INFORME DE AUDITORÍA TI-14-07

25 de enero de 2014

Departamento de Estado

Sistemas de Información Computadorizados

(Unidad 5265 - Auditoría 13657)

Período auditado: 1 de septiembre de 2011 al 9 de marzo de 2012

CONTENIDO

Página

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

25 de enero de 2014

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

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

ALCANCE Y METODOLOGÍA

La auditoría cubrió del 1 de septiembre de 2011 al 9 de marzo de 2012. 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, tales como: entrevistas; examen y análisis de informes y de documentos generados por la unidad auditada o suministrados por fuentes externas; examen y análisis asistidos por herramientas computadorizadas (*CAATs*, por sus siglas en inglés); y confirmaciones de información pertinente.

CONTENIDO DEL INFORME

Este es el tercer y último informe, y contiene 4 hallazgos sobre el resultado del examen que realizamos al acuerdo de prestación de servicios en la

nube *(Cloud Computing)*[1], tipo *Software as a Service (SAAS)*[2], para la División de Corporaciones del Departamento. En el **ANEJO 1** presentamos información sobre los 2 informes emitidos sobre las operaciones de la Oficina de Tecnología Cibernética (OTC) y de los sistemas de información computadorizados del Departamento. Los 3 informes están disponibles en nuestra página en Internet: www.ocpr.gov.pr.

INFORMACIÓN SOBRE LA UNIDAD AUDITADA

El Departamento es una agencia del Gobierno creada por la Sección 6 del Artículo IV de la Constitución. En la Constitución y en la *Ley Núm. 6 del 24 de julio de 1952* se establece el cargo de Secretario de Estado, quien es nombrado por el Gobernador con el consejo y consentimiento del Senado y de la Cámara de Representantes. Este dirige el Departamento.

El Departamento tiene la responsabilidad de fomentar las relaciones culturales, políticas y económicas entre Puerto Rico y países extranjeros, al igual que con otras jurisdicciones de los Estados Unidos de América. Además, realiza diversas funciones de carácter administrativo, tales como:

- Promulgar, publicar, certificar y vender las leyes y los reglamentos del Gobierno de Puerto Rico.
- Reglamentar el uso de la bandera y del escudo de Puerto Rico.
- Expedir licencias para el ejercicio de profesiones u oficios reglamentados por el Estado a través de las juntas examinadoras.
- Preparar y custodiar diversos registros, tales como: cónsules, corporaciones y sociedades, marcas de fábrica, notarios, y propiedad intelectual, entre otros.

[1] Es un modelo para habilitar acceso por demanda a un conjunto compartido de recursos computadorizados, entre estos, redes, servidores, almacenamiento, aplicaciones y servicios, que pueden estar disponibles rápidamente con un esfuerzo mínimo de administración o de interacción con el proveedor de servicios. Las características principales de este modelo son auto-servicio por demanda, acceso amplio desde la red, conjunto de recursos disponibles para varios consumidores, rápida elasticidad de recursos de acuerdo a la necesidad, y servicio medido.

[2] Es uno de los tres modelos de *Cloud Computing* en el que el consumidor utiliza las aplicaciones del proveedor en una infraestructura de nube. Las aplicaciones pueden ser accedidas desde diferentes dispositivos a través de interfaces de cliente.

- Tramitar la solicitud de pasaportes de los ciudadanos de los Estados Unidos, tarea delegada por el Gobierno Federal.
- Coordinar los asuntos de índole protocolar que competen al Gobierno.

Al Secretario de Estado le responde un Subsecretario. A este, a su vez, le responde: el Director de Asuntos Legales y Nombramientos, el Director de Auditoría Interna[3], y los secretarios auxiliares de:

- Asuntos de Gobierno
- Asuntos Protocolares y de Comunicación y Prensa
- Relaciones Exteriores
- Administración[4]
- Juntas Examinadoras
- Servicios[5]

Las operaciones diarias se llevan a cabo desde dos edificios localizados en el Viejo San Juan: Real Intendencia y Diputación Provincial. El servicio al ciudadano se presta a través del Centro Único de Servicios (CUS) ubicado en el edificio Diputación Provincial, y de las oficinas localizadas en Hato Rey, Arecibo, Guayama y Mayagüez.

Del 2006 al 2009, el Departamento comenzó a ofrecer a los ciudadanos los servicios de búsqueda en línea para los siguientes registros: Corporaciones,

---

[3] Este puesto quedó vacante el 31 de octubre de 2009 por la implantación de la *Ley 7-2009, Ley Especial Declarando Estado de Emergencia Fiscal y Estableciendo Plan Integral de Estabilización Fiscal para Salvar el Crédito de Puerto Rico*, según enmendada. Al momento de nuestra auditoría, el Departamento contaba con servicios de auditoría provistos por auditores del Departamento de Recreación y Deportes, según el acuerdo interagencial 2011-000013 del 11 de agosto de 2010.

