INFORME DE AUDITORÍA TI-17-09

16 de marzo de 2017

Banco de Desarrollo Económico para Puerto Rico

División de Sistemas de Información

(Unidad 5193 - Auditoría 14025)

Período auditado: 16 de septiembre de 2015 al 4 de marzo de 2016

CONTENIDO

Página

ALCANCE Y METODOLOGÍA **2**

CONTENIDO DEL INFORME **2**

INFORMACIÓN SOBRE LA UNIDAD AUDITADA **3**

COMUNICACIÓN CON LA GERENCIA **7**

OPINIÓN Y HALLAZGOS **8**

1 - Deficiencias relacionadas con el análisis de riesgos de los sistemas de información computadorizados 8

2 - Falta de un plan de continuidad de negocios y de un centro alterno para la recuperación de las operaciones computadorizadas, y deficiencias del Plan de Contingencia de Sistemas de Información 11

3 - Falta de segregación de las funciones realizadas por un desarrollador de aplicaciones 15

4 - Falta de actualización de los sistema operativos utilizados en los servidores del BDEPR 17

5 - Falta de documentación de las aplicaciones del BDEPR y documentación incompleta de los cambios realizados a las mismas 18

6 - Falta de organización de los cables que se conectaban a los equipos de comunicación del BDEPR 22

7 - Incumplimiento de las recomendaciones incluidas en los informes auditorías externas 24

RECOMENDACIONES **26**

AGRADECIMIENTO **29**

ANEJO 1 - CABLES QUE NO SE MANTENÍAN ORGANIZADOS EN EL CUARTO DE SERVIDORES Y EN EL CUARTO DE DISTRIBUCIÓN DE CABLEADO DEL TERCER PISO **30**

ANEJO 2 - MIEMBROS PRINCIPALES DE LA JUNTA DE DIRECTORES DURANTE EL PERÍODO AUDITADO **32**

ANEJO 3 - FUNCIONARIOS PRINCIPALES DE LA ENTIDAD DURANTE EL PERÍODO AUDITADO **33**

Estado Libre Asociado de Puerto Rico
OFICINA DEL CONTRALOR
San Juan, Puerto Rico

16 de marzo de 2017

Al Gobernador, y a los presidentes del Senado de
Puerto Rico y de la Cámara de Representantes

Realizamos una auditoría de las operaciones de la División de Sistemas de Información (DSI) del Banco de Desarrollo Económico para Puerto Rico (BDEPR) para determinar si las mismas se efectuaron de acuerdo con las normas generalmente aceptadas en este campo, y si el sistema de control interno establecido para el procesamiento de las transacciones era adecuado. Hicimos la misma a base de la facultad que se nos confiere en el Artículo III, Sección 22 de la Constitución del Estado Libre Asociado de Puerto Rico y, en la *Ley Núm. 9 del 24 de julio de 1952*, según enmendada.

ALCANCE Y METODOLOGÍA

La auditoría cubrió del 16 de septiembre de 2015 al 4 de marzo de 2016. El examen lo efectuamos de acuerdo con las normas de auditoría del Contralor de Puerto Rico en lo que concierne a los sistemas de información computadorizados. Realizamos las pruebas que consideramos necesarias, a base de muestras y de acuerdo con las circunstancias, tales como: entrevistas; inspecciones físicas; exámenes y análisis de informes y de documentos generados por la unidad auditada o suministrados por fuentes externas; pruebas y análisis de procedimientos de control interno y de otros procesos; y confirmaciones de información pertinente.

CONTENIDO DEL INFORME

Este *Informe* contiene siete hallazgos sobre el resultado del examen que realizamos de los controles internos establecidos para la administración del programa de seguridad, el acceso físico, la continuidad del servicio, las aplicaciones de sistemas, la segregación de deberes, la documentación de las aplicaciones y los programas desarrollados, y el cumplimiento de las recomendaciones para corregir deficiencias en los controles y el

funcionamiento de los sistemas de información computadorizados, establecidas en los informes de auditorías externas realizadas al BDEPR. El mismo está disponible en nuestra página en Internet: www.ocpr.gov.pr.

INFORMACIÓN SOBRE LA UNIDAD AUDITADA

El BDEPR se creó en virtud de la *Ley Núm. 22 del 24 de julio de 1985, Ley del Banco de Desarrollo Económico para Puerto Rico*, según enmendada. El propósito del BDEPR es brindarle, al pequeño y al mediano empresario puertorriqueño, una fuente de ingreso comprometida con el desarrollo económico del País y las oportunidades de empleo.

Los poderes del BDEPR son ejercidos por una junta de directores, compuesta por 9 miembros: el Presidente del Banco Gubernamental de Fomento para Puerto Rico (BGF), quien actúa como Presidente, el Secretario de Desarrollo Económico y Comercio, el Director Ejecutivo de la Compañía de Turismo de Puerto Rico, el Director Ejecutivo de la Compañía de Fomento Industrial de Puerto Rico, y el Secretario de Agricultura. Los restantes 4 miembros son nombrados por el Gobernador de Puerto Rico con el consejo y consentimiento del Senado. Estos 4 miembros representan al sector privado, y 1 de estos representa al sector agrícola, 1 al sector comercial, y 1 al sector manufacturero. La Junta de Directores nombra al Presidente del BDEPR, quien es el principal ejecutivo del mismo.

Mediante la *Ley 67-1994* se enmendó la *Ley Núm. 22* y se adscribió el BDEPR al BGF. Esto, con el propósito de coordinar la política pública, programática y operacional, y atender las necesidades de financiamiento a pequeños y medianos comerciantes que el BGF no ofrecía.

Las actividades operacionales del BDEPR consisten en otorgar financiamiento a cualquier persona o empresa privada, cuya actividad comercial sea clasificada como pequeña o mediana, que se dedique a la manufactura, el comercio, la agricultura o el turismo, y a otras empresas de servicios.

La estructura organizacional, a través de la cual el BDEPR realiza sus funciones, está compuesta por la Oficina del Presidente, que cuenta con los departamentos de Asuntos Legales, Capital Humano, Finanzas y

Operaciones, Administración de Crédito, Crédito, Negocio y Banca Comercial y Riesgo de Crédito. Estos departamentos se componen de divisiones y son dirigidos por 7 vicepresidentes ejecutivos. Además, el BDEPR cuenta con 4 oficinas de servicio ubicadas en las oficinas del Departamento de Agricultura y las oficinas de la Compañía de Comercio y Exportación de Puerto Rico en Ponce y Mayagüez. El BDEPR también cuenta con 1 Oficina de Auditoría Interna que le responde a la Junta de Directores y al Presidente.

A la fecha de nuestra auditoría, la DSI era dirigida por un gerente de sistemas de información, supervisado por el Vicepresidente Ejecutivo del Departamento de Capital Humano[1]. Además, contaba con 1 supervisor de desarrollo de aplicaciones, 2 desarrolladores de aplicaciones y 2 técnicos de computadoras, y tenía vacantes los puestos de supervisor de apoyo técnico y de oficial de sistemas de telecomunicaciones.

El BDEPR mantiene sus operaciones en forma computadorizada mediante 43 programas y aplicaciones en producción, entre los que se encuentran los siguientes:

- ACH - Programa desarrollado por el BDEPR que genera un archivo en formato requerido por el *Automated Clearing House* (ACH)[2] para debitar las cuentas de los clientes acogidos al pago directo, hacer pagos electrónicos a los proveedores y emitir a los empleados los rembolsos de gastos.
- ACH-TAO - Programa desarrollado por el BDEPR que genera un archivo en el formato utilizado por el ACH para debitar las cuentas de los clientes que realizan los pagos electrónicos mediante la aplicación *Tu Aliado Online* (TAO).
- *Check plus* - Programa adquirido que genera los cheques con las firmas impresas.

