



**BANCO DE DESARROLLO ECONOMICO
PARA PUERTO RICO**

Estado Libre Asociado de Puerto Rico

**ÁREA DE FINANZAS Y OPERACIONES
DIVISIÓN DE SISTEMAS DE INFORMACIÓN**

MANUAL DE SEGURIDAD

BDE-005-SI-Proc.02

Aprobado el 9 de septiembre de 2008

 BANCO DE DESARROLLO ECONOMICO PARA PUERTO RICO Estado Libre Asociado de Puerto Rico		DIVISIÓN DE SISTEMAS DE INFORMACIÓN MANUAL DE SEGURIDAD
Procedimiento Núm.: BDE-005-SI-Proc.02	Deroga a: Manual de Seguridad 27 de junio de 2001	Fecha de aprobación: 9 de septiembre de 2008

TABLA DE CONTENIDO

INTRODUCCIÓN	1
A. PROPÓSITO	1
B. ALCANCE.....	1
C. RESPONSABILIDAD.....	1
D. DEFINICIONES	3
E. CONTROLES DE SEGURIDAD.....	4
F. VULNERABILIDAD DE LOS SISTEMAS DE INFORMACIÓN	11
CAPÍTULO I – CONTROLES DE SEGURIDAD ADMINISTRATIVOS	13
A. SEGURIDAD FÍSICA.....	13
B. ADIESTRAMIENTO DEL PERSONAL	15
C. CONTRATACIÓN DE AYUDA EXTERNA.....	16
D. PROTECCIÓN DE LA INTIMIDAD	18
CAPÍTULO II – CONTROLES DE SEGURIDAD DE ACCESO	21
A. ADMINISTRACIÓN DE CONTRASEÑAS	21
B. VIOLACIÓN Y REPORIES DE SEGURIDAD	29
C. NIVELES DE SEGURIDAD	29
CAPÍTULO III – CONTROLES DE SEGURIDAD PARA EL RESGUARDO DE DATOS (BACKUP).....	30
A. ESTÁNDAR DE RESGUARDO DE DATOS (<i>BACKUP</i>).....	30
B. USO DE COPIAS <i>BACKUP</i>	30
C. PROCEDIMIENTOS DE <i>BACKUP</i>	31
D. MANEJO DE DISCOS.....	31
E. MANEJO DE CINTAS Y CARTUCHOS	32
F. <i>BACKUP</i> COMPUTADORAS Y TERMINALES.....	32

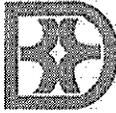


Procedimiento Núm.:
BDE-005-SI-Proc.02

Deroga a:
Manual de Seguridad
27 de junio de 2001

Fecha de aprobación:
9 de septiembre de 2008

CAPÍTULO IV – CONTROLES DE SEGURIDAD DE VIRUS Y PIRATAS	33
A. CONTROLES PARA MINIMIZAR ERROR, ABUSO Y CRÍMENES DE COMPUTADORAS	33
B. RESPONSABILIDADES	34
C. ETAPAS DE INFECCIÓN VIRAL	34
CAPÍTULO V – CONTROLES DE SEGURIDAD RED DE INFORMACIÓN.....	37
A. ESTÁNDAR DE ACCESO	37
B. PROTOCOLOS Y DIRECCIONES	38
C. DISPOSITIVOS DE CONEXIÓN E INTERCONEXIÓN	39
D. SERVIDORES DE ARCHIVOS	40
E. CORREO ELECTRÓNICO.....	41
F. CONEXIÓN REMOTA Y PROCESO DISTRIBUIDO	42
G. CONTROLES DE SEGURIDAD.....	43
H. CONTROLES DE SEGURIDAD PARA LAS ESTACIONES DE TRABAJO.....	46
I. CONTROLES DE SEGURIDAD PARA LOS SERVIDORES.....	48
J. CONTROLES DE SEGURIDAD DE COMPONENTES.....	49
K. CONTROLES DE SEGURIDAD PARA LAS COMUNICACIONES	50
L. CONTROLES DE SEGURIDAD DE LA BASE DE DATOS	51
M. CONTROLES DE SEGURIDAD DE CONEXIÓN AL <i>MAINFRAME</i>	51
N. CONTROLES DE SEGURIDAD ADMINISTRATIVOS	51
CAPÍTULO VI – CONTROLES DE SEGURIDAD <i>SOFTWARE</i>.....	53
A. DERECHOS DE PROPIEDAD INTELECTUAL	53
B. CONTROLES DE SEGURIDAD <i>SOFTWARE</i>	53
C. LICENCIAS DE <i>SOFTWARE</i>	54
D. CONTROLES DE SEGURIDAD DE PROGRAMACIÓN.....	55
E. INSTALACIÓN Y MANTENIMIENTO DE PROGRAMAS.....	56
F. PROCEDIMIENTOS DE OPERACIÓN	57

 BANCO DE DESARROLLO ECONOMICO PARA PUERTO RICO Estado Libre Asociado de Puerto Rico		DIVISIÓN DE SISTEMAS DE INFORMACIÓN MANUAL DE SEGURIDAD
Procedimiento Núm.: BDE-005-SI-Proc.02	Deroga a: Manual de Seguridad 27 de junio de 2001	Fecha de aprobación: 9 de septiembre de 2008

CAPÍTULO VII – SEGURIDAD OCUPACIONAL	59
A. CONTROL Y PREVENCIÓN DE RIESGOS A LA SALUD	59
B. MEDIDAS DE PROTECCIÓN CONTRA INCENDIOS	60
CAPÍTULO VIII – MANTENIMIENTO DE LA SEGURIDAD	61
A. AUDITORÍAS DE SEGURIDAD	61
B. ÓRDENES DE SERVICIO	61
C. ADIESTRAMIENTO DE PERSONAL	61
D. NOTIFICACIÓN DE EVENTOS	62
E. CONTROL DE CAMBIOS	62
F. MANTENIMIENTO DE LA SEGURIDAD	62
CAPÍTULO IX – CLÁUSULAS FINALES.....	64
A. DEROGACIÓN	64
B. RECOMENDACIÓN	64
C. APROBACIÓN.....	64
APÉNDICE	65

 BANCO DE DESARROLLO ECONOMICO PARA PUERTO RICO Estado Libre Asociado de Puerto Rico		DIVISIÓN DE SISTEMAS DE INFORMACIÓN MANUAL DE SEGURIDAD
Procedimiento Núm.: BDE-005-SI-Proc.02	Deroga a: Manual de Seguridad 27 de junio de 2001	Fecha de aprobación: 9 de septiembre de 2008

INTRODUCCIÓN

A. PROPÓSITO

El propósito del Manual de Seguridad de Sistemas de Información es establecer los parámetros y controles que deben seguir el personal de la División de Sistemas de Información y los usuarios de computadoras del Banco de Desarrollo Económico para Puerto Rico para:

1. Garantizar la protección de los Sistemas de Información y asegurar que la información es correcta y confiable.
2. Describir cómo los sistemas de información son vulnerables a destrucción, error y abuso.
3. Completar las auditorías de seguridad para el mantenimiento y cumplimiento de los controles de seguridad establecidos.
4. Completar los procedimientos de operación para la administración adecuada de la seguridad en los Sistemas de Información.
5. Establecer controles de seguridad ocupacionales para evitar lesiones en el trabajo, a través del uso correcto de los sistemas computadorizados.
6. Establecer controles de seguridad para la prevención de fuego y situaciones de emergencia.

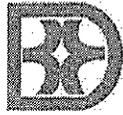
B. ALCANCE

Este Manual de Seguridad aplica a los Sistemas de Información, los equipos que lo componen (*hardware*), a todos los programas y aplicaciones utilizados en el Sistema (*software*) y a todo el personal del Banco de Desarrollo Económico para Puerto Rico (*humanware*).

C. RESPONSABILIDAD

El personal descrito a continuación tiene responsabilidades específicas de seguridad en la **División de Sistemas de Información**:

1. **Oficial de Seguridad de Informática** o designado, es responsable de:
 - Asegurar el cumplimiento de las auditorías de seguridad, planes de acciones correctivas, notificación de eventos y control de cambios en los procedimientos de seguridad establecidos.



Procedimiento Núm.:

BDE-005-SI-Proc.02

Deroga a:

**Manual de Seguridad
27 de junio de 2001**

Fecha de aprobación:

9 de septiembre de 2008

- Asegurar el cumplimiento de los controles de acceso establecidos y de la administración de contraseñas.
 - Asegurar que las Licencias de Usuarios y Contratos de Licencias de Programas (*software*) sean actualizados y mantenidos en conformidad con los controles de seguridad establecidos.
 - Asegurar el cumplimiento de los controles de seguridad establecidos para la operación de la Red de Información, computadoras, terminales y equipos (*hardware*).
 - Asegurar el cumplimiento de los controles de seguridad establecidos por el personal del Centro de Cómputos (Operadores y Técnicos).
 - Asegurar el cumplimiento de los procedimientos de resguardo de datos (*backup*), recobro (*recovery*), seguridad de la base de datos y mantenimiento de la seguridad en los sistemas de información en conformidad con los controles técnicos y procedimientos establecidos.
2. **Supervisor de Desarrolladores** o persona designada, en coordinación con el Oficial de Seguridad, es responsable de:
- Asegurar el cumplimiento de los controles de seguridad establecidos para los programas y aplicaciones (*software*)
 - Asegurar el cumplimiento de los controles de seguridad establecidos por el personal de desarrollo de aplicaciones (Desarrolladores)
3. **Gerente de la División de Sistemas de Información** o persona designada es responsable de:
- Asegurar el cumplimiento de los controles de seguridad administrativos establecidos para el sistema de información.
 - Asegurar que se hayan establecido los procedimientos, planes y controles de seguridad necesarios para la operación segura de los sistemas de información que garanticen la realización de las funciones del Banco, en conformidad con las prácticas de seguridad de aceptación general para los sistemas de información en la industria bancaria y el Gobierno.

En relación con los Sistemas de Información, **personal del Banco** tiene responsabilidades específicas de seguridad descritas a continuación:

1. **Oficial de Seguridad Física (Guardia de Seguridad del Banco)** o persona designada, es responsable de:

 BANCO DE DESARROLLO ECONOMICO PARA PUERTO RICO Estado Libre Asociado de Puerto Rico		DIVISIÓN DE SISTEMAS DE INFORMACIÓN MANUAL DE SEGURIDAD
Procedimiento Núm.: BDE-005-SI-Proc.02	Deroga a: Manual de Seguridad 27 de junio de 2001	Fecha de aprobación: 9 de septiembre de 2008

- Velar por la seguridad física de las facilidades del Banco y de los equipos de computadoras.
2. **Todos los usuarios de los Sistemas de Información** son responsables de:
- Cumplir con los controles y procedimientos de seguridad aplicables a los usuarios de computadoras establecidos en este Manual.
3. **Todos los Vicepresidentes Ejecutivos, Gerentes y Supervisores de las diferentes Áreas o Divisiones del Banco** son responsables de:
- Asegurar que el personal del Banco que está bajo su supervisión cumpla con los procedimientos y controles de seguridad que le sean aplicables, según establecidos en este Manual.

D. DEFINICIONES

1. 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 término presente también incluye el futuro; las palabras usadas en 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.
2. En particular – Las definiciones que aparecen en este inciso, aplican a todo el Manual. Las palabras y frases que a continuación se mencionan son términos cortos o conceptos de las siguientes definiciones:
 - a. BDE o Banco – Se refiere al Banco de Desarrollo Económico para Puerto Rico.
 - b. Contraseña o Código de Acceso – Se refiere al código secreto o que permite el acceso a algo, a alguien o a un grupo de personas antes inaccesible.
 - c. Controles de Seguridad – Son todos los métodos, estándares y procedimientos que aseguran la protección de los activos del Banco, la exactitud y confianza de la información y la adherencia a los estándares de seguridad establecidos a través de medidas automáticas, electrónicas o manuales.
 - d. Crímenes de Computadoras – Se refiere a la comisión de actos ilegales a través del uso de una computadora o en contra de un sistema computadorizado. Algunos ejemplos son: destruir el Centro de Cómputos o los archivos de computadora, robar listas de computadora ilegalmente, lograr acceso no autorizado a un sistema computadorizado, usando una



Procedimiento Núm.:

BDE-005-SI-Proc.02

Deroga a:

**Manual de Seguridad
27 de junio de 2001**

Fecha de aprobación:

9 de septiembre de 2008

computadora desde la casa, o simplemente por lograr acceso a un sistema computadorizado sin autorización, intento de dañar un sistema computadorizado o daños por accidente de un sistema computadorizado. Los crímenes de computadoras incluyen introducción de virus, robo de servicios, interrupción de servicios y robo de servicios de telecomunicaciones o redes de información.

- e. Manual – Se refiere al Manual de Seguridad de Sistemas de Información.
- f. Piratas de Computadoras – Son personas ajenas a la institución que logran acceso no autorizado a la red de información para propósitos criminales, ganancia o placer personal. Se les conoce también como *hackers*.
- g. 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.
- h. Virus de Computadora – Es un programa *software* usado para destruir datos en un computador. Después que se escribe el código del virus, se oculta en un programa existente. Una vez el programa se ejecuta, el código del virus también se activa y agrega copias de sí mismo a otros programas en el sistema. Los programas infectados copian el virus a otros programas.

E. CONTROLES DE SEGURIDAD

Los controles de seguridad de los Sistemas de Información se clasifican en dos (2) grupos principales:

1. **Controles Generales** – establecidos para establecer el control de diseño, seguridad y uso del sistema computadorizado.
2. **Controles de Aplicación** – controles específicos únicos para cada aplicación computadorizada.

Los componentes de los **Controles Generales de la Seguridad de los Sistemas** son: (1) Controles de Implementación, (2) Controles de *software*, (3) Controles Físicos de *hardware*, (4) Controles de Operación, (5) Controles de Seguridad de los datos y (6) Controles Administrativos, descritos a continuación:

1. Controles de Implementación

Son los controles establecidos en la fase de diseño e implementación, que aseguran que el sistema computadorizado es el adecuado y está debidamente controlado y administrado para

 BANCO DE DESARROLLO ECONOMICO PARA PUERTO RICO Estado Libre Asociado de Puerto Rico		DIVISIÓN DE SISTEMAS DE INFORMACIÓN MANUAL DE SEGURIDAD
Procedimiento Núm.: BDE-005-SI-Proc.02	Deroga a: Manual de Seguridad 27 de junio de 2001	Fecha de aprobación: 9 de septiembre de 2008

cumplir con las funciones automatizadas y electrónicas para las cuales fue diseñado. Estos incluyen:

- a. **Auditorías del Sistema** – en la fase de diseño e implementación se completan auditorías del sistema en varios puntos y etapas que aseguren que el diseño fue debidamente implementado y que permita a los usuarios evaluar, aprobar y desaprobado la implementación efectuada.
- b. **Técnicas de Garantía de Calidad** – uso de pruebas para validar el desarrollo de programas, aplicaciones, conversión y calidad de los sistemas de información.
- c. **Documentación apropiada** – documentar todas las actividades e información en la etapa de implementación de las siguientes actividades principales:
 - Flujograma del Sistema (*flowchart*)
 - Diseño de Archivos (*files*)
 - Diseño de Registros (*records*)
 - Lista de Programas y Módulos
 - Gráficas de Estructuras de Programas
 - Narrativa del Programa y Descripción de Módulos
 - Lista de Programas Fuente
 - Referencias de Módulos
 - Condiciones de Error y Acciones Correctivas
 - Terminación Anormal
 - Requisitos de Ajustes de Trabajos (*job setup*)
 - Itinerarios de Corridas de Trabajos (*job run*)
 - Distribución de Reportes y Salidas (*output*)
 - Desarrollador(es) Responsable(s)
 - Lista de Lenguaje Control de Trabajos
 - Procedimientos de Resguardo (*backup*) y Recobro (*recovery*)
 - Procedimientos de Corridas de Control (Validación y Prueba)
 - Procedimientos de Acceso

 BANCO DE DESARROLLO ECONOMICO PARA PUERTO RICO Estado Libre Asociado de Puerto Rico		DIVISIÓN DE SISTEMAS DE INFORMACIÓN MANUAL DE SEGURIDAD
Procedimiento Núm.: BDE-005-SI-Proc.02	Deroga a: Manual de Seguridad 27 de junio de 2001	Fecha de aprobación: 9 de septiembre de 2008

- Requisitos de Operación de los Equipos (*hardware*)
- Diseño de Reportes y Salidas de Muestra (*output*)
- Diseño de Formas de Entrada (*input*) y Pantallas (*screens*)
- Instrucciones de la Preparación de Datos (*data*)
- Instrucciones de Datos de Entradas (*input*)
- Métodos de Seguridad
- Descripción Funcional del Sistema
- Flujo de Trabajos
- Procedimientos de Corregir errores
- Responsabilidad del Usuario
- Procedimientos de Operación de los Procesos
- Descripción de Controles de Calidad y Seguridad

2. Controles de *Software*

Son los controles establecidos para el uso y monitoreo de los programas y aplicaciones en el Sistema de Información, incluyendo evitar el acceso no autorizado. Estos incluyen:

- a. **Recursos** – coordinar y establecer los recursos de computadoras para facilitar la ejecución de programas y aplicaciones.
- b. **Programas** – controlar el uso de compiladores, programas de utilidades, operaciones, reportes, ajuste de archivos, manejo y registros de bibliotecas.
- c. **Datos** – control de programas que procesan datos y archivos de datos.
- d. **Controles de Seguridad** – asegurar que los programas son diseñados para evitar cambios no autorizados a los programas del sistema en ambiente de producción (Control de Cambios).

3. Controles Físicos del *Hardware*

Son los controles que garantizan que los equipos de computadoras están físicamente seguros y cotejan fallas en los equipos. Estos incluyen:

 BANCO DE DESARROLLO ECONOMICO PARA PUERTO RICO Estado Libre Asociado de Puerto Rico		DIVISIÓN DE SISTEMAS DE INFORMACIÓN MANUAL DE SEGURIDAD
Procedimiento Núm.: BDE-005-SI-Proc.02	Deroga a: Manual de Seguridad 27 de junio de 2001	Fecha de aprobación: 9 de septiembre de 2008

- a. **Seguridad Física** – asegurar que los sistemas de información son accedidos sólo por personal autorizado.
- b. **Acceso controlado al Centro de Cómputos** – sólo se permite el acceso a esta área al personal de la División de Sistemas de Información.
- c. **Computadoras del Banco** – son mantenidas en áreas seguras u oficinas cerradas (*locked*).
- d. **Equipos de computadoras** – son protegidos contra fuego, humedad y temperatura extrema.
- e. **Cotejos de Paridad (*parity checks*)** – para detectar fallas responsables de alterar *bits* en *bytes* durante los procesos.
- f. **Cotejos de Validez (*validity checks*)** – para cotejar la estructura del *ON-OFF bits* en *bytes* durante los procesos.
- g. **Cotejos *Echo*** – para verificar que el equipo está listo para operar.

4. **Controles de Operación**

Son los controles establecidos por la División de Sistemas de Información y los procedimientos programados en el sistema, que deben ser correctos y consistentes cuando son aplicados a los datos, archivos de datos almacenados y procesamiento de los datos. Estos incluyen:

- a. Control de ajuste de procesos de trabajo
- b. Programas de Operación
- c. Operación de Computadoras
- d. Resguardo de datos (*backup*)
- e. Recobro de procesos que terminan anormalmente (*recovery*)
- f. Procedimientos de corridas de trabajo automáticas
- g. Procedimientos para evitar y detectar errores
- h. Documentación de *backups*, discos, cintas y cartuchos

 BANCO DE DESARROLLO ECONOMICO PARA PUERTO RICO Estado Libre Asociado de Puerto Rico		DIVISIÓN DE SISTEMAS DE INFORMACIÓN MANUAL DE SEGURIDAD
Procedimiento Núm.: BDE-005-SI-Proc.02	Deroga a: Manual de Seguridad 27 de junio de 2001	Fecha de aprobación: 9 de septiembre de 2008

- i. Detección de errores humanos del operador, técnicos y usuarios
- j. Reporte del sistema detallando todas las actividades durante los procesos, fallas *hardware* y *software*, proceso de recobro de programas de producción, programas en el sistema y archivo de datos, para verificar cambios o errores en el sistema.

5. Control de Seguridad de los Datos

Son los controles establecidos para velar que los archivos de datos en disco, cintas o cartuchos estén protegidos de acceso no autorizado, cambio o destrucción. Estos incluyen:

- a. **Archivos de Datos** – controles para archivos de datos en uso, almacenados y en sistemas *batch* por los operadores que corren los procesos.
- b. **Acceso de Sistemas Online o Real Time** – a través de computadoras o terminales para evitar acceso no autorizado.
- c. **Terminales Físicamente Restringidos** – para ser utilizados solamente por personal autorizado.
- d. **Uso de Contraseñas** – asignados solamente al personal autorizado para que ninguna persona pueda acceder al sistema sin una contraseña válida.
- e. **Restricciones de Seguridad** – conjunto de otras contraseñas desarrolladas para sistemas y aplicaciones específicas que limitan el acceso a archivos específicos.

