**INFORME DE AUDITORÍA TI-18-13**

6 de junio de 2018

**Corporación de Seguros Agrícolas de Puerto Rico**

**Oficina de Sistemas de Información**

(Unidad 5216 - Auditoría 14050)

Período auditado: 19 de enero al 15 de diciembre de 2016

**CONTENIDO**

**Página**

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

6 de junio de 2018

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

Incluimos los resultados de la auditoría de tecnología de información que realizamos de las operaciones de la Oficina de Sistemas de Información (OSI) de la Corporación de Seguros Agrícolas de Puerto Rico (Corporación). 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; y en cumplimiento de nuestro *Plan Anual de Auditorías*.

**OBJETIVO DE AUDITORÍA**

Determinar si las operaciones de la OSI de la Corporación, en lo que concierne a los controles para la administración de la seguridad, el acceso lógico, la continuidad del servicio, los equipos computadorizados, y la entrada, el procesamiento y la salida de los datos del Sistema de Aplicación del Programa de Seguros de Seguros Agrícolas (SAPSSA), se realizaron, en todos los aspectos significativos, de acuerdo con las normas y la reglamentación aplicables; y si dichos controles eran efectivos.

**CONTENIDO DEL INFORME**

Este *Informe* contiene siete hallazgos del resultado del examen que realizamos de las áreas indicadas en la sección anterior. El mismo está disponible en nuestra página en Internet: www.ocpr.gov.pr.

**ALCANCE Y METODOLOGÍA**

La auditoría cubrió del 19 de enero al 15 de diciembre de 2016. En algunos aspectos examinamos transacciones de fechas anteriores. El examen lo efectuamos de acuerdo con las normas de auditoría del Contralor de Puerto Rico. Estas normas requieren que planifiquemos y realicemos la auditoría para obtener evidencia suficiente y apropiada que proporcione una base razonable para nuestros hallazgos y opinión.

En consecuencia, realizamos las pruebas que consideramos necesarias, a base de muestras y de acuerdo con las circunstancias, según nuestro objetivo de auditoría. Realizamos pruebas tales como: entrevistas; inspecciones físicas; exámenes y análisis de informes y de documentos generados por la unidad auditada o suministrado por fuentes externas; pruebas y análisis de procedimientos de control interno y de otros procesos; y confirmaciones de información pertinente.

En relación con el objetivo de la auditoría, consideramos que la evidencia obtenida proporciona una base razonable para nuestros hallazgos y opinión.

## INFORMACIÓN SOBRE LA UNIDAD AUDITADA

La Corporación fue creada por virtud de la *Ley Núm. 166 del 11 de agosto de 1988*[1]. Esto, con el propósito de proveerles seguros a los agricultores contra pérdida o daños a las plantaciones, las cosechas, los animales y demás estructuras y equipos para usos agrícolas en fincas rústicas[2], causados por peligros naturales como los huracanes, las sequías, los incendios y las enfermedades incontrolables.

El 4 de mayo de 1994, mediante el *Plan de Reorganización 1*, se consolidaron e integraron funciones administrativas, programas y servicios dirigidos al desarrollo de la actividad agropecuaria. Conforme a dicho *Plan*, el Departamento de Agricultura de Puerto Rico (Departamento) quedó constituido por la Administración de Servicios y Desarrollo Agropecuario de Puerto Rico (ASDA), la Autoridad de Tierras de Puerto Rico, la Corporación para el Desarrollo Rural y la Corporación.

El 29 de julio de 2010, mediante el *Plan de Reorganización 4, Plan de Reorganización del Departamento de Agricultura de 2010*, se enmendó el Artículo 2 de la *Ley Núm. 12* para proveerle a la Corporación personalidad jurídica separada y distinta del Gobierno de Puerto Rico. También se

[1] Esta *Ley* derogó el Artículo 19 y enmendó el Artículo 20 de la *Ley Núm. 12 del 12 de diciembre de 1966, Ley de Seguros Agrícolas de Puerto Rico*, según enmendada, para restructurar la Oficina de Seguros Agrícolas del Departamento de Agricultura como una corporación.

[2] Extensiones de terreno no urbanizable con casas y que generalmente comprende montes y campos, entre otros.

facultó a la Corporación para proveer seguros contra pérdidas o daños causados por incendios en las estructuras[3] y el equipo agrícola de las fincas rústicas, y por pérdidas de ingreso agrícola[4].

Los poderes de la Corporación son ejercidos por la Junta de Directores (Junta), que determina la política, los planes y los programas de la Corporación. La Junta está compuesta por el secretario de Agricultura, quien es su presidente; el decano de la Facultad de Ciencias Agrícolas del Recinto Universitario de Mayagüez de la Universidad de Puerto Rico; 1 representante del Banco Gubernamental de Fomento designado por el presidente de dicha agencia; y 2 agricultores *bona fide*, que sean patrocinadores de los seguros que provee la Corporación. Los 2 agricultores deben ser nombrados por el Gobernador por un término de 3 años cada uno y hasta que sus sucesores sean nombrados y tomen posesión del cargo.

