

Madeline D. C.



Secretaria

- Ver al dorso
- Para su información
- Notas
- Para mantenerle al día
- Expediente
- Dar Cuenta
- Registrar y Procesar

Senado
DE PUERTO RICO

EL CAPITOLIO
PO Box 9023431
San Juan, Puerto Rico
00902-3431

T: 787.722.3460

787.722.4012

F: 787.723.5413

W: www.senadopr.us

REFERIDO A:

COMISIONES PERMANENTES

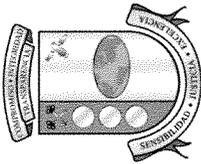
- Hacienda
- Gobierno
- Seguridad Pública y Judicatura
- Salud
- Educación y Asuntos de la Familia
- Desarrollo Económico y Planificación
- Urbanismo e Infraestructura
- Jurídico Penal
- Jurídico Civil
- Agricultura
- Recursos Naturales y Ambientales
- Comercio y Cooperativismo
- Turismo y Cultura
- Trabajo, Asuntos del Veterano y Recursos Humanos
- Bienestar Social
- Asuntos Municipales
- Recreación y Deportes
- Banca, Asuntos del Consumidor y Corporaciones Públicas
- Desarrollo de la Región del Oeste
- Asuntos de la Mujer
- Asuntos Internos
- Reglas y Calendario
- Asuntos Federales
- De la Montaña
- Ética

COMISIONES ESPECIALES

- Puerto de las Américas
- Derecho de Autodeterminación del Pueblo de Puerto Rico
- Sobre Reforma Gubernamental

COMISIONES CONJUNTAS

- Informes Especiales del Contralor
- Donativos Legislativos de Puerto Rico
- Internado Córdova-Fernós
- Internado Pilar Barbosa
- Internado Ramos Comas
- Código Penal
- Revisión y Reforma del Código Civil
- Alianzas Público Privadas
- Auditoría Fiscal y Manejo Fondos Públicos
- Revisión Continua Código Penal y Reforma de las Leves



Estado Libre Asociado de Puerto Rico
Oficina del Contralor

Yesmín M. Valdivieso
Contralora

28 de marzo de 2012

A LA MANO

PRIVILEGIADA Y CONFIDENCIAL

Hon. Thomas Rivera Schatz
Presidente
Senado de Puerto Rico
San Juan, Puerto Rico

Estimado señor Presidente:

Le incluimos copias de los informes de auditoría *TI-12-08* y *TI-12-09* del Centro de Procesamiento Electrónico de Información del Instituto de Ciencias Forenses de Puerto Rico y de los Sistemas de Información Computadorizados de la Comisión para la Seguridad en el Tránsito, respectivamente, aprobados por esta Oficina el 19 de marzo de 2012. Publicaremos dichos informes en nuestra página en Internet: <http://www.ocpr.gov.pr> para conocimiento de los medios de comunicación y de otras partes interesadas.

Estamos a sus órdenes para ofrecerle cualquier información adicional que estime necesaria.

Mejorar la fiscalización y la administración de la propiedad y de los fondos públicos es un compromiso de todos.

Cordialmente,


Yesmín M. Valdivieso

Anejos

RECIBIDO SECRETARIA
SISTEMAS DE P.R.

2012 MAR -9 PM 2:05

2012 MAR 28 AM 11:46

SENADO
THOMAS RIVERA SCHATZ

PO BOX 366069 SAN JUAN PUERTO RICO 00936-6069
105 AVENIDA PONCE DE LEÓN, HATO REY, PUERTO RICO 00917-1136
TEL. (787) 754-3030 FAX (787) 751-6768
E-MAIL: ocpr@ocpr.gov.pr INTERNET: <http://www.ocpr.gov.pr>

INFORME DE AUDITORÍA TI-12-08

19 de marzo de 2012

Instituto de Ciencias Forenses de Puerto Rico

Centro de Procesamiento Electrónico de Información

(Unidad 5342 - Auditoría 13245)

Período auditado: 23 de diciembre de 2008 al 18 de noviembre de 2009

CONTENIDO

Página

INFORMACIÓN SOBRE LA UNIDAD AUDITADA.....	3
RESPONSABILIDAD DE LA GERENCIA	5
ALCANCE Y METODOLOGÍA	6
OPINIÓN	7
RECOMENDACIONES	7
AL PRESIDENTE DE LA JUNTA DIRECTORA DEL INSTITUTO DE CIENCIAS FORENSES DE PUERTO RICO	7
A LA DIRECTORA EJECUTIVA DEL INSTITUTO DE CIENCIAS FORENSES DE PUERTO RICO	7
CARTAS A LA GERENCIA.....	10
COMENTARIOS DE LA GERENCIA	10
AGRADECIMIENTO	11
RELACIÓN DETALLADA DE HALLAZGOS.....	12
CLASIFICACIÓN Y CONTENIDO DE UN HALLAZGO	12
HALLAZGOS EN EL CENTRO DE PROCESAMIENTO ELECTRÓNICO DE INFORMACIÓN DEL INSTITUTO DE CIENCIAS FORENSES DE PUERTO RICO	13
1 - Falta de un informe de avalúo de riesgos de los sistemas de información computadorizados.....	13
2 - Falta de un plan de seguridad.....	15
3 - Deficiencias relacionadas con el Plan Operacional de Emergencias - Plan Multirisgo y con el Plan de Contingencias, y falta de un centro alternativo para la recuperación de los sistemas de información	17

4 - Deficiencias relacionadas con la preparación y con el manejo de los respaldos de los archivos computadorizados de información, y falta de almacenamiento de la documentación de las aplicaciones y los programas, en un lugar seguro fuera de los predios del Instituto	22
5 - Deficiencias relacionadas con las cuentas de acceso con privilegios de administración	25
6 - Deficiencias relacionadas con los formularios para autorizar la creación, la modificación y la cancelación de las cuentas de acceso a los sistemas de información.....	26
7 - Falta de procedimientos escritos para eliminar la información confidencial y los programas antes de transferir o disponer los equipos computadorizados y los medios de almacenamiento electrónico	28
ANEJO 1 - MIEMBROS PRINCIPALES DE LA JUNTA DIRECTORA QUE ACTUARON DURANTE EL PERÍODO AUDITADO	31
ANEJO 2 - FUNCIONARIOS PRINCIPALES QUE ACTUARON DURANTE EL PERÍODO AUDITADO	32

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

19 de marzo de 2012

Al Gobernador, al Presidente del Senado
y a la Presidenta de la Cámara de Representantes

Realizamos una auditoría de las operaciones del Centro de Procesamiento Electrónico de Información (CPEI) del Instituto de Ciencias Forenses de Puerto Rico (Instituto) para determinar si se hicieron 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. Efectuamos 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.