6. Controles Administrativos

Son las reglas, procedimientos formalmente establecidos para asegurar que los controles de seguridad son implantados por la administración y utilizados por el personal. Estos incluyen:

- a. **Segregación de Funciones** – para evitar el riesgo de errores y manipulación fraudulenta: división de responsabilidades del personal de entrada, proceso y salida de los sistemas; separación de funciones de los desarrolladores, técnicos de apoyo y operadores.
- b. **Procedimientos Escritos** – son aprobados por la Gerencia, establecen los controles de operación, estándares del sistema de información y definen claramente las responsabilidades del personal.
- c. **Supervisión del Personal** - asegura que los controles establecidos son seguidos por el personal en conformidad con los procedimientos aprobados.

 BANCO DE DESARROLLO ECONOMICO PARA PUERTO RICO Estado Libre Asociado de Puerto Rico		DIVISIÓN DE SISTEMAS DE INFORMACIÓN MANUAL DE SEGURIDAD
Procedimiento Núm.: BDE-005-SI-Proc.02	Deroga a: Manual de Seguridad 27 de junio de 2001	Fecha de aprobación: 9 de septiembre de 2008

Los componentes de los **Controles de Aplicaciones de la Seguridad** son: (1) Controles de Entrada; (2) Controles de Proceso; y (3) Controles de Salida, descritos a continuación:

1. **Controles de Entrada**

Son los controles establecidos para cotejar que los datos sean exactos y completos al ser entrados al sistema de información. Estos incluyen:

- a. **Autorización de Entrada** – la entrada de datos en el sistema de información es autorizada, registrada y monitoreada por la computadora, incluyendo la identificación o enumeración de los documentos o fuentes de donde se obtienen los datos.
- b. **Conversión de Datos** – los datos entrados al sistema son convertidos por la computadora, sin errores, y transcritos de una forma u otra, incluyendo lector de código de barra y otras técnicas de *scanning*.
- c. **Controles de Totales *batch*** – contar o totalizar los datos en un documento simple o totalizar los campos con cantidades. El total impreso puede reconciliarse manualmente.
- d. **Cotejos *edit*** – son rutinas para verificar errores en los datos entrados antes de ser procesados. Las transacciones que no cumplen los criterios del *edit* son rechazadas. Las rutinas de *edit* generan una lista de errores que pueden ser corregidos posteriormente. Cada transacción de entrada es editada y el operador del Terminal es notificado inmediatamente de cualquier error encontrado. El sistema puede diseñarse para no aceptar ninguna entrada adicional hasta que el error sea corregido o imprimir un reporte de la lista de errores para ser revisado por otras personas. Estos cotejos de *edit* aseguran la razonabilidad y consistencia de los datos.

Los controles de *edit* utilizados generalmente son:

- **Cotejo de Razonabilidad** – los datos deben estar entre los límites previamente establecidos o serán rechazados por el sistema.
- **Cotejo de Formato** – el contenido y firma en los campos de datos son cotejados por el sistema en el formato estándar o *template*.
- **Cotejo de Existencia** – los datos de referencia de entrada son cotejados con tablas o archivos maestros para asegurar que los valores o códigos utilizados son válidos.
- **Cotejo de Dependencia** – existe o se mantiene una relación lógica entre los datos de una misma transacción y cuando no es así, la transacción es rechazada.

 BANCO DE DESARROLLO ECONOMICO PARA PUERTO RICO Estado Libre Asociado de Puerto Rico		DIVISIÓN DE SISTEMAS DE INFORMACIÓN MANUAL DE SEGURIDAD
Procedimiento Núm.: BDE-005-SI-Proc.02	Deroga a: Manual de Seguridad 27 de junio de 2001	Fecha de aprobación: 9 de septiembre de 2008

- **Cotejo de Dígitos** – se entra un código de identificación que posee una relación matemática con los otros dígitos, el cual es recomputado por la computadora y el resultado es comparado con la entrada.

2. Controles de Proceso

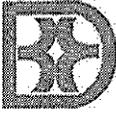
Son los controles establecidos para asegurar que los datos son completos y exactos durante los procesos o durante la actualización de los mismos. Estos incluyen:

- Totales de Control de Corridas** – es la reconciliación de los totales de control de entrada con los totales de cada término (*item*) que ha actualizado su archivo. La actualización puede ser controlada, generando totales de control, para las cantidades críticas y ser comparadas manualmente o por una computadora. Se pueden observar discrepancias en la verificación.
- Comparación por la Computadora (*matching*)** – comparación de los datos de entrada con la información en los archivos maestros o suspensivos, con términos no comparativos, observados en la verificación. La mayor parte de la comparación ocurre en la entrada, y bajo ciertas circunstancias, puede ser necesario asegurar que la actualización ha sido completada. Esta comparación evalúa la razonabilidad de la actualización de los datos.

3. Controles de Salida

Son los controles establecidos que aseguran que los resultados de un proceso computadorizado son exactos, completos y distribuidos correctamente. Estos incluyen:

- Balance de Totales de Salida** – reconciliación de los totales de entrada y de proceso con los totales de salida.
- Logs** – revisión del proceso de la computadora para determinar que todos los trabajos fueron correctamente completados y ejecutados por el sistema durante el proceso.
- Audits** – auditoría de los reportes de salida para verificar que los totales, formatos y detalles críticos son correctos y reconciliables con la entrada.
- Procedimientos** – documentación especificando los recipientes autorizados de reportes de salida, cotejo y otros documentos críticos.

 BANCO DE DESARROLLO ECONOMICO PARA PUERTO RICO Estado Libre Asociado de Puerto Rico		DIVISIÓN DE SISTEMAS DE INFORMACIÓN MANUAL DE SEGURIDAD
Procedimiento Núm.: BDE-005-SI-Proc.02	Deroga a: Manual de Seguridad 27 de junio de 2001	Fecha de aprobación: 9 de septiembre de 2008

Otros mecanismos de control de los Sistemas de Información son establecidos tomando en consideración:

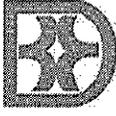
1. **La Importancia de los Datos** – basado en un análisis de costo y beneficio.
2. **Datos Permanentes o Críticos** – datos que pueden afectar las transacciones y fluyen de la entrada a la salida de un sistema. Requieren monitoreo de cerca, pues un error puede afectar muchas o todas las transacciones, cada vez que el archivo sea procesado.
3. **Costo Efectivo de los Controles** – está influenciado por la eficiencia, complejidad y costo de cada técnica para datos críticos como cantidad monetaria y números de cuentas.
4. **Nivel de Riesgo** – evaluar la frecuencia o potencial de que ocurra un error o problema y el daño potencial que causaría (aunque no ocurra) para determinar el costo/beneficio de un control.

F. VULNERABILIDAD DE LOS SISTEMAS DE INFORMACIÓN

Los sistemas computadorizados tienen un rol de suma importancia para el Banco. Los sistemas de información pueden fallar, y como consecuencia, se detiene el trabajo y los procesos requeridos, produciendo pérdidas. La vulnerabilidad de los sistemas de información, debido a eventos o situaciones de emergencia, es uno de los problemas mayores que confrontan las organizaciones que dependen de los sistemas de computadoras. A tal efecto, es necesario establecer controles de seguridad efectivos para proteger la información en el sistema y asegurar que los datos y la información sean exactos y confiables.

Los eventos o situaciones de emergencia que pueden afectar o interrumpir las operaciones computadorizadas son:

- Eventos o desastres naturales
- Fuego
- Sabotaje
- Problemas eléctricos
- Problemas de telecomunicaciones
- Fallas del *hardware*
- Fallas del *software*
- Acciones del personal

 BANCO DE DESARROLLO ECONOMICO PARA PUERTO RICO Estado Libre Asociado de Puerto Rico		DIVISIÓN DE SISTEMAS DE INFORMACIÓN MANUAL DE SEGURIDAD
Procedimiento Núm.: BDE-005-SI-Proc.02	Deroga a: Manual de Seguridad 27 de junio de 2001	Fecha de aprobación: 9 de septiembre de 2008

- Penetración de acceso a terminales
- Robo de datos, servicios o equipos
- Crímenes de computadoras
- Virus de computadoras

Los avances en telecomunicaciones y programas *software* han aumentado la vulnerabilidad de los sistemas de información. Las redes de información *networks* interconectan los sistemas de información en diferentes regiones geográficas, por lo cual, el potencial de acceso no autorizado, abuso o fraude, no está limitado a una sola localización, sino que puede ocurrir en cualquier punto de acceso de la red, incluyendo la propagación de virus de computadora. Los virus de computadoras se propagan rápidamente por los sistemas de computadoras, destruyendo los datos, deteniendo los procesos y afectando los sistemas de memoria.

Existen personas ajenas a la institución que pueden penetrar las redes de información con propósitos criminales, para devengar algún beneficio o por placer personal. **Los controles de seguridad y procedimientos de seguridad establecidos en este Manual** describen los pasos a seguir por el personal del Banco para garantizar la seguridad de los sistemas de información, minimizar la vulnerabilidad de los sistemas y asegurar la realización de las funciones del Banco en una forma continua, segura y confiable.

 BANCO DE DESARROLLO ECONOMICO PARA PUERTO RICO Estado Libre Asociado de Puerto Rico		DIVISIÓN DE SISTEMAS DE INFORMACIÓN MANUAL DE SEGURIDAD
Procedimiento Núm.: BDE-005-SI-Proc.02	Deroga a: Manual de Seguridad 27 de junio de 2001	Fecha de aprobación: 9 de septiembre de 2008

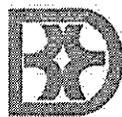
CAPÍTULO I – CONTROLES DE SEGURIDAD ADMINISTRATIVOS

A. SEGURIDAD FÍSICA

El edificio donde está ubicado el Banco tiene un sistema de seguridad física que opera a través del uso de guardias de seguridad en la entrada del edificio en el primer piso. Existe un guardia de seguridad del Banco encargado de la seguridad física de los pisos donde están las oficinas del Banco, velando por los activos del Banco, la seguridad de las facilidades y los equipos computadorizados.

Los procedimientos de seguridad física se describen a continuación:

1. El acceso al Centro de Cómputos está limitado al personal de la División de Sistemas de Información. Los controles de seguridad establecidos son los siguientes:
 - a. La puerta de entrada al Centro de Cómputos, donde están instalados los servidores y la puerta de entrada a la Red de Información, tienen un control de acceso electrónico. El personal de la División de Sistemas de Información puede entrar al área, utilizando una contraseña.
 - b. Solamente el personal autorizado podrá tener acceso al Centro de Cómputos.
 - c. En el evento de ocurrir una falla eléctrica, se podría perder el control de acceso, dejando la puerta abierta. De ocurrir alguna falla en el sistema, hay personal operando el Centro de Cómputos de 5:30 am a 10:30 pm, responsables de controlar el acceso a estas facilidades.
 - d. En el evento de una situación de emergencia, se cerrará con llave la puerta de acceso al Centro de Cómputos, como medida de seguridad, mientras se restaura la energía eléctrica o se presenta algún miembro del personal autorizado de la División de Sistemas de Información para controlar el acceso al lugar.
2. **Cualquier persona no autorizada debe ser escoltada al Centro de Cómputos** por personal autorizado y firmar el Registro de Visitantes a la entrada y salida del mismo.
 - a. El personal no autorizado, que puede ser escoltado al Centro de Cómputos, debe ser: personal operacional del Banco de otras Divisiones o Áreas de trabajo, personal identificado de apoyo, servicio o vendedores. Se debe limitar el acceso a personas conocidas solamente.
 - b. Se deben tomar todas las precauciones necesarias para evitar el acceso no autorizado al área y a los sistemas.



Procedimiento Núm.:

BDE-005-SI-Proc.02

Deroga a:

**Manual de Seguridad
27 de junio de 2001**

Fecha de aprobación:

9 de septiembre de 2008

- c. Se deben cambiar los códigos de acceso al área, cada vez que algún miembro del personal autorizado es removido del área por terminación en el empleo, renuncia o retiro, tan pronto sea posible.

3. La protección de los sistemas de información en el Centro de Cómputos incluye:

- a. **Unidades UPS** – batería o fuente de alimentación ininterrumpida, que sirve de energía de seguridad para los sistemas de computación, cuando la energía eléctrica se interrumpe o baja a un nivel de voltaje inaceptable.
- b. **Unidad de Aire Acondicionado** – el Centro de Cómputos tiene instalada una unidad de aire acondicionado para mantener las especificaciones de temperatura de los sistemas en el Centro de Cómputos y para operar el equipo (*hardware*) de forma segura.
- c. **Humidificador** – el Centro de Cómputos cuenta con una Unidad Humidificadora para controlar la humedad del área, cuando sea necesario.
- d. **Requisitos eléctricos** – el Centro de Cómputos tiene: un panel eléctrico aparte, corriendo con la fuente de energía del edificio; unidades UPS instaladas en los equipos para evitar roturas de disco cuando ocurran fallas eléctricas; y un generador de voltaje o batería para encender las luces de emergencia del Centro de Cómputos.
- e. **Requisitos para prevención de fuego** – El Centro de Cómputos está localizado en un área que no tiene líneas de gas, agua o líquidas, líneas de alto voltaje o radiación magnética adyacentes. Tiene extintores de fuego disponibles, adecuados para protección del equipo en el evento de un fuego y que no causan daño a las personas, además de un sistema de GAS FM-200. Además, tiene detectores de humo instalados.

4. Las reglas de trabajo y prácticas de limpieza en el Centro de Cómputos son las siguientes:

- a. No está permitido fumar, tomar o comer alimentos en el Centro de Cómputos.
- b. Los operadores y técnicos son responsables de mantener el área de trabajo limpia y organizada.
- c. Los operadores no repararán ningún equipo sin la autorización del Gerente de Sistemas de Información o en consulta con el personal de mantenimiento externo o interno correspondiente.
- d. Los operadores y técnicos no alterarán ningún programa sin autorización específica del Gerente de la División de Sistemas de Información.

 BANCO DE DESARROLLO ECONOMICO PARA PUERTO RICO Estado Libre Asociado de Puerto Rico		DIVISIÓN DE SISTEMAS DE INFORMACIÓN MANUAL DE SEGURIDAD
Procedimiento Núm.: BDE-005-SI-Proc.02	Deroga a: Manual de Seguridad 27 de junio de 2001	Fecha de aprobación: 9 de septiembre de 2008

- e. No utilizarán los sistemas de información para otras funciones que no sean las operaciones asignadas.
5. **Existe un Plan de Contingencia** para el recobro y continuar las operaciones del Banco en el evento de un desastre, emergencia, falla del *hardware* o *software*. (Refiérase al Manual de Procedimientos de Sistemas de Información)
 6. **El personal de Operación de la División de Sistemas de Información es responsable de conocer:**
 - a. La localización de las alarmas de fuego, extintores y controles de seguridad para combatir incendios en los sistemas.
 - b. Los procedimientos de apagar/encender equipos, de salida de emergencia y restauración luego de la emergencia.
 - c. Los procedimientos de emergencia para notificar a los bomberos, al Gerente de la División de Sistemas de Información y al personal gerencial designado en el evento de una emergencia.
 7. Toda falla que ocurra en los sistemas de información o en el Centro de Cómputos debe ser **documentada en el Libro de Registro del área**, describiendo lo siguiente:
 - a. Condiciones generales al momento de la falla.
 - b. Actividad no usual observada en cualquiera de las unidades de entrada o salida (*I/O*).
 - c. Información recibida para corregir el problema y la persona o compañía de servicio.
 - d. Fecha y hora en que ocurrió la falla, acciones tomadas y la hora en que se reactivó el sistema.
 - e. Firma del Operador o Técnico que corrigió la situación.

B. ADIESTRAMIENTO DEL PERSONAL

El adiestramiento del personal de la División de Sistemas de Información comienza con la **orientación del personal** nuevo, que incluye:

1. Adiestramiento sobre el Manual de Seguridad del Banco.

 BANCO DE DESARROLLO ECONOMICO PARA PUERTO RICO Estado Libre Asociado de Puerto Rico		DIVISIÓN DE SISTEMAS DE INFORMACIÓN MANUAL DE SEGURIDAD
Procedimiento Núm.: BDE-005-SI-Proc.02	Deroga a: Manual de Seguridad 27 de junio de 2001	Fecha de aprobación: 9 de septiembre de 2008

2. Adiestramiento en Guías y Normas de Seguridad para el Usuario de Computadoras contenidas en el Manual de Procedimientos de Sistemas de Información.
3. Normas y Procedimientos para el Envío y Recibo de Correo Electrónico y Correspondencia Interna detallado en el Manual de Procedimientos de Sistemas de Información.
4. Política Administrativa para la Seguridad de Información contenida en la Política de Sistemas de Información del Banco.

El Adiestramiento incluirá los procedimientos de operación del puesto y del área donde trabajará el empleado, contenidos en los Manuales de Operación de la División de Sistemas de Información. Entre éstos:

1. Manual de Procedimientos de la División de Sistemas de Información.
2. Manual de Seguridad de la División de Sistemas de Información
3. Plan Operacional de Emergencias adoptado por el Banco.
4. Manual de Desarrollo de Aplicaciones de la División de Sistemas de Información (siempre que aplique)
5. Otros procedimientos que apliquen, de acuerdo a la evaluación del Gerente de la División de Sistemas de Información.

El personal nuevo será adiestrado en el trabajo por un recurso interno del Banco, tutor o mentor en los procesos críticos y en forma paulatina. A medida que el nuevo empleado domine los procesos y tareas del puesto, será autorizado a continuar dichas tareas bajo su responsabilidad.

El personal regular recibirá adiestramientos para el desarrollo y fortalecimiento de destrezas, mantenerse al corriente de las innovaciones tecnológicas y para el mejoramiento continuo de la calidad de los servicios.

C. CONTRATACIÓN DE AYUDA EXTERNA

Servicios especiales de contratación de ayuda externa o apoyo operacional pueden ser necesarios para manejar proyectos o servicios, según la capacitación que se requiera para llevarlos a cabo, la necesidad de recursos en la División o la carga de trabajo que tengan los empleados de la División de Sistemas de Información en ese momento. La contratación de ayuda externa puede incluir:

1. Consultores Profesionales



Procedimiento Núm.:

BDE-005-SI-Proc.02

Deroga a:

**Manual de Seguridad
27 de junio de 2001**

Fecha de aprobación:

9 de septiembre de 2008

2. Mantenimiento y Servicio de Equipos (*hardware*)
3. Desarrollo de Programas o Aplicaciones (*software*)
4. Manufactureros de Equipos (*hardware*)
5. Manufactureros de Programas (*software*)
6. Proveedores de Adiestramientos Técnicos
7. Proveedores de Equipos, Materiales y Equipos Misceláneos para la operación de la División de Sistemas de Información.

El proceso de selección para la **contratación de asistencia externa** debe estar dirigido a:

1. Seleccionar al contratista que provea el servicio que necesita la División y para la fecha que se necesita.
2. Seleccionar el mejor precio y la mejor calidad para el servicio solicitado (Ejemplo: Subastas).
3. No debe existir relación cercana o familiar entre la firma a contratarse y el personal que tiene autoridad de selección en la División o en el Banco.
4. Solicitud de cotización de servicios y todos los acuerdos deben estar definidos en un Contrato Legal del Banco con el representante de la firma. El contrato debe contener los criterios de desempeño y la cláusula de cancelación.
5. Utilizar los servicios de la División de Compras y de la División Legal del Banco para todo tipo de contratación de servicios u órdenes de compra.
6. La administración de Sistemas de Información recibirá las facturas por los servicios prestados. El pago de las mismas debe ser autorizado por el Gerente de Sistemas de Información o la persona designada, luego de que se revise el contrato y se verifique que el servicio se rindió, según lo pactado.
7. Deben establecerse requisitos de metas, fechas de entrega o de servicio, precio por servicio, plan del proyecto, servicios de emergencia y reportes rutinarios escritos del progreso de los proyectos.
8. Establecer requisitos de especificaciones, alcance, documentación de las calificaciones profesionales y técnicas del proveedor de servicio y monitoreo del progreso de los proyectos.