[1] La supervisión se limitaba a la aprobación de los proyectos de sistemas de información.

[2] Red electrónica para las transacciones financieras en los Estados Unidos. Mediante esta red se procesan grandes volúmenes de transacciones de crédito y débito en lotes.

- Originación Centro de Banca Empresarial (CBE) - Aplicación desarrollada por el BDEPR que mantiene un registro de las orientaciones ofrecidas por el Área de Servicio al Cliente, y controla el procesamiento de las solicitudes de financiamiento para asegurarse de que estas incluyan todos los documentos requeridos.
- Originación Crédito - Aplicación desarrollada por el BDEPR que mantiene el flujo de la solicitud de financiamiento desde su análisis hasta su denegación o aprobación.
- Originación Informes - Programa desarrollado por el BDEPR que provee informes de los distintos procesos y etapas de la solicitud de financiamiento.
- *Premier* - Aplicación adquirida que se utiliza para crear, modificar o eliminar la información del sistema financiero del BDEPR.
- *Prime* - Aplicación adquirida que crea una base de datos *MS SQL* con la información del sistema financiero para ser utilizada en otros programas del BDEPR.
- Solicitudes Web - Aplicación desarrollada por el BDEPR dentro de su página en Internet, que permite completar la solicitud de financiamiento, enviar los documentos solicitados al cliente y revisar el progreso de la solicitud.
- TAO - Aplicación desarrollada por el BDEPR, dentro de su página en Internet, que permite al cliente registrarse para ver la información de sus préstamos y realizar los pagos electrónicos.

Para procesar las aplicaciones y los programas, el BDEPR cuenta con 2 computadoras (*mainframes*)[3], 25 servidores físicos[4] y 5 servidores virtuales[5]. Además, tiene una red local y una red virtual privada (*VPN*, por

[3] Un *mainframe* es una computadora grande, potente y costosa que permite el procesamiento de una gran cantidad de datos.

[4] Un servidor físico es un ordenador destinado a almacenar, gestionar, procesar información y proveerla a otras computadoras en la red.

[5] Un servidor virtual es una partición dentro de un servidor que habilita varias máquinas independientes, a las que se le asigna un límite de espacio en disco para el uso de la Unidad Central de Procesamiento (CPU) y de memoria RAM, entre otros.

sus siglas en inglés)[6] que permiten la comunicación entre los equipos ubicados en el edificio principal y las 4 oficinas de servicios ubicadas en Ponce y Mayagüez. Al 4 de febrero de 2016, la red local tenía 142 computadoras instaladas.

Para mantener la seguridad de los sistemas de información computadorizados, el BDEPR implantó el uso de equipos y aplicaciones de *firewall*[7], sistemas para filtrar los accesos a la Internet y a los correos electrónicos (*Anti Spam*), sistemas para evitar los ataques de virus y otros programas maliciosos (*Antivirus* y *Spywares*), y el uso de protocolos de la red[8] que permitían la transmisión segura de los datos.

Las operaciones de los sistemas de información computadorizados del BDEPR se rigen por la reglamentación interna aprobada, que considera la *Ley 151-2004, Ley de Gobierno Electrónico*, y las normas generalmente aceptadas en la industria bancaria[9]. Además, el BDEPR utiliza como guía las cartas circulares emitidas por la Oficina de Gerencia y Presupuesto (OGP).

Los recursos para los gastos de funcionamiento del BDEPR provienen de ingresos propios, principalmente de intereses que se generan mediante la actividad de las inversiones y los préstamos que otorga. Los presupuestos operacionales, aprobados para los años fiscales del 2013-14 al 2015-16, ascendieron a $11,189,206, $11,247,965 y $11,425,000, respectivamente. El presupuesto de la DSI estaba integrado al presupuesto operacional del BDEPR.

---

[6] Una red virtual privada (*Virtual Private Network*) es una conexión virtual punto a punto mediante uso de conexiones dedicadas, cifrado o la combinación de ambos métodos que permite una extensión segura de la red local (*LAN*) sobre una red pública o no contralada como el Internet. Esta conexión es una red de área amplia (*WAN*) entre los sitios pero al usuario le parece como si fuera un enlace privado.

[7] Aplicación, equipo o conjunto de ambos que protege los recursos de la red de accesos no autorizados.

[8] Los protocolos de la red son reglas o estándares implementados por equipos o programas que definen la sintaxis, la semántica y la sincronización de la comunicación, y los métodos de recuperación en caso de errores.

[9] La industria bancaria está regulada, entre otros, por el *Gramm Leach Bliley Act de 1999* y el Título 12 del *Code of Federal Regulation.*

Los **anejos 2 y 3** contienen una relación de los miembros de Junta del BDEPR y de los funcionarios principales que actuaron durante el período auditado.

El BDEPR cuenta con una página en Internet, a la cual se puede acceder mediante la siguiente dirección: www.bde.pr.gov. Esta página provee información acerca de la entidad y de los servicios que presta.

COMUNICACIÓN CON LA GERENCIA

Las situaciones comentadas en los **hallazgos** de este *Informe* y otras situaciones determinadas durante la auditoría, relacionadas con los controles internos establecidos para la entrada de datos en la aplicación Solicitudes Web, fueron remitidas al Sr. Joey Cancel Planas, entonces Presidente del BDEPR, mediante carta de nuestros auditores del 19 de mayo de 2016. En la referida carta se incluyeron anejos con detalles sobre las situaciones comentadas.

Mediante carta del 10 de junio, el entonces Presidente remitió sus comentarios, los cuales fueron considerados en la redacción del borrador de este *Informe*.

El borrador de los **hallazgos** de este *Informe* se remitió para comentarios, por carta del 1 de noviembre de 2016, al entonces Presidente del BDEPR. En este se indicaron datos específicos, tales como: información del sistema operativo utilizado y nombres de servidores, los cuales, por seguridad, no se incluyen en este *Informe*. Con el mismo propósito, remitimos el borrador del **Hallazgo 7** al Lcdo. Alberto Bacó Bagué, entonces Presidente de la Junta de Directores; y a la Lcda. Melba Acosta Febo, ex-Presidenta de la Junta de Directores; mediante cartas del 1 de noviembre de 2016.

El 9 de noviembre de 2016 el entonces Presidente solicitó una prórroga para remitir sus comentarios, la cual le concedimos hasta el 1 de diciembre. El 29 de noviembre solicitó una prórroga adicional, la cual concedimos hasta el 16 de diciembre. El entonces Presidente contestó el borrador mediante carta del 15 de diciembre. En los **hallazgos** se incluyeron algunos de sus comentarios.

El 22 de noviembre de 2016 se enviaron cartas de seguimiento al licenciado Bacó Bagué y a la licenciada Acosta Febo, y se les concedió hasta el 30 de noviembre para remitir sus comentarios; no obstante, no contestaron.

OPINIÓN Y HALLAZGOS

Opinión favorable con excepciones

Las pruebas efectuadas y la evidencia en nuestro poder demostraron que las operaciones de la DSI del BDEPR, en lo que concierne a los controles internos establecidos para la administración del programa de seguridad, el acceso lógico y físico, la continuidad del servicio, las aplicaciones de sistemas, la segregación de deberes, la documentación de las aplicaciones y los programas desarrollados, el control de acceso a la aplicación Solicitudes Web y el cumplimiento de las recomendaciones para corregir deficiencias en los controles y el funcionamiento de los sistemas de información computadorizados, establecidas en los informes de auditorías externas realizadas al BDEPR, se realizaron sustancialmente conforme a las normas generalmente aceptadas en este campo, excepto por los **hallazgos del 1 al 7** que se comentan a continuación.