INFORMACIÓN SOBRE LA UNIDAD AUDITADA

El Instituto se creó por virtud de la *Ley Núm. 13 del 24 de julio de 1985, Ley del Instituto de Ciencias Forenses de Puerto Rico*, según enmendada. Este tiene entre sus funciones investigar, con el objetivo de determinar la causa, la manera y las circunstancias de la muerte de cualquier persona, cuyo deceso se produzca bajo alguna de las situaciones especificadas en esta *Ley*; y evaluar y analizar la prueba resultante de cualquier otro delito que sea traído a su atención, preservando y presentando la evidencia derivada de su investigación para exonerar, o para establecer, más allá de duda razonable, la culpabilidad del acusado. A fin de que pueda cumplir el propósito fundamental de salvaguardar la objetividad investigativa, el Instituto opera con autonomía administrativa y fiscal.

El Instituto es dirigido por una Junta Directora (Junta), quien tiene la responsabilidad de establecer la política administrativa y operacional del mismo. La Junta está constituida por el Secretario de Justicia, quien la preside, el Superintendente de la Policía, el Rector del Recinto de Ciencias Médicas de la Universidad de Puerto Rico, la Directora Administrativa de los Tribunales, el Secretario de Salud, y tres miembros adicionales, nombrados por el Gobernador, con el consejo y consentimiento del Senado de Puerto Rico. Los tres miembros adicionales son personas de reconocida capacidad: un abogado, un médico y un ciudadano particular, quienes representan el interés público.

La Junta, además, es responsable de nombrar al Director Ejecutivo del Instituto. Este tiene entre sus funciones, asignar las labores administrativas a base de criterios que permitan el uso más eficaz de los recursos humanos. Esto tomando en consideración, entre otros factores, la asignación y la distribución racional de funciones; la distribución de poder acorde con las responsabilidades; la selección acertada del personal; y la asignación de recursos a tono con las necesidades del Instituto y sus secciones. Para cumplir con estos objetivos, el Instituto presta sus servicios a toda la demarcación territorial de Puerto Rico, a través de la oficina central en Río Piedras, sus tres laboratorios regionales localizados en Arecibo, Mayagüez y Ponce, y la Unidad de Investigadores Forenses en Ponce.

El Instituto cuenta con las siguientes áreas para llevar a cabo sus funciones: Oficina del Director, el Laboratorio de Criminalística, el Programa de Detección de Sustancias Controladas, y las divisiones de Patología Forense, Investigación de Campo y Seguridad, Finanzas y Presupuesto, Servicios Auxiliares, y Recursos Humanos y Relaciones Laborales. El CPEI responde a la Directora Ejecutiva y es dirigido por una Oficial Principal de Informática.

Los **anejos 1 y 2** contienen una relación de los miembros principales de la Junta y de los funcionarios principales del Instituto, respectivamente, que actuaron durante el período auditado.

A la fecha de nuestra auditoría, el CPEI tenía en operación una red de comunicaciones (red) compuesta por 32 servidores y 325 computadoras personales, con sus respectivos equipos periferales. Mediante dicha red se comparten, a nivel central y con los laboratorios de Ponce, Mayagüez y Arecibo, los recursos de información, tales como: correo electrónico, Internet, e impresoras, y las aplicaciones que residen en los diferentes servidores de la red.

El presupuesto asignado al Instituto proviene de resoluciones conjuntas del Fondo General del Estado Libre Asociado de Puerto Rico. Además, recibe fondos de asignaciones federales y especiales, y de ingresos propios. Los gastos operacionales del Instituto para los años fiscales 2007-08 y 2008-09 ascendieron a \$18,325,000 y \$18,135,000, respectivamente.

El Instituto cuenta con una página en Internet, a la cual se puede acceder mediante la siguiente dirección: <http://www.icf.gobierno.pr>. Esta página provee información acerca de la entidad y de los servicios que presta.

RESPONSABILIDAD DE LA GERENCIA

La gerencia de todo organismo gubernamental debe considerar los siguientes *Diez Principios para Lograr una Administración Pública de Excelencia*. Estos se rigen por principios de calidad y por los valores institucionales:

1. Adoptar normas y procedimientos escritos que contengan controles internos de administración y de contabilidad eficaces, y observar que se cumpla con los mismos.
2. Mantener una oficina de auditoría interna competente.
3. Cumplir con los requisitos impuestos por las agencias reguladoras.
4. Adoptar un plan estratégico para las operaciones.
5. Mantener el control presupuestario.
6. Mantenerse al día con los avances tecnológicos.
7. Mantener sistemas adecuados de archivo y de control de documentos.
8. Cumplir con el *Plan de Acción Correctiva* de la Oficina del Contralor de Puerto Rico, y atender las recomendaciones de los auditores externos.

9. Mantener un sistema adecuado de administración de personal que incluya la evaluación del desempeño, y un programa de educación continua para todo el personal.

10. Cumplir con la *Ley de Ética Gubernamental del Estado Libre Asociado de Puerto Rico*, lo cual incluye divulgar sus disposiciones a todo el personal.

El 27 de junio de 2008, mediante la *Carta Circular OC-08-32*, divulgamos la revisión de los mencionados diez principios, establecidos en nuestra *Carta Circular OC-98-09* del 14 de abril de 1998. Se puede acceder a ambas cartas circulares a través de nuestra página en Internet: <http://www.ocpr.gov.pr>.

ALCANCE Y METODOLOGÍA

La auditoría cubrió del 23 de diciembre de 2008 al 18 de noviembre de 2009. En algunos aspectos examinamos transacciones de fechas anteriores. 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.

Para efectuar la auditoría utilizamos la siguiente metodología:

- entrevistas a funcionarios, a empleados y a particulares
- inspecciones físicas
- examen y análisis de informes y de documentos generados por la unidad auditada
- examen y análisis de informes y de documentos suministrados por fuentes externas
- pruebas y análisis de información financiera, de procedimientos de control interno y de otros procesos
- confirmaciones de información pertinente.

OPINIÓN

Las pruebas efectuadas demostraron que las operaciones del CPEI en lo que concierne a la administración del programa de seguridad, los controles de acceso, y la continuidad del servicio, no se realizaron conforme a las normas generalmente aceptadas en este campo.

Los **hallazgos del 1 al 7**, clasificados como principales, se comentan en la parte de este *Informe* titulada **RELACIÓN DETALLADA DE HALLAZGOS**.

