponibilidad del generador de electricidad para trabajar con el UPS del Centro de Cómputos.

g. De no haber servicio de electricidad ni el generador de electricidad, el **Supervisor del Área Técnica** utilizará el servidor preparado como "*back-up*" para moverse a otro lugar y trabajar fuera del edificio, de ser necesario, con una conexión entre computadoras, y con las computadoras que sean necesarias en caso de que el principal falle.

h. El **Supervisor de Desarrollo de Aplicaciones**, se comunicará con la compañía de recuperación para coordinar la recuperación del sistema de "*Clear-Path*" y el Sistema Financiero.

Para notificar que es una llamada relacionada a una situación de emergencia y no una llamada de prueba, se debe tener disponible la siguiente información:

- Nombre de la compañía
- Nombre de la persona que está llamando (responsable)
- Contraseña, si aplica
- Número de teléfono donde se le podrá conseguir
- Indicar el tipo de emergencia (huracán, fuego, terremoto, falla en el sistema)
- Tipo de recuperación que está solicitando
- En caso de que sea necesario viajar, informar la hora aproximada de llegada al Centro de Recuperación.

i. Según el acuerdo con la compañía de recuperación, en 48 horas o menos deben de tener el lugar o ambiente idéntico a nuestro sistema. Este sistema es corroborado cada seis (6) meses.

j. De ser necesario, el **Gerente de Sistemas de Información** asigna al personal de su División para continuar las operaciones desde la base que asigne la compañía de recuperación en los Estados Unidos.

k. El **Supervisor del Área Técnica** de la División de Sistemas de Información coordina los pasajes y la estadía del personal que viajará.

XVI. GUÍAS Y NORMAS DE SEGURIDAD PARA EL USUARIO DE COMPUTADORAS

A. Propósito

La División de Sistemas de Información tiene la responsabilidad de establecer las guías y normas de seguridad para el uso de las computadoras. De igual forma, es responsable de orientar a los usuarios sobre el uso de los equipos y sus aplicaciones. El propósito de establecer guías y normas para el uso de las computadoras es para proteger todo tipo de información, particularmente la producida, guardada y transmitida por el computador. Los controles de seguridad deben existir para minimizar la vulnerabilidad de la información y el daño a los equipos.

De no existir una seguridad adecuada estaríamos expuestos a:

- daños a equipos sofisticados, y, por consiguiente, pérdida de dinero
- daños a la reputación del Banco
- divulgación de información confidencial (intencional o no intencional)
- uso indebido o mal uso de los sistemas
- demandas por violación a la confidencialidad y privacidad
- infección o entrada al sistema de virus

Como usuario de computadoras y empleado del Banco, se debe cumplir con lo siguiente:

- proveer protección a los equipos, programas y la información de las computadoras.
- controlar esencialmente el uso de las computadoras y cubrir extensamente las aplicaciones técnicas del Banco, procesamiento de datos, modelos de hojas de trabajo electrónicas y programas computadorizados.
- incorporar los controles adecuados a los sistemas.

B. Seguridad de Información

Es importante que todos los usuarios protejan la información y los medios donde éstas se almacenan contra divulgación, pérdida y daño.

1. Proteja su Clave de Acceso ("*PASSWORD*")

El "*Password*" es la clave que permite el acceso a la información a través de la computadora. Debe mantener la clave para uso exclusivo, no se puede divulgar a ninguna otra persona ni escribir en lugares visibles. A continuación se incluye una lista de acciones que se deben hacer y que **NO** se deben hacer para proteger la clave de acceso.

Qué debe hacer:

- Mantenga su "*password*" para su uso exclusivo.
- El "*password*" puede ser una combinación de letras y/o números.
- Cambie el "*password*" periódicamente, por ejemplo, cada **30 días** el sistema le solicita un cambio automáticamente.
- Cambie su "*password*" inmediatamente si el mismo es conocido por otro usuario de las computadoras. Comuníquese con la División de Sistemas de Información para servicio.