El secretario de Agricultura deberá nombrar, con el consentimiento de la Junta, al director ejecutivo de la Corporación. Este le responde a dicha Junta. A la fecha de nuestra auditoría, la estructura organizacional de la Corporación se componía de las oficinas de Administración y Finanzas; Inspección y Ajuste en Adjuntas; Programas y Seguros Agrícolas; y Sistemas de Información. Los directores de estas oficinas respondían al director ejecutivo. Además, la Corporación contaba con personal en las oficinas regionales del Departamento ubicadas en Arecibo, Caguas, Lares, Mayagüez, Naranjito, Ponce, San German y Utuado. Mediante estas oficinas se ofrecían servicios directos a los agricultores, tales como, asesoramiento y adiestramientos sobre técnicas modernas en las diferentes empresas agrícolas. Además, este personal realizaba visitas a las fincas para asesorar a los agricultores y trabajadores agrícolas sobre prácticas

[3] Las estructuras agrícolas incluyen las edificaciones para granjas avícolas, pesca, vaquerías y porquerizas, cercas, agroindustrias, invernaderos, almacenes, alambrados, armazones o tinglados utilizados para sostener o almacenar cualquier cosecha o plantación, producto animal y pesca cubierta por una póliza de seguros.

[4] El ingreso agrícola es la remuneración recibida por la venta o disposición de bienes producidos en una unidad asegurada.

recomendadas; certificaba el uso adecuado de las ayudas e incentivos; y ofrecía seguimiento efectivo al desarrollo de las empresas para asegurar la operación eficiente del negocio agrícola.

La OSI era dirigida por un director que estaba a cargo de la planificación, dirección, coordinación y supervisión de las actividades que se realizaban en la misma, y de las relacionadas con los sistemas de información de la Corporación. Además, contaba con dos operadores de entrada de datos que colaboran en el registro de la información de las pólizas de seguro de la Corporación.

Desde el 2010, la Corporación utilizaba el SAPSSA, para mantener un registro de la información sobre los agricultores que solicitan las pólizas de seguro, y la evaluación, aprobación o denegación de estas solicitudes. Además, la Corporación utilizaba el sistema *Microsoft Dynamics Great Plains* (*Microsoft Dynamics*) para mantener los registros de contabilidad.

Los fondos para financiar las actividades de las operaciones de la Corporación provienen de los ingresos propios generados por las ventas de las primas de seguros agrícolas a los agricultores. El presupuesto asignado a la Corporación, para los años fiscales del 2013-14 al 2015-16, ascendió a $4,780,000, $4,675,000 y $4,645, 000, respectivamente.

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

La Corporación cuenta con una página en Internet a la cual se puede acceder mediante la siguiente dirección: www.csa.pr.gov. Esta página provee información acerca de los servicios que presta dicha entidad.

## COMUNICACIÓN CON LA GERENCIA

Las situaciones comentadas en los **hallazgos del 1 al 5-a. y 7** de este *Informe*, y otras situaciones determinadas durante la auditoría, fueron remitidas al Agro. Carlos E. Irrizarry Ruiz, mediante cartas de nuestros auditores, del 1 de noviembre y 22 de diciembre de 2016[5]. En las referidas cartas se incluyeron anejos con detalles sobre las situaciones comentadas.

[5] Este ocupó el puesto de director ejecutivo hasta el 15 de diciembre de 2016.

Las situaciones comentadas en los **hallazgos 5-b. y 6** de este *Informe*, fueron remitidas al Lcdo. Javier A. Lugo Rullán, director ejecutivo de la Corporación, mediante carta de nuestros auditores del 2 de febrero de 2017. En la referida carta se incluyó un anejo con detalles sobre las situaciones comentadas.

Mediante carta del 21 de noviembre de 2016 el entonces director ejecutivo contestó la carta de nuestros auditores del 1 de noviembre de 2016. Sin embargo, no contestó la del 22 de diciembre. El director ejecutivo contestó mediante carta del 2 de febrero de 2017. Los comentarios de estos se consideraron al redactar el borrador de este *Informe*.

El borrador de este *Informe* se remitió al director ejecutivo, para comentarios, por carta del 30 de abril de 2018. En el mismo se indicaron datos específicos, tales como: nombres de cuentas de acceso y de compañías, y números de propiedad.

Con el mismo propósito, remitimos el borrador de los **hallazgos** de este *Informe* al Agro. Carlos E. Irrizarry Ruiz, y del **Hallazgo 6** al Agro. Carlos M. Rodríguez Cabrera, ex directores ejecutivos, mediante cartas del 30 de abril de 2018, por correo certificado con acuse de recibo, a direcciones provistas por la Corporación.

El 15 de mayo el director ejecutivo contestó el borrador de los hallazgos de este *Informe*. En los **hallazgos** incluidos se consideraron algunos de sus comentarios.

El 5 de junio se recibió en la Oficina, devuelto por el correo, la carta que le fue remitida al agrónomo Irizarry Ruiz. El agrónomo Rodríguez Cabrera no contestó.

## CONTROL INTERNO

La gerencia de la Corporación es responsable de establecer y mantener una estructura del control interno efectiva para proveer una seguridad razonable en el logro de:

- la eficiencia y eficacia de las operaciones
- la confiabilidad de la información financiera

- el cumplimiento de las leyes y la reglamentación aplicables.

Nuestro trabajo incluyó la comprensión y evaluación de los controles significativos para el objetivo de este *Informe*. Utilizamos dicha evaluación como base para establecer los procedimientos de auditoría apropiados a las circunstancias, pero no con el propósito de expresar una opinión sobre la efectividad de la estructura del control interno de la Corporación.

En los **hallazgos** de este *Informe* se comentan las deficiencias de control interno significativas, dentro del contexto del objetivo de nuestra auditoría, identificadas a base del trabajo realizado.