 BANCO DE DESARROLLO ECONOMICO PARA PUERTO RICO Estado Libre Asociado de Puerto Rico		DIVISIÓN DE SISTEMAS DE INFORMACIÓN MANUAL DE SEGURIDAD
Procedimiento Núm.: BDE-005-SI-Proc.02	Deroga a: Manual de Seguridad 27 de junio de 2001	Fecha de aprobación: 9 de septiembre de 2008

- Solicitud de garantías de equipo, reparaciones, programas y compatibilidad con equipos o programas de existencia.

D. PROTECCIÓN DE LA INTIMIDAD

Los sistemas de información pueden afectar **la intimidad de los individuos** porque crean oportunidades de cambio social y generan **información personal de los empleados o clientes del Banco**.

Los códigos de conducta profesional de la Asociación de Maquinaria Computadorizada (AMC) han establecido las siguientes normas de conducta profesional y social para los Sistemas de Información.

- Conducta profesional que contribuya a la sociedad y a la humanidad.
- Evitar hacer daño a otras personas, a través de computadoras o sistemas de información.
- Ser honesto y confiable en el uso de computadoras y sistemas de información.
- Honrar los derechos de propiedad, incluyendo derechos de autor y patentes de equipo (*hardware*) y programas (*software*).
- Dar crédito propio a propiedad intelectual de equipo (*hardware*) y programas (*software*).
- Acceder a los recursos de computadoras solamente con autorización de acceso.
- Respetar la privacidad de otros en el uso de información del sistema.

Las dimensiones morales de los Sistemas de Información incluyen:

- Protección de la Privacidad** – los archivos con información personal de empleados o clientes, deben mantenerse con acceso autorizado a la División del Banco que la genera o la utiliza. Cualquier información de accesos impresa en papel debe estar archivada bajo llave para garantizar su confidencialidad. Toda información confidencial o de accesos impresa que se vaya a descartar, debe ser destruida en un cortador de papel (*paper shredder*).

Algunos ejemplos de información confidencial son:

- Información personal de Empleados

 BANCO DE DESARROLLO ECONOMICO PARA PUERTO RICO Estado Libre Asociado de Puerto Rico		DIVISIÓN DE SISTEMAS DE INFORMACIÓN MANUAL DE SEGURIDAD
Procedimiento Núm.: BDE-005-SI-Proc.02	Deroga a: Manual de Seguridad 27 de junio de 2001	Fecha de aprobación: 9 de septiembre de 2008

- Información de nombres, seguro social, direcciones y números de teléfonos de clientes del Banco
 - Lista de clientes morosos
2. **Prácticas de Información Justa (*Fair Information Practices*)** – conjunto de principios que gobiernan la recopilación y uso de información sobre individuos, basados en las Leyes de Protección de la Intimidad Personal y el derecho a la privacidad de los individuos. Los principios incluidos en estas prácticas son:
- No deben existir registros de información personal privilegiada.
 - Los individuos tienen derecho a acceso, inspección, revisión y actualización de los sistemas que contienen información sobre su persona.
 - No se debe usar la información personal para otros propósitos que no sea para el cual se recopiló y autorizó por la persona. Para cualquier otro uso, debe solicitarse la autorización o consentimiento de la persona.
 - El Gerente de Sistemas de Información es responsable de velar por el cumplimiento de los estándares de seguridad de la información personal de los empleados y clientes del Banco.
3. **Las Leyes de Privacidad que afectan las Instituciones**
- *Fair Credit Reporting Act*, 1970
 - *Family Educational Rights and Privacy Act*, 1978
 - *Right to Financial Privacy Act*, 1978
 - *Privacy Protection Act*, 1980
4. **Errores de Sistema o de Calidad** – La responsabilidad legal por las consecuencias de los actos no intencionales en el uso de los sistemas de información utilizados puede evaluarse en términos de:
- Calidad aceptable y tecnológicamente posible de un sistema para evitar errores.
 - Desastres naturales.

 BANCO DE DESARROLLO ECONOMICO PARA PUERTO RICO Estado Libre Asociado de Puerto Rico		DIVISIÓN DE SISTEMAS DE INFORMACIÓN MANUAL DE SEGURIDAD
Procedimiento Núm.: BDE-005-SI-Proc.02	Deroga a: Manual de Seguridad 27 de junio de 2001	Fecha de aprobación: 9 de septiembre de 2008

- Errores tecnológicos inevitables.
- Situaciones predecibles o errores que el personal del área pudo evitar o corregir.
- Capacidad económica de la Institución para corregir los errores en el Sistema de Información.
- Responsabilidad del manufacturero que vendió el equipo (*hardware*) o programa (*software*) a la Institución.
- Pobre desempeño de los equipos (*hardware*) o programas (*software*).
- Calidad de la entrada de datos por el usuario del sistema de información.
- Cotejo de errores y protección por módulos de *software* para garantizar la exactitud y confiabilidad de los datos, evitar fallas de *hardware* o *software* y minimizar errores.

5. Las situaciones que representan dimensiones éticas en el uso de los sistemas de información deben ser definidas:

- Identificando los valores y derechos envueltos.
- Buscando soluciones que se pueden implementar en forma razonable.
- Estableciendo los estándares de conducta o de operación que se desarrollarán para solucionar los conflictos.
- Asegurando el cumplimiento de las leyes relacionadas al uso de los sistemas computadorizados.
- Buscando soluciones adecuadas a los conflictos generados, que aún no hayan sido incluidos en las leyes vigentes.

 BANCO DE DESARROLLO ECONOMICO PARA PUERTO RICO Estado Libre Asociado de Puerto Rico		DIVISIÓN DE SISTEMAS DE INFORMACIÓN MANUAL DE SEGURIDAD
Procedimiento Núm.: BDE-005-SI-Proc.02	Deroga a: Manual de Seguridad 27 de junio de 2001	Fecha de aprobación: 9 de septiembre de 2008

CAPÍTULO II – CONTROLES DE SEGURIDAD DE ACCESO

A. ADMINISTRACIÓN DE CONTRASEÑAS

El control de acceso a los Sistemas de Información es uno de los controles de seguridad más importantes para evitar errores y abusos de los sistemas computadorizados.

El acceso al sistema de información está controlado por el uso de **contraseñas para cada usuario** (*username, USER ID*) o **códigos de acceso** (*access code, ID codes*). La contraseña es una palabra o un código utilizado como un medio de seguridad para controlar el acceso al sistema de información para los usuarios autorizados solamente y evitar el acceso no autorizado.

El **Oficial de Seguridad de Informática** o el designado de la **División de Sistemas de Información** es la persona responsable de la administración de contraseñas al personal autorizado del Banco. Las contraseñas se manejan mediante un sistema operativo de administración de la Base de Datos. La computadora verifica la legitimidad de la contraseña de acceso al sistema.

Como **medida de seguridad**, las contraseñas se cambian cada 30 días para todos los usuarios autorizados del Banco.

Para solicitar las contraseñas para nuevos usuarios del sistema y para reportar cualquier problema de acceso, se utiliza la **Solicitud de Servicio**, la cual se entrega directamente al Técnico de Computadoras o a la persona designada para proveer o coordinar el servicio. El adiestramiento o readiestramiento del uso correcto de contraseñas en el sistema de información es ofrecido al usuario por su propia División de trabajo. Cuando sea necesario, el Oficial de Seguridad de Informática le proporcionará el adiestramiento.

Procedimiento de Administración de Contraseñas:

- Una vez recibida la Solicitud de Servicio, el **Oficial de Seguridad de Informática** o la persona designada, procederá a determinar el tipo de acceso solicitado o requerido para las funciones del empleado o puesto que ocupa, basado en los niveles de acceso y autorizaciones requeridas descritas a continuación:
 - Monetario** – Usuario emite pagos en la División de Contraloría y desembolsos en la División de Crédito.
 - No-Monetario** – Otros procedimientos del Banco en el sistema de información que no son monetarios.



Procedimiento Núm.:

BDE-005-SI-Proc.02

Deroga a:

**Manual de Seguridad
27 de junio de 2001**

Fecha de aprobación:

9 de septiembre de 2008

- **Consulta (*inquiry*)** – Acceso a los archivos para observar los datos e informes solamente. El usuario no puede hacer entradas ni dar mantenimiento a los mismos.
- **Instituciones** – Acceso a individuos autorizados a las diferentes Instituciones.

Descripción	Número de Institución
Banco (BDE)	1
Corporación (CCDCA)	2
Préstamos de Garantía	3

- **Aplicaciones Financieras** – Acceso a individuos autorizados a las diferentes aplicaciones financieras.
 - Mayor General
 - Préstamos
 - Colateral
 - Archivo del Cliente
2. El **Oficial de Seguridad de Informática** o la persona designada, evalúa si la contraseña es para el uso de la Red de Información.
- **RED de Información** – usuarios del Banco de programas de procesamiento de palabras, correo electrónico y otras.
 - **Clear Path de Unisys** – personal de la División de Sistemas de Información como: Operadores, Técnicos, Desarrolladores, Supervisores y usuarios del Banco como:
 - Contabilidad – Pagos
 - Oficiales de Recobros – Asesoría Legal
 - Crédito – Creación y desembolsos de préstamos
 - Oficiales o Ejecutivos de Cuentas – Para información crediticia de los clientes
 - Otros usuarios - Para consulta solamente



Procedimiento Núm.:

BDE-005-SI-Proc.02

Deroga a:

**Manual de Seguridad
27 de junio de 2001**

Fecha de aprobación:

9 de septiembre de 2008

3. El **Oficial de Seguridad de Informática** o la persona designada, define la descripción o niveles de seguridad de acceso en los sistemas, procesa la entrada de la contraseña por el usuario, confidencialmente, y está presente para asegurar que el sistema funcione correctamente, durante este acceso inicial o cambio de contraseña. Por razones de seguridad, no se describen los pasos de los procedimientos de asignación de contraseña en este Manual, pero ilustramos lo siguiente:

- Pantallas de acceso que el usuario observará durante el proceso de acceso
- Niveles de autorización
- Cuentas
- Límite monetario
- Transacciones
- Horario de uso regular y temporero

De igual forma, existen varias pantallas de seguridad de acceso a la RED de Información que se ilustran a continuación:

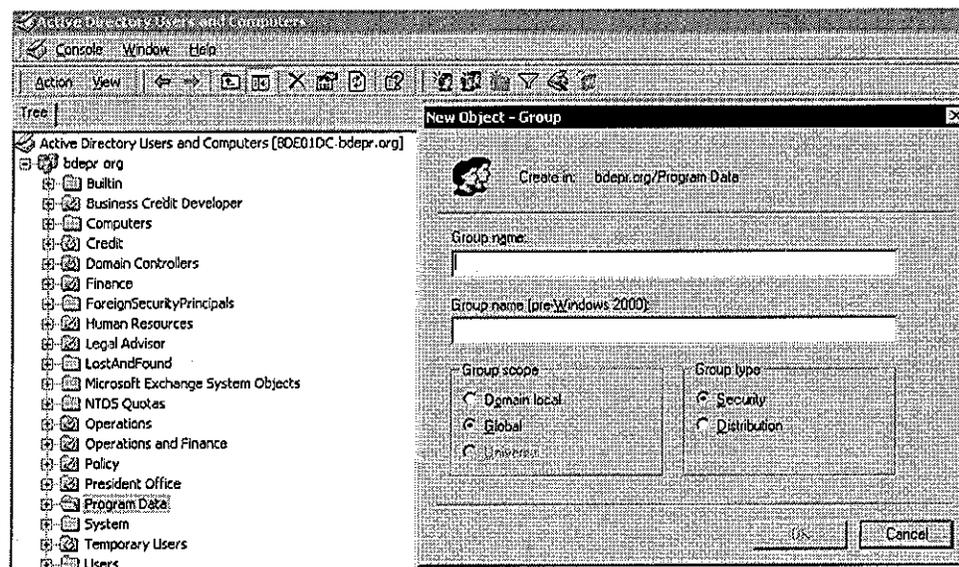


Ilustración # 1 Pantalla de Acceso por Grupos



Procedimiento Núm.:
BDE-005-SI-Proc.02

Deroga a:
Manual de Seguridad
27 de junio de 2001

Fecha de aprobación:
9 de septiembre de 2008

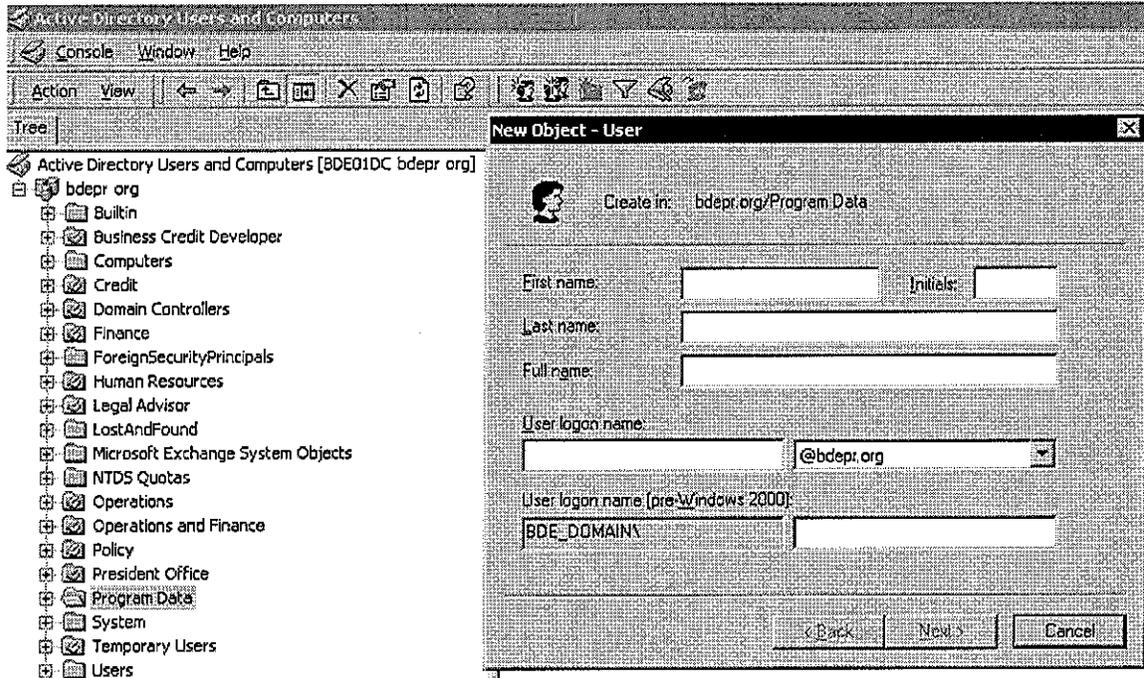


Ilustración #2 Pantalla de *Profile* de Usuarios



Procedimiento Núm.:
BDE-005-SI-Proc.02

Deroga a:
Manual de Seguridad
27 de junio de 2001

Fecha de aprobación:
9 de septiembre de 2008

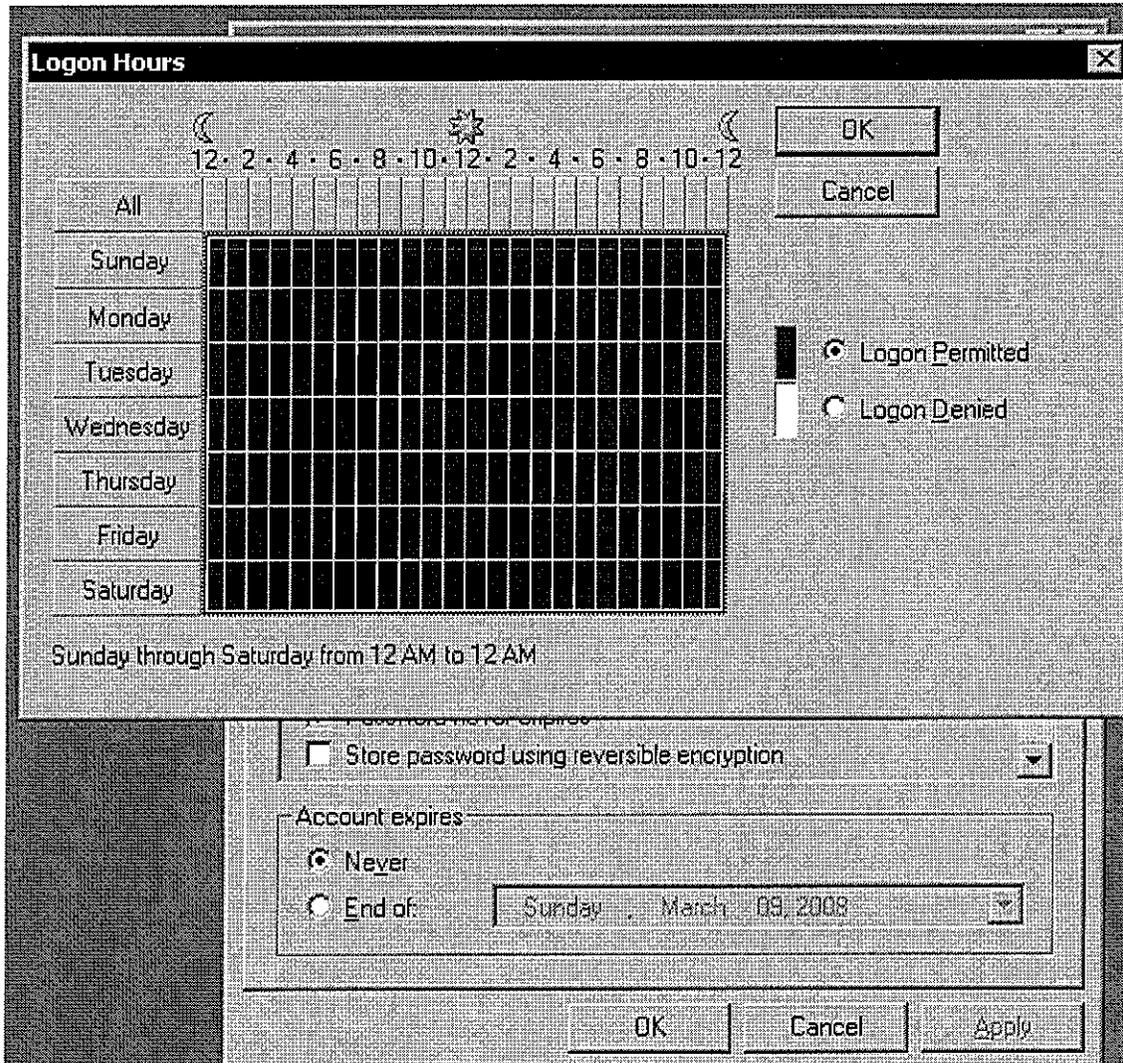


Ilustración #3 Pantalla de Horario de Uso del Sistema

4. Para el uso de la computadora, envío y recibo de correo electrónico y correspondencia interna, el empleado firma un Acuerdo de Confidencialidad y Seguridad de Información. (En la siguiente página encontrará copia del Acuerdo).



**BANCO DE DESARROLLO ECONOMICO
PARA PUERTO RICO**

Estado Libre Asociado de Puerto Rico

**DIVISIÓN DE SISTEMAS DE
INFORMACIÓN**

MANUAL DE SEGURIDAD

Procedimiento Núm.:

BDE-005-SI-Proc.02

Deroga a:

**Manual de Seguridad
27 de junio de 2001**

Fecha de aprobación:

9 de septiembre de 2008



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

**Acuerdo de Confidencialidad y Seguridad de Información
Sistemas de Información
Revisión Anual**

Al otorgárseme acceso a los sistemas de información del Banco Desarrollo Económico para Puerto Rico (BDE), me comprometo a hacer buen uso de los sistemas de información computadorizados y a la información contenida en los mismos.

Entiendo que divulgar cualquiera de mis códigos de acceso ("password") o información de la Institución, que no sea de dominio público a través de mi código, va en violación a la confidencialidad de la información, a las políticas de seguridad de información y protección de los equipos del Banco; y ya sea intencional o accidentalmente podrá conllevar medidas disciplinarias que serán establecidas y administradas por el Equipo de Recursos Humanos de nuestra Institución.

Los Sistemas de Información computadorizados asignados para llevar a cabo las funciones oficiales son propiedad del BDE. Estos sistemas incluyen los programas y los archivos electrónicos, y sólo se utilizarán para fines estrictamente oficiales. La información desarrollada, transmitida o almacenada en los sistemas también es propiedad del BDE y estará accesible para ser examinada y utilizada por el personal autorizado por el nivel de autoridad correspondiente y/o su representante autorizado. Los usuarios del Sistema no deberán interceptar información que le ha sido restringida. Se prohíbe el envío de copia de correspondencia electrónica ("e-mails") a otras personas sin el consentimiento del remitente. A éste se le deberá notificar, por lo menos, a través del envío de una copia de la información. El usuario deberá borrar periódicamente, por lo menos cada 15 días, la correspondencia electrónica archivada, de manera que se pueda utilizar al máximo el espacio en disco. Cada usuario deberá establecer su contraseña para tener acceso a los sistemas, la cual deberá cambiarse cada 30 días. Se prohíbe revelar la contraseña ("password"). Está prohibido utilizar sistemas computadorizados de índole personal para llevar a cabo tareas oficiales e instalar y utilizar programas que no sean los oficiales del BDE.