Qué NO debe hacer:

- NO divulgue su "*password*", preste o transfiera a otro usuario.
- NO escriba ni coloque el "*password*" cerca del terminal.
- NO use un "*password*" que lo asocie a usted, tal como su fecha de nacimiento, su apodo, iniciales o una abreviación de su nombre.

2. Proteja los documentos

A continuación se presenta una serie de actividades que se pueden hacer y que **NO** se deben hacer para proteger los documentos.

Qué debe hacer:

- Guarde los documentos con nombres relacionados con el contenido.
- Procure guardar los documentos constantemente para evitar pérdida de información.
- Guarde siempre los documentos en los cartapacios asignados en el servidor. De esta manera, se podrán recuperar si por alguna razón se corrompen o los borran sin querer.
- Si tiene que salir del escritorio, guarde la información. Presione Ctrl + Alt + Del y luego "*Lock*" para bloquear el documento y no permitir que accedan a su computadora.

Qué NO debe hacer:

- NO deje un archivo visible, ciérrelo si va a estar fuera de su escritorio. Recuerde que la información es confidencial.
- NO guarde los documentos en el disco duro c:\, ya que no se podrá tomar "*back-up*" en caso de que haya problemas con el documento o la computadora.
- NO deje la computadora sin bloquear cuando salga de su lugar de trabajo.

3. Protéjase contra los Virus

Un virus es un programa que puede causar daño a otros programas o archivos. Estos programas tienen la capacidad de copiarse y esconderse en otro programa de su máquina. A continuación se incluye una lista de acciones que se deben hacer y que **NO** se debe hacer para proteger la computadora contra virus.

Qué debe hacer

- Observe e informe conducta impropia e inadecuada con las computadoras, como por ejemplo, cambios imprevistos o inexplicables en los archivos.
- Utilice una computadora individual para las demostraciones de programas/aplicaciones por parte del vendedor.
- Cree el hábito de mantener el "*drive*" A abierto, sin ningún disco dentro, a menos que esté trabajando con él.
- Solicite al personal técnico de Sistemas de Información que verifique y active el programa antivirus si ve algo sospechoso en su computadora o muestra algún comportamiento inusual.

Qué NO debe hacer

- NO utilice programas de origen desconocido, ilegal, o que se ofrecen gratis, aún cuando éstos hayan sido provistos por algún "amigo".
- NO utilice programas que no estén relacionados directamente con las funciones de su Equipo o del Banco (juegos, otros).
- NO prenda su computadora con un "*diskette*" desconocido insertado en el "drive" A.
- NO utilice "*diskettes*" de programas de demostración que usted no ha solicitado a un suplidor reconocido.

4. Medidas de Prevención

   a. Elimine de la pantalla información sensible cuando no se encuentre utilizando la computadora.

   b. Elimine la información sensible cuando no sea necesaria.

   c. Proteja la información clasificada durante la impresión de la misma.

   d. Guarde los trabajos en los "*fólder*" asignados cada 15-20 minutos para prevenir que pierda datos por fallas en la electricidad, en los programas o en las máquinas.

   e. Mantenga la computadora bloqueada mientras no esté en su lugar de trabajo.

C. Seguridad de Equipos

El Banco provee equipos de computadoras sofisticados para uso exclusivo de sus empleados en sus funciones operacionales. El uso de estos equipos es administrado por la División de Sistemas de Información.

Sin embargo, el cuidado y seguridad de los mismos depende del usuario. A continuación le ofrecemos ciertas reglas básicas para la protección de los equipos de computadoras:

1. Proteja el Equipo contra Hurto o Acceso No Autorizado

Qué debe hacer:

- Mantenga un inventario actualizado de los equipos de su División.
- Mantenga los "*CD*" de programas y "*diskettes*" que contienen la información bajo llave después de horas de trabajo regulares.
- Registre todos los programas y equipos prestados.

Qué NO debe hacer:

- NO preste ningún equipo a un empleado, para uso fuera de las facilidades del Banco, sin la autorización del Oficial a cargo del Equipo y el registro del mismo.

2. Proteja el Equipo contra Daño Físico

Qué debe hacer:

- Evite el movimiento excesivo del equipo.
- Utilice protectores de seguridad de electricidad necesarios y adecuados (UPS).