Las deficiencias comentadas no contienen necesariamente todos los aspectos de control interno que pudieran ser situaciones objeto de hallazgo. Esto, debido a que dichas deficiencias fueron identificadas como resultado de la evaluación de las operaciones, los procesos, las actividades y los sistemas relacionados con el objetivo de la auditoría.

## OPINIÓN Y HALLAZGOS

### Opinión cualificada

Las pruebas efectuadas y la evidencia en nuestro poder revelaron que las operaciones de la OSI de la Corporación, en lo que concierne a los controles objeto de este *Informe*, se realizaron, en todos los aspectos significativos, de acuerdo con las normas y la reglamentación aplicables; y que dichos controles eran efectivos. Esto, excepto por los **hallazgos del 1 al 7** que se comentan a continuación.

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

**Situación**

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.

Al 27 de abril de 2016, en la Corporación no se había preparado el informe del análisis de riesgos de los sistemas de información computadorizados.

**Criterios**

La situación comentada se aparta de 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 Tecnológica para los Organismos Gubernamentales*, aprobada el 8 de diciembre de 2004 por la directora de la Oficina de Gerencia y Presupuesto (OGP); y en la *Política TIG-015, Programa de Continuidad Gubernamental*, aprobada el 22 de septiembre de 2011 por el director de la OGP[6].

**Efectos**

La situación comentada impide a la Corporación estimar el impacto que los elementos de riesgos tendrían en las áreas y en los sistemas críticos de esta, y considerar cómo protegerlos para reducir los riesgos de daños materiales y la pérdida de información. Además, dificultan desarrollar un plan de continuidad de negocios donde se establezcan las medidas de control que minimicen los riesgos previamente identificados a un nivel aceptable, y los pasos a seguir para restablecer las operaciones de la Corporación, en caso de que surja alguna eventualidad. **[Hallazgo 2-a.]**

---

[6] 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**

La situación comentada se atribuye a que el entonces director ejecutivo desconocía que debía promulgar una directriz para la preparación y la documentación del análisis de riesgos de los sistemas de información computadorizados, según lo establecido en las políticas *TIG-003* y *TIG-015*.

**Comentarios de la Gerencia**

El director ejecutivo nos indicó, entre otras cosas, que, para corregir la situación comentada, esperan preparar el análisis de riesgo al 31 de agosto de 2018.

**Véanse las recomendaciones 1 y 2.**

**Hallazgo 2 - Falta de un plan de continuidad de negocios, un plan de contingencias y un centro alterno para la recuperación de los sistemas de información**

**Situaciones**

a. Al 27 de abril de 2016, la Corporación carecía de un plan de continuidad de negocios que incluyera los planes específicos, completos y actualizados de los sistemas de información computadorizados. Esto es necesario para lograr el pronto funcionamiento de dichos sistemas y restaurar las operaciones de la Corporación, en caso de riesgos como: variaciones de voltaje, virus de computadoras, ataques maliciosos a la red, o desastres naturales, entre otros.

b. Al 26 de octubre de 2016, la Corporación carecía de un plan de contingencias que incluyera los siguientes requisitos, que son necesarios para atender situaciones de emergencia:

    - Los procedimientos a seguir cuando el centro de cómputos no pueda recibir ni transmitir información de los usuarios que acceden mediante conexiones remotas a los sistemas de información

    - La identificación de los archivos críticos de la Corporación

- Una lista detallada con todos los medios de comunicación de los diferentes miembros de cada grupo de recuperación
- El inventario actualizado de los equipos, los sistemas operativos y las aplicaciones
- El detalle de toda la configuración de los equipos críticos (equipo de comunicación y servidores) y del contenido de los respaldos, así como los nombre de las librerías y los archivos
- El detalle de toda la configuración de los sistemas de información utilizados en la Corporación y requeridos para efectuar una restauración en un centro de información alterno
- Un itinerario de restauración que incluya el orden de las aplicaciones a restablecer 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 la entidad
- Una hoja de cotejo para verificar los daños ocasionados por la contingencia.

c. Al 11 de abril de 2016, la Corporación no contaba con un centro alterno para restaurar sus operaciones críticas computadorizadas en casos de emergencia.

**Criterios**

Lo comentado en el **apartado a.** es contrario a lo establecido en la *Política TIG-003* de la *Carta Circular 77-05* y en la *Política TIG-015*.

Las mejores prácticas en el campo de la tecnología, utilizadas para garantizar la confiabilidad, integridad y disponibilidad de los sistemas de información computadorizados, sugieren que, como parte del plan de continuidad de negocios, se debe preparar un plan de contingencias. Este es una guía que garantiza la continuidad de las operaciones normales de los sistemas de información computadorizados cuando se presenten

eventualidades inesperadas que afecten su funcionamiento. El mismo debe estar aprobado por el funcionario de máxima autoridad de la entidad y debe incluir todos los procesos necesarios para recuperar cualquier segmento de la operación 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 b.]**

Además, estas prácticas 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. En dichos convenios debe incluirse 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 c.]**

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

**Efectos**

Las situaciones comentadas en los **apartados a. y b.** 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 y de interrupciones prolongadas de los servicios ofrecidos a los usuarios de la Corporación.

La situación comentada en el **apartado c.** podría afectar las funciones de la Corporación, ya que no tendría disponibles unas instalaciones para operar después de una emergencia o de un evento que afectara su funcionamiento. Esto podría atrasar o impedir el proceso de restauración de archivos y el pronto restablecimiento de las operaciones normales de la Corporación.