Hallazgo 1 - Deficiencias relacionadas con el análisis de riesgos de los sistemas de información computadorizados

Situaciones

a. El análisis de riesgos es un proceso a través del cual se identifican los activos de los sistemas de información computadorizados existentes en la entidad, sus vulnerabilidades, y las amenazas a las que se encuentran expuestos, así como la probabilidad de ocurrencia y el impacto de las mismas. Esto, con el fin de determinar las medidas de seguridad y los controles adecuados a ser implementados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo, y proteger dichos activos, de manera que no se afecten adversamente las operaciones de la entidad. Mediante este proceso se asegura que las medidas de seguridad y los controles a ser implementados sean costo-efectivos, pertinentes a las operaciones de la entidad y que respondan a las posibles amenazas identificadas.

El 16 de septiembre de 2015 se nos suministró el *Avalúo de Riesgos de los Controles Internos* (*Avalúo de Riesgos*) que fue preparado por el Gerente de Sistemas de Información. El *Avalúo de Riesgos* incluía una matriz que identificaba los factores de riesgos para 10 procesos realizados en la DSI. El examen realizado al *Avaluó de Riesgos* reveló que este:

1) No incluía un inventario de todos los activos de sistemas de información que detallara los equipos, programas y datos que eran impactados por los procesos realizados en la DSI, y la valoración y clasificación de estos de acuerdo con la misión y los servicios del BDEPR.

2) No detallaba la clasificación de criticidad de los 10 procesos para los cuales se identificaron los factores de riesgos. Además, no consideraba los procesos realizados en la DSI para la remoción y disposición de programas y computadoras; la revisión de la red para identificar accesos indebidos y los errores relacionados con el funcionamiento de los servidores; la recuperación de incidentes de seguridad que afecten las operaciones de la DSI; el procesamiento de las transacciones mediante el *ACH* y la página en Internet; y la creación y modificación de las aplicaciones y los programas del BDEPR.

3) No incluía las posibles amenazas que tenían el potencial de impactar los procesos realizados en la DSI, y que podían afectar los archivos y las operaciones del BDEPR.

4) No incluía las vulnerabilidades que tenía cada proceso realizado en la DSI y los activos relacionados con estos.

Criterios

Las situaciones comentadas son contrarias a lo establecido en la parte C.3 del *Manual de Seguridad (BDE-005-SI-Proc.02)*, aprobado el 9 de septiembre de 2008 por la Presidenta del BDEPR. En este se indica que el Gerente de Sistemas de Información debe asegurarse de que se establezcan los procedimientos y controles de seguridad, necesarios para la operación de los sistemas de información computadorizados, y de

que estos garanticen la realización de las funciones del BDEPR, en conformidad con las prácticas de seguridad de aceptación general para los sistemas de información en la industria bancaria y el Gobierno. Esto se logra, en parte, mediante el establecimiento de un análisis de riesgos que permita implementar los controles de seguridad necesarios para proteger los activos de sistemas de información computadorizados que son críticos para las operaciones del BDEPR.

Las situaciones comentadas en el **apartado a.1), 3) y 4)** son contrarias a lo establecido en la *Política TIG-003, Seguridad de los Sistemas de Información*, de la *Carta Circular 77-05, Normas sobre la Adquisición e Implantación de los Sistemas, Equipos y Programas de Información Tecnológica para los Organismos Gubernamentales*, aprobada el 8 de diciembre de 2004 por la Directora de la OGP; y en la *Política TIG-015, Programa de Continuidad Gubernamental*, aprobada el 22 de septiembre de 2011 por el Director de la OGP[10].

Además, son contrarias a lo establecido en el Appendix D-2, *Interagency Guidelines Establishing Information Security Standards, Part III. B.* del *Membership of State Banking Institutions in the Federal Reserve System (Regulation H), 12 CFR, Chapter II, Part 208*. En este se indica:

> Each bank shall: 1. Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems. 2. Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information.3. Assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks.

Efecto

Las situaciones comentadas impiden al BDEPR estimar el impacto que los elementos de riesgos tendrían sobre las áreas y los sistemas críticos de este, y considerar cómo protegerlos para reducir los riesgos de daños materiales y la pérdida de información.

[10] La *Carta Circular 77-05* y la *Política TIG-015* fueron derogadas por la *Carta Circular 140-16, Normas Generales sobre la Implantación de Sistemas, Compra de Equipos y Programas y Uso de la Tecnología de Información para los Organismos Gubernamentales*, aprobada el 7 de noviembre de 2016 por el Director de la OGP. Esta contiene disposiciones similares a las de la *Carta Circular* y *Política* derogadas.

Causa

Las situaciones comentadas se debieron, en parte, a que el Gerente de Sistemas de Información no consideró las normas de seguridad generalmente aceptadas para los sistemas de información del Gobierno y la industria bancaria, para la preparación del análisis de riesgos.

Comentarios de la Gerencia

El entonces Presidente nos indicó en su carta, entre otras cosas, lo siguiente:

> […] a pesar de no necesariamente tener un Avalúo de Riesgos como se requiere en este informe, sí ponemos en práctica diariamente los controles de seguridad necesarios para salvaguardar la información bancaria de nuestros clientes y empleados. No obstante, comenzaremos tan pronto como en enero de 2017, un nuevo Avalúo de Riesgos que incluya todos los activos y programas del Banco, todo el inventario de nuestros activos de equipo y programas y todos los procesos contemplando sus vulnerabilidades, potenciales amenazas y su impacto. [*sic*]

Véanse las recomendaciones 1 y 4.a.

Hallazgo 2 - Falta de un plan de continuidad de negocios y de un centro alterno para la recuperación de las operaciones computadorizadas, y deficiencias del Plan de Contingencia de Sistemas de Información

Situaciones

a. Al 30 de septiembre de 2015, el BDEPR carecía de un plan de continuidad de negocios que incluyera los planes específicos, completos y actualizados de la DSI. Esto era necesario para lograr el pronto funcionamiento de los sistemas de información computadorizados y restaurar las operaciones del BDEPR, en caso de riesgos como: variaciones de voltaje, virus de computadoras, ataques maliciosos a la red, o desastres naturales, entre otros.

b. Al 29 de septiembre de 2015, el BDEPR no contaba con un centro alterno de sistemas de información para restaurar las aplicaciones Originación CBE, Originación Crédito, *Prime*, TAO y los programas ACH y *Check Plus*, los cuales eran esenciales para mantener sus

operaciones críticas. A la fecha de nuestro examen el BDEPR sólo mantenía un centro alterno para restaurar las operaciones de la aplicación *Premier*.

c. El BDEPR contaba con el *Plan de Contingencia de Sistemas de Información*, incluido en la *Sección XV* del *Manual de Procedimientos* (*BDE-005-SI-Proc.01*), aprobado el 30 de agosto de 2010 por la Presidenta del BDEPR. Este *Plan* se estableció con el objetivo de incluir los procedimientos a seguir por el grupo de trabajo de la DSI para la prevención y recuperación efectiva de los sistemas, y para minimizar el impacto que puedan sufrir las funciones críticas del BDEPR, luego de un desastre o situación de emergencia.