El acceso a la Internet será provisto solamente al personal que sea autorizado por su Supervisor, Gerente, Vicepresidente o Presidente, con la debida justificación para el uso del mismo y solamente para uso oficial.

Es responsabilidad de cada empleado leer las Políticas de Sistemas de Información sobre la Seguridad de Información (V), Seguridad para el Usuario de Computadora (VII), Envío y Recibo de Correo Electrónico (VIII) y Utilización de la Internet (X), incluidas en el "Public Folder".

Entendiendo las normas citadas, acepto que cualquier violación a las mismas pueda ser causa suficiente para el inicio de un proceso disciplinario y me comprometo a ser buen uso de los sistemas y leer las Políticas de Sistemas de Información.

Firma empleado

Nombre letra de molde

Fecha

 BANCO DE DESARROLLO ECONOMICO PARA PUERTO RICO Estado Libre Asociado de Puerto Rico		DIVISIÓN DE SISTEMAS DE INFORMACIÓN MANUAL DE SEGURIDAD
Procedimiento Núm.: BDE-005-SI-Proc.02	Deroga a: Manual de Seguridad 27 de junio de 2001	Fecha de aprobación: 9 de septiembre de 2008

5. El **Oficial de Seguridad de Informática**, una vez definido el acceso autorizado y creados los accesos necesarios para el usuario, documenta el Formulario para solicitar acceso a los sistemas, describiendo el acceso autorizado. Luego, lo entrega al empleado solicitante para su firma y la firma del Supervisor de la División (Vicepresidente o Gerente). Éste lo devuelve a Sistemas de Información para autorización y archivo.

6. El acceso es autorizado solamente durante el turno de trabajo promedio del usuario. En situaciones especiales, el usuario deberá solicitar (a través de una solicitud de servicio), extensión de este horario, con la autorización del Gerente o Vicepresidente de la División en que trabaja. El limitar el acceso a horarios laborables para el personal del Banco es un control de seguridad física del Sistema de Información de aceptación general. (En la siguiente página encontrará un Modelo del Formulario para otorgar el Acceso a los sistemas del Banco y Acceso al Sistema de Préstamos).

7. Los usuarios de las diferentes regiones e instituciones del Banco solicitan el acceso al Oficial de Seguridad de Informática y se lleva a cabo el mismo procedimiento interno.



**BANCO DE DESARROLLO ECONOMICO
PARA PUERTO RICO**

Estado Libre Asociado de Puerto Rico

**DIVISIÓN DE SISTEMAS DE
INFORMACIÓN**

MANUAL DE SEGURIDAD

**Procedimiento Núm.:
BDE-005-SI-Proc.02**

**Deroga a:
Manual de Seguridad
27 de junio de 2001**

**Fecha de aprobación:
9 de septiembre de 2008**



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

DIVISION SISTEMAS DE INFORMACION

Formulario para Solicitar Acceso al Sistema de Préstamos

Se está autorizando a _____, User-Id _____ de la _____ al acceso al Sistema de Préstamos Institución 1 del Banco de Desarrollo Económico para Puerto Rico (ITI Premier II) a realizar las siguientes transacciones:

Funciones	Premier	CIS	LAS1	LAS2	IES	FMS	FA&PTM	AP&SEM	COO	OC	POB
Creación											
Consulta											
Mantenimiento											
Movimiento											
Otro											

Firma Supervisor Inmediato - División
Peticionaria

Nombre Letra de Moide

Fecha

Firma Empleado

Nombre Letra de Moide

Fecha

Puesto que ocupa empleado

Firma Autorizada Gerente o VP
División Contabilidad

Nombre Letra de
Moide

Firma Autorizada Gerente o VP
Crédito

Nombre Letra de
Moide

PARA USO EXCLUSIVO DE SISTEMAS DE INFORMACIÓN

Funciones	Premier	CIS	LAS1	LAS2	IES	FMS	FA&PTM	AP&SEM	COO	OC	POB
1											
2											
3											
4											
5											
6											
7											
8											
9											
A											
B											
C											
D											
E											
F											

Firma Oficial de Seguridad Informática

Nombre Letra de Moide

Fecha

Firma Gerente Sistemas de Información

Nombre Letra de Moide

Fecha

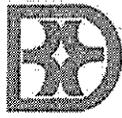
Leyenda:

Fecha de Activación

APS - Accounts Payable System

PD\$ - Premier Image Director

FAS - Fixed Assets System



Procedimiento Núm.:
BDE-005-SI-Proc.02

Deroga a:
Manual de Seguridad
27 de junio de 2001

Fecha de aprobación:
9 de septiembre de 2008

B. VIOLACIÓN Y REPORTES DE SEGURIDAD

El usuario entra su contraseña e identificación para acceder al sistema. El **subsistema de seguridad** lee la información de entrada en la pantalla y se asegura que todos los requisitos de seguridad se han completado satisfactoriamente.

Cuando se traspasan los controles de seguridad, el subsistema de seguridad identifica cuándo y dónde ocurrió. Cuando los límites de violación son excedidos, el empleado es suspendido, eliminado o el Terminal es desconectado. Para reinstalación, hay que notificar al Oficial de Seguridad de Informática. El **Oficial de Seguridad de Informática** documentará una Notificación del Evento, para establecer las acciones correctivas a seguir para evitar recurrencia, incluyendo el adiestramiento del personal cuando sea necesario.

Se pueden imprimir reportes para revisar cualquier cambio hecho en los datos de control de seguridad.

El **Oficial de Seguridad de Informática** documentará cualquier cambio o evento relacionado a la Seguridad del Sistema en el Formulario de Control de Cambios.

C. NIVELES DE SEGURIDAD

El acceso al sistema es controlado por el uso de niveles de seguridad o jerarquía de clasificación de funciones por niveles de autoridad y limitaciones de seguridad para cada nivel de acceso, según se describen a continuación:

Nivel	Clasificación
1	Personal clerical
3	Supervisores, Monetarios
5	Gerentes de División y Gerencia media
7	Presidente y Vicepresidentes Ejecutivos
9	Oficial de Seguridad de Informática, Gerente de Sistemas de Información

 BANCO DE DESARROLLO ECONOMICO PARA PUERTO RICO Estado Libre Asociado de Puerto Rico		DIVISIÓN DE SISTEMAS DE INFORMACIÓN MANUAL DE SEGURIDAD
Procedimiento Núm.: BDE-005-SI-Proc.02	Deroga a: Manual de Seguridad 27 de junio de 2001	Fecha de aprobación: 9 de septiembre de 2008

CAPÍTULO III – CONTROLES DE SEGURIDAD PARA EL RESGUARDO DE DATOS (*BACKUP*)

A. ESTÁNDAR DE RESGUARDO DE DATOS (*BACKUP*)

El **resguardo de datos** se conoce en el lenguaje de computadoras como *backup*. El *backup* es una disciplina en los sistemas de información y un estándar de seguridad que consiste en copiar la base de datos y los programas *software* en diferentes medios de almacenamiento como prevención contra emergencias, fallas *hardware* y *software* y para asegurar la información en el sistema computadorizado.

Las copias de seguridad legibles de *backup* se hacen en cartuchos en forma **diaria, semanal, mensual y anual**.

Se guarda la copia diaria en una **caja de seguridad** a prueba de fuego (*mossler*) en el Centro de Cómputos conocida como **Bóveda Interna** del Banco. Las cintas de fin de semana son almacenadas en una **Bóveda Externa** a una distancia segura de la localización del Banco. La Bóveda Externa del Banco está en *International Safe Deposit* en San Patricio Plaza, en Guaynabo, Puerto Rico.

B. USO DE COPIAS *BACKUP*

Las **copias de seguridad de *backup*** del Sistema de Información se utilizan para proteger la información en situaciones de emergencia, mal uso y acceso no autorizado al sistema. Estas copias facilitan un control de todos los procedimientos de *backup*, almacenamiento, recobro y retención de las copias de seguridad de la base de datos y programas del sistema de información.

El **resguardo (*backup*) y la restauración (*recovery*)** es una combinación de procedimientos manuales y de máquina, mediante los cuales pueden recuperarse los datos perdidos por una eventual falla del equipo (*hardware*) o programas (*software*) o luego de una situación de emergencia o desastre.

El ***backup* rutinario** a las frecuencias establecidas son parte del programa de respaldo y restauración de:

- La Base de Datos
- Programas (*software*)
- Bitácoras del Sistema (*logs*)
- Auditorías del Sistema (*audits*)
- Registros y Operaciones del Sistema de Información

 BANCO DE DESARROLLO ECONOMICO PARA PUERTO RICO Estado Libre Asociado de Puerto Rico		DIVISIÓN DE SISTEMAS DE INFORMACIÓN MANUAL DE SEGURIDAD
Procedimiento Núm.: BDE-005-SI-Proc.02	Deroga a: Manual de Seguridad 27 de junio de 2001	Fecha de aprobación: 9 de septiembre de 2008

C. PROCEDIMIENTOS DE *BACKUP*

Los procedimientos de *backups* de los Sistemas de Información aparecen descritos en la Red de Información de la División de Sistemas de Información.

En términos generales, los procedimientos de *backups* incluyen:

1. *Software* Nuevo – Se deben resguardar o hacer *backup* de acuerdo a las especificaciones del fabricante. El *software* luego de copiarse, debe probarse para verificar si se observa algún problema. Los discos o CD de *software* copiados deben estar protegidos con un seguro (*write protected*).
2. *Backup* Diario – al final de cada día de trabajo, todos los datos nuevos, base de datos y programas son copiados en cintas o cartuchos.
3. Otros procedimientos de *backup* incluyen:
 - *Backup* Semanal
 - *Backup* Mensual
 - *Backup* Anual
4. Se mantiene un inventario perpetuo documentado de las copias de *backup* en Bóveda Interna y Bóveda Externa, actualizado diariamente.

D. MANEJO DE DISCOS

El **manejo correcto de discos** asegura la disponibilidad de los datos para los trabajos y reduce errores de lectura y escritura. El manejo correcto de discos incluye los siguientes procedimientos:

1. Almacenamiento en envases adecuados cuando no estén en las unidades de discos en las máquinas.
2. Los envases con los discos son archivados en un lugar seguro cuando no están en uso.
3. Los empaques de discos en las unidades se mantienen tapados o cerrados, excepto cuando son cargados o descargados con los paquetes de discos.
4. El contenido de los discos está identificado con etiquetas externas.



Procedimiento Núm.:

BDE-005-SI-Proc.02

Deroga a:

**Manual de Seguridad
27 de junio de 2001**

Fecha de aprobación:

9 de septiembre de 2008

5. Las etiquetas en los discos *floppy* se colocan al frente del *diskette* con la descripción del contenido.

E. MANEJO DE CINTAS Y CARTUCHOS

El **manejo correcto de cintas de cartuchos** incluye los siguientes procedimientos:

1. Manejar los cartuchos con las manos limpias.
2. Limpiar los cabezales de lectura/escritura de las unidades de cintas de acuerdo a las recomendaciones del manufacturero.
3. Se deben mantener en sus envases de protección cuando no están en uso.
4. Para asegurar que los cartuchos de *backup* no sean borrados, hay que colocarles el seguro de protección.
5. Las puertas de acceso de las unidades de cartuchos se mantienen cerradas cuando no tienen cintas o cartuchos instalados.

F. BACKUP DE COMPUTADORAS Y TERMINALES

El resguardo o *backup* de computadoras de los usuarios del Banco incluye los siguientes procedimientos:

1. Cada empleado será responsable de grabar toda la información en su fólдер, reservado en el servidor.
2. La División de Sistemas de Información desarrolló un procedimiento que orienta al empleado cómo guardar sus documentos en su fólдер, utilizando los directorios asignados en un Servidor. De esta manera, sus documentos no se pierden después de guardados. También se preparó el procedimiento de resguardo de los servidores. Estos procedimientos están localizados en el Manual de Procedimientos de la División de Sistemas de Información.

 BANCO DE DESARROLLO ECONOMICO PARA PUERTO RICO Estado Libre Asociado de Puerto Rico		DIVISIÓN DE SISTEMAS DE INFORMACIÓN MANUAL DE SEGURIDAD
Procedimiento Núm.: BDE-005-SI-Proc.02	Deroga a: Manual de Seguridad 27 de junio de 2001	Fecha de aprobación: 9 de septiembre de 2008

CAPÍTULO IV – CONTROLES DE SEGURIDAD DE VIRUS Y PIRATAS

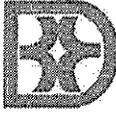
A. CONTROLES PARA MINIMIZAR ERROR, ABUSO Y CRÍMENES DE COMPUTADORAS

Para detectar y eliminar virus de computadoras se utiliza un antivirus *software* y los procedimientos de *screening* para reducir las oportunidades de infección. El antivirus *software* es especialmente diseñado para cotejar el sistema computadorizado y los discos para la presencia de varios virus de computadoras.

En ocasiones, el *software* puede eliminar el virus del área afectada y podría ser necesario efectuar un procedimiento de limpieza del sistema (*cleanup*). Los controles de seguridad de acceso a la Red de Información son necesarios para evitar la propagación de virus de computadoras por la penetración de acceso de Piratas (*hackers*) a la red.

Los virus pueden invadir los sistemas de información de discos infectados de una fuente externa o de máquinas infectadas. Para evitar este tipo de invasión, los controles de seguridad incluyen:

1. Instalar en cada computadora un programa para detectar virus.
2. Guardar una copia limpia del sistema operativo con el seguro de protección en una posición que impida seguir grabando en ellos. De esta manera, será posible restablecer un entorno limpio a partir del cual comenzar a atacar la infección.
3. Evitar el acceso de virus o piratas por alguna de las máquinas de la red, con enlace por módem, con control de acceso seguro y con contraseñas específicas. Controlar que las contraseñas sean difíciles de adivinar y cambiarlas en intervalos de tiempo adecuados.
4. Orientar a los empleados sobre la importancia de mantener confidencial el nombre y contraseña de usuario al sistema, para evitar el acceso no autorizado.
5. Los virus sólo pueden invadir un sistema si alguien los coloca en él. Es necesario pasar por el programa antivirus todo *diskette* que entre en la institución para evitar el uso de *diskettes* infectados en los terminales del Banco. Los usuarios no pueden introducir *diskettes* del exterior sin la autorización del Administrador del Sistema y verificación correspondiente de virus.
6. Restringir el acceso físico al servidor de ficheros en el Centro de Cómputos.
7. Hacer que los usuarios sólo accedan aquellos directorios que necesiten para trabajar y los demás directorios para consulta solamente, cuando sea necesario.

 BANCO DE DESARROLLO ECONOMICO PARA PUERTO RICO Estado Libre Asociado de Puerto Rico		DIVISIÓN DE SISTEMAS DE INFORMACIÓN MANUAL DE SEGURIDAD
Procedimiento Núm.: BDE-005-SI-Proc.02	Deroga a: Manual de Seguridad 27 de junio de 2001	Fecha de aprobación: 9 de septiembre de 2008

8. Mantenimiento interno de computadoras y terminales del Banco mensualmente para auditorías de programas, identificar programas no autorizados y verificar detección de virus en terminales y *software*.
9. Para evitar contaminación de terminales con virus, el Banco provee todos los equipos *hardware* y programas *software* del sistema. Los usuarios no pueden traer equipos computadorizados o *software* al Banco sin la autorización del Oficial de Seguridad de Informática del sistema y verificación de virus correspondiente.
10. Estaciones de trabajo sin unidad lectora de *diskettes*, de manera que los programas se carguen solicitándolos del servidor de ficheros, cuando se determine necesario.
11. Uso de programas de comunicaciones de llamada revertida (*call back*) a la red, a través de una lista de usuarios autorizados por sus números de módem. El usuario se pone en comunicación, entra la contraseña correcta, el sistema cuelga o se desconecta inmediatamente y establece por su parte la comunicación, luego de verificar el acceso correspondiente. También se puede intercalar un control local, de manera que el sistema de información quede separado de la red general, hasta que haya efectuado las verificaciones necesarias antes de comunicarse.

B. RESPONSABILIDADES

Cada usuario del sistema de información es responsable de asegurar la integridad y exactitud de la información generada en su trabajo, en transacciones, datos de entrada y salida de datos del sistema y debe evitar la introducción de virus al sistema de información.

La División de Sistemas de Información es responsable de orientar al personal del Banco sobre los controles de seguridad establecidos que aseguren: la calidad y funcionamiento correcto de los sistemas de información, evitar la penetración de acceso no autorizado, virus, crímenes de y abuso de computadoras.

C. ETAPAS DE INFECCIÓN VIRAL

El grado de daño a un sistema computadorizado se puede determinar por el nivel de penetración del virus en varias etapas, descritas a continuación:

Primera Etapa: El virus está contenido en la memoria local principal.

- Afecta la aplicación en ejecución en el momento.
- Es simple de remover.
- La introducción del virus, tiene efecto limitado si se detecta y elimina en esta etapa.



Procedimiento Núm.:

BDE-005-SI-Proc.02

Deroga a:

**Manual de Seguridad
27 de junio de 2001**

Fecha de aprobación:

9 de septiembre de 2008

Segunda Etapa: El virus se mueve de la memoria local principal al área de almacenamiento local fijo (*fixed local storage*).

- Puede infectar todas las aplicaciones almacenadas.
- Daño potencial a los datos locales.
- Requiere tiempo para removerse (de 1 a 5 horas/hora aproximadamente).
- Daño moderado si se detecta a tiempo y se elimina en esta etapa.

Tercera Etapa: El virus se auto-replica e infecta los sistemas de archivos compartidos (*shared file system*)

- Puede infectar las utilidades, compiladores, editores, herramientas (*tools*), aplicaciones compartidas (*shared applications*), comunicaciones y archivos del sistema (*system files*).
- La infección se dispersa por el sistema de información.
- Puede ocasionar daño sustancial al sistema.
- Requiere una recuperación compleja para restaurar los sistemas dañados y remover el virus de los sistemas infectados.

Cuarta Etapa: Infección de los medios removibles del sistema (*system wide removable media*).

- Puede infectar los discos (*floppy*), se escribe una vez y se lee por muchos discos. Puede infectar los discos duros removibles y las copias en cinta de *backups*.
- La infección de discos *floppy* y escritura-lectura por varios discos, se puede dispersar fácilmente, es difícil de localizar o detectar en los procedimientos de restauración y limpieza.
- La infección de discos duros removibles y copias en cinta de *backups* son almacenados por tiempo considerable y pueden reintroducir una infección anterior.
- La recuperación es extremadamente difícil, la infección de los medios removibles del sistema puede no ser detectada, y la probabilidad de volver a infectarse es extremadamente alta.
- Los procedimientos de limpieza requieren tiempo, monitoreo continuo y un entorno limpio, a partir del cual, empezar a atacar y erradicar la infección.

 BANCO DE DESARROLLO ECONOMICO PARA PUERTO RICO Estado Libre Asociado de Puerto Rico		DIVISIÓN DE SISTEMAS DE INFORMACIÓN MANUAL DE SEGURIDAD
Procedimiento Núm.: BDE-005-SI-Proc.02	Deroga a: Manual de Seguridad 27 de junio de 2001	Fecha de aprobación: 9 de septiembre de 2008

La experiencia general es que se detecta el virus en la primera o segunda etapa y se procede a removerlo inmediatamente. Los procedimientos de mantenimiento preventivo interno para detectar programas no autorizados, detección de virus, corridas antivirus de todos los programas y terminales con programas para detectar virus, deben evitar la introducción de virus al sistema en forma rutinaria.

Los usuarios deben asegurarse de usar discos *floppy* y terminales con corridas antivirus para evitar infección del sistema. En cualquier evento que se detecte infección de virus en el sistema, deben notificar al Oficial de Seguridad de Informática para tomar las acciones correctivas necesarias, inmediatamente.

Las etapas de penetración de virus deben evaluarse en detalle en cada incidente que ocurra, para asegurar que las partes del sistema con potencial de infección, sean debidamente restauradas, limpiadas y el virus sea removido y erradicado en los puntos de infección. Debe controlarse la probabilidad de volver a infectarse con un virus previamente removido.

Todo incidente de infección con virus será documentado por el Oficial de Seguridad de Informática en una Notificación de Evento, describiendo las acciones correctivas tomadas para evitar recurrencia. Para mas detalle, puede referirse al Manual de Procedimientos de la División de Sistemas de Información.