**Causas**

Las situaciones comentadas en los **apartados a. y b.** se atribuyen a la falta de un análisis de riesgos de los sistemas de información computadorizados de la Corporación que sirviera de base para la preparación y la revisión de un plan de continuidad de negocios, que incluyera un plan de contingencia con los requisitos necesarios para atender eventos o situaciones de emergencia. **[Véase el Hallazgo 1]**

La situación comentada en el **apartado c.** se debió a que el entonces director de sistemas de información desconocía que debían contar con un centro alterno para restaurar las operaciones críticas computadorizadas de la Corporación en casos de emergencias.

**Véanse las recomendaciones 1, 3.a. y b., y 4.**

**Hallazgo 3 - Deficiencias relacionadas con la preparación, el almacenamiento y el control de los respaldos; y falta de procedimientos para validar la integridad de los datos, y de pruebas periódicas de restauración de información**

**Situaciones**

a. Hasta el 29 de mayo de 2015, el director de Sistemas de Información utilizaba el sistema Veritas para preparar automáticamente los respaldos de las bases de datos del SAPSSA, el sistema *Microsoft Dynamics*, y el sistema de ponches ITS. Además, verificaba la integridad de los respaldos y los almacenaba en una unidad de cintas. Sin embargo, el sistema Veritas y la unidad de cintas se averiaron, por lo que estos respaldos se dejaron de realizar hasta el 1 de julio de 2016. A partir de esta fecha, los respaldos se preparaban de forma manual, mediante una copia de las bases de datos a un disco duro externo que se mantenía en el cuarto de servidores de la Oficina Central. Estos respaldos proveían una copia adicional en caso de fallas en la unidad de discos, entre los cuales se distribuían los datos.

El examen realizado sobre el proceso de preparación, almacenamiento y control de los respaldos de información reveló que, al 5 de diciembre de 2016, en la Corporación:

1) No se realizaban los respaldos semanales, mensuales y anuales ni se mantenían las cinco generaciones de respaldos, conforme a lo requerido en el *Manual de Sistemas de Información* (*Manual*), aprobado en enero de 2015 por el director ejecutivo. Solo se mantenía el respaldo de las bases de datos realizado diariamente y almacenado en el disco duro externo.

2) No se mantenían copias de los respaldos diarios fuera de la Oficina Central de la Corporación.

3) No se mantenía un registro de los respaldos diarios realizados a las bases de datos, en el cual se detallara la descripción de los archivos respaldados, el nombre del servidor donde se mantenían, la última fecha de actualización de la información, el nombre del empleado que lo realizó y las situaciones especiales ocurridas, si alguna, durante la preparación de los mismos.

b. Al 5 de diciembre de 2016, en la Corporación no se realizaban procedimientos para la verificación y validación de la integridad de los datos respaldados. Tampoco se habían realizado pruebas periódicas de restauración de los respaldos de los archivos del SAPSSA, el sistema *Microsoft Dynamics* y el sistema de ponches ITS, para verificar que se pudiera recuperar la información en caso de una falla de las aplicaciones o los equipos.

**Criterios**

La situación comentada en el **apartado a.1)** es contraria a lo establecido en la sección Procedimiento de Copias de Resguardo del *Manual*. En este se establece, entre otras cosas, que se deben realizar respaldos diarios, semanales, mensuales y anuales, y se deben mantener, por lo menos, cinco generaciones de los respaldos diarios.

Lo comentado en el **apartado a.2)** es contrario a lo establecido en la *Política ATI-003, Seguridad de los Sistemas de Información*, de la *Carta Circular 140-16*. En esta se establece que las agencias deben establecer procedimientos de respaldo recurrente de la información de los programas de aplicación y de sistemas esenciales e importantes, para las operaciones de la entidad. En consonancia con dicha *Política*, es necesario, entre otras cosas, que toda la 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 fuera de los predios de la entidad. Esto, con el propósito de que se pueda recuperar la mayor cantidad de información posible, en caso de una emergencia o desastre.

Las mejores prácticas en el campo de la tecnología de información sugieren que debe mantenerse un registro de los respaldos que identifique los archivos respaldados, y permita establecer un método de rotación adecuado. Además, sugieren que los respaldos de información se sometan a pruebas periódicas de restauración. Esto es necesario para garantizar que la información de los respaldos esté completa y disponible en caso de que ocurra un evento inesperado que requiera la utilización de los mismos. **[Apartados a.3) y b.]**

**Efectos**

Las situaciones comentadas en los **apartados a.1) y 2), y b.** pueden ocasionar que, en casos de emergencia, la Corporación no pueda disponer de los respaldos de información necesarios para la continuidad de sus operaciones; y la pérdida permanente de información importante, sin la posibilidad de recuperarla. Además, la falta de respaldos provocó que en el 2015, la Corporación tuviera que adquirir servicios técnicos por $40,691 para la recuperación de los datos del SAPSSA.

La situación comentada en el **apartado a.3)** priva a la Corporación de una herramienta que le permita identificar y controlar los respaldos; y de la documentación sobre el cumplimiento de los procedimientos establecidos en el *Manual*.

**Causas**

Las situaciones comentadas se debieron a que el director de Sistemas de Información:

- Consideraba que no se debía invertir en la reparación de la unidad de cintas, porque su utilización no resultaba costo-efectiva para la Corporación. Además, se evaluaba la posibilidad de transferir los sistemas a una nube. **[Apartado a.1)]**

- No consideró la importancia y los beneficios de mantener varias generaciones de respaldos para restaurar la información en caso de pérdida de datos. **[Apartado a.1)]**

- Entendía que la copia de respaldo realizada era suficiente para recuperar los datos, y que era riesgoso y difícil replicar los sistemas virtuales en producción para probar los respaldos. **[Apartados a.2) y b.]**

- No se había percatado de la necesidad y los beneficios de mantener un registro de respaldo. **[Apartado a.3)]**

**Comentarios de la Gerencia**

El director ejecutivo nos indicó, entre otras cosas, las medidas implementadas y las que están en proceso, para corregir las situaciones comentadas.