RECOMENDACIONES

AL PRESIDENTE DE LA JUNTA DIRECTORA DEL INSTITUTO DE CIENCIAS FORENSES DE PUERTO RICO

1. Ver que la Directora Ejecutiva del Instituto cumpla con las **recomendaciones de la 2 a la 5** de este *Informe*. **[Hallazgos del 1 al 7]**

A LA DIRECTORA EJECUTIVA DEL INSTITUTO DE CIENCIAS FORENSES DE PUERTO RICO

2. Asegurarse de que se realice y se documente el análisis de riesgos, según se establece en la *Política Núm. TIG-003, Seguridad de los Sistemas de Información, de la Carta Circular Núm. 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 Oficina de Gerencia y Presupuesto, y se sugiere en las mejores prácticas en el campo de tecnología. El informe, producto de este análisis de riesgos, debe ser remitido a la Junta Directora para revisión y aprobación. **[Hallazgo 1]**

3. Remitir para la consideración y la aprobación de la Junta Directora:

- a. El *Plan Operacional de Emergencias - Plan Multirriesgo (Plan de Emergencias)* **[Hallazgo 3-a.1)]**

- b. El *Plan de Contingencias* [Hallazgo 3-b.1)]
- c. El *Procedimiento Proceso de Respaldos (Backups) del ICF*. [Hallazgo 4-a.1)]
4. Ejercer una supervisión eficaz sobre la Oficial Principal de Informática para asegurarse de que:
 - a. Prepare un plan de seguridad que incluya los criterios descritos en el **Hallazgo 2**, el cual debe ser remitido a la Junta Directora para revisión y aprobación. Una vez aprobado, se asegure de que se divulgue a los empleados y a los funcionarios concernientes y de que se realicen pruebas periódicas del mismo.
 - b. Revise el *Plan de Contingencias* para que el mismo esté actualizado conforme a lo indicado en el **Hallazgo 3-b.2)** e incluya los aspectos comentados en el **Hallazgo 3-b.4)**.
 - c. Mantenga una copia del *Plan de Contingencias* y de la documentación sobre las instalaciones, las configuraciones, los programas de aplicaciones y las actualizaciones realizadas a los sistemas de información, en un lugar seguro fuera de las instalaciones del Instituto. [Hallazgos 3-b.3) y 4-b.]
 - d. Realice las gestiones necesarias para identificar un lugar disponible y adecuado como centro alternativo para restaurar las operaciones críticas del Instituto, en caso de una emergencia o desastre que afecte sus sistemas de información. [Hallazgo 3-c.]
 - e. Establezca los controles necesarios para la producción de respaldos semanales y mensuales. [Hallazgo 4-a.2)]
 - f. Se asegure de que diariamente se trasladen los respaldos efectuados, a la caja fuerte que el Instituto tiene alquilada en una institución bancaria. [Hallazgo 4-a.3)]

- g. Establezca un registro de los respaldos diarios enviados a la caja fuerte que el Instituto tiene alquilada, que incluya la información actualizada y necesaria para mantener el control de estos respaldos. **[Hallazgo 4-a.4)]**
 - h. Identifique todas las cuentas de acceso con privilegios de administración de servidores y del dominio, y, en coordinación con los funcionarios principales de las áreas a las que pertenecen los usuarios de las mismas, realice una evaluación de los privilegios otorgados a dichas cuentas, basado en el principio de menor privilegio. Una vez realizada la evaluación, documente la justificación para aquellas cuentas que requieran el privilegio de administración. **[Hallazgo 5]**
 - i. Requiera a todos los directores de división u oficina que remitan para cada uno de los funcionarios, empleados o contratistas, el formulario actualizado de *Solicitud de Acceso a los Sistemas y Tecnologías de Información del ICF (Solicitud de Acceso)*, debidamente revisado y autorizado por estos. Además, mantenga debidamente archivados dichos formularios. **[Hallazgo 6-a.1)]**
 - j. Se asegure de firmar los formularios *Solicitud de Acceso* y de velar por que estos estén completados en todas sus partes, antes de proceder a la creación o modificación de las cuentas de acceso. **[Hallazgo 6-a.2)]**
 - k. Prepare un procedimiento para eliminar la información confidencial y los programas, archivados en los equipos computarizados y en los medios de almacenamiento electrónico, antes de transferir o de descartar los mismos. Una vez preparado, el procedimiento debe ser remitido a la Junta Directora para revisión y aprobación. **[Hallazgo 7]**
5. Asegurarse de que se mantenga la documentación sobre el resultado de las pruebas o simulacros efectuados al *Plan de Emergencias*. Mediante estos se verifica si el *Plan de Emergencias* está completo, es preciso, y cumple con el propósito de prevenir y reducir los efectos directos o indirectos, antes, durante y después de una emergencia o desastre. **[Hallazgo 3-a.2)]**

CARTAS A LA GERENCIA

Las situaciones comentadas en los **hallazgos del 1 al 7**, incluidos en la parte de este *Informe* titulada **RELACION DETALLADA DE HALLAZGOS**, se informaron a la Dra. María S. Conte Miller, Directora Ejecutiva del Instituto, en carta de nuestros auditores del 12 de enero de 2010.

El borrador de los **hallazgos** de este *Informe* se remitió a la Directora Ejecutiva, para comentarios, en carta del 17 de marzo de 2011. Con el mismo propósito, remitimos el borrador de los **hallazgos** de este *Informe* al Dr. José Rodríguez Orengo, ex Director Ejecutivo del Instituto, en carta de esa misma fecha, por correo certificado con acuse de recibo, a una dirección provista por el Instituto.

El 5 de abril de 2011, se recibió en la Oficina, devuelta por el correo, la carta con el borrador de los **hallazgos** de este *Informe* que le fue referido al doctor Rodríguez Orengo, debido a que la misma no fue reclamada. Ese mismo día, se envió una carta de seguimiento al ex Director Ejecutivo del Instituto y se le concedió hasta el 11 de abril de 2011 para remitir los comentarios al borrador de los **hallazgos** de este *Informe*. Esta carta no fue devuelta por el correo.

COMENTARIOS DE LA GERENCIA

El 12 de febrero de 2010, la Directora Ejecutiva remitió sus comentarios sobre los **hallazgos** incluidos en la carta de nuestros auditores. Sus observaciones fueron consideradas en la redacción del borrador del *Informe*.

El 1 de abril de 2011, la Directora Ejecutiva solicitó una prórroga para remitir sus comentarios al borrador de los **hallazgos** de este *Informe*. Ese mismo día, le concedimos a la Directora Ejecutiva la prórroga hasta el 15 de abril de 2011. La Directora Ejecutiva contestó el borrador de los **hallazgos** de este *Informe*, mediante carta recibida en esta Oficina el 15 de abril de 2011, firmada por el Sr. Juan E. Hernández Dávila, Ayudante Especial del Área Administrativa, en su representación. Sus comentarios fueron considerados en la redacción

final de este *Informe*; y se incluyen en la segunda parte de este *Informe*, titulada **RELACIÓN DETALLADA DE HALLAZGOS**, bajo la sección de HALLAZGOS EN EL CENTRO DE PROCESAMIENTO ELECTRÓNICO DE INFORMACIÓN DEL INSTITUTO DE CIENCIAS FORENSES DE PUERTO RICO.