 BANCO DE DESARROLLO ECONOMICO PARA PUERTO RICO Estado Libre Asociado de Puerto Rico		DIVISIÓN DE SISTEMAS DE INFORMACIÓN MANUAL DE SEGURIDAD
Procedimiento Núm.: BDE-005-SI-Proc.02	Deroga a: Manual de Seguridad 27 de junio de 2001	Fecha de aprobación: 9 de septiembre de 2008

CAPÍTULO V – CONTROLES DE SEGURIDAD RED DE INFORMACIÓN

A. ESTÁNDAR DE ACCESO

Los **estándares de redes de información** definen una topología que se debe emplear y un sistema de control de acceso al medio. La red de información del Banco es *Fast Ethernet*.

Algunos conceptos básicos de las características que presentan las redes y los distintos elementos que la forman son:

- **Velocidad de Transmisión** – Mide la cantidad de información, en bits, que una red puede transportar en un segundo (bits por segundo o bps). Suelen emplearse múltiplos de esta unidad como Kbps (Kilobits por segundo o miles de bits transmitidos en un segundo), Mbps (Megabits por segundo, o millones de bites que se transmiten en un segundo) y Gigabits.
- **Tipo de Transmisión** – Está determinado por los tipos de cables o enlaces utilizados, como por ejemplo: coaxiales o fibras ópticas que pueden transportar las señales en un único canal o en varios. La transmisión del primer tipo se denomina en banda base (*base band*) y el segundo tipo se conoce como transmisión de banda ancha (*broad band*).
- **Segmento y longitud máxima de segmento** – Se denomina segmento a cada porción de cableado o enlace situado entre dos (2) repetidores. La máxima longitud de segmento para un medio de transmisión dado es la que se puede alcanzar entre dos (2) estaciones sin necesidad de intercalar repetidores.
- **Repetidores** – En todas las redes, las señales se debilitan con la distancia. Cuando la longitud es tan grande que la señal se vuelve ininteligible, se intercala en el medio de transmisión un repetidor. El repetidor es un dispositivo que recoge las señales débiles que le llegan por un extremo, las regenera y las inyecta de nuevo en la red.

El control de acceso CSMA/CD (*Carrier Sense Multiple Access/Collision Detection*) es un sensor de onda, portadora de accesos múltiples, para detección de colisiones como método de acceso en las comunicaciones. Cuando un dispositivo trata de ganar acceso a la red, verifica si la misma está libre. Si no lo está, espera una cantidad aleatoria de tiempo antes de intentarlo de nuevo. Si la red está libre y dos (2) dispositivos tratan de ganar acceso exactamente al mismo tiempo, ambos se retractan para evitar colisión y luego cada uno espera una cantidad aleatoria de tiempo antes de reintentarlo.



Procedimiento Núm.:
BDE-005-SI-Proc.02

Deroga a:
Manual de Seguridad
27 de junio de 2001

Fecha de aprobación:
9 de septiembre de 2008

B. PROTOCOLOS Y DIRECCIONES

Los controles técnicos de protocolos y direcciones permiten la comunicación en la red en forma segura.

Los **protocolos** son conjuntos de normas que definen los múltiples aspectos que intervienen en una comunicación, según se describen a continuación:

- ¿Cómo iniciarla?
- ¿Cómo terminarla?
- ¿Qué secuencia de mensajes emplear?
- ¿Cómo identificar a nuestros interlocutores?
- ¿Qué hacer cuando el interlocutor se hace el sordo?

La mayoría de la información en una red viaja en paquetes. Los protocolos definen desde el formato que han de tener los paquetes, hasta las órdenes que un dispositivo puede aceptar. Cada red tiene un conjunto de protocolos únicos para su operación.

En toda red se asigna a cada dispositivo o nodo capaz de comunicarse, **una dirección de nodo o código único** que los demás pueden emplear cuando le transmiten información, equivalente a una dirección postal. Esta dirección de nodo depende del protocolo que se emplee. Cada protocolo emplea su propio esquema para las direcciones. En algunos casos, un mismo nodo puede funcionar con más de un protocolo y tener una dirección distinta para cada uno de ellos.

Los protocolos también se utilizan para asignar direcciones a las redes, conocida como dirección de la red, que suele formar parte de la dirección de cada nodo, de forma tal que al emplearla se sabe también la red a la que pertenece.

Los protocolos enrutables, están diseñados para que nodos pertenecientes a redes distintas puedan comunicarse. **Los protocolos no enrutables** se usan cuando no es así. Los principales protocolos utilizados son:

- **NetBIOS** – Protocolos definidos por IBM y Microsoft para redes de área local o metropolitana.
- **TCP/IP** – (*Transmisión Control Protocol/Internet Protocol*) Protocolos desarrollados por el Departamento de Defensa de los Estados Unidos para su red de conmutación de paquetes

 BANCO DE DESARROLLO ECONOMICO PARA PUERTO RICO Estado Libre Asociado de Puerto Rico		DIVISIÓN DE SISTEMAS DE INFORMACIÓN MANUAL DE SEGURIDAD
Procedimiento Núm.: BDE-005-SI-Proc.02	Deroga a: Manual de Seguridad 27 de junio de 2001	Fecha de aprobación: 9 de septiembre de 2008

ARPA. El Internet se ha convertido en un protocolo de uso general, muy extendido y la "lengua franca" de las redes en máquinas UNIX.

- **IPX/SPX** – (*Internet Packet Exchange/Sequential Packet Exchange*). Protocolos definidos por la compañía Novell como soporte de sus redes de área local.
- **Apple Talk** – Protocolos desarrollados por la compañía *Apple* para redes de ordenadores *Apple*.

C. DISPOSITIVOS DE CONEXIÓN E INTERCONEXIÓN

Los controles técnicos de los dispositivos en forma segura de conexión e interconexión permiten la entrada y acceso a la red.

La entrada y acceso a una red es la conexión de nuestro computador a la misma. La forma en que se realiza depende del sistema de cables coaxiales o enlace que empleemos y del tipo de computador que poseemos.

La conexión física entre la computadora y la red se establece siempre a través de un **puerto o conector** que permite enlazar el medio de transmisión con el circuito de acceso a la red.

Además de **los conectores** que facilitan el acceso a la red, se necesitan otros que establezcan las conexiones entre los distintos segmentos o ramales y otros que faciliten la interconexión con otras redes. Los dispositivos de interconexión utilizados son:

- **Repetidores** – dispositivos intercalados en la red a distancias determinadas, recogen y amplifican la señal a la entrada y la introducen nuevamente a la red, amplificada y regenerada.
- **Repetidores Multipuestos (HUB)** – conectan una estación con un dispositivo que ejerce de nodo central, conocido como repetidor multipuestos. Son repetidores dotados de más de dos (2) puertos cuya función es amplificar señales recogidas por uno de ellos e inyectarlas a todos los demás. Además de los puertos RJ-45, los repetidores multipuestos pueden llevar también a uno de dos (2) puertos AUI o BNC, para conectarlos a un enlace central entre redes, o unos con otros.
- **Unidades de Acceso Multiestación (MAU)** – ejercen la misma función que los anteriores, pero las señales provenientes de una puerta sólo se transmiten a la siguiente, siguiendo el funcionamiento en anillo.
- **Concentradores Multimedia** – son variantes del repetidor multipuesto *HUB* o *MAU* compuestos de un bastidor al que se añaden tarjetas, cada una de las cuales trabaja como un



Procedimiento Núm.:

BDE-005-SI-Proc.02

Deroga a:

**Manual de Seguridad
27 de junio de 2001**

Fecha de aprobación:

9 de septiembre de 2008

medio de conexión distinto y el bastidor proporciona alimentación a todas las tarjetas y las conecta entre sí.

- **Puentes (*Bridges*)** – conectan entre sí dos (2) segmentos de la misma red y reconocen en qué segmento de los que conectan, está cada estación. Filtran los paquetes que les llegan, dejando pasar de uno a otro segmento sólo aquellos paquetes originados en uno cuya estación de destino está en el otro. Los puentes se usan para aislar el tráfico local de cada segmento, evitando que afecte a otros y permitiendo la comunicación entre estaciones conectadas en distintos segmentos.
- **Encaminadores (*Routers*)** – son dispositivos empleados para conectar entre sí redes distintas que empleen los mismos protocolos y pueden usarse pequeños ordenadores para esta función. Sólo reconocen los paquetes de los protocolos para los cuales han sido diseñados. Ejercen una primera función de puente, permitiendo el paso entre sus puertos a los paquetes cuyo destino sea una red distinta a la de origen. Además, intercambian información periódicamente entre ellos, lo que les permite hacerse una idea de la configuración de la red general y del estado de la misma en cada momento. Cuando le llega un paquete, examina toda la información que ha acumulado y elige la vía más rápida y segura para transferir el paquete a la red de destino.
- **Puentes/Encaminadores (*Brouters*)** – es un encaminador para los paquetes de unos determinados protocolos y para los demás protocolos, actúa como puente.
- **Pasarelas (*Gateways*)** – son dispositivos que traducen los lenguajes, convenciones y costumbres de una y otra red. Se evita su uso, siempre que es posible, por el problema de toda traducción que nunca es un reflejo exacto del original.

D. SERVIDORES DE ARCHIVOS

Los servidores en la red permiten el almacenamiento seguro de la información, datos y archivos en la red.

Los **servidores de archivos** son ordenadores o computadoras conectadas a una red que provee sus dispositivos de almacenamiento, principalmente sus discos duros, en parte o en su totalidad. Funcionan como biblioteca pública donde además de retirar documentos, podemos guardar nuestros documentos. Los servidores de archivos ofrecen la ventaja de una mayor capacidad de almacenamiento, además que permiten compartir la información, centralizar las copias de seguridad y facilitar la distribución e instalación de aplicaciones.

Los **servidores dedicados** son servidores de archivo también, pero se usan única y exclusivamente para servicio de almacenamiento de otros ordenadores.



Procedimiento Núm.:

BDE-005-SI-Proc.02

Deroga a:

**Manual de Seguridad
27 de junio de 2001**

Fecha de aprobación:

9 de septiembre de 2008

Los **servidores no dedicados** permiten a los usuarios de la red acceder sus discos y pueden ser empleados simultáneamente para el trabajo normal del usuario. Son como pequeñas bibliotecas privadas cuyos dueños permiten a los vecinos usarlas.

Los **servidores de impresión** son ordenadores conectados a la red. Se conectan a él un número suficiente de impresoras para cubrir las necesidades de impresión de todos los usuarios de la misma.

Las **impresoras de red** son impresoras conectadas directamente a la red y no a un ordenador, y pueden ser accedidas por todos los usuarios de la misma.

E. CORREO ELECTRÓNICO¹

El **Correo Electrónico** es un servicio de comunicación y archivo de la red. El Correo Electrónico es uno de los servicios más frecuentes en la red a través de una Central de Correo con un conjunto de archivos almacenados en un servidor de la red o servidor de archivo. La Central está compuesta por todos los buzones de los usuarios del correo.

La dirección de Correo de cada usuario es la etiqueta de su buzón, nombre o código de la Central de Correos. Cada usuario de Correo emplea un pequeño programa conocido como **Cliente de Correo** en su computadora personal. El Cliente de Correo tiene integrado un pequeño procesador de textos para escribir los mensajes y algún sistema para seleccionar las direcciones. Una vez escrito el mensaje y seleccionada la dirección, el cliente se pone en contacto con la Central para depositarlo o el propio cliente se encarga de depositar el mensaje en el buzón correspondiente. Hay redes que tienen un servidor de correo y el cliente se pone en contacto con el servidor y le entrega el mensaje.

El **Servidor de Correo** examina la dirección y la deposita en el buzón correspondiente de los usuarios.

Para leer un mensaje, cada usuario emplea su propio Cliente de Correo y éste le informa al usuario de los nuevos mensajes que han llegado. La mayoría de los Clientes de Correo efectúan esta operación automáticamente cada cierto tiempo, y aunque el usuario esté trabajando en algún otro programa, le avisan cuando llega un nuevo mensaje. Otros controles del Correo Electrónico incluyen:

¹ Puede referirse al Manual de Procedimientos de la División de Sistemas de Información para conocer más acerca de las normas y procedimientos para el envío y recibo de correo electrónico y correspondencia interna.

 BANCO DE DESARROLLO ECONOMICO PARA PUERTO RICO Estado Libre Asociado de Puerto Rico		DIVISIÓN DE SISTEMAS DE INFORMACIÓN MANUAL DE SEGURIDAD
Procedimiento Núm.: BDE-005-SI-Proc.02	Deroga a: Manual de Seguridad 27 de junio de 2001	Fecha de aprobación: 9 de septiembre de 2008

- **Copias Múltiples** - enviar el mismo mensaje a varios destinatarios o con las direcciones de otros usuarios, con algunas características en común, por listas de distribución, añadiendo las direcciones manualmente o especificando alguna de las direcciones.
- **Copia Pública o Secreta** – se envía un mensaje a un usuario destinatario principal y una copia a otro. La copia puede ser pública y se informa al destinatario principal que se ha enviado una copia o puede ser secreta y el destinatario principal no saberlo.
- **Acuse de Recibo** – el usuario envía el mensaje y recibe una confirmación del servidor en el momento que el destinatario lo lee.
- **Reenvío** - se añaden comentarios personales a un mensaje recibido y se envía de nuevo a otros usuarios que pudieran estar interesados.
- **FAX de Red** – es un fax conectado a la red a la que pueden acceder los usuarios de la misma y es controlado por un servidor de fax, que se encarga de recibir los documentos que se desean enviar, junto con los números de destino. Se pueden almacenar o imprimir los documentos que se reciben. Se puede combinar con el Correo Electrónico y definir una serie de usuarios de correo “Tipo Fax” y los mensajes dirigidos a ellos se encaminarán automáticamente al fax.

El sistema de correo controla el reintentar la conexión si hay problemas, de informar el desarrollo de la misma y de cualquier otro aspecto del envío o recibo. Utilizando un “Fax” de última generación es posible identificar un “Fax” entrante el código del usuario a quien va destinado y depositarlo automáticamente en su buzón.

F. CONEXIÓN REMOTA Y PROCESO DISTRIBUIDO

Los controles técnicos de conexión remota y proceso distribuido se describen a continuación:

La **emulación de terminal** es como hacer una visita personal a otro computador, conectándose a éste como un terminal propio. Para ello hemos de conseguir que nuestro teclado y nuestro monitor funcionen como si estuviesen conectados directamente a la computadora que deseamos “visitar”.

El servicio que facilita este tipo de conexión se denomina **emulación de terminal** y se apoya sobre el servicio básico de interconexión, donde se crea un terminal ficticio, prestando al computador remoto la pantalla y teclado, en todo o en parte directamente conectados. A esta conexión se le conoce como **sesión**.

Para poder establecer una emulación de terminal, se necesita que el computador asignado disponga del **programa de emulación de terminales** y tener acceso al computador con el que se va a

 BANCO DE DESARROLLO ECONOMICO PARA PUERTO RICO Estado Libre Asociado de Puerto Rico		DIVISIÓN DE SISTEMAS DE INFORMACIÓN MANUAL DE SEGURIDAD
Procedimiento Núm.: BDE-005-SI-Proc.02	Deroga a: Manual de Seguridad 27 de junio de 2001	Fecha de aprobación: 9 de septiembre de 2008

establecer una sesión, a través de un nombre de usuario y código de acceso que serán reconocidos por el computador remoto.

Terminales X-Windows – son una conexión con un computador remoto dotándolo de capacidades gráficas. Las sesiones se establecen entre dos (2) computadores conectados mediante una red. El computador que establece la conexión, funciona como un servidor X y el computador remoto trabaja un programa complementario llamado Cliente X. Los programas ven al Cliente X como un terminal gráfico y lo gobiernan para su entrada y salida.

El **Control Remoto** se utiliza cuando la emulación de terminal en el sentido clásico no es posible, enlazando el teclado de un computador con el monitor del computador remoto, para controlar el computador remoto desde el otro. Un computador equipado con control remoto puede controlar otros computadores remotos que también estén instalados o varios simultáneamente. En una forma más controlada, se puede usar para examinar desde un monitor las pantallas de otros computadores, sin alterar nada en el funcionamiento de los remotos.

Los **Servidores de Acceso Remoto** son computadores con uno o más módems conectados a ellos y con conexión a la red. Cuando el servidor recibe una llamada a través del módem, identifica al usuario que está al otro extremo y si todo es correcto, establece un puente entre él y la red, de forma que la información que le llega vía módem es introducida en la red, como si se hubiese originado allí. La información destinada al usuario remoto es recogida y retransmitida por línea telefónica. El usuario emplea un **Cliente de Acceso Remoto** que es un programa que se encarga de establecer la conexión y la identificación ante el servidor de acceso remoto.

El **Proceso Distribuido** consiste en que dos (2) computadores se ponen de acuerdo para efectuar un determinado trabajo, cada uno con las tareas que mejor se adaptan a sus capacidades.

El **Sistema Operativo** de la Red de Información del Banco es Microsoft Windows 2000 y 2003, que es un servidor que funciona sobre las máquinas en la red Ethernet y soporta múltiples protocolos. **Windows para Trabajo en Grupo** es una aplicación que incorpora capacidades de servidor de archivo e impresora y funciona sobre cualquier computadora Windows, incluye Correo Electrónico y Agenda Electrónica de Grupo.

G. CONTROLES DE SEGURIDAD

Los conceptos básicos y controles técnicos de los componentes de la red (Cliente, Servidor y Red de Información) fueron descritos en las secciones anteriores de este Capítulo para facilitar la comprensión de los controles de seguridad de cada uno de estos componentes a la seguridad total de la Red de Información. Los componentes de la red los podemos clasificar en las siguientes categorías:



Procedimiento Núm.:
BDE-005-SI-Proc.02

Deroga a:
Manual de Seguridad
27 de junio de 2001

Fecha de aprobación:
9 de septiembre de 2008

1. Componentes del *Hardware*

- Computadoras
- Módem
- Impresoras
- CD's
- Unidades de *Backup* (Discos, cartuchos)
- Servidores de Archivo
- Microcomputador y minicomputadoras

2. Conexión de los componentes *Hardware*

- Configuraciones
- Red de Área Local (LAN) – varias computadoras conectadas vía un servidor de archivo
- Red de Área Ancha (WAN) – varios LANs conectados vía puentes o encaminadores
- Conexión del LAN al *Mainframe* o microcomputadora (Ejemplo: vía una pasarela)
- Redes externas (Servicio de *Bulletin Board BBS*, Internet y otras redes del Gobierno)
- Cables, puentes, encaminadores, pasarelas y otros
- Servicio telefónico
- Líneas de transmisión de los datos (Microondas, Satélite o Celular)

3. Componentes del *Software*

- Sistema Operativo que corre los servidores: *Windows NT Server 4.0, Windows 2000, Windows 2003*
- Servidor de control primario BDE-dc1 – componentes del cliente, usuarios o grupos y componentes del servidor. Componentes principales:
 - *Windows 2000 Server*
- Servidor de PDC BDE-PDC
 - *Windows 2000 Server*

 BANCO DE DESARROLLO ECONOMICO PARA PUERTO RICO Estado Libre Asociado de Puerto Rico		DIVISIÓN DE SISTEMAS DE INFORMACIÓN MANUAL DE SEGURIDAD
Procedimiento Núm.: BDE-005-SI-Proc.02	Deroga a: Manual de Seguridad 27 de junio de 2001	Fecha de aprobación: 9 de septiembre de 2008

- Servidores de Aplicaciones
- Servidor de Documentos
- Servidor de Impresoras
- Servidores de Bases de Datos (Cantidad 4) – manejador de la Base de Datos y restauración de base de datos (SQL). Tiene los siguientes componentes principales:
 - *Windows 2000 y Windows 2003*
 - Servidor de Aplicaciones
 - SQL 2000
- Servidor de dominio BDE-SNA – manejador de comunicaciones con otras Microcomputadoras en el exterior (BGF, Inversiones). Componentes principales:
 - Windows NT Server 4.0
 - SNA Server
- Servidor de dominio *Backup Control* y servicio de correo electrónico “BDE – 01mail”
 - *Windows 2003 Server*
 - *Microsoft Exchange Server 2003*
- Servidor de Dominio RAS “BDE-RAS” – usado para conexión remota
 - *Windows 2000*
 - Equinos
 - RAS Connection

4. Componentes del *Humanware*

- Gerencia: Vicepresidentes Ejecutivos y Gerentes de cada División
- Personal de Apoyo Operacional de la División de Sistemas de Información (Supervisores, Operadores, Técnicos de Sistemas, Desarrolladores, Oficial de Seguridad de Informática)
- Usuarios del Banco
- Administrador de la Red
- Oficial de Seguridad – Oficial de Seguridad de Informática de Sistemas de Información
- Suplidores o Vendedores – de Equipo *hardware* y Programas *software*

 BANCO DE DESARROLLO ECONOMICO PARA PUERTO RICO Estado Libre Asociado de Puerto Rico		DIVISIÓN DE SISTEMAS DE INFORMACIÓN MANUAL DE SEGURIDAD
Procedimiento Núm.: BDE-005-SI-Proc.02	Deroga a: Manual de Seguridad 27 de junio de 2001	Fecha de aprobación: 9 de septiembre de 2008

- Consultores – Ayuda externa contratada por la División de Sistemas de Información
- Auditores – auditoría de cumplimiento con los procedimientos establecidos del Banco

5. Los controles de seguridad básicos de la Red de Información incluyen:

- Procedimientos y prácticas de seguridad debidamente establecidos por escrito
- Supervisión, adiestramiento y auditoría para asegurar que las prácticas y procedimientos de seguridad son seguidos por el personal.
- Acceso controlado al Centro de Cómputos, equipo *hardware*, programas *software* y datos.
- Reportar las violaciones de seguridad y asegurar que no se repitan mediante planes de acciones correctivas (Notificación de Eventos).
- Reportar los cambios en los controles técnicos y de seguridad de la red y evaluarlos para aprobación (Control de Cambios).