Qué NO debe hacer:

- NO coloque equipos, tales como radios cerca del CPU.
- NO coloque alimentos o bebidas cerca de los equipos.
- NO abra archivos si no sabe exactamente lo que está haciendo o de qué trata.
- NO coloque plantas o tiestos sobre la computadora.
- NO pegue papeles de notas en las partes de ventilación de la computadora.
- NO trabaje con grapas o sujetadores de papel sobre el teclado.
- NO debe forzar un "*diskette*" para que entre o salga del "*drive*" A.
- NO fume cerca de la computadora.

D. Responsabilidades

La Gerencia del Banco y todos sus empleados son responsables por cumplir las reglas establecidas en este documento. Sin embargo, algunas áreas tienen responsabilidades específicas relacionadas con sus funciones. Estas se describen a continuación:

1. Equipo de Sistemas de Información

   a. Administrar el acceso de los usuarios a los distintos sistemas y programas y la identificación y claves de acceso ("*User ID*" y "*passwords*") de los mismos, según le son solicitados.

b. Preparar y mantener al día una lista de usuarios con sus identificaciones y el acceso que se le ha otorgado a cada sistema o programa.

c. Mantener un inventario actualizado de los programas y equipos existentes en cada División del Banco.

d. Mantener al día las licencias necesarias para el uso de los programas y un registro de las mismas.

e. Copiar toda información considerada de un nivel crítico y manejada en las computadoras, de acuerdo a unas bases periódicas y resguardarla en un lugar interno y externo.

f. Preparar, implantar y administrar un Plan de Seguridad de Información y de Contingencia para toda la configuración (red local o externa) de las computadoras que procesan información crítica o sensitiva.

g. Probar los programas y las aplicaciones desarrolladas internamente o adquiridas antes de pasarlas al ambiente de producción y darle acceso a los usuarios.

h. Documentar los programas y los procedimientos para que los usuarios puedan hacer el mejor uso de ellos.

i. Asegurarse que los programas cumplan los requerimientos de calidad, seguridad, documentación y apoyo del vendedor.

j. Asegurarse que todo el personal asignado a desarrollar sistemas de aplicaciones, programas u hojas electrónicas en las computadoras estén propiamente adiestrados para esas funciones.

2. Equipo de Recursos Humanos

a. Mantener informado al Gerente de Sistemas de Información de reclutamientos, transferencias, promociones, renuncias, despidos, vacaciones y separación de los deberes de los empleados o personal que estén autorizados a acceder los sistemas de información,

computadoras y programas, con el propósito de cambiar o dejar sin efecto el nivel de acceso de éste.

b. Comunicarle a los empleados el acceso que tendrán a sistemas y programas de información, y la existencia de las políticas establecidas con relación a la seguridad de información y equipos. Obtener la firma de éstos en el Formulario BDE-F.035 *Acuerdo de Confidencialidad y Seguridad de Información y Protección de Equipos* como evidencia de que fue informado de las normas establecidas. Entregar el Formulario una vez firmado a la División de Sistemas de Información.

c. Coordinar adiestramientos con el personal del Banco para proveerles el conocimiento necesario para utilizar eficientemente los equipos y programas de computadoras.

3. Empleados del Banco

a. Es responsable de mantenerse adiestrado en los nuevos programas que se instalen en sus máquinas.

b. Utilizar responsablemente el equipo que está a su cargo.

c. Mantener en buenas condiciones el equipo (limpieza exterior).

d. En caso de las "*laptops*" protegerlas contra robo, manejarla adecuadamente, no exponerla a altas temperaturas y no ingerir alimentos en el momento de su uso.

XVII. PROCEDIMIENTO DE CAMBIO DE CLAVES DE ACCESO LÓGICO A LOS EMPLEADOS

Proceso mediante el cual la División de Sistemas de Información realiza cambios de claves de acceso lógico en los sistemas de información, conforme a la información de reclutamientos, cambios, renuncias, suspensiones o separaciones de empleados del Banco provista por la División de Recursos Humanos.