AGRADECIMIENTO

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

Por:

Agencia del Centra
Spinnin m. Robinson

RELACIÓN DETALLADA DE HALLAZGOS

CLASIFICACIÓN Y CONTENIDO DE UN HALLAZGO

En nuestros informes de auditoría se incluyen los hallazgos significativos determinados por las pruebas realizadas. Estos se clasifican como principales o secundarios. Los principales incluyen desviaciones de disposiciones sobre las operaciones de la unidad auditada que tienen un efecto material, tanto en el aspecto cuantitativo como en el cualitativo. Los secundarios son los que consisten en faltas o errores que no han tenido consecuencias graves.

Los hallazgos del informe se presentan según los atributos establecidos conforme a las normas de redacción de informes de nuestra Oficina. El propósito es facilitar al lector una mejor comprensión de la información ofrecida. Cada uno de ellos consta de las siguientes partes:

Situación - Los hechos encontrados en la auditoría indicativos de que no se cumplió con uno o más criterios.

Criterio - El marco de referencia para evaluar la situación. Es principalmente una ley, un reglamento, una carta circular, un memorando, un procedimiento, una norma de control interno, una norma de sana administración, un principio de contabilidad generalmente aceptado, una opinión de un experto o un juicio del auditor.

Efecto - Lo que significa, real o potencialmente, no cumplir con el criterio.

Causa - La razón fundamental por la cual ocurrió la situación.

En la sección sobre los **COMENTARIOS DE LA GERENCIA** se indica si el funcionario principal y los exfuncionarios de la unidad auditada efectuaron comentarios sobre el borrador de los hallazgos del informe, que les envía nuestra Oficina. Dichos comentarios se consideran al revisar el borrador del informe y se incluyen al final del hallazgo correspondiente en la sección de **HALLAZGOS EN EL CENTRO DE PROCESAMIENTO ELECTRÓNICO DE INFORMACIÓN DEL INSTITUTO DE CIENCIAS FORENSES DE PUERTO RICO**, de

forma objetiva y conforme a las normas de nuestra Oficina. Cuando la gerencia no provee evidencia competente, suficiente y relevante para refutar un hallazgo, este prevalece y se añade al final del mismo la siguiente aseveración: Consideramos las alegaciones de la gerencia, pero determinamos que el hallazgo prevalece.

HALLAZGOS EN EL CENTRO DE PROCESAMIENTO ELECTRÓNICO DE INFORMACIÓN DEL INSTITUTO DE CIENCIAS FORENSES DE PUERTO RICO

Hallazgo 1 - Falta de un informe de avalúo de riesgos de los sistemas de información computadorizados

a. Un avalúo de riesgos es un método para identificar las vulnerabilidades y las amenazas a los recursos de sistemas de información. Además, evalúa los posibles daños para determinar dónde implantar las medidas de seguridad para poder alcanzar y cumplir con los objetivos de la entidad gubernamental. Este método se utiliza para asegurar que las medidas de seguridad a ser implantadas sean costo-efectivas, pertinentes a las operaciones de la entidad gubernamental y respondan a las posibles amenazas identificadas. El avalúo de riesgos tiene cuatro objetivos:

- Identificar los activos y el valor monetario asignado a los mismos.
- Identificar las vulnerabilidades y las amenazas de los recursos de sistemas de información.
- Cuantificar la probabilidad y el impacto de las amenazas potenciales en las operaciones de la entidad gubernamental.
- Proveer un balance económico entre el impacto de las amenazas y el costo de las medidas de seguridad a implantarse.

Al 2 de julio de 2009, en el Instituto no se había realizado un avalúo de riesgos sobre los sistemas de información computadorizados.

En la *Política Núm. TIG-003 de la Carta Circular Núm. 77-05* se establece, entre otras cosas, que cada agencia deberá implantar controles que minimicen los riesgos de que los sistemas de información dejen de funcionar correctamente y de que la información sea accedida de forma no autorizada. Para esto, deberá realizar un análisis de riesgos que incluya:

- Un inventario de los activos de sistemas de información, que incluya el equipo, los programas y los datos. Todos los activos deberán ser clasificados de acuerdo con el nivel de importancia para la continuidad de las operaciones. En particular, los datos electrónicos deberán ser clasificados de acuerdo con su nivel de confidencialidad. Esto permitirá establecer qué es lo que se va a proteger.
- Las posibles amenazas contra los sistemas de información (robos, desastres naturales, fallas, virus y acceso indebido a los datos, entre otras), junto con un análisis del impacto en las operaciones y la probabilidad de que ocurran esas amenazas. Esto permitirá establecer cómo se van a proteger los activos identificados anteriormente.

La situación comentada impidió al Instituto evaluar 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 de pérdida de información.

La situación comentada se atribuye a que la Directora Ejecutiva no había impartido las directrices para la preparación y la documentación del avalúo de riesgos sobre los sistemas de información del Instituto, según se establece en la *Carta Circular Núm. 77-05*.

La Directora Ejecutiva, en la carta que nos envió, informó, entre otras cosas, lo siguiente:

La OTI de la OGP entregó Informe de Análisis de riesgo en mayo de 2010. Del mismo, surgieron “issues de seguridad” clasificados como severos que requirieron de la intervención de un especialista con vasta experiencia de la compañía [...] a través del acuerdo contractual establecido con la OTI de la OGP. [sic]

Hallazgo 2 - Falta de un plan de seguridad

- a. Al 2 de julio de 2009, el Instituto no tenía un plan de seguridad que incluyera, entre otras cosas, disposiciones en cuanto a:
- La documentación de la validación de las normas de seguridad¹
 - La evidencia de un análisis de riesgos actualizado, que sea la base del plan
 - La responsabilidad de la gerencia, de los oficiales de seguridad y de los demás componentes de la unidad, tales como: los dueños y los usuarios de los recursos de información, el personal administrativo del CPPI, el personal a cargo del procesamiento de los datos y los administradores de seguridad, entre otros
 - Un programa de adiestramiento especializado al equipo clave de seguridad
 - Un programa de adiestramiento continuo sobre seguridad que incluya a los nuevos empleados, los contratistas y los usuarios, y el cual permita mantener los conocimientos actualizados
 - La documentación de los controles administrativos, técnicos y físicos de los activos de información (datos, programación, equipos y personal, entre otros).

En la *Política Núm. TIG-003 de la Carta Circular Núm. 77-05* se establece que las entidades gubernamentales tendrán la responsabilidad de desarrollar políticas específicas de

¹ La validación de las normas de seguridad se efectúa mediante la prueba de los controles para eliminar o mitigar las amenazas y las vulnerabilidades detectadas en el avalúo de riesgos. Además, se valida mediante los resultados de los simulacros efectuados para probar la efectividad del plan de seguridad.

seguridad de acuerdo con las características propias de los ambientes de tecnología de la agencia, particularmente sus sistemas de misión crítica. También se establece que las entidades gubernamentales son responsables de:

- Proveer adiestramientos a toda la gerencia y a los supervisores de la entidad gubernamental para que estén al tanto de los controles de seguridad y los beneficios correspondientes.
- Proveer adiestramientos al personal de sistemas de información y de telecomunicaciones para que se les transmitan los conocimientos actualizados sobre los aspectos de seguridad de sus áreas.
- Crear mecanismos de capacitación para que todos los empleados conozcan los procedimientos de seguridad que les apliquen.