6. Los controles de seguridad de los componentes de la red establecidos deben garantizar:

- Compromiso de la Gerencia a través de políticas, reglamentos y procedimientos escritos para proteger los servicios de la red.
- Mantener la confidencialidad de las contraseñas o códigos de acceso a la red, acceso restringido al Centro de Cómputos y Servidor de Ficheros.
- Asegurar la integridad de la información que garantice que la información es completa y correcta.
- Disponibilidad del Sistema de Información y procedimientos de recuperación.
- Uso de instalación correctos de los componentes de la red que aseguren su funcionamiento correcto y seguro.

H. CONTROLES DE SEGURIDAD PARA LAS ESTACIONES DE TRABAJO

Los controles de seguridad para las Estaciones de Trabajo de los usuarios del Banco incluyen:

1. Áreas seguras y cerradas donde estén instalados los equipos de computadoras

 BANCO DE DESARROLLO ECONOMICO PARA PUERTO RICO Estado Libre Asociado de Puerto Rico		DIVISIÓN DE SISTEMAS DE INFORMACIÓN MANUAL DE SEGURIDAD
Procedimiento Núm.: BDE-005-SI-Proc.02	Deroga a: Manual de Seguridad 27 de junio de 2001	Fecha de aprobación: 9 de septiembre de 2008

2. Los usuarios están capacitados en cómo:

- Encender y apagar la computadora y periferales
- Activar y usar los programas o aplicaciones.
- Manejar y almacenar correctamente los diskettes, cintas y CD's.
- Hacer *backups* de la información diariamente o a intervalos más frecuentes, cuando sea necesario.
- Establecer y terminar las comunicaciones.
- Mantener el área limpia.
- Establecer y mantener el cotejo de virus en programas y en cada computadora.

3. La seguridad física:

- Acceso físico restringido a computadoras con información en proceso confidencial.
- Poner seguro a las unidades lectoras de discos y cubiertas de computadoras.
- Colocar cables a los equipos.
- Siempre salir del sistema (*sign out*) para *laptops* y computadoras, al abandonar el área de trabajo.

4. Control de la Seguridad Lógica y la protección de las contraseñas cuando:

- Realiza acceso inicial a la computadora (*logon*) para protección al *software*
- Acceso al servidor de archivo de la red a través de la seguridad de la Red (*Windows 2000 y Windows 2003*)
- Acceso a los servidores y las computadoras a través de los sistemas de seguridad de los mismos
- Acceso a programas o aplicaciones a través de los sistemas de seguridad internos de cada aplicación.

 BANCO DE DESARROLLO ECONOMICO PARA PUERTO RICO Estado Libre Asociado de Puerto Rico		DIVISIÓN DE SISTEMAS DE INFORMACIÓN MANUAL DE SEGURIDAD
Procedimiento Núm.: BDE-005-SI-Proc.02	Deroga a: Manual de Seguridad 27 de junio de 2001	Fecha de aprobación: 9 de septiembre de 2008

- Cambio de contraseñas, a los intervalos establecidos por el Oficial de Seguridad (CSO)

5. Controles Programación

- Para todo cambio, innovación o uso de sistemas, programas, formas nuevas o modificaciones, éstos deben documentarse en el Formulario de Control de Cambios y obtener autorización o aprobación gerencial para su uso e implementación.
- Usar diferentes directorios o archivos para los programas en ambiente de producción y ambiente de prueba, para diferenciarlos.
- Establecer y cumplir con los estándares de prueba de programas, antes de ser implementados en ambiente de producción.
- Establecer y cumplir con los controles de acceso a programas en ambiente de prueba y de producción.

6. Documentación

- Completar los procedimientos y documentación requerida en los estándares de Control de Calidad establecidos en este Manual.
- Mantener una lista del inventario de computadoras del Banco, dónde están localizadas y quién está autorizado a utilizarlas.

7. Plan de Recuperación de Desastre

- Identificar las aplicaciones críticas que corren en las computadoras.
- Completar los procedimientos de recuperación descritos en el Plan Operacional de Emergencias del Banco.

I. CONTROLES DE SEGURIDAD PARA LOS SERVIDORES

Procedimientos de seguridad para los servidores:

1. Los servidores están instalados en el Centro de Cómputos con control de acceso para su seguridad física.
2. Los controles de acceso lógico incluyen acceso restringido al personal y la supervisión del Administrador de la Red.

 BANCO DE DESARROLLO ECONOMICO PARA PUERTO RICO Estado Libre Asociado de Puerto Rico		DIVISIÓN DE SISTEMAS DE INFORMACIÓN MANUAL DE SEGURIDAD
Procedimiento Núm.: BDE-005-SI-Proc.02	Deroga a: Manual de Seguridad 27 de junio de 2001	Fecha de aprobación: 9 de septiembre de 2008

3. La contraseña del Administrador de la Red, debe estar escrita y almacenada en un sobre sellado en una localización segura.
4. El acceso al servidor de archivo tiene acceso restringido de contraseña por usuario, por horario de trabajo, derechos de acceso a archivos y programas (*access rights*), y control de acceso a computadoras y utilidades (*Norton*).
5. Se lleva a cabo un *Audit/Log* del sistema para investigar los eventos no usuales en la red.
6. Se mantiene una lista actualizada de los usuarios autorizados de la red. Esta lista se actualiza cada vez que algún empleado termina sus labores en el Banco o es transferido de División de Trabajo.
7. Se mantiene cotejo de virus en los programas de los servidores.

Controles operacionales:

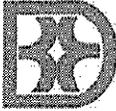
Los **controles operacionales** incluyen los procedimientos de operación contenidos en el Manual de Procedimientos de la División de Sistemas de Información:

- Activar los servidores, programas y módulos
- Desactivar los servidores, programas y módulos
- Procedimientos de *backup*

J. CONTROLES DE SEGURIDAD DE COMPONENTES

Los controles de seguridad en la administración de la Red de Información incluyen:

1. Desarrollar diagramas de localización de:
 - Cada computadora y servidor, dónde está y quién lo utiliza
 - Cablerías por piso, División, edificio y por tipo de conexión (computadora a servidor y otros)
 - Componentes de la RED: Impresora, *HUB*, puentes, *routers*, *Firewall*, *switch* y *módems*.
2. Identificar los componentes de la Red:
 - Por orden de encendido

 BANCO DE DESARROLLO ECONOMICO PARA PUERTO RICO Estado Libre Asociado de Puerto Rico		DIVISIÓN DE SISTEMAS DE INFORMACIÓN MANUAL DE SEGURIDAD
Procedimiento Núm.: BDE-005-SI-Proc.02	Deroga a: Manual de Seguridad 27 de junio de 2001	Fecha de aprobación: 9 de septiembre de 2008

- Por orden de apagado
 - Computadoras o servidores con acceso a líneas telefónicas
 - Líneas directas o número telefónico para llamadas de salida (hacia las regiones, *dialing out*) y de entrada al Banco.
3. El Centro de Cómputos tiene acceso restringido a los componentes de la red y los cables están debidamente protegidos en sus puntos de conexión a través del techo, piso y paredes, por cubiertas que controlan su acceso.
4. Los controles de acceso lógico incluyen:
- Uso de pared de fuego *Firewall* o *New Buss World* en el servidor de comunicaciones para interceptar el acceso a la red interna y determinar si el acceso es permitido.
 - La programación de los *routers*, *switches*, *firewall* tienen acceso restringido y sólo pueden cambiarse por autorización y documentación en el Formulario de Control de Cambios.

K. CONTROLES DE SEGURIDAD PARA LAS COMUNICACIONES

Los controles de seguridad para las comunicaciones y el acceso lógico a las comunicaciones en la red está controlado por:

- Acceso autorizado a otras redes
- Acceso a personal autorizado solamente
- Acceso controlado por nodo
- Acceso controlado al horario de trabajo.
- Acceso autorizado de usuarios externos a la red, de otras sucursales, regiones o agencias del gobierno.
- Acceso controlado a los sistemas en la red interna del Banco.
- Uso de contraseñas en paquetes de comunicaciones para cada computadora.

 BANCO DE DESARROLLO ECONOMICO PARA PUERTO RICO Estado Libre Asociado de Puerto Rico		DIVISIÓN DE SISTEMAS DE INFORMACIÓN MANUAL DE SEGURIDAD
Procedimiento Núm.: BDE-005-SI-Proc.02	Deroga a: Manual de Seguridad 27 de junio de 2001	Fecha de aprobación: 9 de septiembre de 2008

- Monitoreo continuo y reportes *Logs* de acceso a la red interna para vigilancia de piratas que traten de penetrar la red sin acceso autorizado.
- Monitoreo de acceso de comunicaciones (Internet y otros accesos telefónicos)

L. CONTROLES DE SEGURIDAD DE LA BASE DE DATOS

El Sistema de Administración de la Base de Datos es la base del ambiente de aplicación cliente/servidor que incluye los siguientes controles de seguridad:

- Uso y control de la Base de Datos
- Acceso restringido a tablas de relación, base de datos, programas y utilidades
- Los programas y tablas de relación de la base de datos no son públicas
- Capacitación del personal en los programas y tablas de relación de la base de datos
- Control de las herramientas de desarrollo como SQL, para que no acceda a la información de producción sin los controles apropiados.
- Mantenimiento de un inventario actualizado de tablas de relación de la base de datos, programas y usuarios autorizados.
- Añadir la seguridad y control técnico como un parámetro de evaluación del sistema de administración de la Base de Datos.

M. CONTROLES DE SEGURIDAD DE CONEXIÓN AL *MAINFRAME*

La seguridad de las conexiones al *Mainframe* y controles requeridos incluyen:

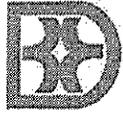
- Conocer dónde se conecta la red al *Mainframe*
- Mantenimiento de la conexión (Ejemplo: pasarelas)
- Conocer la operación de mecanismo de conexión (Ejemplo: pasarelas)

N. CONTROLES DE SEGURIDAD ADMINISTRATIVOS

Los controles de seguridad administrativos de la RED incluyen la implementación de paquetes de seguridad o mecanismos de acceso controlado a:

 BANCO DE DESARROLLO ECONOMICO PARA PUERTO RICO Estado Libre Asociado de Puerto Rico		DIVISIÓN DE SISTEMAS DE INFORMACIÓN MANUAL DE SEGURIDAD
Procedimiento Núm.: BDE-005-SI-Proc.02	Deroga a: Manual de Seguridad 27 de junio de 2001	Fecha de aprobación: 9 de septiembre de 2008

- Cada computadora
- Cada Servidor
- Servidor de Archivo
- Sistema de Administración de la base de datos cliente/servidor
- Sistema de comunicaciones



Procedimiento Núm.:

BDE-005-SI-Proc.02

Deroga a:

**Manual de Seguridad
27 de junio de 2001**

Fecha de aprobación:

9 de septiembre de 2008

CAPÍTULO VI – CONTROLES DE SEGURIDAD *SOFTWARE*

A. DERECHOS DE PROPIEDAD INTELECTUAL

Los sistemas de información han contribuido al desarrollo de leyes y prácticas sociales que protegen la propiedad intelectual.

Propiedad intelectual **se considera la propiedad intangible creada por individuos o corporaciones y está protegida legalmente por tres (2) prácticas legales: Derechos de Autor (*Copyright*) y Patentes (*Patent Law*).**

Cada una provee diferentes tipos de protección al *software* como propiedad intelectual.

Los Derechos de Autor (*Copyright*) es un estatuto de garantía que protege al creador de la propiedad intelectual. En el 1960, la Oficina de Derechos de Autor comenzó a registrar los programas *software*. En el 1980 se aprobó el Acta de Derechos de Autor de *software* Computarizado, que provee protección del código fuente y objeto, copias del original vendidos comercialmente y los derechos del comprador que usa el *software*, pero el creador retiene el Título Legal de Propietario. La Ley de Protección es explícita en proteger el *software* de copias de los programas completos o sus partes.

La **Ley de Patentes** garantiza al dueño el provecho exclusivo de sus ideas de una invención por hasta veinte (20) años, sujeto al cumplimiento de ciertos requisitos. Esta ley fue diseñada para asegurar que los inventores de nuevas máquinas o nuevos métodos, sean recompensados por su labor, mientras se disemina en el mercado, el uso de su invención. Desde 1981, la Corte Suprema decidió que los Programas de Computadoras *software* pueden ser parte del proceso de patentes.

B. CONTROLES DE SEGURIDAD *SOFTWARE*

Los usuarios de los Sistemas de Información del Banco utilizarán los programas *software* de acuerdo al Contrato de Licencia de Usuario. La duplicación de *software* con derechos de autor, excepto para *backup* y archivo, es una violación a la Ley y es contraria a los estándares de conducta del Banco. Los siguientes controles de seguridad deben seguirse para cumplir con los Contratos de Licencias de *software*:

1. Se usará todo *software* de acuerdo a su Contrato de Licencia.
2. Se proveerá *software* legítimo a todos los usuarios del Banco que estén autorizados por la División de Sistemas de Información a utilizarlos.



Procedimiento Núm.:

BDE-005-SI-Proc.02

Deroga a:

**Manual de Seguridad
27 de junio de 2001**

Fecha de aprobación:

9 de septiembre de 2008

3. Ningún asociado del Banco hará copias no autorizadas de *software* bajo ninguna circunstancia. Cualquier usuario que se encuentre copiando *software* estará sujeto a acciones disciplinarias.
4. No se permitirá el uso de copias de *software* en el Banco. Cualquier persona que reproduzca *software* estará sujeta a penalidades civiles y criminales, incluyendo multas y confinamiento, como individuo legalmente responsable.
5. Ningún usuario del Banco proveerá copias de *software* a personas ajenas al Banco, incluyendo clientes, contratistas, consultores, familiares, amistades y otros.
6. Cualquier usuario que observe uso inadecuado del *software* en el Banco, notificará al Gerente de su División, a la División Legal o al Auditor General del Banco.
7. Todo el *software* utilizado en el Banco, será comprado e instalado en las computadoras, siguiendo los procedimientos legales, de acuerdo a los Contratos de Licencia de los mismos.

C. LICENCIAS DE *SOFTWARE*

Las **Licencias de Usuario de *software*** son un permiso legal o derecho para usar un programa. También establecen restricciones en cuanto al número de personas y número de máquinas que utilizarán el programa en el Banco. Las **Licencias Locales (*Site License*)** permiten el uso ilimitado del *software*, siempre que sea en el interior del Banco. Hay programas que se crean por encargo (***Custom made***) para instituciones con **Licencia Exclusiva**, a su nombre, para evitar que el autor venda copias a la competencia.

Al comprarse un *software*, se debe solicitar al proveedor o autor del programa:

1. El código fuente o protección para que en el caso que desaparezca la empresa del *software*, el autor deposite el código fuente en manos de un tercero que actúe como fideicomisario.
2. El proveedor del *software* debe proveer una documentación adecuada o programa de formación al cliente o usuario.
3. Solicitar instalación de programas prototipo, para correr pruebas y cuando aplique, solicitar modificaciones, previo a la implementación.
4. Se debe planificar, siempre que se pueda, para mantener un sistema de información único, adquirido de un solo proveedor, para evitar programas no compatibles entre sí. De lo contrario, previo a la compra del *software* se debe solicitar al proveedor requisitos de compatibilidad con los programas existentes en el sistema o añadidos a un sistema en existencia.

 BANCO DE DESARROLLO ECONOMICO PARA PUERTO RICO Estado Libre Asociado de Puerto Rico		DIVISIÓN DE SISTEMAS DE INFORMACIÓN MANUAL DE SEGURIDAD
Procedimiento Núm.: BDE-005-SI-Proc.02	Deroga a: Manual de Seguridad 27 de junio de 2001	Fecha de aprobación: 9 de septiembre de 2008

5. Debe solicitarse al proveedor, en el momento de la compra del *software*, asistencia post-venta y también la garantía aplicable.
6. El comprador de *software* debe evaluar la Licencia de Uso del *software*, previo a la compra para determinar los requisitos de uso en el Banco.
7. Luego de la compra del *software*, el proveedor debe mantener al Banco al corriente de las innovaciones técnicas, para actualizar el mismo, cuando sea necesario.
8. Debe evaluarse con el proveedor del *software* la seguridad que provee el fabricante o la instalación de sistemas de seguridad en *software* para la protección de la Base de Datos, cuando se determine necesario.

El **Oficial de Seguridad de Informática** o la persona designada, mantendrá un archivo de las Licencias de Usuario del *software* disponibles en el Banco y se asegurará de que:

1. Si se han añadido máquinas o usuarios que excedan los términos del Contrato, notificará al proveedor del *software* y solicitará una Licencia de Usuario Actualizada y procesará órdenes de compra, donde sea necesario para cubrir el exceso.
2. Solicitará, mensualmente, al personal de programación la instalación de programas prototipo y correr pruebas de *software* nuevo, previo a su implementación y compra.
3. Solicitará al Gerente de Sistemas de Información, la instalación de *software* actualizado, conjuntamente con en el Mantenimiento Preventivo Interno de *software* en las computadoras del Banco.
4. Solicitará al personal de Desarrollo de Aplicaciones la evaluación de la seguridad que provee el fabricante o instalación de sistemas de seguridad al *software* nuevo para la protección de la base de datos y mantenimiento de un sistema de seguridad uniforme.
5. Los procedimientos establecidos de identificación, selección, programación, prueba, implementación y control de los sistemas de operación de programas, aplicaciones y *software* en general, se cumplen en forma rutinaria para la integridad de los datos y programas almacenados en los sistemas de información.

D. CONTROLES DE SEGURIDAD DE PROGRAMACIÓN

Todos los programas desarrollados por el personal de Desarrollo de Aplicaciones de la División de Sistemas de Información son propiedad del Banco. **En la institución no se escribirán programas para uso propio sin autorización.** El Manual de Desarrollo de Aplicaciones

 BANCO DE DESARROLLO ECONOMICO PARA PUERTO RICO Estado Libre Asociado de Puerto Rico		DIVISIÓN DE SISTEMAS DE INFORMACIÓN MANUAL DE SEGURIDAD
Procedimiento Núm.: BDE-005-SI-Proc.02	Deroga a: Manual de Seguridad 27 de junio de 2001	Fecha de aprobación: 9 de septiembre de 2008

establece los procedimientos a seguir por el personal de Desarrollo de Aplicaciones para el mantenimiento de prácticas uniformes de programación a través del Banco. Solamente se usarán procedimientos de programación documentados y aprobados. La documentación de programas se refiere a la escritura de programas en forma estructurada, siguiendo las prácticas de desarrollo de aplicaciones (programación) de aceptación general en la industria. Los controles de seguridad para la programación de aplicaciones y programas se describen a continuación:

1. Se revisarán las especificaciones del sistema y de los programas, previo a su instalación.
2. Se usarán técnicas estándares de codificación.
3. El código fuente incluirá el nombre del programador, nombre del programa, fecha y otra información pertinente, requerida por el **Supervisor de Desarrollo de Aplicaciones** o designado.
4. Se verificará la lógica del programa y se construirán árboles de decisión para los datos a probar para todas las excepciones, así como condiciones normales en el programa.
5. Se probarán los programas codificados para detectar errores de sintaxis, lógicos y de comunicación.
6. Se documentarán los programas para definir la manera en que el programa será corrido, establecer los controles requeridos del programa y proveer información al personal que lo operará.
7. Se harán comentarios o notas para explicar técnicas especiales matemáticas y de programación, en el lugar del programa donde serán utilizados.