FUNCIONARIO Y SU RESPONSABILIDAD

- **Gerente de Sistemas de Información**
- **Vicepresidente de Recursos Humanos o persona en quien éste delegue**

1. El **Vicepresidente Ejecutivo de Recursos Humanos o la persona en quien éste delegue**, notifica, mediante correo electrónico, al **Gerente de Sistemas de Información** cuando ocurra un cambio, renuncia, separación o al reclutar nuevos empleados para que realice los cambios necesarios en las claves de acceso lógico.
2. En caso de que el **Gerente de Sistemas de Información** obtenga conocimiento de que haya ocurrido algún reclutamiento, renuncia, separación, cambio en puesto o área de trabajo de algún empleado del Banco y no haya sido notificado por el Vicepresidente Ejecutivo de Recursos Humanos o la persona en quien éste delegue, le enviará la notificación vía correo electrónico al Vicepresidente Ejecutivo de Recursos Humanos para que valide la información. El **Gerente de Sistemas de Información** deberá recibir la validación de parte del **Vicepresidente Ejecutivo de Recursos Humanos** o la persona en quien éste delegue, previo a tomar la acción de cambio de claves de acceso lógico.
3. Toda notificación de suspensiones o separaciones de empleados se trabajará el mismo día en que sea recibido por el **Gerente de Sistemas de Información**, dando de baja los accesos a los Sistemas. Antes de procesar la baja, la División de Sistemas de Información deberá recibir la Certificación de Entrega de Propiedad y Saldo de Deudas Contraídas (**BDE-F.140**) debidamente firmada por las diferentes Divisiones del Banco.
4. Los casos de empleados nuevos o cambios de empleados existentes se trabajarán no más tarde del próximo día laborable, luego de recibir el correo electrónico de parte del **Vicepresidente Ejecutivo de Recursos Humanos.**

XVIII. NORMAS Y PROCEDIMIENTOS PARA EL ENVÍO Y RECIBO DE CORREOS ELECTRÓNICOS Y CORRESPONDENCIA INTERNA

A. Propósito

La División de Sistemas de Información imparte estas normas y procedimientos para el envío y recibo de correspondencia con los siguientes propósitos:

1. Maximizar el uso del Correo Electrónico, lo cual redunda en:

   a. una reducción en el gasto de papel como resultado de una disminución en la impresión de documentos;
   b. mantener records de notificaciones importantes enviadas;
   c. acelerar el envío y recibo de la correspondencia interna;
   d. disminución de interrupciones por llamadas telefónicas;
   e. la transferencia de archivos y documentos sin necesidad de utilizar disquetes.

2. Reducir los costos de impresión de documentos y de uso de "*diskettes*", y

3. Estandarizar el tipo de papel a usar para correspondencia interna y externa.

B. Uso del Correo Electrónico

Con el propósito de reducir el uso del papel y de disquetes, se debe sustituir los documentos impresos con el correo electrónico. Un aviso en el correo electrónico puede ser más efectivo que una llamada telefónica, ya que el destinatario puede recibir el mensaje en el momento más oportuno para él. El procedimiento para el recibo y envío de mensajes a través del correo electrónico es el siguiente:

1. Todos los empleados con facilidades de correo electrónico aparecen en la lista del sistema en el "***Address Book***" (símbolo en forma de libro abierto). Si el destinatario de su correspondencia no aparece en esta lista, envíe la correspondencia al Apoyo Administrativo de la División correspondiente, quien lo imprimirá y entregará al destinatario. Este proceso no elimina la impresión del documento, pero acelera el envío y entrega del mismo.

2. El mensaje en el correo electrónico se redacta, utilizando la opción "***File***", "***New***" o el ícono de "***New Message***". También se puede transmitir un documento preparado en Word, Excel o PowerPoint a través del menú "***File***", "***Send***" que se encuentra en cada uno de estos programas.

3. Designe a una persona en cada División para enviar mensajes informativos a otras divisiones del Banco. Esto evita duplicidad del mensaje, ahorro en tiempo y mantiene cierto estilo de uniformidad en la redacción de los mensajes.