Las mejores prácticas en el campo de tecnología de información sugieren que las entidades deben mantener un plan escrito que describa claramente el programa de seguridad y los procedimientos relacionados con este. El mismo debe considerar los sistemas y las instalaciones principales e identificar los deberes de los dueños y de los usuarios de los sistemas de información de la entidad, y de los empleados responsables de velar por la seguridad de dichos sistemas.

La falta de un plan de seguridad podría provocar la inversión de recursos en medidas de control inadecuadas, el desconocimiento y la falta de entendimiento de las responsabilidades relacionadas con la seguridad, y la protección inadecuada de los recursos críticos.

La situación comentada se atribuye a que la Directora Ejecutiva no había impartido las directrices para la preparación del plan de seguridad.

La Directora Ejecutiva, en la carta que nos envió, informó, entre otras cosas, lo siguiente:

La OTI de la OGP entregó Informe de Análisis de riesgo en mayo de 2010. [...] El resto de los “issues de seguridad” presentados en el informe se continúan solucionando por personal del ICF, y forman parte del Plan de Seguridad del Centro de Cómputos que se está desarrollando, según recomendado por sus auditores durante su intervención en los sistemas de información del ICF. [sic]

Hallazgo 3 - Deficiencias relacionadas con el Plan Operacional de Emergencias - Plan Multirisgo y con el Plan de Contingencias, y falta de un centro alterno para la recuperación de los sistemas de información

- a. En junio de 2009, la Directora Ejecutiva aprobó el *Plan Operacional de Emergencias - Plan Multirisgo (Plan de Emergencias)*, cuyo propósito era coordinar todas las acciones asignadas a las oficinas y dependencias, para prevenir o reducir los efectos directos o indirectos; antes, durante y después de una emergencia o desastre. Dicho *Plan de Emergencias* contempla por quién, cuándo, dónde, cómo y por qué se van a realizar las tareas durante las fases de preparación, mitigación, respuesta y recuperación. El Instituto contaba con una Coordinadora de Emergencia que era la persona responsable, entre otras cosas, de conducir el adiestramiento y los simulacros necesarios para medir la efectividad del *Plan de Emergencias* y dar mantenimiento al mismo. El examen realizado reveló lo siguiente:
 - 1) El *Plan de Emergencias* no estaba debidamente aprobado por la Junta Directora del Instituto.
 - 2) Al 20 de noviembre de 2009, no se encontró ni se nos suministró para examen documentación sobre los resultados de las pruebas o simulacros efectuados para verificar si el *Plan de Emergencias* estaba completo, era preciso y cumplía con el propósito de prevenir o reducir los efectos directos o indirectos; antes, durante y después de una emergencia o desastre.

b. El examen efectuado, en agosto de 2009, sobre el *Plan de Contingencias (Plan)* del CPPI reveló las siguientes deficiencias:

- 1) No estaba aprobado por la Junta Directora, a pesar de haber sido aprobado en julio de 1994 por la Directora Ejecutiva.
- 2) No estaba actualizado conforme a los cambios de equipos, sistemas de información y personal, ocurridos desde su aprobación.
- 3) No se mantenía una copia en un lugar seguro fuera de los predios de las instalaciones del Instituto.
- 4) No incluía los siguientes requisitos que son necesarios para atender situaciones de emergencia en las operaciones de los sistemas de información:
 - las estrategias a utilizarse para efectuar y documentar las pruebas o los simulacros, que certifiquen la efectividad del *Plan*
 - el detalle de la configuración crítica y del contenido de los respaldos, así como el nombre de las librerías y de los archivos
 - el detalle de la configuración de los sistemas principales utilizados en el CPPI requeridos para efectuar una restauración en un centro de sistemas de información alternativo (centro alterno)
 - un itinerario de restauración que incluya el orden de las aplicaciones a restaurar y los procedimientos para restaurar los respaldos
 - una lista de los proveedores principales, que incluya el número de teléfono y el nombre del personal de enlace con el Instituto
 - los procesos para restablecer las operaciones en un centro alterno
 - el procedimiento para efectuar pruebas en un centro alterno

- el procedimiento para probar los respaldos de información, para asegurar que los mismos puedan ser recuperados, cuando sea necesario
- una hoja de cotejo para verificar los daños ocasionados por la contingencia.

En el Artículo 4 de la *Ley Núm. 13* se establece, entre otras cosas, que la Junta Directora tendrá la responsabilidad de establecer la política administrativa y operacional del Instituto. Además, en el Artículo 8 se establece, entre otras cosas, que la Junta Directora formulará la reglamentación necesaria para definir las funciones de las secciones o departamentos y del personal profesional, técnico y administrativo del Instituto.

Las mejores prácticas en el campo de la tecnología utilizadas para garantizar la confiabilidad, la integridad y la disponibilidad de los sistemas de información computarizados sugieren que como parte del *Plan de Continuidad de Negocios* se deberá preparar un *Plan de Contingencias*. Este es una guía que garantiza la continuidad de las operaciones normales de los sistemas de información computarizados cuando se presentan eventualidades inesperadas que afecten su funcionamiento. El mismo deberá estar aprobado por el funcionario de máxima autoridad de la entidad y deberá incluir todos los procesos necesarios para recuperar cualquier segmento de la operación del centro de cómputos o, si fuese necesario, relocalizar las operaciones en el menor tiempo posible y de la forma más ordenada y confiable. Además, se deben efectuar procedimientos para realizar pruebas o simulacros, por lo menos una vez al año, revisar el *Plan* anualmente o en un término menor, según las necesidades del Instituto, y darlo a conocer a todo el personal que llevará a cabo los procesos del mismo y mantener una copia de este fuera de las instalaciones principales de la agencia.

Las situaciones comentadas pueden 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, e interrupciones prolongadas de los servicios ofrecidos a los usuarios del Instituto.

Además, la situación comentada en el **apartado b.3)** podría ocasionar que, de ocurrir una emergencia que impida el acceso al Instituto, el encargado de activar el *Plan de Contingencias* no tuviera acceso a este para iniciar el proceso de reconstrucción de archivos y programas, y el restablecimiento y la continuidad de las operaciones normales de los sistemas de información, en un tiempo razonable.

Las situaciones comentadas en los **apartados a.1) y b.1)** se debían a que la Directora Ejecutiva no remitió para la revisión y la aprobación de la Junta Directora, el *Plan de Emergencias* ni el *Plan de Contingencias*.

La situación comentada en el **apartado a.2)** se atribuye a que la Coordinadora de Emergencia del Instituto no se aseguró de mantener la documentación histórica de los resultados de las pruebas o simulacros.