**Véanse las recomendaciones 1, y 3.c. y d.**

**Hallazgo 4 - Deficiencias en los parámetros de contraseñas para las cuentas de acceso del servidor principal de la Corporación**

**Situaciones**

a. La OSI contaba con un servidor principal configurado como *primary domain controller*, mediante el cual se controlaba el acceso a los recursos de la red de la Corporación. En este servidor había 111 cuentas de usuarios activas para acceder a la red.

El examen realizado el 8 de febrero de 2016 a estas cuentas reveló las siguientes deficiencias:

1) Veintitrés cuentas genéricas estaban configuradas para que la contraseña no expirara (*password expires - no*).

2) Quince cuentas genéricas estaban configuradas para que la contraseña no fuera cambiada (*password can be changed - no*).

**Criterio**

Las situaciones comentadas son contrarias a lo establecido en la *Política TIG-003* de la *Carta Circular 77-05*. En esta se establece, entre otras cosas, que las entidades gubernamentales deben implementar 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 establece, en parte, mediante la renovación de la contraseña de cada usuario, según las necesidades de la entidad y los procedimientos establecidos.

**Efectos**

Las situaciones mencionadas pueden 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 dichos sistemas sin que puedan ser detectados a tiempo para fijar responsabilidades.

**Causa**

Las situaciones comentadas se debieron a que el director de Sistemas de Información no se aseguró de que se pusieran en vigor los parámetros de contraseñas para las cuentas de acceso que proveen los sistemas operativos. Además, no había establecido procedimientos para dar mantenimiento a las cuentas de acceso genéricas utilizadas durante los períodos de ventas de seguros.

**Comentarios de la Gerencia**

El director ejecutivo nos indicó, entre otras cosas, lo siguiente:

> Todas las cuentas referenciadas en este inciso a excepción de las de SAPSSA y […], fueron inactivadas y movidas al objeto DESABILITADOS. [*sic*]
>
> Las cuentas SAPSSA son utilizadas durante el periodo de venta de seguros (1 de abril a 31 de mayo). Es al principio del periodo que las cuentas se activan nuevamente con una contraseña distinta a la utilizada el año anterior. [*sic*]
>
> Para evitar que estas queden activas luego del periodo, se procederá a crear un procedimiento operacional que contemple como manejar estas cuentas.

**Véanse las recomendaciones 1, y 3.e. y f.1).**

**Hallazgo 5 - Deficiencias relacionadas con el mantenimiento de las cuentas de acceso al SAPSSA y a las computadoras**

**Situaciones**

a. Al 8 de febrero de 2016, no se habían desactivado 21 cuentas de acceso genéricas que no eran utilizadas y permitían acceso al SAPSSA. Habían transcurrido entre 830 y 2,110 días desde su último acceso al sistema.

b. Al 29 de abril de 2016, la Corporación contaba con una red local que incluía 27 computadoras de escritorio ubicadas en la Oficina Central. Esta red era administrada por el director de Sistemas de Información, mediante un sistema operativo que permitía el establecimiento de las políticas de seguridad, y la creación de las cuentas de los usuarios y sus privilegios de acceso.

   El sistema operativo utilizado en las computadoras requería la creación de un perfil de usuario para cada cuenta de acceso utilizada y producía un registro de seguridad (*security log*), que mantenía los accesos a las computadoras y la red, y los clasificaba por tipo.

   El examen realizado el 20 de julio de 2016 a los registros mantenidos en 6 computadoras de la Corporación, reveló que en 3 de estas se utilizaron las cuentas de acceso local de 3 exempleados. Los accesos

> mediante estas cuentas ocurrieron, entre el 7 de abril de 2015 y el 12 de julio de 2016, luego de haber transcurrido entre 5 y 735 días desde la fecha de separación de estos empleados.

**Criterio**

Las situaciones comentadas son contrarias a la *Política TIG-003* de la *Carta Circular 77-05*. En esta se establece, entre otras cosas, que las entidades gubernamentales deben implementar 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 establece, en parte, mediante la inhabilitación de las cuentas de acceso genéricas, de exconsultores y de exempleados. **[Apartados a. y b.]**

**Efectos**

Las situaciones comentadas impiden a la Corporación mantener un control adecuado sobre la administración de las cuentas y del equipo de computadoras. Además, propicia que personas no autorizadas puedan utilizar estas cuentas para lograr acceso a información confidencial mantenida en los sistemas de información y hacer uso indebido de esta. También propicia la comisión de irregularidades y la alteración, por error o deliberadamente, de los datos contenidos en dichos sistemas sin que puedan ser detectados a tiempo para fijar responsabilidades.

**Causas**

Las situaciones comentadas se debieron a que los procedimientos incluidos en los manuales de sistemas de información aprobados no establecían directrices para el mantenimiento de las cuentas de exempleados, y el respaldo de los documentos mantenidos en sus perfiles de usuario, que en ocasiones eran necesarios para dar continuidad a los trabajos relacionados.