4. Si interesa mantener acuse de recibo y lectura de los mensajes del correo electrónico, debe realizar lo siguiente:

   Seleccione a través del menú "*Tools – Options – Preferences – E-mail options, Tracking options*". Marcar ☐ "*Request a read receipt for all messages I send*". Este record se recibe en su "*folder* ***Inbox***" y puede retenerlo como un acuse de recibo de la correspondencia enviada.

5. Los mensajes emitidos son retenidos temporeramente en el cartapacio de "***Outbox***" hasta tanto son enviados electrónicamente.

6. Se debe archivar los mensajes de los cartapacios ("*folders*") por lo menos una vez al mes. Para esto, debe verificar los mensajes en sus cartapacios "***Sent Items***" e "***Inbox***". Archive los mensajes que estime pertinente y borre los que no necesite guardar. El usuario deberá borrar periódicamente, por lo menos cada quince (15) días, la correspondencia electrónica archivada, de manera que se pueda utilizar al máximo el espacio en disco.

   Para borrar los mensajes, realice lo siguiente:

   a. Mueva los mensajes de estos cartapacios al cartapacio de "***Deleted Items***", utilizando la opción "***Delete***".

   b. Elimine permanentemente los mensajes del cartapacio de "***Deleted Items***", utilizando nuevamente la opción de "***Delete***".

C. Impresión de Documentos

Con el propósito de disminuir los costos de operación, en específico de compra de papel, sin afectar la calidad de los documentos, se incluyen unas guías para imprimir.

1. Imprimir los documentos de uso interno en papel blanco de 20 libras, igual que el utilizado en las fotocopiadoras.

   Si desea incluir el logo del Banco en el documento, la División de Sistemas de Información ha enviado el logo a las computadoras de cada empleado a través del correo electrónico en un documento de Word llamado LOGO.BDE. Se sugiere que se incluya el logo en la opción "*Auto Text*" o "*Auto Correct*" de Word para facilitar su acceso. El proceso es el siguiente:

BANCO DE DESARROLLO ECONOMICO
PARA PUERTO RICO
Estado Libre Asociado de Puerto Rico

"AutoText"

Cómo incluir el logo en la opción "*AutoText*":

⇒ *Acceda el documento LOGO.BDE en* Word.

⇒ Marque ("*click*") encima del logo una vez. Verá un recuadro negro alrededor del mismo.

⇒ Acceda la opción "*Edit/AutoTerxt*"

⇒ Incluya LOGO.BDE en el campo "*Name*"

⇒ Seleccione la opción "*Add*"

Para acceder el logo una vez incluido en "*AutoText*":

⇒ Posicione el cursor en el área del documento donde desea incluir el logo.

⇒ Acceda la opción "*Edit/AutoText*"

⇒ Seleccione el logo deseado y la opción "*Insert*"

"AutoCorrect"

Cómo incluir el logo en la opción "*Auto Correct*":

⇒ Acceda el documento LOGO.BDE en Word.

⇒ Marque ("*click*") encima del logo una vez. Verá un recuadro negro alrededor del mismo.

⇒ Acceda la opción "*Tools/AutoCorrect*"

⇒ Incluya LOGO.BDE en el campo "*Replace*"

⇒ Seleccione la opción "*OK*"

Para acceder el logo una vez incluido en "*AutoText*":

⇒ Posicione el cursor en el área del documento donde desea incluir el logo.

⇒ Escriba la palabra LOGO.BDE y presione "*Enter*". Obtendrá el logo del Banco.

2. Utilice papel timbrado para correspondencia externa solamente.

Es importante que los clientes externos identifiquen claramente al Banco. El logo y los colores ayudan a lograrlo. Es por eso que se utiliza papel timbrado **solamente** para correspondencia cuyo destinatario es externo al Banco. El logo del Banco es de color dorado.

3. Imprima en las dos caras del papel.

Como medida de reducción de gastos y de protección al ambiente, se debe considerar imprimir algunos documentos en las dos caras del papel. El empleado debe utilizar su discreción a estos efectos, especialmente cuando se preparan borradores. De igual forma, se debe utilizar el mecanismo de fotocopiar los documentos en los dos lados del papel.