Las situaciones comentadas en el **apartado b.2) y 4)** se debían, en parte, a que la Directora Ejecutiva no había promulgado una directriz sobre la implantación y continua actualización del *Plan*. Tampoco había requerido que se preparara un avalúo de riesgos (**Véase el Hallazgo 1)** para que sirviera de base para el desarrollo, la aprobación y la implantación de dicho *Plan*, a fin de que sirva como herramienta para responder ante cualquier incidente o desastre que ocurra.

La situación comentada en el **apartado b.3)** se atribuye, en parte, a que la Oficial Principal de Informática no había impartido directrices para que se mantuviera una copia del *Plan* en un lugar seguro fuera de las instalaciones del Instituto.

- c. El Instituto no contaba con un centro alerno para restaurar las operaciones críticas computarizadas en casos de emergencia. Tampoco había formalizado acuerdos con otra entidad para establecer un centro alerno en las instalaciones de esta.

Las mejores prácticas en el campo de la tecnología de información sugieren que, como parte integral del *Plan de Continuidad de Negocios*, deben existir convenios 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:

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

La situación comentada podría afectar las funciones del Instituto y los servicios del CPEI, ya que no tendrían disponibles unas instalaciones para operar después de una emergencia o evento que afectara su funcionamiento. Esto podría atrasar o impedir el proceso de restauración de archivos y el pronto restablecimiento de las operaciones normales del CPEI.

La situación comentada se atribuye a que la Oficial Principal de Informática no había coordinado la identificación de un lugar disponible y adecuado como centro alerno, de manera que la Directora Ejecutiva pudiera formalizar los acuerdos escritos necesarios para la utilización del mismo en casos de emergencia.

La Directora Ejecutiva, en la carta que nos envió, informó, entre otras cosas, lo siguiente:

La Directora Ejecutiva del ICF impartió instrucciones a la Especialista de Seguridad del ICF para que documente el resultado de las pruebas o simulacros que actualmente se llevan a cabo periódicamente en el ICF. De igual manera, instruyó a la Especialista de Sistemas de Información de la agencia a que actualice el Plan de Contingencia del CPEI, mantenga una copia en el Laboratorio de Mayagüez, y realice y documente todo simulacro que se realice con los sistemas de información del ICF. A su vez, complete la documentación de la configuración de todos los sistemas de información del ICF en forma detallada y en orden de ejecución de los procesos de operación y prueba que se realicen en el CPEI, según se requiere durante la restauración de un centro alerno. [sic]

Hallazgo 4 - Deficiencias relacionadas con la preparación y con el manejo de los respaldos de los archivos computadorizados de información, y falta de almacenamiento de la documentación de las aplicaciones y los programas, en un lugar seguro fuera de los predios del Instituto

a. El CPEI era responsable de preparar los respaldos de los datos mantenidos en los servidores, incluso en los ubicados en las oficinas regionales, que contenían los directorios de usuarios y las diferentes aplicaciones. El Instituto tenía alquilada una caja de seguridad en una institución bancaria, con el propósito de mantener los respaldos de los archivos y de los programas de los sistemas de información computadorizados, en un lugar seguro fuera de los predios donde está ubicado.

El examen realizado en noviembre de 2009, sobre la preparación y el manejo de los respaldos de los archivos y de los programas de los sistemas de información computadorizados del Instituto, reveló las siguientes deficiencias:

1) El *Procedimiento Proceso de Respaldos (Backups) del ICF* para la realización de los respaldos diarios de información no había sido aprobado por la Junta Directora. Además, no incluía la fecha de efectividad ni indicaba quién es responsable de realizar los respaldos y de trasladarlos a la caja de seguridad de la institución bancaria.

En el Inciso (g) del Artículo 8 de la *Ley Núm. 13* se establece, entre otras cosas, que la Junta Directora formulará la reglamentación necesaria para definir las funciones de las secciones o departamentos y del personal profesional, técnico y administrativo del Instituto.

2) No se efectuaban respaldos semanales, mensuales ni anuales. Solo se efectuaban respaldos diarios.

3) Entre el 26 de febrero de 2008 y el 5 de noviembre de 2009, solo se habían trasladado a la caja de seguridad de la institución bancaria, los respaldos diarios de información correspondientes a 16 días. Esto implica que, durante la mayoría de los días comprendidos en dicho período, no se mantuvieron copias de los respaldos diarios de información, en un lugar seguro fuera de los predios donde está ubicado el Instituto.

4) No se mantenía un registro de los respaldos diarios que eran llevados a la caja de seguridad de la institución bancaria, que permitiera mantener el control de los mismos.

En la *Política Num. TIG-003 de la Carta Circular Num. 77-05* se establece que deberán existir procedimientos para tener y mantener una copia de respaldo (*backup*) recurrente de la información y de los programas de aplicación y de sistemas esenciales e importantes para las operaciones de la entidad gubernamental. En consonancia con dicha política pública es necesario, entre otras cosas, que toda información almacenada en medios electrónicos que se utilice como parte de la operación normal de la entidad, sea duplicada periódicamente y guardada en un lugar seguro fuera de los predios de la entidad. Esto, con el propósito de recuperar la mayor cantidad de información posible en caso de una emergencia o desastre. Además, es necesario mantener un inventario detallado de las cintas de respaldos y que las mismas estén debidamente rotuladas para facilitar su localización y para sustituir periódicamente por cintas nuevas, las utilizadas para respaldos.

Las situaciones comentadas impiden mantener un control adecuado de los respaldos de información y pueden ocasionar que en casos de emergencias el Instituto no pueda disponer de los respaldos de información necesarios para la continuidad de sus operaciones.

- b. No se mantenía copia de la documentación sobre las instalaciones, las configuraciones, los programas de aplicaciones y las actualizaciones realizadas a los sistemas de información, en un lugar seguro fuera de los predios del edificio donde está ubicado el Instituto.

Como norma de sana administración y de control interno, se requiere que las entidades gubernamentales mantengan una copia actualizada de los manuales de operación de los sistemas de información y de la documentación de las aplicaciones y de los programas, en un lugar seguro fuera del edificio donde radica el centro. Además, se requiere que los respaldos de información se sometan a pruebas periódicas de restauración. Esto es necesario para garantizar la continuidad de las operaciones prontamente en caso de que ocurra un evento inesperado en las instalaciones del Instituto.

La situación comentada podría afectar la continuidad de las operaciones normales del CPFI si ocurriera alguna eventualidad que afectara las instalaciones de esta y destruyera toda la documentación y los manuales que allí se almacenan.