   El examen realizado el 7 de octubre de 2015 sobre el *Plan* reveló las siguientes deficiencias:

   1) El *Plan* no había sido revisado desde el 2010, por lo que no consideraba las aplicaciones y los programas desarrollados en la DSI luego de esa fecha, tales como: las aplicaciones TAO y Solicitudes Web, que eran esenciales para las operaciones principales del BDEPR.

   2) El *Plan* no incluía los siguientes requisitos necesarios para atender eventos o situaciones de emergencias:

      a) Los procedimientos a seguir cuando el cuarto de servidores de la DSI no puede recibir ni transmitir información a los usuarios ubicados en las oficinas de servicio en Ponce y Mayagüez

      b) El inventario actualizado de los equipos, los sistemas operativos y las aplicaciones

      c) El detalle de la configuración de los equipos críticos (equipos de comunicación y servidores) y del contenido de los respaldos, así como los nombres de las librerías y de los archivos

      d) El nombre de la compañía que ofrece los servicios de recuperación en un centro alterno para la aplicación

Premier, y la información sobre los acuerdos de servicio y la configuración de los sistemas, necesaria para efectuar la restauración de la aplicación

e) Una hoja de cotejo para verificar los daños ocasionados por la contingencia.

Criterios

Las situaciones comentadas son contrarias a lo establecido en la parte C.3 del *BDE-005-SI-Proc.02*.

La situación comentada en el **apartado a.** es contraria a lo establecido en la *Política TIG-003* de la *Carta Circular 77-05*.

Las mejores prácticas en el campo de la tecnología de información y la industria bancaria[11] utilizadas para garantizar la confiabilidad, integridad y disponibilidad de los sistemas de información computadorizados sugieren que, como parte integral del plan de continuidad de negocios, deben existir convenios con otras entidades donde se estipulen las necesidades y los servicios requeridos para afrontar una emergencia. Debe incluirse, además, una cláusula que especifique el lugar o los lugares donde podrían ser requeridos dichos servicios. Estos lugares, de acuerdo con la capacidad de la agencia, podrían ser los siguientes: **[Apartado b.]**

- Una entidad pública o privada de similar configuración y tamaño
- Una compañía dedicada a servicios de restauración
- Un centro alterno de la propia entidad.

Estas prácticas también sugieren que, como parte del plan de continuidad de negocios, se prepare un plan de contingencias. Este es una guía que garantiza la continuidad de las operaciones normales de los sistemas de información computadorizados cuando se presentan eventualidades inesperadas que afecten su funcionamiento. El mismo deberá incluir todos los procesos necesarios para recuperar cualquier segmento de la operación

[11] En la guía *Business Continuity Planning* emitida por el *Federal Financial Institutions Examination Council* (FFIEC) para asistir a los examinadores que evalúan las instituciones financieras, se establece que la junta de directores debe asegurarse de que se implemente un plan de continuidad de negocios que incluya la recuperación, la reanudación y el mantenimiento de todos los aspectos del negocio, sin limitarse a los componentes tecnológicos. El plan debe reflejar el ambiente operacional actual, incluir acuerdos formales para un centro alterno y ser probado con regularidad.

del centro de cómputos o, si fuera necesario, relocalizar las operaciones en el menor tiempo posible y de la forma más ordenada y confiable. **[Apartado c.]**

Efectos

Las situaciones comentadas en los **apartados a. y c.** podrían propiciar la improvisación y, que en casos de emergencia, se tomen medidas inapropiadas y sin orden alguno. Esto representa un alto riesgo de incurrir en gastos excesivos e innecesarios de recursos y de interrupciones prolongadas de los servicios ofrecidos a los usuarios de la BDEPR.

La situación comentada en el **apartado b.** podría afectar las operaciones del BDEPR y los servicios de la DSI, ya que no tendrían disponibles unas instalaciones para operar después de una emergencia o de un evento que afecte su funcionamiento. Esto podría atrasar o impedir el proceso de restauración de archivos y el pronto restablecimiento de las operaciones normales de la DSI.

Causas

La situación comentada en el **apartado a.** se atribuye a que el Presidente del BDEPR no había promulgado una directriz para la preparación de un plan de continuidad de negocios.

La situación comentada en el **apartado b.** se debe a que el Gerente de Sistemas de Información entendía que el BDEPR sólo necesitaba un centro alterno para la aplicación *Premier*, y no había considerado la importancia de otras aplicaciones para mantener la continuidad de las operaciones.

Las situaciones comentadas en el **apartado c.** se debe a que en la DSI no se había completado el proyecto para la virtualización de los servidores, y el Gerente de Sistemas de Información determinó que actualizaría el *Plan* una vez se completara el mismo y se estableciera la nueva configuración de los equipos.

Comentarios de la Gerencia

El entonces Presidente nos indicó en su carta, entre otras cosas, las medidas que están en proceso para corregir las situaciones comentadas en los **apartados a. y c.** del **Hallazgo**. Además, nos indicó lo siguiente:

> A pesar de tener un Centro Alterno con la Compañía […] para la recuperación de nuestro Sistema Financiero y de Préstamos

> (Premier), sí carecemos de un Centro alterno para la restauración de las otras aplicaciones que se le toman resguardo de la información y se almacenan en bóvedas externas. Se evaluará la alternativa de compartir el Centro de Cómputos con otras Agencias para la recuperación de las demás aplicaciones, utilizando la tecnología de virtualización o la contratación de una Compañía dedicada a servicios de restauración. [*sic*] **[Apartado b.]**

Véanse las recomendaciones 1 y 4 de la b. a la d.

Hallazgo 3 - Falta de segregación de las funciones realizadas por un desarrollador de aplicaciones

Situación

a. Al 26 de octubre de 2015, un desarrollador de aplicaciones de la DSI, como parte de las funciones de su puesto, era responsable de, entre otras cosas, desarrollar y dar mantenimiento a las aplicaciones y a la página en Internet, crear la documentación de la aplicación, adiestrar a los usuarios, y analizar el estudio de necesidades de los usuarios. Además, realizaba la tarea correspondiente al puesto de operador, de actualizar en el ambiente de producción los cambios realizados a las aplicaciones y los programas del BDEPR. Las funciones realizadas como desarrollador y operador resultan incompatibles y conflictivas al ser realizadas por una misma persona. Esta situación se agravaba al no existir un control alterno de supervisión por parte del Supervisor de Desarrollo de Aplicaciones.

Criterios

La situación comentada es contraria a lo establecido en la parte E.6 del *BDE-005-SI-Proc.02*. En este se establece que debe existir una segregación de funciones para evitar el riesgo de errores y la manipulación fraudulenta. Para esto, deben dividirse las responsabilidades asignadas al personal que realiza los procesos de entrada, procesamiento y salida de datos de los sistemas de información computadorizados, y deben segregarse las funciones realizadas por los desarrolladores, técnicos de apoyo y operadores. Además, es contraria a lo establecido en las partes de la A. a la C. del Capítulo VII, Copia de Programa a Ambiente de Producción, del *Manual de Desarrollo de Aplicaciones* (*BDE-005-SI-Proc.03*), aprobado el 3 de abril de 2009 por la Presidenta

del BDEPR. En este se establece que la transferencia de un programa desarrollado a estado operacional requiere la revisión de la documentación y un procedimiento de aprobación por parte del cliente y del Supervisor de Desarrollo de Aplicaciones. El Desarrollador de Aplicaciones verifica con el operador designado del centro de cómputos que el programa nuevo o revisado sea respaldado y documentado correctamente, luego el programa se compila para crear el programa ejecutable y se copia en el área de producción.

Efecto

La situación comentada podría propiciar que se realizaran cambios a la programación sin la autorización requerida.