Si la impresora que usualmente utiliza no tiene la capacidad de impresión por ambos lados del papel, puede imprimir en la impresora más cercana que esté conectada a la Red de Sistemas de Información.

XIX. PROCEDIMIENTO PARA ACTUALIZAR LA PÁGINA DE INTERNET

A. Propósito

Establecer un mecanismo de control uniforme para mantener actualizada la información, realizar revisiones periódicas y autorizar cambios a la página electrónica (en Internet) del Banco.

B. Alcance

La División de Sistemas de Información tiene la responsabilidad de realizar, a través de un Desarrollador de Aplicaciones, aquellos cambios solicitados, debidamente autorizados, a la página de Internet del Banco. Las Áreas o Divisiones del Banco deberán someter los cambios pertinentes, utilizando el Formulario **BDE-SI-F.125** Petición de Cambios a la Página de Internet del BDE.

C. Empleado y su Responsabilidad

- **Gerente de Sistemas de Información**
- **Supervisor de Desarrollo de Aplicaciones**
- **Desarrollador de Aplicaciones**
- **Vicepresidente Ejecutivo de Finanzas y Operaciones**
- **Usuarios**

D. Peticionarios que Solicitan cambios a la Página de Internet

- **Vicepresidente Ejecutivo de Desarrollo de Negocios**
- **Gerente de Comunicaciones**
- **Supervisor de Administración de Propiedades**
- **Gerente de Recursos Humanos**
- **Oficial de Cumplimiento**
- **Asistente Administrativo**

E. Asignación de Responsabilidad

1. Será responsabilidad de cada **Peticionario** revisar cada quince (15) días la información contenida en la página de Internet del Banco relacionada a su Área o División de trabajo; y verificar que la misma contiene la información correcta y actualizada.

2. Si al revisar la página se percata que existe la necesidad de realizar algún cambio a la misma, deberá informarlo al Gerente de Sistemas de Información, utilizando el Formulario BDE-SI-F.125 creado para este propósito e indicar la vigencia o vencimiento de la información a modificar.

3. Si no hay cambios, deberá notificarlo, utilizando el correo electrónico, al Desarrollador de Aplicaciones y copiar al Gerente de Sistemas de Información, confirmando que se hizo la revisión y que no hay necesidad de cambio.

4. De surgir cambios antes de la fecha de revisión, será responsabilidad de cada Peticionario someter el Formulario de cambios, una vez tenga conocimiento de la necesidad de actualizar la página.

    a. Cada Peticionario deberá completar en el Formulario BDE-SI-F.125 la información solicitada en la parte de: <u>INFORMACIÓN DEL PETICIONARIO</u>.

    b. Debe ser claro y específico en cuanto a la petición, cambio o información solicitada; y de ser necesario, presentar evidencia o justificación para dicho cambio e indicar su vigencia/vencimiento, si aplica.

    c. El **Gerente de Sistemas de Información** recibirá la petición y la referirá al **Supervisor de Desarrollo de Aplicaciones** o a la persona designada por éste.

5. El **Desarrollador de Aplicaciones** o **persona designada** por el **Gerente de Sistemas de Información**, recibirá el Formulario con los cambios solicitados. Realizará los mismos en la página de Internet del Banco.

De surgir alguna duda, se comunicará con el **Peticionario** para aclarar las mismas. Si la información tiene fecha de vigencia o vencimiento, deberá anotarlo en su agenda electrónica para que le avise automáticamente cuando tiene que realizar los cambios.

Una vez finalizado el servicio, completará la información correspondiente en el Formulario y lo referirá al **Gerente de Sistemas de Información** para que revise y certifique que la información es correcta.

6. El Peticionario revisará y firmará en la parte de **CERTIFICACIÓN DE ACEPTACIÓN** y devolverá la misma al **Gerente de Sistemas de Información**.

7. El Gerente de Sistemas de Información referirá el Formulario al **Vicepresidente Ejecutivo de Finanzas y Operaciones** para su firma.

8. Luego de completadas las firmas requeridas, el **Asistente Administrativo** de la División de Sistemas de Información archivará el documento original en la División.