Las situaciones comentadas en el **apartado a.1)** se debían a que la Oficial Principal de Informática no había revisado el *Procedimiento Proceso de Respaldos (Backups) del ICF* para remitirlo a la consideración de la Directora Ejecutiva, y que esta, a su vez, lo remitiera a la Junta Directora para aprobación. Además, no se aseguró de que:

- Se establecieran los controles necesarios para la protección de los respaldos. **[Apartado a.2) y 4)]**
- Se realizara diariamente el traslado de los respaldos a la caja de seguridad que el Instituto tiene contratada en la institución bancaria. **[Apartado a.3)]**
- Se mantuviera copia de la documentación relacionada con las configuraciones del sistema computadorizado, las aplicaciones y los programas utilizados, en un lugar seguro fuera de los predios del Instituto. **[Apartado b.)]**

La Directora Ejecutiva, en la carta que nos envió, informó, entre otras cosas, lo siguiente:

La Directora Ejecutiva del ICF someterá a la Junta de Directores el procedimiento de los procesos de respaldos (backups) del ICF para su debida aprobación. Se indica también, que se añadieron los tipos de respaldos mensuales y anuales a los tipos existentes (diarios y semanales) de los datos y los sistemas de información del ICF a partir de enero de 2010 en que se implantó el nuevo SAN y su nueva unidad de respaldos con capacidad superior a la unidad que se utilizaba en el ICF. Además, a partir de noviembre de 2010 se adquirió una caja de seguridad adicional en el banco con cabida para resguardar los tipos de resguardo adicionales. [src]

Hallazgo 5 - Deficiencias relacionadas con las cuentas de acceso con privilegios de administración

- a. En el Instituto existían 18 y 19 cuentas de acceso creadas dentro de los grupos Administrador (*Administrator*)² y Administradores de Dominio (*Domain Admins*)³, respectivamente. Estas cuentas tenían privilegios de administración del dominio, que permitían, entre otras cosas, acceso sin restricciones a través de los sistemas operativos, para efectuar cambios que afectan a otros usuarios, tales como: modificar la configuración de la seguridad, instalar programas y equipos, acceder a todos los archivos en un equipo y realizar cambios en las cuentas de usuarios.

El examen efectuado el 10 de julio de 2009 sobre las cuentas de acceso y los grupos creados para la administración de los servidores de la red de comunicaciones, reveló lo siguiente:

- 1) En el grupo Administrador se identificaron cuatro cuentas asignadas a personas que, por sus funciones, no deberían pertenecer a dicho grupo. Estas eran una Auxiliar de Sistemas de Oficina II, un Contratista, un empleado de una compañía de consultoría y una Programadora de Sistemas Electrónicos⁴.
- 2) En el grupo Administradores de Dominio se identificaron tres personas que, por sus funciones, no deberían pertenecer a este grupo. Estos eran una Asistente de Recursos Humanos, un empleado de una compañía de consultoría y una Programadora de Sistemas Electrónicos⁴.

² Las cuentas de acceso configuradas dentro del grupo Administrador pueden administrar y acceder sin restricciones todos los servidores principales del dominio.

³ Las cuentas de acceso configuradas dentro del grupo Administradores de Dominio pueden administrar y acceder sin restricciones a los recursos del dominio.

⁴ Los nombres de las personas con acceso, que no deberían pertenecer a este grupo, se incluyeron en el borrador de los hallazgos de este *Informe* remitido a la Directora Ejecutiva para comentarios.

En la *Política Núm. TIG-003 de la Carta Circular Núm. 77-05* se establece que las entidades gubernamentales deberán implantar controles que minimicen los riesgos de que los sistemas de información dejen de funcionar correctamente y de que la información sea accedida de forma no autorizada. Esta norma se instrumenta, en parte, mediante la asignación de privilegios a las cuentas de acceso de usuarios a base de la necesidad de los trabajos a realizar en la red.

Las situaciones comentadas podrían propiciar que personas no autorizadas puedan lograr acceso a información confidencial y hacer uso indebido de esta. Además, pueden propiciar la comisión de irregularidades y la alteración, por error o deliberadamente, de los datos contenidos en los sistemas de información, sin que puedan detectarse a tiempo para fijar responsabilidades.

Las situaciones comentadas se debían a que la Oficial Principal de Informática no se aseguró de otorgar privilegios de acceso, conforme al principio de menor privilegio, y de acuerdo con los deberes y las responsabilidades de quienes utilizan las cuentas de acceso.

La Directora Ejecutiva, en la carta que nos envió, informó, entre otras cosas, lo siguiente:

Se provee evidencia de los miembros del grupo administrador de dominio cuyos integrantes son los empleados asignados al manejo de la red [...] y los servidores adscritos a ésta. [sic]

Hallazgo 6 - Deficiencias relacionadas con los formularios para autorizar la creación, la modificación y la cancelación de las cuentas de acceso a los sistemas de información

- a. En el Instituto se utilizaba el formulario *Solicitud de Acceso a los Sistemas y Tecnologías de Información del ICF (Solicitud de Acceso)* para autorizar la creación, la modificación y la cancelación de las cuentas de acceso a los sistemas de información. En dicho formulario se requería, entre otras cosas, el nombre y el puesto de los usuarios, la fecha de solicitud para la creación de las cuentas de acceso, la fecha de autorización y procesamiento de la

solicitud, la justificación para obtener acceso a Internet, la firma del solicitante y del Director del Área a la que pertenece el empleado al que se le solicita el acceso, y la firma del Oficial Principal de Informática.

Entre el 1 de enero y el 31 de julio de 2009, se realizaron 36 transacciones de personal que incluyeron 9 nombramientos, 8 cambios de puestos regulares a puestos de confianza, 4 reinstalaciones a puestos regulares y 15 renunciaciones. Treinta y cuatro de estas transacciones correspondían a usuarios del sistema. El examen efectuado sobre el uso de los formularios *Solicitud de Acceso* para las transacciones de personal, cuyos usuarios tenían acceso al sistema, reveló lo siguiente:

- 1) No se encontró ni nos fueron suministrados para examen 20 (59 por ciento) de los 34 formularios de *Solicitud de Acceso*.
- 2) De los 14 formularios examinados, 12 (86 por ciento) no contenían la firma de la Oficial Principal de Informática y 3 (21 por ciento) no establecían el tipo de acción que se solicitaba mediante los mismos (otorgar o modificar acceso, modificar acceso temporalmente, suspender o cancelar acceso).

En el Inciso k, del Artículo VI de las *Políticas para el Uso de los Sistemas de Información del ICF*, aprobadas el 22 de diciembre de 2008 por el Director Ejecutivo, se establece que todo acceso o cuenta de acceso a los sistemas de información del Instituto de Ciencias Forenses o al uso de su infraestructura de telecomunicaciones, deberá ser petitionado a través del formulario *Solicitud de Acceso a los Sistemas y Tecnologías de Información del ICF*. El acceso deberá estar autorizado por el Director de la División u Oficina a que esté adscrito el empleado o contratado, o su representante autorizado, para que el Oficial Principal de Informática del CPEI, o su Representante, autorice el mismo. Del usuario ser un contratado, será obligatorio que se incluya la fecha de vencimiento del contrato. De igual manera, será responsabilidad del Director de la División u Oficina solicitar la modificación, eliminación, activación o desactivación de cuentas de acceso a través del formulario.