Causas

La situación comentada se debió a que la DSI no contaba con un operador, debido a que la persona que ocupaba dicho puesto fue cesanteada como parte de la reducción de empleados que surgió con la implementación de la *Ley 7-2009, Ley Especial Declarando Estado de Emergencia Fiscal y Estableciendo Plan Integral de Estabilización Fiscal para Salvar el Crédito de Puerto Rico*, según enmendada. Además, el Gerente de Sistemas de Información no revisó el *BDE-005-SI-Proc.02* y el *BDE-005-SI-Proc.03* para actualizarlos conforme al personal disponible y los procesos realizados en la DSI.

Comentarios de la Gerencia

El entonces Presidente nos indicó en su carta, entre otras cosas, lo siguiente:

> Según lo establecido en los manuales de Sistemas de Información donde se menciona la segregación de funciones; actualmente, no está como indican los manuales y esto se debe a la disminución de personal en la División Sistemas de Información. Se solicitará el reclutamiento de personal adicional para realizar estas tareas, dentro de la realidad fiscal y presupuestaria del Banco y de las leyes y normativa aplicable al reclutamiento de personal. [*sic*]
>
> El Manual tendrá severos cambios dirigidos al personal que tenemos actualmente, e incluirá el sistema que actualmente se utiliza en la DSI para el "Log" de registro de informes y programas creados o modificados. [*sic*]

Véanse las recomendaciones 1, y 4.e. y f.

Hallazgo 4 - Falta de actualización de los sistema operativos utilizados en los servidores del BDEPR

Situación

a. El sistema operativo de un servidor es un programa que permite administrar la seguridad y los recursos en una red cliente servidor, incluidos las computadoras, los equipos periferales y las aplicaciones, entre otros.

   El examen realizado el 16 de octubre de 2015 sobre los sistemas operativos instalados en 25 servidores físicos del BDEPR reveló que en 8 servidores se utilizaba un sistema operativo que había sido descontinuado por el proveedor desde el 14 de julio de 2015. Este sistema no tenía disponible los servicios de apoyo técnico y las actualizaciones, necesarios para mejorar la seguridad y corregir errores en el funcionamiento. En estos servidores se mantenían las operaciones del servidor principal, las bases de datos de las aplicaciones de mayor relevancia para el BDEPR, y el servidor para la conexión VPN, entre otros.

Criterio

La situación comentada es contraria a lo establecido en la parte C.3. del *BDE-005-SI-Proc.02*.

Efectos

La situación comentada aumenta los riesgos de ataques maliciosos a los servidores a través de las vulnerabilidades del sistema operativo, lo que podría ocasionar la pérdida de información personal de los clientes del BDEPR. Además, priva al BDEPR de los servicios de apoyo técnico necesarios para garantizar la continuidad de las operaciones de estos servidores.

Causas

La situación comentada se debía a que la Junta de Directores del BDEPR no aprobó con prontitud los fondos necesarios para completar el proyecto para la virtualización de los servidores, que incluía el remplazo de los sistemas operativos obsoletos. Además, los servidores existentes no contaban con las especificaciones mínimas requeridas para la instalación de las versiones actualizadas del sistema operativo utilizado.

Comentarios de la Gerencia

El entonces Presidente nos indicó en su carta, entre otras cosas, lo siguiente:

> A la fecha de la intervención, no se había comenzado con los proyectos contemplados, no obstante, ya estamos encaminados a la actualización de estos sistemas operativos y con la virtualización de servidores. [*sic*]

Véanse las recomendaciones 1, 2 y 4.g.

Hallazgo 5 - Falta de documentación de las aplicaciones del BDEPR y documentación incompleta de los cambios realizados a las mismas

Situaciones

a. La DSI contaba con dos desarrolladores de aplicaciones que se encargaban del desarrollo, la documentación y el mantenimiento de las aplicaciones y los programas. Las directrices para documentar, verificar, validar, y probar los programas desarrollados estaban establecidas en el *BDE-005-SI-Proc.03*, y requerían que se preparara un expediente que incluyera, lo siguiente:

   - Las solicitudes de servicio con la descripción del proyecto, el propósito y los objetivos
   - La información general del proyecto que incluyera la propuesta, una descripción breve del mismo, los nombres de las personas que participaron, las funciones realizadas y el análisis costo-beneficio del proyecto
   - La página titular con el nombre del proyecto, el número de identificación, la fecha de efectividad y el nombre y título del desarrollador de aplicaciones que trabajó en el mismo
   - Los formularios para el control de cambios
   - Las especificaciones del sistema, los programas, los archivos y las bases de datos
   - La descripción de entrada con el nombre, la fecha, el estado de la entrada, los campos en los registros, el tipo y el largo, el número de registros por ciclo y la disposición de la entrada antes de ser recibida en el sistema

- La definición de salida con el nombre y número del informe, la localización y el largo de cada campo en el diseño del informe, el número de copias y la relación de los campos en el informe con la fuente de información de la descripción de entrada
- La documentación del programa con la identificación del programa con un número, el objetivo general o uso del programa con una breve narrativa del propósito del programa, los flujogramas del programa, las instrucciones operacionales, los requisitos de entrada y salida, el código fuente del programa y evidencia de las pruebas realizadas
- El procedimiento de respaldo y recuperación de las aplicaciones y los programas.

Al 13 de octubre de 2015, se habían desarrollado los programas ACH-TAO y Originación Informe, y las aplicaciones Originación CBE, Originación Crédito, TAO y Solicitudes Web. El examen realizado el 28 de octubre de 2015 sobre los expedientes que incluían la documentación de estos programas y aplicaciones reveló que carecían de las solicitudes de servicio, el análisis costo-beneficio del proyecto, la página titular, las especificaciones del sistema, los programas, los archivos y las bases de datos, la descripción de entrada, la definición de salida, y la documentación del programa requerida en el *BDE-005-SI-Proc.03.*

b. En el Capítulo XX, Procedimiento para la Solicitud de Creación, Modificación o Impresión de Informes, del *BDE-005-SI.01* se incluían los procedimientos para la creación o modificación de los informes utilizados en la operación del BDEPR. Para esto, el solicitante debía preparar el *Formulario de Solicitud de Creación, Modificación o Impresión de Informe (Formulario Solicitud de Informe)* autorizado por el Vicepresidente Ejecutivo del área. El *Formulario Solicitud de Informe* autorizado era referido al Gerente de Sistemas de Información, quien lo entregaba al Supervisor de Desarrollo de Aplicaciones, si existía la necesidad de crear un

informe nuevo, o a los técnicos de computadoras, si solamente se requería imprimirlo. El recurso asignado entregaba el informe solicitado al Vicepresidente Ejecutivo del área, quién debía firmar el *Formulario Solicitud de Informe* para documentar la aceptación final. Toda solicitud debía ser firmada y autorizada por el Vicepresidente Ejecutivo de Finanzas y Operaciones o por el Presidente del BDEPR.