**Comentarios de la Gerencia**

El director ejecutivo nos indicó, entre otras cosas, lo siguiente:

> Las cuentas SAPSSA tienen como propósito ser utilizadas durante el periodo de venta de seguros. Puede dares el caso, de que algunas de estas permanezcan activas durante todo el año para ofrecerle a los agricultores de hortalizas la flexibidad de llenar sus seguros ya sea en la Región y/o las oficinas locales del

Departamento de Agricultura o de la CSA. Es responsabilidad del Director de Sistemas de Información o su representante, inactivar las mismas al final del periodo. [*sic*] **[Apartado a.]**

**Véanse las recomendaciones 1, y 3.f. y g.**

**Hallazgo 6 - Deficiencias en el módulo de calidad del SAPSSA**

**Situación**

a. El 30 de diciembre de 2009 la Corporación otorgó, a una compañía, el contrato *2010-000007*, por $92,055, para el desarrollo del SAPSSA, que incluía, entre otras cosas, la creación del módulo de Control de Calidad. El SAPSSA permitiría manejar el registro de ventas de pólizas de seguros agrícolas y cumplir con los parámetros de formato predefinidos para los datos y de control de calidad, establecidos por la Federal Crop Insurance Corporation (FCIC)[7].

En la propuesta presentada el 6 de abril de 2009 por la compañía, se establecía que el módulo de Control de Calidad permitiría realizar una evaluación del desempeño de los inspectores que validaban la información incluida por los agricultores en la solicitud de póliza. Para esto, el sistema seleccionaba al azar las muestras a base de los años de experiencia del inspector en la Corporación. Si el inspector tenía 3 años o menos de experiencia, el sistema debía seleccionar una muestra del 2% de los casos asignados a este, por tipo de cultivo. Si el inspector tenía más de 3 años, debía seleccionar una muestra del 2% de los casos que le habían sido asignados. Además, el módulo permitiría el registro del resultado de la evaluación y la recomendación.

Al 13 de septiembre de 2011, la Corporación había desembolsado $88,255, los cuales incluían la implementación del módulo de Control de Calidad.

El examen realizado el 14 de noviembre de 2016 sobre el funcionamiento del módulo de Control de Calidad reveló que este no identificaba correctamente el universo de inspectores contratados

[7] Agencia federal coaseguradora de los seguros de la Corporación.

> para el período examinado, y de los cuales debían seleccionarse las muestras. La cantidad total de inspectores identificados excedía los contratados para el período de inspección. Además, incluía inspectores que ya no laboraban en la Corporación.

**Criterio**

Esta situación es contraria a lo establecido en la *Política TIG-011, Mejores Prácticas de Infraestructura Tecnológica*, de la *Carta Circular 77-05*. En esta se establece que toda aplicación que se desarrolle debe tener una garantía que asegure que funciona apropiadamente, y estar de acuerdo con los propósitos para los cuales fue desarrollada.

**Efecto**

La situación comentada ocasionó que la Corporación tuviera que duplicar esfuerzos para mantener un registro adicional de las inspecciones realizadas, que le permitiera realizar manualmente los procedimientos de control de calidad requeridos por la FCIC.

**Causas**

Atribuimos la situación comentada, entre otras cosas, a que el exdirector de Sistemas de Información, que fungió como gerente de proyecto, no realizó todas las pruebas necesarias con los usuarios para asegurarse de que el módulo de Control de Calidad funcionara adecuadamente. Además, el director de Sistemas de Información no había realizado las gestiones necesarias para ver que se corrigieran las situaciones que afectaban el funcionamiento de este módulo.

**Comentarios de la Gerencia**

El director ejecutivo nos indicó, entre otras cosas, lo siguiente:

> Según nos expresara el exdirector de Sistemas, se realizaron las pruebas necesarias para este módulo según su mejor recuerdo. El exdirector de Pólizas y Seguro, confirmó que el modulo se corrió exitosamente para más de un inspector. Según ambos nos informaran, la aplicación todavía estaba en etapa de pruebas y correcciones cuando hubo el cambio de administración. […] nos comprometemos a de aquí en adelante, velar para que en futuros desarrollos trabajemos siguiendo sus recomendaciones.[…] [*sic*]

**Véanse las recomendaciones 1, y 3.h. e i.**

**Hallazgo 7 - Falta de control de los equipos computadorizados y programas de la Corporación**

**Situaciones**

a. El examen relacionado con el control de los equipos computadorizados de la Corporación reveló las siguientes deficiencias:

1) Al 29 de abril de 2016, el *Inventario de Equipo Computadorizado con valor mayor de $500* (*Inventario*) y el *Registro de Propiedad menor de $500* (*Registro*), provistos por la subdirectora de Administración y Finanzas, no estaban actualizados. Estos no incluían información de 2 servidores, 1 unidad de almacenamiento de discos y 3 *switches*, que fueron adquiridos por $66,976 el 14 de diciembre de 2009.

2) Al 25 de abril de 2016, dos *switches*, que estaban incluidos en el *Inventario* y se mantenían en el cuarto de servidor de la Oficina de Inspección y Ajuste en Adjuntas, no estaban identificados con un número de propiedad. Según el *Inventario*, estos fueron adquiridos por $2,018.

3) Al 29 de abril de 2016, el *Inventario* y el *Registro* incluían 30 impresoras y 33 computadoras portátiles asignadas a empleados de la Corporación y a los promotores contratados para contactar, orientar y vender las pólizas a los agricultores. El examen realizado el 28 de julio de 2016 reveló que en la Corporación no se mantenían los recibos por propiedad en uso de 10 impresoras y 10 computadoras, que fueron adquiridas por $15,012.

b. Al 11 de abril de 2016, el director de Sistemas de Información no proveyó para examen el registro de los programas adquiridos e instalados en cada computadora. Este registro debía incluir, entre otras cosas, el número de licencia de los programas instalados, el

nombre del usuario, el número de propiedad y la descripción de la computadora donde estaban instalados los programas, y el costo de los mismos.