E. INSTALACIÓN Y MANTENIMIENTO DE PROGRAMAS

Para transferir un programa a ambiente de producción, se requiere una revisión y aprobación para uso operacional. Este procedimiento aplica a todos los programas (los desarrollados internamente y los comprados), como se describe a continuación:

1. Las pruebas realizadas a los programas serán revisadas por el Desarrollador de Sistema para asegurar que se obtuvieron los resultados correctos previos a la aceptación de los resultados de la prueba.
2. Se verificará que la documentación del programa cumpla con las especificaciones establecidas.
3. Luego de ser formalmente aprobado, se transferirá el programa al ambiente de producción.

 BANCO DE DESARROLLO ECONOMICO PARA PUERTO RICO Estado Libre Asociado de Puerto Rico		DIVISIÓN DE SISTEMAS DE INFORMACIÓN MANUAL DE SEGURIDAD
Procedimiento Núm.: BDE-005-SI-Proc.02	Deroga a: Manual de Seguridad 27 de junio de 2001	Fecha de aprobación: 9 de septiembre de 2008

El mantenimiento de los programas instalados en ambiente de producción seguirá los procedimientos estándares de prueba establecidos, previo a su instalación. Estos procedimientos estándares de prueba incluyen lo siguiente:

1. **Revisiones del Programa:** son cambios menores sin hacer cambios lógicos mayores al Programa.
2. **Modificaciones de Programas:** son cambios que envuelven el rediseño de la lógica del programa o las relaciones de los subprogramas.
3. **Revisiones de Programas Comprados:** son correcciones hechas por el proveedor del *software* y enviados al cliente a ningún costo (siempre y cuando estén bajo garantía o contrato de mantenimiento), para su implementación.
4. **Actualización de Programas Comprados:** son provistos a un costo nominal por el proveedor del *software* y deben ser tratados como un programa nuevo en la instalación.

Toda modificación debe ser según el Procedimiento para la Solicitud de Creación o Modificación de Programas Creados por Sistemas de Información, que se encuentra en el Manual de Procedimientos. Las pruebas realizadas a los programas revisados, modificados o actualizados, deben asegurar que los cambios fueron hechos correctamente y que las secciones del programa que no fueron cambiadas están funcionando correctamente.

F. PROCEDIMIENTOS DE OPERACIÓN

La unidad de Desarrollo de Aplicaciones de la División de Sistemas de Información ha establecido procedimientos de operación en el Manual de Desarrollo de Aplicaciones para:

- Identificar
- Seleccionar
- Programar
- Probar
- Implementar
- Controlar los sistemas de operación de programas, aplicaciones y *software* en general.

El cumplimiento de los controles de calidad, auditoría, pruebas y seguridad, establecidos en los procedimientos de operación, asegurará la integridad de los datos y de los programas almacenados en los sistemas de información.

 BANCO DE DESARROLLO ECONOMICO PARA PUERTO RICO Estado Libre Asociado de Puerto Rico		DIVISIÓN DE SISTEMAS DE INFORMACIÓN MANUAL DE SEGURIDAD
Procedimiento Núm.: BDE-005-SI-Proc.02	Deroga a: Manual de Seguridad 27 de junio de 2001	Fecha de aprobación: 9 de septiembre de 2008

Se revisará y auditará el impacto en la seguridad de los datos procesados a través de los programas para evaluar:

- Restricciones de seguridad de acceso provistas en los programas.
- Restricciones de capacidades de programación o mantenimiento en programas en ambiente de producción.
- Cuáles terminales han sido configurados como consolas de programación y que los mismos tengan restricciones de seguridad lógica y física adecuadas para garantizar el acceso a los mismos por personal autorizado solamente de Desarrollo de Aplicaciones.
- Que los programas comprados a proveedores con contraseñas de instalación sean cambiadas al momento de la instalación como un procedimiento rutinario del área de programación.

 BANCO DE DESARROLLO ECONOMICO PARA PUERTO RICO Estado Libre Asociado de Puerto Rico		DIVISIÓN DE SISTEMAS DE INFORMACIÓN MANUAL DE SEGURIDAD
Procedimiento Núm.: BDE-005-SI-Proc.02	Deroga a: Manual de Seguridad 27 de junio de 2001	Fecha de aprobación: 9 de septiembre de 2008

CAPÍTULO VII – SEGURIDAD OCUPACIONAL

A. CONTROL Y PREVENCIÓN DE RIESGOS A LA SALUD

Para controlar y prevenir los riesgos a la salud por el uso de computadoras, se ha desarrollado la Tecnología de Ingeniería de Seguridad y los Controles Administrativos descritos a continuación:

1. Controles de Ingeniería – Las enfermedades ocupacionales de *Repetitive Strain Injury (RSI)* y *Carpal Tunnel* se pueden evitar utilizando: estaciones de trabajo diseñadas para posicionar la muñeca en posición neutral sobre un descanso de muñeca que le dé sostén firme a la altura correcta; ajuste adecuado del monitor, a través de uso de una base correctamente posicionada a la altura de la visión; descanso de los pies; y uso de sillas ergonómicas. También existen teclados ergonómicos que deben ser provistos al personal que haya reportado algún tipo de enfermedad RSI por el uso de computadoras.
2. Controles Administrativos – Estas medidas de ingeniería industrial deben ser acompañadas de controles administrativos adecuados como recesos de descanso frecuentes, rotación de usuarios en diferentes trabajos, uso de técnicas de entrada de datos *scanner* y añadiendo otras tareas que no requieran el uso de computadoras en la jornada de trabajo. La práctica en la industria es proveer recesos de periodos de quince (15) minutos cada dos (2) horas y proveer equipo ergonómicamente diseñado que proteja al empleado de enfermedades *RSI*, dolor de espalda, dolor de cuello, cansancio o dolor de los pies, por el uso de estaciones de trabajo con pobre diseño ergonómico.
3. Para proveer al empleado equipo ergonómicamente diseñado se requiere que el empleado reporte y presente evidencia de que padece algún tipo de condición o enfermedad por la cual necesite el uso de dicho equipo.

En términos generales, la seguridad ocupacional de los usuarios de computadoras debe incluir:

1. El entorno del área de trabajo debe estar ergonómicamente diseñado para la protección del usuario de computadoras con mobiliario, escritorio, silla, teclado y monitor localizados ergonómicamente a la altura y posición correcta de uso.
2. La iluminación del edificio debe ser adecuada para fomentar una visibilidad correcta y evitar esfuerzos visuales del empleado por pobre iluminación.
3. Los niveles de ruido deben ser mínimos en las áreas de trabajo.
4. Los programas de computadoras deben ser adecuados a la tarea y al uso que le da el usuario.

 BANCO DE DESARROLLO ECONOMICO PARA PUERTO RICO Estado Libre Asociado de Puerto Rico		DIVISIÓN DE SISTEMAS DE INFORMACIÓN MANUAL DE SEGURIDAD
Procedimiento Núm.: BDE-005-SI-Proc.02	Deroga a: Manual de Seguridad 27 de junio de 2001	Fecha de aprobación: 9 de septiembre de 2008

5. El Síndrome de Visión de Computadora (CVS) se puede controlar usando cubiertas de terminales, provistas en el mercado de computadoras para controlar la emisión de campos eléctricos no ionizados y magnéticos de bajas frecuencias en los terminales de video con tubos catódicos que afectan la visión.
6. A petición del empleado se proveen las cubiertas para los terminales. Dicha petición se debe realizar conforme al Procedimiento para las Compras de Bienes en General del Banco.

B. MEDIDAS DE PROTECCIÓN CONTRA INCENDIOS

Como parte de los programas de seguridad ocupacional deben establecerse controles para la protección de fuego en el Centro de Cómputos y en las operaciones de procesamiento de datos en el Banco, de acuerdo a los estándares generales de medidas de protección aceptados, como:

1. Estándares de protección de fuego para el edificio, promulgadas por el Departamento de Bomberos de Puerto Rico.
2. Seguros de Protección de los Activos del Banco en el evento de un fuego, incluyendo los sistemas de computadoras.
3. Inspecciones efectuadas por los Bomberos al edificio y facilidades del Banco.
4. Adiestramiento del personal en combatir un fuego, uso de extintores, procedimientos de emergencia, fuego, agua e incidentes de alarmas.
5. Informar al personal de la División de Sistemas de Información la localización de alarmas de fuego, extintores de fuego, interruptores eléctricos auxiliares y regulares, suministro de agua, sistema de aire acondicionado y cualquier otro aditamento de emergencia que se deba utilizar en una emergencia.
6. Llevar a cabo simulacros, con el personal de la División de sistemas de Información, de una situación de emergencia por incendio, por lo menos una vez al año.

Los procedimientos de seguridad relacionados a la protección de fuego del Centro de Cómputos de la División de Sistemas de Información fueron descritos en el Capítulo I de este Manual, como parte de los Controles de Seguridad Física.

 BANCO DE DESARROLLO ECONOMICO PARA PUERTO RICO Estado Libre Asociado de Puerto Rico		DIVISIÓN DE SISTEMAS DE INFORMACIÓN MANUAL DE SEGURIDAD
Procedimiento Núm.: BDE-005-SI-Proc.02	Deroga a: Manual de Seguridad 27 de junio de 2001	Fecha de aprobación: 9 de septiembre de 2008

CAPÍTULO VIII – MANTENIMIENTO DE LA SEGURIDAD

A. AUDITORÍAS DE SEGURIDAD

Una vez establecidos los controles de seguridad, procedimientos y políticas, es necesario verificar la adecuacidad, cumplimiento y efectividad de los mismos a través de auditorías internas de seguridad.

En el Apéndice se incluye una Lista de Cotejo para Auditoría Interna de Seguridad de cada uno de los subsistemas de seguridad. El **Oficial de Seguridad de Informática** de la División de Sistemas de Información o designado, llevará a cabo una Auditoría de Seguridad mensualmente de uno de los subsistemas de Seguridad, hasta completar una auditoría interna anual de cada uno de los subsistemas de seguridad.

La persona designada para preparar la auditoría preparará un reporte escrito preliminar al Gerente de la División en un periodo de una semana de completada la auditoría interna de Seguridad.

El reporte final será distribuido al personal responsable para completar las acciones correctivas y al Oficial de Seguridad de Informática.

En el mismo reporte original de auditoría, se documentará el seguimiento a los señalamientos realizados y se someterá nuevamente al personal responsable para su revisión.

Los procedimientos de Auditoría Interna son aplicables a las Auditorías Internas de Seguridad, aunque el Plan de Auditoría Interna está desglosado en las Listas de Cotejo de cada subsistema de seguridad, para facilitar su ejecución.

B. ÓRDENES DE SERVICIO

Los usuarios de los sistemas de información llenarán la Solicitud de Servicio y la entregarán al Oficial de Seguridad de Informática, para solicitar acceso, cambio de contraseña y otros servicios que apliquen a restricciones o autorizaciones de acceso y en relación a la seguridad de los sistemas de información.

C. ADIESTRAMIENTO DE PERSONAL

Se establecerán programas de adiestramiento para los miembros del grupo de trabajo de la División de Sistemas de Información y las orientaciones necesarias para los usuarios de computadoras en el Banco. La persona responsable de organizar las orientaciones es el **Oficial de Seguridad de Informática**.

 BANCO DE DESARROLLO ECONOMICO PARA PUERTO RICO Estado Libre Asociado de Puerto Rico		DIVISIÓN DE SISTEMAS DE INFORMACIÓN MANUAL DE SEGURIDAD
Procedimiento Núm.: BDE-005-SI-Proc.02	Deroga a: Manual de Seguridad 27 de junio de 2001	Fecha de aprobación: 9 de septiembre de 2008

D. NOTIFICACIÓN DE EVENTOS

Los eventos no rutinarios, las violaciones de seguridad o fallas en los sistemas de seguridad, las excepciones a los procedimientos y los errores humanos que impactan la seguridad de los sistemas de información, serán documentados en el Formulario de Notificación de Eventos por el Oficial de Seguridad de Informática o por la persona designada, cuando aplique.

E. CONTROL DE CAMBIOS

Los cambios en los sistemas de seguridad de los Sistemas de Información serán documentados en el Manual de Procedimientos de la División de Sistemas de Información y en este Manual de Seguridad.

F. MANTENIMIENTO DE LA SEGURIDAD

El mantenimiento rutinario de la seguridad en las áreas generales es completado por el **Oficial de Seguridad de Informática**. Para los procesos, controles de seguridad, *hardware*, *software* y bases de datos, el mantenimiento está a cargo del **personal designado de la División de Sistemas de Información**. Dicho mantenimiento incluye lo siguiente:

1. Agregar y borrar empleados o clientes en el acceso a los sistemas de información.
2. Mantener, probar y limpiar equipos *hardware*.
3. Actualizar o revisar programas de aplicación o *software*.
4. Mantener discos y archivos que han sufrido fragmentación.
5. Hacer *backups* de los datos y programas en las frecuencias establecidas.
6. Hacer corridas *Audits* y *Logs* del Sistema en las frecuencias establecidas.
7. Monitoreo de transacciones rechazadas a través de informes del Sistema.
8. Prevención de infección de virus.
9. Prevención de acceso no autorizado de piratas.
10. *Computer Edits* para eliminar datos ilógicos o evitar que entren a la base de datos.
11. Uso de *Templates*, cuando apliquen.



Procedimiento Núm.:

BDE-005-SI-Proc.02

Deroga a:

**Manual de Seguridad
27 de junio de 2001**

Fecha de aprobación:

9 de septiembre de 2008

12. Cambiar contraseñas cada treinta (30) días.
13. Transmisiones codificadas (*encrypted*), cuando apliquen.
14. Mantenimiento de los controles de seguridad física, seguridad ocupacional y prevención de incendios.
15. Mantener Licencias de *software* por número de máquinas o usuarios, en forma rutinaria.
16. Instalación y Mantenimiento de Programas *software* en forma rutinaria.
17. Mantener los controles de Seguridad de *software* y de programación establecidos.

 BANCO DE DESARROLLO ECONOMICO PARA PUERTO RICO Estado Libre Asociado de Puerto Rico		DIVISIÓN DE SISTEMAS DE INFORMACIÓN MANUAL DE SEGURIDAD
Procedimiento Núm.: BDE-005-SI-Proc.02	Deroga a: Manual de Seguridad 27 de junio de 2001	Fecha de aprobación: 9 de septiembre de 2008

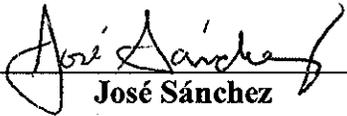
CAPÍTULO IX – CLÁUSULAS FINALES

A. DEROGACIÓN

Este documento deroga al Manual de Seguridad de la División de Sistemas de Información, aprobado el 27 de junio de 2001.

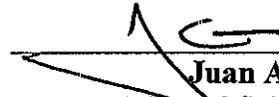
B. RECOMENDACIÓN

El Manual de Seguridad de la División de Sistemas de Información ha sido revisado y recomendado por el Gerente de Sistemas de Información y por el Primer Oficial Ejecutivo de Finanzas y Operaciones del Banco de Desarrollo Económico para Puerto Rico.



José Sánchez
Gerente

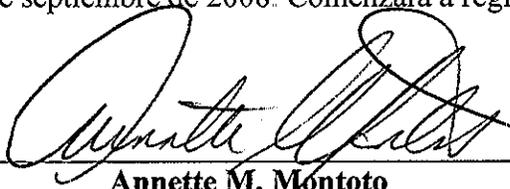
División de Sistemas de Información
Banco de Desarrollo Económico
para Puerto Rico



Juan A. Vargas
Primer Oficial Ejecutivo de
Finanzas y Operaciones
Banco de Desarrollo Económico
para Puerto Rico

C. APROBACIÓN

El Manual de Seguridad de la División 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 9 de septiembre de 2008. Comenzará a regir inmediatamente después de su aprobación.



Annette M. Montoto
Presidenta
Banco de Desarrollo Económico
para Puerto Rico

 BANCO DE DESARROLLO ECONOMICO PARA PUERTO RICO Estado Libre Asociado de Puerto Rico		DIVISIÓN DE SISTEMAS DE INFORMACIÓN MANUAL DE SEGURIDAD
Procedimiento Núm.: BDE-005-SI-Proc.02	Deroga a: Manual de Seguridad 27 de junio de 2001	Fecha de aprobación: 9 de septiembre de 2008

APÉNDICE

Inspección Interna de Seguridad

(Lista de Cotejo)

Itinerario Anual de Auditorías de Seguridad para los Subsistemas de Seguridad de los Sistemas de Información:

1. El Oficial de Seguridad de Informática o persona designada, completará las auditorías internas de cada uno de los subsistemas de seguridad, mensualmente, por lo menos una (1) vez al año, utilizando las Listas de Cotejo incluidas en este Apéndice.
2. Las Listas de Cotejo incluidas a continuación son:

Descripción	Título	Fecha (Mes/Año)
Subsistema I	Controles de Seguridad Administrativos	
Subsistema II	Controles de Seguridad de Acceso	
Subsistema III	Controles de Seguridad de <i>Backup</i>	
Subsistema IV	Controles de Seguridad Virus y Piratas	
Subsistema V	Controles de Seguridad Red de Información	
Subsistema VI	Controles de Seguridad <i>Software</i>	
Subsistema VIII	Mantenimiento de la Seguridad	

3. Cuando el cumplimiento resulte no satisfactorio, se documentarán las observaciones hechas o se adjuntará a la Lista de Cotejo la evidencia que justifique las observaciones, como por ejemplo: Formularios no documentados o documentados incompletos, informes de datos electrónicos del sistema, respuestas del personal al Auditor y otros.
4. Cada subsistema en la Lista de Cotejo corresponde al Capítulo con igual numeración en el Capítulo del Manual, para la preparación y consulta de la persona encargada de la auditoría, cuando sea necesario.



Procedimiento Núm.:
BDE-005-SI-Proc.02

Deroga a:
Manual de Seguridad
27 de junio de 2001

Fecha de aprobación:
9 de septiembre de 2008

Subsistema I:

Controles de Seguridad

Fecha Auditoría: _____

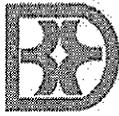
Administrativos

Auditor Interno: _____

Iniciales Auditor: _____

LISTA DE COTEJO

CONTROLES DE SEGURIDAD	CUMPLIMIENTO		OBSERVACIONES (Evidencia encontrada en relación con cumplimiento No Satisfactorio)
	Satisfactorio (v)	No Satisfactorio (v)	
1. El personal de Sistemas de Información se registra al entrar al Centro de Cómputos.			
2. El control de acceso electrónico al Centro de Cómputos está operando.			
3. El personal de la División de Sistemas de Información usa contraseña autorizada para acceder al Centro de Cómputos.			
4. Cuando no hay personal, en el tercer turno y los fines de semana, se cierra la puerta del Centro de Cómputos con llave.			
5. El personal no autorizado es escoltado al Centro de Cómputos por personal autorizado y se documenta en el Registro de Visitantes a la entrada y salida del Centro de Cómputos.			
6. Los siguientes equipos de protección están presentes y operando correctamente en el Centro de Cómputos:			
a. Unidades UPS			
b. Unidad de Aire			



Procedimiento Núm.:

BDE-005-SI-Proc.02

Deroga a:

**Manual de Seguridad
27 de junio de 2001**

Fecha de aprobación:

9 de septiembre de 2008

Acondicionado			
c. Humidificador			
d. Panel Eléctrico aparte, corriendo con la fuente de energía del Edificio			
7. Los siguientes requisitos de precaución de fuego están presentes y operando en el Centro de Cómputos:			
a. No hay líneas de gas, agua, líquidos, alto voltaje o radiación magnética adyacentes.			
b. Tiene disponibles extintores de fuego de gas Halón			
c. Tiene detectores de humo instalados			
d. Tiene luces de emergencia			
8. Los siguientes controles de seguridad son para la prevención de fuego:			
a. Inspección realizada por el Departamento de Bomberos al Edificio.			
b. Seguros de protección de activos del Banco en el evento de un fuego.			
c. Adiestramiento del personal de la División en combatir fuego, uso de extintores, procedimientos de emergencia, fuego, agua e incidentes de alarmas.			
d. El personal de la División conoce la localización de alarmas de fuego, extintores de fuego, interruptores eléctricos auxiliares y regulares, suministro de agua, sistema de aire acondicionado y cualquier otro aditamento de			