El examen realizado sobre la documentación de 20 cambios de informes realizados, entre el 3 de julio de 2014 y el 8 de octubre de 2015, al programa Originación Informes reveló las siguientes deficiencias:

1) En 19 cambios no se había completado el *Formulario Solicitud de Informe.*
2) En 17 cambios no se mantenía documentación de la autorización del Vicepresidente Ejecutivo del área.
3) En 20 cambios no se mantenía documentación de la aprobación del Supervisor de Desarrollo de Aplicaciones.
4) En 18 cambios no se mantenía documentación de la aprobación del Gerente de Sistemas de Información.
5) En 7 cambios no se mantenía documentación de los cambios realizados al programa para producir los informes solicitados.

c. En el Capítulo XXI, Procedimiento para la Solicitud de Creación o Modificación de Programas Creados por Sistemas de Información del *BDE-005-SI.01*, se incluían los procedimientos para controlar las solicitudes para la creación o modificación de los programas. Para esto, el solicitante preparaba el *Formulario de Solicitud para la Creación o Modificación de Programas a Sistemas de Información (Formulario Solicitud de Programas)* autorizado por el Vicepresidente Ejecutivo de área. El Gerente de Sistemas de Información refería el formulario al Supervisor de Desarrollo de Aplicaciones para su evaluación. Si el desarrollo era uno complejo, el Comité de Tecnología debía aprobarlo. De lo contrario, se asignaba a uno de los desarrolladores de aplicaciones, quién debía requerirle al

solicitante que firmara el formulario una vez aceptara el programa o la aplicación solicitada. Además, debía recibir la aprobación del Vicepresidente Ejecutivo de Finanzas y Operaciones o del Presidente del BDEPR. El formulario original se archivaba en la DSI.

El examen realizado sobre la documentación de 28 cambios realizados, entre el 5 de febrero y el 16 de octubre de 2015, a las aplicaciones Originación Crédito, Originación CBE y Solicitudes Web, reveló las siguientes deficiencias:

1) En 22 cambios no se había completado el *Formulario Solicitud de Programas.*
2) En 21 cambios no se mantenía la documentación de la autorización del Vicepresidente Ejecutivo del área.
3) En 28 cambios no se mantenía documentación de la aprobación del Supervisor de Desarrollo de Aplicaciones.
4) En 24 cambios no se mantenía documentación de aprobación del Gerente de Sistemas de Información.
5) En 11 cambios no se mantenía documentación de los cambios realizados a las aplicaciones.

Criterios

La situación comentada en el **apartado a.** es contraria a lo establecido en el Capítulo VI, Documentación de Programas, del *BDE-005-SI-Proc.03.*

Las situaciones comentadas en los **apartados b. y c.** son contrarias a lo establecido en el Capítulo XX y XXI del *BDE-005-SI.01*.

Efectos

Las situaciones comentadas podrían dificultar a los desarrolladores de aplicaciones, al personal de la DSI, a los usuarios y a los auditores, el entendimiento del funcionamiento de los procesos, de los controles de las aplicaciones mencionadas, y del contenido de su base de datos. Además, privan al BDEPR de información esencial para darle mantenimiento a dichas aplicaciones, y dificultan mantener el control de los cambios a la programación y a la base de datos.

Causas

Las situaciones comentadas se debieron a que el Presidente consideraba que los manuales existentes estaban obsoletos, y sus disposiciones retrasaban los procesos de toma de decisiones y desarrollos. Además, el Gerente de Sistemas de Información no revisó el *BDE-005-SI-Proc.03* ni el *BDE-005-SI.01* para actualizarlos conforme a los procesos realizados en la DSI.

Comentarios de la Gerencia

El entonces Presidente nos indicó en su carta, entre otras cosas, lo siguiente:

> El Manual está obsoleto y tendrá cambios dirigidos a la utilización del sistema de "Log" de Registro de Informes y Programas que actualmente utilizan los Desarrolladores y con las nuevas prácticas de documentación utilizando "Microsoft Team Server". [*sic*]
>
> El sistema que estamos utilizando actualmente debe actualizarse enfocado a mantener una buena documentación y la manera de aprobación de cambios, donde tenga la aprobación electrónica de las aplicaciones solicitadas, creadas y modificadas. [*sic*]

Véanse las recomendaciones 1, y 4.f. y h.

Hallazgo 6 - Falta de organización de los cables que se conectaban a los equipos de comunicación del BDEPR

Situación

a. La red de comunicación del BDEPR contaba con un cuarto de servidores en el cuarto piso y dos cuartos de distribución de cableado, uno en el primer piso y otro en el tercer piso de su edificio. En estas áreas se habían instalado estantes para organizar y proteger los equipos de comunicación que mantenían las conexiones necesarias para interconectar las computadoras que recibían servicio de la red.

   El examen efectuado sobre los controles físicos y ambientales existentes en dichas áreas reveló que, al 24 de septiembre de 2015, no se mantenían organizados los cables que se conectaban a los equipos de comunicación mantenidos en el cuarto de servidores y en el cuarto de distribución de cableado ubicado en el tercer piso. **[Véase el ANEJO 1]**

Criterios

La situación comentada es contraria a lo establecido en la parte C.3 del *BDE-005-SI-Proc.02*.

Además, es contraria a lo establecido en la *Política TIG-003* de la *Carta Circular 77-05*. En esta se establece que cada agencia será responsable de desarrollar políticas específicas de seguridad de acuerdo con las características propias de sus ambientes de tecnología, particularmente sus sistemas críticos. Esto implica que, como norma de sana administración, las agencias deberán tener los cuidados necesarios para proteger los equipos computadorizados contra daños y averías, y para mantener el funcionamiento óptimo de los mismos. Para garantizar razonablemente la seguridad de los equipos y de los sistemas computadorizados, es necesario que se mantengan organizados los cables que conectan los equipos de comunicación. Esto permite atender y corregir oportunamente los problemas de comunicación, y detectar cualquier conexión no autorizada.

Efecto

La situación comentada dificulta los trabajos realizados por el personal de la DSI para atender los problemas de conexión en un tiempo razonable.

Causa

La situación comentada se debió a que el Gerente de Sistemas de Información no había impartido instrucciones para que se organizaran los cables conectados a los equipos de comunicación.

Comentarios de la Gerencia

El entonces Presidente nos indicó en su carta, entre otras cosas, lo siguiente:

> Todos los cuartos de conexiones contienen “patch cable” y todos ellos están identificados con números, según el puerto de conexión de cada usuario y existe un diagrama de conexiones de cada piso. Ciertamente, hay que realizar una reorganización del cableado. No obstante, esto se realizará una vez se culmine el proyecto de virtualización, el cual reducirá drásticamente la cantidad de servidores y el cableado asociado a los mismos.

Véanse las recomendaciones 1 y 4.i.

Hallazgo 7 - Incumplimiento de las recomendaciones incluidas en los informes auditorías externas

Situaciones

a. El BDEPR contrataba anualmente auditores externos para realizar las auditorías de los sistemas de información computadorizados. Esto, en respuesta a una recomendación incluida en un informe de auditoría del 2005 realizado por la Oficina del Comisionado de Instituciones Financieras (OCIF).

La Oficina de Auditoría Interna del BDEPR era supervisada por el Auditor General y daba seguimiento a las recomendaciones de los informes de los auditores externos a través de los planes de acción correctiva. Además, colaboraba en la preparación de dichos planes presentados a la OCIF. El examen realizado, entre el 1 de octubre de 2015 y el 27 de abril de 2016, sobre los planes de acción correctiva para atender las recomendaciones de los informes de auditoría, realizados del 2013 al 2015, reveló lo siguiente:

1) El BDEPR no había corregido 25 deficiencias comentadas en el informe de auditores externos realizado en el 2013. En el *Plan Acción Correctiva* más reciente, realizado al 10 de octubre de 2014, se informaba que las recomendaciones para corregir 24 de estas deficiencias se encontraban parcialmente cumplimentadas, mientras que la de 1 no estaba cumplimentada. Las deficiencias estaban relacionadas con la falta de un plan de recuperación de desastres y de las pruebas de restauración de los respaldos, la falta de control de acceso físico al cuarto de servidores, las deficiencias en los procedimientos para la administración y la configuración de las cuentas de acceso, el cableado no identificado y desorganizado, la falta de control de las contraseñas de la aplicación CBE, la falta de revisión y aprobación de los planes estratégicos, las deficiencias en el análisis de riesgos, la falta de funcionamiento del Comité de Tecnología, el incumplimiento de las recomendaciones de los

informes de la auditoría anteriores, la deficiencia de validación en los campos de la aplicación CBE y las deficiencias en el panel acceso a las áreas del BDEPR.