**Criterios**

Las situaciones comentadas en el **apartado a.** son contrarias a lo establecido en el Artículo 10(a) de la *Ley Núm. 230 del 23 de julio de 1974, Ley de Contabilidad del Gobierno de Puerto Rico*, según enmendada. En este se establece que la custodia y el control físico de la propiedad pública será responsabilidad del jefe de la propia dependencia, el cuerpo legislativo o la entidad corporativa. Además, son contrarias a los artículos III, VI, VII, y IX, de las *Normas y Procedimientos para el Control de la Propiedad Mueble*, aprobadas el 23 de octubre de 1992 por el presidente de la Junta. En estas se establece que el encargado de la propiedad deberá:

- Llevar un registro actualizado de la propiedad, donde anotará toda la información relacionada, tal como el número de propiedad, el número de la orden de compra, el número del comprobante de pago, la descripción, el costo, el receptor, la fecha de recibo, la localización de la propiedad adquirida y las observaciones en estricto orden numérico de unidad. [Artículo VII] **[Apartado a.1]**

- Asignar un número de propiedad a cada unidad adquirida por la Corporación y marcar el equipo de la Oficina con una placa metálica. [Artículo VI] **[Apartado a.2]**

- Preparar un *Recibo de Propiedad en Uso* al entregar al custodio la propiedad adquirida, y retener el original en un archivo. [Artículo IX]. Además, conservar los recibos por propiedad en uso firmados por cada funcionario que tenga bajo su custodia un equipo. [Artículo III] **[Apartado a.3]**

La situación comentada en el **apartado b.** se aparta de lo establecido en el *Manual*. Es este se establece que el inventario de programas incluirá la cantidad de licencias instaladas en la Corporación, y que dicho inventario se realizará una vez al año. Además, es contraria a lo establecido en la *Política TIG-008, Uso de Sistemas de Información, de la Internet y del Correo Electrónico*, de la *Carta Circular 77-05*. En esta se establece que los sistemas de información de las entidades gubernamentales, incluidos los programas, las aplicaciones y los archivos electrónicos, son propiedad del Estado Libre Asociado de Puerto Rico, por lo que deben constar en el inventario de las respectivas entidades gubernamentales.

**Efectos**

Las situaciones comentadas en el **apartado a.** aumentan el riesgo de pérdida y uso indebido de la propiedad, e impiden detectar irregularidades a tiempo para fijar responsabilidades. Además, no permiten mantener registros actualizados y confiables de la propiedad existente en la Corporación.

Lo comentado en el **apartado b.** le impide a la Corporación mantener un control efectivo sobre los programas y las licencias correspondientes. Además, propicia el ambiente para la instalación y el uso de programas no autorizados, sin que se puedan detectar estas situaciones a tiempo para fijar responsabilidades, con los consiguientes efectos adversos para la Corporación.

**Causas**

La situación comentada en el **apartado a.** se atribuye en parte, a que, entre el 16 de diciembre de 2015 y el 1 de julio de 2016, la Corporación no tuvo un encargado de la propiedad y el director de Administración y Finanzas no se aseguró de mantener un inventario y los registros de propiedad completos y actualizados.

Lo comentado en el **apartado b.** se debió a que el director de Sistemas de Información no preparó un registro de los programas adquiridos e instalados en cada computadora.

**Comentarios de la Gerencia**

El director ejecutivo nos indicó, entre otras cosas, las medidas que están en proceso para corregir las situaciones comentadas.

**Véanse las recomendaciones 1, 3.j. y 5.**

## RECOMENDACIONES

**A la Junta de Directores de la Corporación de Seguros Agrícolas de Puerto Rico**

1. Ver que el director ejecutivo cumpla con las **recomendaciones de la 2 a la 5** de este *Informe*. **[Hallazgos de 1 al 7]**

**Al Director Ejecutivo de la Corporación de Seguros Agrícolas de Puerto Rico**

2. Asegurarse de que se realice y se documente un análisis de riesgos, según se establece en las políticas *ATI-003* y *ATI-015, Programa de Continuidad Gubernamental*, de la *Carta Circular 140-16*. El informe, producto de este análisis de riesgos, debe ser remitido para revisión y aprobación de la Junta. Una vez aprobado, ver que se revise cada vez que surja un cambio significativo dentro de la infraestructura operacional y tecnológica de la Corporación, para asegurarse de que se mantenga actualizado. **[Hallazgo 1]**