Las situaciones comentadas impiden mantener la evidencia requerida de las autorizaciones para otorgar, modificar o cancelar los accesos y los privilegios a los usuarios. También propician que personas no autorizadas puedan lograr acceso a información confidencial y hacer uso indebido de esta.

La situación comentada en el **apartado a.1)** se debía a que la Oficial Principal de Informática no se aseguró de requerirles, a los directores de división u oficina a la que esté adscrito el empleado o contratado que requiera acceso a los sistemas de información del Instituto, el formulario *Solicitud de Acceso*, debidamente autorizado por estos.

La situación comentada en el **apartado a.2)** obedece a que la Oficial Principal de Informática no se aseguró de firmar los formularios *Solicitud de Acceso*, y de velar por que estos estuvieran completados en todas sus partes, antes de proceder a la creación o modificación de las cuentas de acceso.

La Directora Ejecutiva, en la carta que nos envió, informó, entre otras cosas, lo siguiente:

La Directora Ejecutiva le instruyó a la Encargada del CPEI que no se procesen cuentas de acceso hasta que no se reciba el formulario de Solicitud de Accesos a los Sistemas de Tecnologías de Información del ICF debidamente cumplimentado. Además, instruyó al Director de Recursos Humanos (RH) a someterle al Centro de Cómputos un informe semestral de los empleados activos en el ICF. Dicho informe es utilizado en el CPEI para actualizar los usuarios autorizados en el servidor que otorga el acceso a los sistemas de tecnologías de información del ICF. Finalmente, el CPEI devuelve al Director del RH un informe como evidencia de los usuarios activos en dicho servidor. [sic]

Hallazgo 7 - Falta de procedimientos escritos para eliminar la información confidencial y los programas antes de transferir o disponer los equipos computadorizados y los medios de almacenamiento electrónico

- a. A septiembre de 2009, no se habían desarrollado procedimientos escritos para eliminar la información confidencial y los programas, grabados en los equipos computadorizados y en

Los medios de almacenamiento electrónico, antes de transferirlos o de descartar los mismos.

Estos procedimientos deben estar aprobados por la Junta Directora e incluir, entre otras cosas:

- El responsable de borrar los archivos de los equipos y de los medios de almacenamiento electrónico, a ser reutilizados o destruidos
- La metodología y las herramientas computarizadas a utilizar para asegurarse de eliminar la información de los equipos y de los medios de almacenamiento electrónico
- El procedimiento de destrucción cuando el medio de almacenamiento electrónico no será reusado.

En la *Política Núm. TIG-008, Uso de Sistemas de Información, de la Internet y del Correo Electrónico, de la Carta Circular Núm. 77-05* se establece que cada agencia debe establecer las políticas necesarias para garantizar el uso adecuado, efectivo y seguro de los sistemas de información y de las herramientas de trabajo que estos proveen. Esto implica que, como norma de sana administración, se adopten procedimientos escritos para eliminar la información confidencial y los programas, archivados en los equipos computarizados y en los medios de almacenamiento electrónico, de una forma segura que permita mantener el control de los mismos, y evitar que sean accedidos por personas no autorizadas.

La situación comentada puede propiciar que, al momento de transferir o de descartar los equipos computarizados y los medios de almacenamiento electrónico, no se considere la eliminación de la información confidencial y de los programas almacenados en los mismos. Esto, a su vez, puede propiciar que personas no autorizadas accedan a información confidencial y que la misma sea divulgada o utilizada indebidamente, lo que ocasionaría situaciones que afecten los derechos de terceros, por las cuales se responsabilice al Instituto.

La situación comentada se debía a que la Oficial Principal de Informática no se aseguró de establecer los controles de seguridad necesarios para la reutilización o disposición de los equipos y los medios de almacenamiento electrónico, que contenían información confidencial.

La Directora Ejecutiva, en la carta que nos envió, informó, entre otras cosas, lo siguiente:

El Instituto de Ciencias Forenses se rige por la Administración de Servicios Generales del Estado Libre Asociado de Puerto Rico para la Administración de Documentos Públicos, tal y como establece su Reglamento Núm. 23 (2da. Rev.) y Reglamento Núm. 4285 [...]. En la sección X de la guía para fijar períodos de conservación de los documentos fiscales del reglamento Núm. 23 se establece el período de retención de todo documento bajo la clasificación “Programas, Cintas y Otros Documentos relacionados a los Sistemas Electrónicos. [...] Además, se incluye la documentación de los procedimientos para la transferencia de activos (equipos, programados, dispositivos o medios electrónicos de almacenaje que se realizan en el CPFI y copia de la Hoja de Transferencia de Activo(s) de Tecnologías de Información. [sic]

Consideramos las alegaciones de la Directora Ejecutiva, pero determinamos que el **hallazgo** prevalece, debido a que la situación presentada en el mismo no está relacionada con los períodos de retención de documentos, establecidos en el Reglamento Núm. 23, al que hace referencia. Además, el procedimiento que se incluye como evidencia en la contestación no tenía fecha ni estaba aprobado.

ANEJO 1

**INSTITUTO DE CIENCIAS FORENSES DE PUERTO RICO
CENTRO DE PROCESAMIENTO ELECTRONICO DE INFORMACION
MIEMBROS PRINCIPALES DE LA JUNTA DIRECTORA QUE
ACTUARON DURANTE EL PERÍODO AUDITADO**

NOMBRE	CARGO O PUESTO	PERÍODO
		DESDE HASTA
Lcdo. Antonio Sagardia de Jesús	Presidente ⁵	24 feb. 09 18 nov. 09
Lcdo. Roberto J. Sánchez Ramos	"	23 dic. 08 31 dic. 08

⁵ El puesto de Presidente estuvo vacante del 1 de enero al 23 de febrero de 2009.

ANEXO 2

INSTITUTO DE CIENCIAS FORENSES DE PUERTO RICO
CENTRO DE PROCESAMIENTO ELECTRÓNICO DE INFORMACIÓN
**FUNCIONARIOS PRINCIPALES QUE ACTUARON
DURANTE EL PERÍODO AUDITADO**

NOMBRE	CARGO O PUESTO	PERÍODO
		DESDE HASTA
Dra. María S. Conte Miller	Directora Ejecutiva	16 en. 09 18 nov. 09
Dr. José F. Rodríguez Orengo	Director Ejecutivo	23 dic. 08 15 en. 09
Dr. Francisco J. Dávila Toro	Subdirector ⁶	23 dic. 08 31 dic. 08
Dra. Ida I. Rivera Meléndez	Oficial Principal de Informática	23 dic. 08 18 nov. 09

⁶ El puesto de Subdirector estuvo vacante del 1 de enero al 18 de noviembre de 2009.