XX. PROCEDIMIENTO PARA LA SOLICITUD DE CREACIÓN, MODIFICACIÓN O IMPRESIÓN DE INFORMES A SISTEMAS DE INFORMACIÓN

A. Propósito

Establecer un mecanismo de control para la Solicitud de Creación, Modificación o Impresión de Informes a la División de Sistemas de Información para evitar la duplicidad y gastos de papel al centralizar los mismos en el Intranet.

B. Alcance

La División de Sistemas de Información tiene la responsabilidad de adoptar nuevos controles en la solicitud de Informes, debidamente autorizados por el Vicepresidente Ejecutivo de Área del Banco donde se origina la solicitud y el Vicepresidente Ejecutivo de Finanzas y Operaciones o por la Presidenta.

La autorización de los Informes localizados en el Intranet se hace una sola vez. Si se requiere la integración de un informe nuevo, la solicitud debe hacerse utilizando el Formulario de Solicitud para la Creación, Modificación o Impresión de Informes a Sistemas de Información.

Todos los informes generados internamente y utilizados en la operación del Banco deben estar autorizados conforme a este Procedimiento.

C. Empleado y su Responsabilidad

- **Gerente de Sistemas de Información**
- **Supervisor de Desarrollo de Aplicaciones**
- **Técnico de Computadoras**
- **Peticionarios**
- **Vicepresidente Ejecutivo de Área**
- **Vicepresidente Ejecutivo de Finanzas y Operaciones o Presidente**

1. Será responsabilidad de cada **Peticionario** que requiera un Informe, completar el Formulario de Solicitud de Creación, Modificación o Impresión de Informe; y que la misma sea autorizada por el **Vicepresidente**

Ejecutivo del Área. En ésta se debe indicar si el informe es de uso recurrente para ser ubicado en el Intranet.[2]

2. Una vez autorizada la petición en el Formulario, éste debe ser entregado al **Gerente de Sistemas de Información** para canalizar la petición al recurso necesario. Si requiere la creación de un Informe nuevo, se canalizará a través del **Supervisor de Desarrollo de Aplicaciones**. Si la solicitud es para imprimir un informe, se refiere a los **Técnicos de Computadoras**, según determine el **Gerente de Sistemas de Información**.

3. El recurso que desarrolle o imprima el Informe, lo entregará al **Peticionario** o al **Vicepresidente Ejecutivo del Área**, tomando la firma de éste en el Formulario, como Aceptación, una vez finalizado.

4. La petición debe ser revisada y autorizada por el **Vicepresidente Ejecutivo de Finanzas y Operaciones** o por el **Presidente** del Banco.

5. El Formulario original será archivado en la División de Sistemas de Información.

[2] Informes de uso NO recurrente no serán incluidos en el Intranet

XXI. PROCEDIMIENTO PARA LA SOLICITUD DE CREACIÓN O MODIFICACIÓN DE PROGRAMAS CREADOS POR SISTEMAS DE INFORMACIÓN

A. Propósito

Establecer un mecanismo de control para la solicitud de creación o modificación de programas creados en la División de Sistemas de Información, de manera que éstos sean planificados y evaluados en términos de la necesidad de mejorar los servicios en las diferentes áreas de trabajo del Banco.

B. Alcance

La División de Sistemas de Información tiene la responsabilidad de adoptar nuevos controles en la solicitud de desarrollo de programas debidamente autorizados por el Comité de Tecnología, el Vicepresidente Ejecutivo de Área, y el Vicepresidente Ejecutivo de Finanzas y Operaciones o por el Presidente del Banco.

La solicitud de algún programa debe hacerse utilizando el Formulario de Solicitud para la Creación o Modificación de Programas a Sistemas de Información; y debe ser revisada por el Comité de Tecnología.

C. Empleados y su Responsabilidad

- **Gerente de Sistemas de Información**
- **Supervisor de Desarrollo de Aplicaciones**
- **Desarrollador de Aplicaciones**
- **Peticionarios**
- **Vicepresidente Ejecutivo de Área**
- **Vicepresidente Ejecutivo de Finanzas y Operaciones o Presidente**
- **Comité de Tecnología**

1. Será responsabilidad de cada **Peticionario** que requiera la creación de un programa o la modificación de uno ya existente, completar el Formulario de Solicitud de Creación o Modificación de Programas; y que la misma sea autorizada por el **Vicepresidente Ejecutivo de Área**.