Procedimiento Núm.:
BDE-005-SI-Proc.02

Deroga a:
Manual de Seguridad
27 de junio de 2001

Fecha de aprobación:
9 de septiembre de 2008

emergencia.			
e. Llevan a cabo prácticas de una situación de emergencia de fuego, por lo menos una vez al año como preparación a una emergencia real.			
f. Existe un Plan de Contingencia para el plan de recobro en caso de un desastre por fuego.			
9. Las prácticas de limpieza y reglas de trabajo son seguidos por el personal del Centro de Cómputos:			
a. No está permitido fumar, ni ingerir bebidas o alimentos.			
b. El área de trabajo está limpia, organizada y segura.			
c. Las reparaciones de equipo se completan con autorización del Gerente o en consulta con el personal de mantenimiento interno o externo.			
d. El personal no altera ningún programa sin autorización específica del Gerente u Oficial de Seguridad de Informática de la División.			
e. No se usan los sistemas de información para otras funciones que no sean las asignadas.			
10. Existe un Plan Operacional de Emergencias para continuar las operaciones del Banco en el evento de una emergencia, desastre o falla del <i>hardware/software</i> .			
11. En el último adiestramiento ofrecido al personal de la División de Sistemas de Información en procedimientos de			



Procedimiento Núm.:
BDE-005-SI-Proc.02

Deroga a:
Manual de Seguridad
27 de junio de 2001

Fecha de aprobación:
9 de septiembre de 2008

emergencia:			
a. Se ofreció el adiestramiento una vez al año.			
b. Se enseñó la localización de alarmas de fuego, extintores y controles de seguridad para combatir incendios.			
c. Se discutieron los procedimientos de apagar y encender equipos en el Centro de Cómputos.			
d. Se ilustró la salida de Emergencia.			
e. Se adiestró sobre la restauración luego de una emergencia.			
f. Se orientó sobre la notificación al Departamento de Bomberos, Gerente y personal Gerencial designado en el evento de una emergencia.			
12. Toda falla ocurrida en los sistemas de información del Centro de Cómputos es documentada en el Libro de Registro del Área.			
13. Los procedimientos descritos a continuación son seguidos por la División de Sistemas de Información.			
a. Selección de Personal a ser adiestrado			
b. Adiestramiento del Personal Nuevo			
c. Adiestramiento del Personal Regular			
d. Evaluaciones de Desempeño			
e. Disciplina y procedimientos de terminación			
f. Contratación de Ayuda			



**BANCO DE DESARROLLO ECONOMICO
PARA PUERTO RICO**

Estado Libre Asociado de Puerto Rico

**DIVISIÓN DE SISTEMAS DE
INFORMACIÓN**

MANUAL DE SEGURIDAD

**Procedimiento Núm.:
BDE-005-SI-Proc.02**

**Deroga a:
Manual de Seguridad
27 de junio de 2001**

**Fecha de aprobación:
9 de septiembre de 2008**

Externa			
14. Se cumplen las Leyes de Protección de la Intimidad Personal descritas a continuación:			
a. Se cumplen los derechos de propiedad, autor y patentes de equipo <i>hardware</i> y programas <i>software</i> .			
b. Accede los recursos de computadoras con autorización de acceso solamente.			
c. Información de clientes del Banco o personal en papel impreso es guardada en archivos con llaves, o es destruida en cortador de papel (<i>shredder</i>) antes de ser descartada a la basura.			
d. No existen registros de información del personal o clientes cuya existencia sea secreta.			
e. No se usa la información personal para otros propósitos que no sea para la cual fue autorizada por las personas.			
f. Errores de sistema o de calidad son documentados en Notificaciones de Eventos con un Plan de Acción Correctiva a implementarse.			
g. Los cambios que impacten en la seguridad son documentados en procedimientos e incluidos en los manuales correspondientes y son aprobados por la Gerencia.			



Procedimiento Núm.:
BDE-005-SI-Proc.02

Deroga a:
Manual de Seguridad
27 de junio de 2001

Fecha de aprobación:
9 de septiembre de 2008

Subsistema II:

Controles de Seguridad

Fecha Auditoría: _____

Acceso

Auditor Interno: _____

Iniciales Auditor: _____

LISTA DE COTEJO

CONTROLES DE SEGURIDAD	CUMPLIMIENTO		OBSERVACIONES (Evidencia encontrada en relación con cumplimiento No Satisfactorio)
	Satisfactorio (√)	No Satisfactorio (√)	
La administración de contraseñas a los usuarios se lleva a cabo de la manera siguiente:			
a. Órdenes de servicio para solicitud de contraseñas con autorización del Supervisor inmediato del usuario.			
b. Se da acceso a la red y servidores basado en los niveles de acceso establecidos para el trabajo del usuario en el Banco y en horas laborables.			
c. La contraseña de acceso es entrada por el usuario en forma confidencial.			
d. Mensualmente o cada treinta (30) días se actualizan las contraseñas para todos los usuarios del Banco.			
e. Recursos Humanos envía la Hoja de Usuarios Terminados para revocar el acceso al sistema de información.			



Procedimiento Núm.:
BDE-005-SI-Proc.02

Deroga a:
Manual de Seguridad
27 de junio de 2001

Fecha de aprobación:
9 de septiembre de 2008

Subsistema III:

Controles de Seguridad

Fecha Auditoría: _____

Backups

Auditor Interno: _____

Iniciales Auditor: _____

LISTA DE COTEJO

CONTROLES DE SEGURIDAD	CUMPLIMIENTO		OBSERVACIONES (Evidencia encontrada en relación con cumplimiento No Satisfactorio)
	Satisfactorio (N)	No Satisfactorio (N)	
1. Se hacen las copias de seguridad legibles o <i>backups</i> en las frecuencias establecidas:			
a. Diario			
b. Semanal			
c. Mensual			
d. Anual			
2. Se guardan originales y copias de <i>backup</i> en:			
a. Bóveda Interna del Centro de Cómputos en la caja de seguridad <i>Mossler</i>			
b. Bóveda Externa (en <i>International Safe Deposit</i>)			
3. Se documenta y actualiza en forma diaria el inventario perpetuo de cintas y cartuchos de <i>backup</i> .			
4. Se guardan copias adicionales o de <i>backup</i> de <i>software</i> nuevo con seguro (<i>write protected</i>).			
5. Se manejan correctamente los discos para asegurar la disponibilidad de los datos y reducir errores de lectura y			



Procedimiento Núm.:

BDE-005-SI-Proc.02

Deroga a:

**Manual de Seguridad
27 de junio de 2001**

Fecha de aprobación:

9 de septiembre de 2008

escritura. Esto incluye:			
a. Almacenamiento en envases adecuados cuando no estén instalados en los servidores y unidades de <i>backup</i> .			
b. Los envases con discos son archivados o guardados en un lugar seguro cuando no están en uso.			
c. Los empaques de los <i>backups</i> se mantienen tapados o cerrados, excepto cuando los discos son cargados o descargados.			
d. El contenido de los <i>backups</i> está identificado.			
6. Se manejan correctamente los cartuchos. Esto incluye:			
a. Manejar los cartuchos con las manos limpias.			
b. Cuando no están en uso, se mantienen en sus envases y lugar seguro.			
c. Se les coloca seguro de protección para evitar que sean borrados.			
d. Las puertas de acceso a los cartuchos se mantienen cerradas cuando no tienen cartuchos instalados.			



**Procedimiento Núm.:
BDE-005-SI-Proc.02**

**Deroga a:
Manual de Seguridad
27 de junio de 2001**

**Fecha de aprobación:
9 de septiembre de 2008**

Subsistema IV:

Controles de Seguridad

Fecha Auditoría: _____

Virus y Piratas

Auditor Interno: _____

Iniciales Auditor: _____

LISTA DE COTEJO

CONTROLES DE SEGURIDAD	CUMPLIMIENTO		OBSERVACIONES (Evidencia encontrada en relación con cumplimiento No Satisfactorio)
	Satisfactorio (N)	No Satisfactorio (N)	
1. Existe un <i>software</i> Antivirus para detectar y eliminar virus del sistema.			
2. Existen controles de seguridad de acceso para evitar penetración de acceso a la red por personal no autorizado, personas ajenas a la institución con propósito criminal (<i>hackers</i>).			
3. Todos los discos, terminales y programas son cotejados y mantenidos en forma mensual para presencia de virus y se verifica que tengan corrida antivirus.			
4. Cada computadora tiene instalado un programa para detectar virus.			
5. Enlace por módem y control de acceso seguro a la red.			
6. Se guarda una copia limpia del sistema operativo con seguro de protección que impida seguir grabando en ellos.			
7. Los usuarios no introducen al Banco <i>diskettes</i> , programas o terminales del exterior, sin la			



**BANCO DE DESARROLLO ECONOMICO
PARA PUERTO RICO**

Estado Libre Asociado de Puerto Rico

**DIVISIÓN DE SISTEMAS DE
INFORMACIÓN**

MANUAL DE SEGURIDAD

Procedimiento Núm.:

BDE-005-SI-Proc.02

Deroga a:

**Manual de Seguridad
27 de junio de 2001**

Fecha de aprobación:

9 de septiembre de 2008

autorización del Gerente de Sistemas de Información y verificación correspondiente de virus.			
8. Para evitar contaminación de virus, el Banco provee todo el equipo <i>hardware</i> , programas y discos a los usuarios del Banco.			
9. Uso de programas de llamada revertida (<i>call back</i>) en la red a través de lista de usuarios por número de módem.			
10. Se documentan infecciones virales, etapas y procedimientos de limpieza llevados a cabo en notificaciones de eventos.			



Procedimiento Núm.:
BDE-005-SI-Proc.02

Deroga a:
Manual de Seguridad
27 de junio de 2001

Fecha de aprobación:
9 de septiembre de 2008

Subsistema V:

Controles de Seguridad

Fecha Auditoría: _____

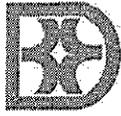
Red de Información

Auditor Interno: _____

Iniciales Auditor: _____

LISTA DE COTEJO

CONTROLES DE SEGURIDAD	CUMPLIMIENTO		OBSERVACIONES (Evidencia encontrada en relación con cumplimiento No Satisfactorio)
	Satisfactorio (√)	No Satisfactorio (√)	
1. La Red de Información es estándar Ethernet (IEEE 802.3)			
2. Red de topología bus o árbol con sistema de control de acceso al medio CSMA/CD.			
3. La comunicación en la red está controlada por el uso de protocolos y direcciones.			
4. Dispositivos de conexión e interconexión controlan la entrada, acceso y conexión de cada computador a la Red. Estos incluyen:			
a. Cables coaxiales			
b. Puerto o conector			
c. Repetidores			
d. Repetidores Multipuertos (HUBS)			
e. Unidades de Acceso de Multiestación (MAU)			
f. Concentradores Multimédios			
g. <i>Bridges</i>			
h. <i>Routers</i>			
i. <i>Gateways</i>			
5. Servidores de la Red que proveen			



Procedimiento Núm.:

BDE-005-SI-Proc.02

Deroga a:

**Manual de Seguridad
27 de junio de 2001**

Fecha de aprobación:

9 de septiembre de 2008

servicios de almacenamiento.			
6. Impresora Seros está conectada directamente a la Red.			
7. El Correo Electrónico es uno de los servicios a la Red compuesto por:			
a. Central de correos			
b. Buzones de los usuarios			
c. Dirección de correo			
d. Cliente de correo			
e. Copias múltiples de mensajes			
f. Copia pública o secreta de mensajes			
g. Acuse de recibo			
h. Reenvío			
i. Mensaje			
j. Teléfono o charla			
k. Fax de la Red			
8. Conexión remota y proceso distribuido a través de:			
a. Emulación de Terminal			
b. Sesión			
c. Terminales X-Windows			
d. Control Remoto			
e. Servidores de acceso remoto			
f. Acceso remoto			
g. Cliente acceso remoto			
h. Proceso distribuido			
i. Sistema Operativo Windows 2000			
9. Los controles operacionales			
a. Activar/desactivar servidores, programas y módulos, equipos e impresora.			
b. Backup			
c. Procedimientos rutinarios y no rutinarios, para corregir fallas o completar órdenes de servicio.			
10. Existen diagramas de localización			



Procedimiento Núm.:
BDE-005-SI-Proc.02

Deroga a:
Manual de Seguridad
27 de junio de 2001

Fecha de aprobación:
9 de septiembre de 2008

de cada computadora, servidor, cables y componentes de la Red.			
11. Acceso lógico a las comunicaciones está controlado por:			
a. Acceso autorizado a otras Redes			
b. Personal interno autorizado solamente.			
c. Controlado por nodo.			
d. Controlado al horario de trabajo			
e. Usuarios externos autorizados			
f. Uso de contraseñas para paquetes de comunicaciones.			
12. Administración de la Base de Datos en la Red, incluye:			
a. Uso y control de datos			
b. Acceso restringido a las tablas de relación (no son públicas)			
c. Capacitación del personal en programas y tablas de relación			
d. Control de herramientas de desarrollo (ejemplo: SQL Windows, Visual Basic).			
13. La conexión de la Red al <i>Mainframe</i> es conocida por el personal, se le da mantenimiento y tiene acceso controlado al <i>Mainframe</i> .			
14. Los controles de seguridad de los archivos de datos requieren mantenimiento y son tolerantes a fallas o redundancia como:			
a. Doble escritura en discos (<i>Disk Mirroring</i>)			
b. Controlador de disco dual (<i>RAID Technology</i>)			
c. Suministro de energía redundante			
d. Toda falla de redundancia			



**BANCO DE DESARROLLO ECONOMICO
PARA PUERTO RICO**

Estado Libre Asociado de Puerto Rico

**DIVISIÓN DE SISTEMAS DE
INFORMACIÓN**

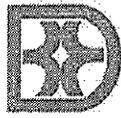
MANUAL DE SEGURIDAD

Procedimiento Núm.:
BDE-005-SI-Proc.02

Deroga a:
Manual de Seguridad
27 de junio de 2001

Fecha de aprobación:
9 de septiembre de 2008

15. Se llevan a cabo los procedimientos de <i>backup</i> de los archivos de datos en Red a las frecuencias establecidas. Se guardan copias de seguridad de <i>backup</i> en Bóveda Interna o Externa.			
16. Existe un Plan de Contingencia para la restauración de la Red de Información luego de un desastre o emergencia.			



Procedimiento Núm.:
BDE-005-SI-Proc.02

Deroga a:
Manual de Seguridad
27 de junio de 2001

Fecha de aprobación:
9 de septiembre de 2008

Subsistema VI:

Controles de Seguridad

Fecha Auditoría: _____

Software

Auditor Interno: _____

Iniciales Auditor: _____

LISTA DE COTEJO

CONTROLES DE SEGURIDAD	CUMPLIMIENTO		OBSERVACIONES (Evidencia encontrada en relación con cumplimiento No Satisfactorio)
	Satisfactorio (v)	No Satisfactorio (v)	
1. Se cumplen con las leyes y prácticas sociales que protegen los derechos de propiedad intelectual de <i>software</i> .			
a. Derechos de Autor (<i>Copyright</i>)			
b. Patentes			
2. La División de Sistemas de Información utiliza los programas <i>software</i> :			
a. De acuerdo al Contrato de Licencia de Usuario			
b. No se duplica <i>software</i> excepto para <i>backup</i> o archivo.			
c. Se provee <i>software</i> legítimo a todos los usuarios del Banco que están autorizados a usarlo.			
d. No se permite el uso de copias de <i>software</i> en el Banco.			
e. Todo <i>software</i> es comprado e instalado en las computadoras siguiendo los procedimientos establecidos de acuerdo a los Contratos de Licencias de los mismos.			
3. Las Licencias de Usuario de			



Procedimiento Núm.:
BDE-005-SI-Proc.02

Deroga a:
Manual de Seguridad
27 de junio de 2001

Fecha de aprobación:
9 de septiembre de 2008

<i>software</i> son un permiso legal para usar el programa y establece restricciones en cuanto a:			
a. Número de personas			
b. Número de máquinas			
c. El Supervisor de Desarrollo de Aplicaciones o persona designado, se asegura que si aumenta el número de máquinas o usuarios del <i>software</i> , se notifique al proveedor y se actualice la Licencia de Usuario del mismo.			
4. Se mantiene y solicita al proveedor o autor del <i>software</i>			
a. Código fuente, documentación adecuada o programa de formación del <i>software</i>			
b. Compatibilidad con los programas			
c. Asistencia postventa			
d. Licencia de Uso			
e. Proveedor debe mantener al Banco al corriente de las innovaciones técnicas para actualizar <i>software</i> o instalación de sistemas de seguridad para la protección de la Base de Datos.			
5. Los controles de programación por la División de Sistemas de Información incluyen los siguientes controles de seguridad:			
a. Todos los programas desarrollados por el personal de desarrollo de aplicaciones son propiedad del Banco.			
b. No se escribirán programas para uso propio en la			



Procedimiento Núm.:
BDE-005-SI-Proc.02

Deroga a:
Manual de Seguridad
27 de junio de 2001

Fecha de aprobación:
9 de septiembre de 2008

institución sin autorización.			
c. Solamente se usarán procedimientos de programación documentados y aprobados.			
d. Se revisarán las especificaciones del sistema y los programas previos a su instalación.			
e. Se usarán técnicas estándares de codificación.			
f. El código fuente incluye el nombre del programador, nombre del programa, fecha y otra información pertinente requerida por el Supervisor de Desarrolladores de Aplicaciones o persona designada.			
g. Se verifica la lógica del programa y se construyen árboles de decisión para los datos a probar para todas las condiciones normales y excepciones en el programa.			
h. Se hacen pruebas a los programas codificados para detectar errores de sintaxis, lógicos y de comunicación.			
i. Se documentan los programas para definir la manera en que el programa será corrido, controles requeridos y para proveer información a los usuarios que lo operan.			
j. Se harán comentarios o notas para explicar técnicas matemáticas o de programación, en el punto en el programa donde se vayan a utilizar.			



Procedimiento Núm.:

BDE-005-SI-Proc.02

Deroga a:

**Manual de Seguridad
27 de junio de 2001**

Fecha de aprobación:

9 de septiembre de 2008

6. La Instalación y Programas de Aplicación, incluye los siguientes controles de seguridad:			
a. Instalación de programas prototipos para <i>software</i> comprado, correr pruebas y cuando aplique, solicitar modificaciones previo a la implementación.			
b. Para transferir un programa desarrollado internamente a ambiente de producción, se requiere una revisión y aprobación para uso operacional. También aplica a programas comprados.			
c. Se revisarán las pruebas a realizarse a los programas para asegurar que se obtuvieron los resultados correctos, previo a su implementación.			
d. Se verificará que la documentación del programa interno o externo cumple con las especificaciones establecidas.			



Procedimiento Núm.:
BDE-005-SI-Proc.02

Deroga a:
Manual de Seguridad
27 de junio de 2001

Fecha de aprobación:
9 de septiembre de 2008

Subsistema VIII:

**Mantenimiento de
Seguridad**

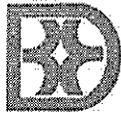
Fecha Auditoría: _____

Auditor Interno: _____

Iniciales Auditor: _____

LISTA DE COTEJO

CONTROLES DE SEGURIDAD	CUMPLIMIENTO		OBSERVACIONES (Evidencia encontrada en relación con cumplimiento No Satisfactorio)
	Satisfactorio (√)	No Satisfactorio (√)	
1. El Oficial de Seguridad de Informática o persona designada, genera, revisa o elimina los procedimientos de seguridad incluidos en el Manual de Seguridad, cuando es necesario, para mantener actualizados los mismos.			
2. Cada seis (6) meses se entrega el formulario de Revisión de los accesos al Sistema Financiero y luego la entregan al Oficial de Seguridad para realizar cualquier cambio en los accesos otorgados.			
3. Se documenta el Formulario de Notificación de Eventos para reportar fallas en la seguridad y establecer acciones correctivas para evitar recurrencia.			
4. Se auditaron todos los formularios requeridos en este Manual de Seguridad para asegurar:			
a. Están siendo documentados correctamente, en todos los espacios provistos y conocen el lugar donde están siendo			



Procedimiento Núm.:

BDE-005-SI-Proc.02

Deroga a:

**Manual de Seguridad
27 de junio de 2001**

Fecha de aprobación:

9 de septiembre de 2008

archivados.			
b. El Oficial de Seguridad de Informática revisó aquellos formularios que se determinen necesarios para fomentar el cumplimiento de los controles de seguridad.			
5. Se auditará el mantenimiento rutinario de seguridad en los siguientes procedimientos:			
a. Agregar y borrar empleados o clientes en el acceso.			
b. Auditar procedimientos <i>backup</i> , Bóveda Interna/Externa e inventario perpetuo.			
c. Corridas <i>Audits</i> y <i>Logs</i> del Sistema.			
d. Monitoreo de transacciones rechazadas a través de informes del sistema.			
e. Prevención de infección de virus o acceso no autorizado de piratas.			
f. Cambiar contraseñas cada treinta (30) días y en el sistema financiero cada sesenta (60) días.			
g. Acceso limitado a horas laboiables.			
h. Mantener Licencias de <i>software</i> .			
i. Instalación, prueba y mantenimiento de programas <i>software</i> .			
j. Controles de seguridad de <i>software</i> y de programación .			