Durante nuestra auditoría determinamos que las deficiencias del análisis de riesgos y la falta de organización del cableado no habían sido corregidas. **[Véanse los hallazgos 1 y 6]**

2) El BDEPR no había corregido 8 deficiencias comentadas en el informe de auditores externos realizado en el 2015. Al 9 de octubre de 2015, las recomendaciones para corregir 7 de estas deficiencias se encontraban parcialmente cumplimentadas y 1 no estaba cumplimentada. Las deficiencias estaban relacionadas con la falta de un plan de continuidad de negocios, la falta de actualización de procedimientos, el uso de sistemas operativos sin apoyo técnico, la falta de control en el uso de dispositivos personales para almacenar datos, y deficiencias en la configuración de la seguridad, la administración de las cuentas de acceso y la configuración de un equipo de comunicación.

   Durante nuestra auditoría determinamos que las deficiencias relacionadas con la falta de un plan de continuidad de negocios, el uso de sistemas operativos sin apoyo técnico y la falta de actualización de procedimientos, no habían sido corregidas. **[Véanse los hallazgos 2, 4 y 5]**

   Además, estas situaciones fueron comentadas en un informe de auditoría anterior preparado por los auditores externos contratados por el BDEPR.

Criterio

Las normas para una sana administración pública requieren que los jefes de las entidades gubernamentales cumplan con las recomendaciones incluidas en los informes de auditores internos o externos. Esto, con el propósito de tomar a tiempo las medidas correctivas necesarias sobre las deficiencias comentadas y evitar que las mismas se repitan.

Efecto

Las situaciones comentadas podrían poner en riesgo los sistemas de información computadorizados y las operaciones principales del BDEPR.

Causa

Las situaciones comentadas se debieron a que la DSI tuvo una reducción de sus recursos económicos y su personal, lo que le dificultó al Gerente de Sistemas de Información la atención y el cumplimiento de las recomendaciones establecidas en los informes de auditorías externas.

Comentarios de la Gerencia

El entonces Presidente nos indicó en su carta, entre otras cosas, lo siguiente:

> La situación comentada se debió a reducción de recursos económicos y de personal.
>
> No obstante, hemos tomado las medidas necesarias para asegurar la continuidad y la seguridad de la información que manejamos diariamente en el Banco.
>
> Anualmente, con el poco personal en la división, se trabajan los hallazgos señalados en las auditorías de Sistemas de Información y se cumplen con los señalamientos, siempre que los recursos humanos y económicos lo permitan. [*sic*]
>
> No obstante, nuestro plan de trabajo va dirigido a cumplir con los mismos, a la vez que, cumplimos con el plan de trabajo anual, los proyectos especiales, los procesos diarios y problemas de emergencia que surgen y con todas las auditorías. [*sic*]

Véanse las recomendaciones 2 y 3.

RECOMENDACIONES

Al Presidente de la Junta de Directores del Banco de Desarrollo Económico para Puerto Rico

1. Asegurarse de que el Presidente del BDEPR cumpla con la **Recomendación 4**, de manera que se corrijan y no se repitan las situaciones comentadas en este *Informe*. **[Hallazgos del 1 al 6]**

2. Evaluar la posibilidad de identificar y asignar los recursos que permitan completar el proyecto para la virtualización de los servidores, necesario para actualizar los sistemas operativos **[Hallazgo 4]**, y atender las recomendaciones presentadas en los informes de auditorías externas. **[Hallazgo 7]**

3. Impartir instrucciones al Auditor General del BDEPR para que dé seguimiento y se asegure de que atiendan, en un tiempo razonable, las recomendaciones presentadas en los informes de auditorías externas. **[Hallazgo 7]**

Al Presidente del Banco de Desarrollo Económico para Puerto Rico

4. Ejercer una supervisión efectiva sobre el Gerente de Sistemas de Información para asegurarse de que:

   a. Revise el *Avalúo de Riesgo* del BDEPR para que se consideren e incluyan en el mismo los aspectos de análisis de riesgos indicados en el **Hallazgo 1**, según se establece en el *12 CFR* y en las políticas *TIG-003* y *TIG-015*. Una vez revisado, lo remita para su aprobación y vea que se revise cada vez que ocurra un cambio significativo dentro de la infraestructura operacional y tecnológica de del BDEPR. Esto, para asegurarse de que este documento se mantenga actualizado.

   b. Prepare y remita para su aprobación un plan de continuidad de negocios que incluya los planes específicos, completos y actualizados de la DSI para lograr el pronto funcionamiento de los sistemas de información computadorizados y restaurar las operaciones del BDEPR, en caso de emergencia. Una vez este documento sea aprobado, tomar las medidas necesarias para asegurarse de que el mismo se mantenga actualizado y se conserve copia en un lugar seguro fuera de los predios del BDEPR. Además, asegurarse de que sea distribuido a los funcionarios y a los empleados concernientes, y de que se realicen pruebas periódicas para garantizar la efectividad del mismo. **[Hallazgo 2-a.]**

   c. Identifique, como centro alterno, un lugar que no esté expuesto a los mismos riesgos que la DSI, y que cuente con la infraestructura y los equipos necesarios para restaurar las operaciones críticas del BDEPR, en caso de emergencia. Además, si el lugar identificado como centro alterno está localizado en otra entidad, realice las gestiones que permitan

formalizar los acuerdos que sean necesarios para la utilización del mismo. Dichos acuerdos deben estipular, entre otras cosas, las necesidades y los servicios requeridos para afrontar una emergencia, y el lugar o los lugares donde podrían ser requeridos dichos servicios. **[Hallazgo 2-b.]**

d. Actualice el *Plan* para que incluya las medidas de seguridad adecuadas y necesarias para mantener las operaciones principales del BDEPR. Una vez actualizado, remita el *Plan* para su aprobación. **[Hallazgo 2-c.]**

e. Reasigne las tareas del puesto de operador a un empleado que no realice cambios en la programación o, en su lugar, establezca las medidas de control alterno para que se supervisen las tareas conflictivas realizadas por el Desarrollador de Aplicaciones. **[Hallazgo 3]**

f. Revise los manuales *BDE-005-SI.01*, *BDE-005-SI-Proc.02* y *BDE-005-SI-Proc.03* para actualizarlos conforme al personal disponible, los procesos realizados y los controles necesarios para llevar a cabo las operaciones de la DSI. Una vez revisados, remita dichos manuales para su aprobación. **[Hallazgos 3 y 5]**

g. Realice los cambios necesarios para actualizar los sistemas operativos de los servidores comentados en el **Hallazgo 4**, de manera que puedan contar con los servicios de apoyo técnico y las actualizaciones de seguridad.

h. Imparta instrucciones al Supervisor de Desarrollo de Aplicaciones para que se asegure de que se mantenga la documentación completa de las aplicaciones y los programas, y de las autorizaciones para realizarles cambios, ya sea de forma manual o computadorizada. Además, se actualicen los manuales existentes conforme a los procesos de documentación realizados en la DSI y al sistema utilizado para documentar las aplicaciones y los programas, y las autorizaciones de cambios. **[Hallazgo 5]**

i. Establezca un plan de trabajo para que se organice el cableado de los equipos de comunicación en el cuarto de servidores y los cuartos de distribución de cableado. **[Hallazgo 6]**

AGRADECIMIENTO

A los funcionarios y a los empleados del BDEPR, les agradecemos la cooperación que nos prestaron durante nuestra auditoría.