2. Una vez autorizada la petición en el Formulario, éste debe ser entregado al **Gerente de Sistemas de Información** para canalizar la petición al recurso necesario. Si requiere la creación de un programa nuevo, se canalizará a través del **Supervisor de Desarrollo de Aplicaciones**. Si requiere la creación de un programa nuevo, se canalizará a través del **Supervisor de Desarrollo de Aplicaciones**. Dependiendo de la complejidad del programa a crear, ésta será revisada por el Comité de Tecnología para determinar si es necesaria y viable con los recursos disponibles. El Comité de Tecnología toma la decisión de aprobar o rechazar la solicitud de creación de programas.

3. Si la solicitud es para modificar un programa existente, se refiere al **Desarrollador de Aplicaciones** que lo creó o a la persona a cargo del mismo.

4. El recurso que desarrolle o modifique un programa, lo entregará al **Peticionario**, tomando la firma de éste en el Formulario, como aceptación, una vez finalizado.

5. Además, la petición debe ser aceptada por el **Vicepresidente Ejecutivo de Finanzas y Operaciones** o por el **Presidente** del Banco.

6. El Formulario original será archivado en la División de Sistemas de Información.

XXII. DEROGACIONES

El ***Manual de Procedimientos de la División de Sistemas de Información*** deroga los siguientes Procedimientos:

A. SI-P.003 – Verificación del Acceso de Entrada al Centro de Cómputos 2 de abril de 2001

B. SI-P.001 – Solicitud de Acceso al Sistema de Préstamos de 2 de abril de 2001

C. SI-P.002 – Verificación del Informe de Excepciones de 2 de abril de 2001

D. SI-P.004 – Recibo, Almacenamiento e Inventario de Aplicaciones de 2 de abril de 2001

E. SI-P.005 – Resguardo de Servidores de 30 de junio de 2005

F. SI-P.006 – Corrida Nocturna en el Centro e Cómputos (OFF-LINE) de 2 de abril de 2001

G. SI-P.008 – Recuperación ante Incidentes de Seguridad de 30 de junio de 2005

H. SI-P.009 – Apagar y Encender las Baterías del Centro de Cómputos de 30 de junio de 2005

I. PC-SI-P.001 – Plan de Contingencia de 2 de abril de 2001

J. Guías y Normas de Seguridad para el Usuario de Computadoras de 29 de agosto de 1996

K. Normas y Procedimientos para el Envío y Recibo de Correo Electrónico y Correspondencia Interna de 29 de agosto de 1996 y enmendadas el 22 de junio de 2001

L. SI-P.007 – Procedimiento para Actualizar la Página de Internet de 1 de noviembre de 2005

XXIII. RECOMENDACIÓN

El ***Manual de Procedimientos de Sistemas de Información*** ha sido recomendado por el Gerente de Sistemas de Información y la Vicepresidenta Ejecutiva de Finanzas y Operaciones del Banco de Desarrollo Económico para Puerto Rico.

Jorge Samalot Laboy
Gerente
División de Sistemas de Información
Banco de Desarrollo Económico
para Puerto Rico

Ivonne Otero Guzmán
Vicepresidenta Ejecutiva
Área de Finanzas y Operaciones
Banco de Desarrollo Económico
para Puerto Rico

XXIV. APROBACIÓN

El ***Manual de Procedimientos de Sistemas de Información*** ha sido aprobado por la Presidenta del Banco de Desarrollo Económico para Puerto Rico, en San Juan de Puerto Rico el 12 de diciembre de 2006 y enmendado el 31 de enero de 2008, 14 de octubre de 2009 y 30 de agosto de 2010. Estará vigente inmediatamente después de su aprobación.

Lizzie M. Rosso Tridas
Presidenta
Banco de Desarrollo Económico
para Puerto Rico