3. Ejercer una supervisión efectiva sobre el director de Sistemas de Información, para asegurarse de que:

    a. Prepare un plan de continuidad de negocios que cumpla con lo requerido en las políticas *ATI-003* y *ATI-015* de la *Carta Circular 140-16*. Este plan debe ser remitido para la revisión y aprobación de la Junta. Una vez sea aprobado, asegurarse de que se mantenga actualizado y se conserve copia en un lugar seguro fuera de los predios de la Corporación. Además, asegurarse de que se distribuya a los funcionarios y a los empleados concernientes, y de que se realicen pruebas periódicas para garantizar su efectividad. **[Hallazgo 2-a.]**

b. Prepare un plan de contingencias que incluya los aspectos comentados en el **Hallazgo 2-b.**

c. Implemente una metodología costo-efectiva que permita mantener los respaldos necesarios para garantizar la disponibilidad de los datos en caso de emergencia. Además, se asegure de que los respaldos se mantengan en un lugar externo, el sistema de respaldo utilizado provea controles que validen la integridad de los datos, y se realicen pruebas periódicas a estos. **[Hallazgo 3-a.1) y 2), y b.]**

d. Mantenga un registro de los respaldos diarios realizados a las bases de datos, que incluya los criterios comentados en el **Hallazgo 3-a.3).**

e. Vea que las políticas de seguridad configuradas se apliquen a las cuentas de usuarios activos de la red para que sus contraseñas expiren y puedan ser cambiadas. **[Hallazgo 4-a.]**

f. Revise el *Manual* para incluir los procedimientos necesarios para la creación, el mantenimiento y el control de las cuentas de acceso a los sistemas en producción, la red e Internet. Además, se asegure de que el procedimiento considere:

   1) Las directrices para dar mantenimiento a las cuentas de acceso genéricas para el SAPSSA, que son utilizadas durante el período de la venta de seguros. **[Hallazgo 4-a. y 5-a.]**

   2) Las directrices para respaldar la información mantenida en los perfiles de usuario de los exempleados, que sea necesaria para dar continuidad a las labores relacionadas, y desactivar sus cuentas de acceso al dominio y a las computadoras. **[Hallazgo 5-b.]**

g. Desactive las cuentas de acceso genéricas que se comentan en el **Hallazgo 5-a.** Además, vele por que, en lo sucesivo, dichas cuentas y los perfiles de sus usuarios se desactiven en el momento en que no sean necesarias.

h. Vea que, cuando se realicen desarrollos o cambios a las aplicaciones, se efectúen pruebas con los usuarios para comprobar el funcionamiento correcto de estos. **[Hallazgo 6]**

i. Establezca los controles de validación necesarios y vele por que se corrijan las fallas en la programación que propician la situación comentada en el **Hallazgo 6**.

j. Mantenga un registro de los programas adquiridos por la Corporación e instalados en las computadoras. Este registro debe incluir, entre otra información, el número de la licencia y el costo de los programas instalados, el nombre del usuario, y el número de propiedad y la descripción de la computadora donde están instalados los mismos. Esto, con el fin de mantener un inventario de los mismos y detectar la instalación de programas no autorizados. **[Hallazgo 7-b.]**

4. Formalizar un acuerdo escrito con un centro alterno que acepte la utilización de sus respectivos equipos en casos de desastres o emergencias en la Corporación, o considerar establecer su propio centro alterno en alguna de sus instalaciones que no esté expuesta a los mismos riesgos que el lugar donde se encuentra la OSI. **[Hallazgo 2-c.]**

5. Ejercer una supervisión efectiva sobre el director de Administración y Finanzas, para asegurarse de que cumpla con lo establecido en la *Ley Núm. 230* y en las *Normas y Procedimientos para el Control de la Propiedad Mueble*, relacionado con el control y manejo de los equipos de computadoras. Además, designe a un encargado de la propiedad para que mantenga los registros de propiedad completos y actualizados. **[Hallazgo 7-a.]**

**APROBACIÓN**

A los funcionarios y a los empleados de la Corporación, les exhortamos a velar por el cumplimiento de la ley y la reglamentación aplicables, y a promover el uso efectivo, económico, eficiente y ético de los recursos del Gobierno en beneficio de nuestro Pueblo. Les agradecemos la cooperación que nos prestaron durante nuestra auditoría.

Oficina del Contralor de Puerto Rico

Aprobado por:

**ANEJO 1**

CORPORACIÓN DE SEGUROS AGRÍCOLAS DE PUERTO RICO
OFICINA DE SISTEMAS DE INFORMACIÓN

**MIEMBROS PRINCIPALES DE LA JUNTA DE DIRECTORES DURANTE EL PERÍODO AUDITADO**

| NOMBRE | CARGO O PUESTO | PERÍODO | |
|---|---|---|---|
| | | DESDE | HASTA |
| Dra. Myrna Comas Pagán | Presidenta | 19 ene. 16 | 15 dic. 16 |
| Sra. Marisol Suárez Cruz | Secretaria[8] | 19 ene. 16 | 30 sep. 16 |

[8] Este puesto estuvo vacante del 1 de octubre al 15 de diciembre de 2016.

**ANEJO 2**

CORPORACIÓN DE SEGUROS AGRÍCOLAS DE PUERTO RICO
OFICINA DE SISTEMAS DE INFORMACIÓN

**FUNCIONARIOS PRINCIPALES DE LA ENTIDAD DURANTE EL PERÍODO AUDITADO**

| NOMBRE | CARGO O PUESTO | PERÍODO | |
|---|---|---|---|
| | | DESDE | HASTA |
| Agro. Carlos E. Irizarry Ruiz | Director Ejecutivo | 19 ene. 16 | 15 dic. 16 |
| Sr. Iván R. Castañer Santos | Director de Administración y Finanzas | 19 ene. 16 | 15 dic. 16 |
| Sr. Mariano III Argüelles Ramos | Director de Sistemas de Información[9] | 1 jul. 16 | 15 dic. 16 |
| Sr. Noel A. Herrera Mena | " | 19 ene. 16 | 18 may. 16 |

[9] Este puesto estuvo vacante del 19 de mayo al 30 de junio de 2016.

**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-18-19* del 27 de abril de 2018, 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, extensiones 2801 o 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