Oficina del Contralor

Por: Yesmín M. Valdivieso

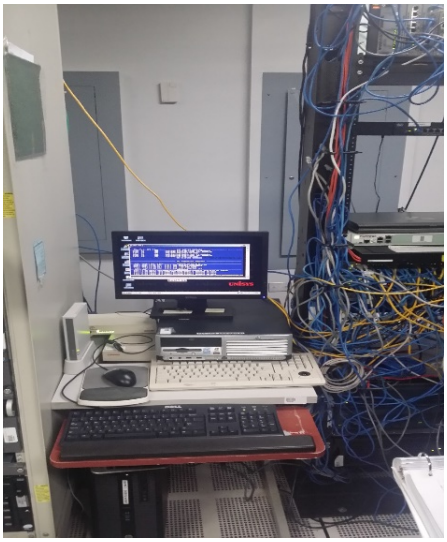
ANEJO 1

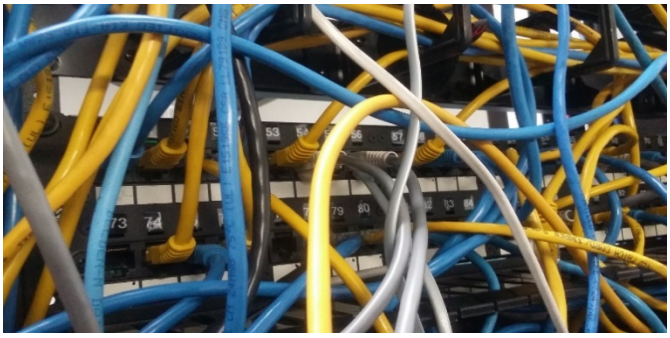
BANCO DE DESARROLLO ECONÓMICO PARA PUERTO RICO
DIVISIÓN DE SISTEMAS DE INFORMACIÓN

CABLES QUE NO SE MANTENÍAN ORGANIZADOS EN EL CUARTO DE SERVIDORES Y EN EL CUARTO DE DISTRIBUCIÓN DE CABLEADO DEL TERCER PISO

[Hallazgo 6]

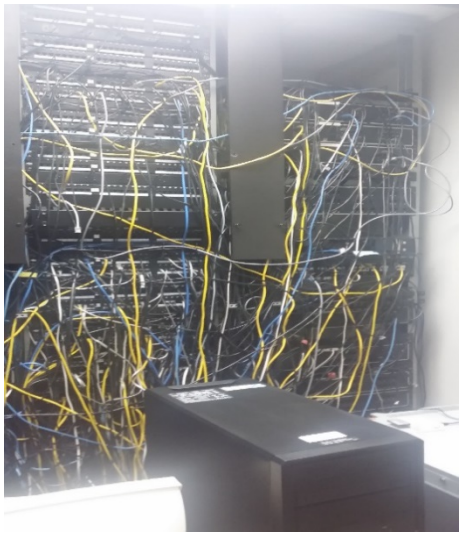
Cuarto de Servidores

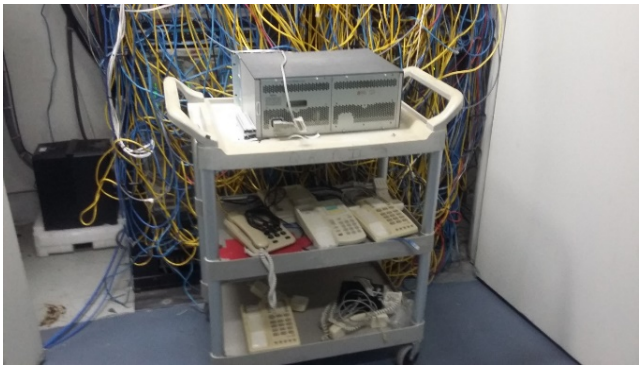




Continuación **ANEJO 1**

Cuarto de Distribución de Cableado del tercer piso





ANEJO 2

BANCO DE DESARROLLO ECONOMICO PARA PUERTO RICO
DIVISIÓN DE SISTEMAS DE INFORMACIÓN
MIEMBROS PRINCIPALES DE LA JUNTA DE DIRECTORES
DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Lcda. Melba Acosta Febo	Presidenta	16 sep. 15	4 mar. 16
Lcdo. Alberto Bacó Bagué	Vicepresidente	16 sep. 15	4 mar. 16
Lcdo. Eduardo Delgado Robles	Secretario	16 sep. 15	4 mar. 16

ANEJO 3

BANCO DE DESARROLLO ECONÓMICO PARA PUERTO RICO
DIVISIÓN DE SISTEMAS DE INFORMACIÓN
FUNCIONARIOS PRINCIPALES DE LA ENTIDAD
DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Sr. Joey Cancel Planas	Presidente	16 sep. 15	4 mar. 16
Sr. Víctor Maldonado Martínez	Vicepresidente Ejecutivo a cargo de Capital Humano	16 sep. 15	4 mar. 16
CPA José A. López Piñeiro	Auditor General	16 sep. 15	4 mar. 16
Sr. José E. Sánchez Meléndez	Gerente de Sistemas de Información	16 sep. 15	4 mar. 16

MISIÓN

Fiscalizar las transacciones de la propiedad y de los fondos públicos, con independencia y objetividad, para determinar si se han realizado de acuerdo con la ley, y atender otros asuntos encomendados.

Promover el uso efectivo, económico, eficiente y ético de los recursos del Gobierno en beneficio de nuestro Pueblo.

PRINCIPIOS PARA LOGRAR UNA ADMINISTRACIÓN PÚBLICA DE EXCELENCIA

La Oficina del Contralor, a través de los años, ha identificado principios que ayudan a mejorar la administración pública. Dichos principios se incluyen en la *Carta Circular OC-08-32* del 27 de junio de 2008, disponible en nuestra página en Internet.

QUERELLAS

Las querellas sobre el mal uso de la propiedad y de los fondos públicos pueden presentarse, de manera confidencial, personalmente o por teléfono al (787) 754-3030, extensión 2805, o al 1-877-771-3133 (sin cargo). También se pueden presentar mediante el correo electrónico Querellas@ocpr.gov.pr o mediante la página en Internet de la Oficina.

INFORMACIÓN SOBRE LOS INFORMES DE AUDITORÍA

En los informes de auditoría se incluyen los hallazgos significativos determinados en las auditorías. En nuestra página en Internet se incluye información sobre el contenido de dichos hallazgos y el tipo de opinión del informe.

La manera más rápida y sencilla de obtener copias libres de costo de los informes es mediante la página en Internet de la Oficina.

También se pueden emitir copias de los mismos, previo el pago de sellos de rentas internas, requeridos por ley. Las personas interesadas pueden comunicarse con el Administrador de Documentos al (787) 754-3030, extensión 3400.

INFORMACIÓN DE CONTACTO

Dirección física:
105 Avenida Ponce de León
Hato Rey, Puerto Rico
Teléfono: (787) 754-3030
Fax: (787) 751-6768

Dirección postal:
PO Box 366069
San Juan, Puerto Rico 00936-6069

Internet:
www.ocpr.gov.pr

Correo electrónico:
ocpr@ocpr.gov.pr