[4] Esta Secretaría tiene bajo supervisión las siguientes cinco oficinas: Recursos Humanos, Compras, Presupuesto y Finanzas, OTC, y Servicios Generales, Transportación y Seguridad.

[5] Esta Secretaría tiene bajo su supervisión las siguientes cinco oficinas: CUS, Registro de Transacciones Comerciales, Registro de Marcas y Nombres Comerciales, Registro de Corporaciones, y Certificaciones y Reglamentos.

Juntas Examinadoras, Reglamentos, y Marcas y Nombres Comerciales. A partir del 2010, el ciudadano puede efectuar los siguientes procesos, a través de la página en Internet del Departamento:

- Registrar una corporación.
- Remitir el Informe Anual de Corporaciones.
- Solicitar o validar el certificado de *good standing*.
- Registrar marcas y nombres comerciales.

La OTC del Departamento cuenta con un Director, quien supervisa y dirige las funciones que se realizan en esta Oficina, y a este le asiste un Especialista en Tecnología Cibernética. La infraestructura tecnológica del Departamento consiste en una red de área amplia que agrupa 4 redes de área local, compuesta por 16[6] servidores que se intercomunican a través de *routers*[7], *switches*[8] y líneas dedicadas T1. El acceso a Internet es provisto a través de una conexión que mantiene el Departamento con la Oficina de Gerencia y Presupuesto (OGP). Además, el Departamento comparte información del Registro de Transacciones Comerciales y el de Corporaciones con 2 proveedores de servicio externo.

El **ANEJO 2** contiene una relación de los funcionarios principales del Departamento que actuaron durante el período auditado.

Los gastos operacionales de la OTC eran sufragados del presupuesto operacional del Departamento, que para los años fiscales del 2008-09 al 2010-11 fue de $14,513,000, $11,211,000 y $10,110,000, respectivamente.

El Departamento cuenta con una página en Internet, a la cual se puede acceder mediante la siguiente dirección: www.estado.gobierno.pr. Esta página provee información acerca de los servicios que presta dicha entidad.

---

[6] Uno de estos servidores pertenece a una compañía privada.

[7] Dispositivos que distribuyen tráfico entre redes. La decisión sobre a dónde enviar los datos se realiza a base de la información de nivel de red y las tablas de direccionamiento.

[8] Dispositivos de comunicación central que conectan dos o más segmentos de red y permiten que ocurran transmisiones simultáneas, sin afectar el ancho de banda de la red para una comunicación más eficiente.

COMUNICACIÓN CON LA GERENCIA

Las situaciones comentadas en los **hallazgos** de este *Informe* fueron remitidas al Sr. Kenneth McClintock Hernández, entonces Secretario de Estado, mediante carta de nuestros auditores, del 21 de marzo de 2012. En la referida carta se incluyeron anejos con detalles sobre las situaciones comentadas.

Mediante carta del 30 de marzo de 2012, el entonces Secretario de Estado contestó la comunicación de nuestros auditores. Sus comentarios fueron considerados al redactar el borrador de este *Informe*.

El borrador de los **hallazgos** de este *Informe* se remitió al Hon. David E. Bernier Rivera, Secretario de Estado, y al ex-Secretario de Estado, por cartas del 7 de mayo de 2013. En este se indicaron datos específicos que por seguridad no se incluyen en este *Informe*.

El 6 de junio de 2013 el Sr. Javier B. González Arroyo, Secretario de Estado Interino, contestó el borrador de los **hallazgos** de este *Informe*. Sus comentarios fueron considerados en la redacción final de este *Informe*, y se incluyen en la sección titulada **OPINIÓN Y HALLAZGOS**.

El 7 de junio de 2013 el ex-Secretario de Estado contestó el borrador de los **hallazgos** de este *Informe*. Sus comentarios fueron considerados en la redacción final de este *Informe*.

OPINIÓN Y HALLAZGOS

Las pruebas efectuadas revelaron que las operaciones relacionadas con los sistemas de información computadorizados del Departamento; en lo que concierne al acuerdo de prestación de servicios en la nube *(Cloud Computing)*, tipo *Software as a Service (SAAS)*, para la División de Corporaciones del Departamento; se realizaron sustancialmente conforme a las normas generalmente aceptadas en este campo, excepto por los **hallazgos del 1 al 4** que se comentan a continuación.

Hallazgo 1 - Información incompleta en los informes provistos por la compañía contratada, y falta de acceso a información que permita realizar una reconciliación completa, correcta y oportuna del total de transacciones procesadas por la compañía y las modificaciones realizadas

Situaciones

a. En enero de 2009 el Departamento buscaba alternativas para poner al día los atrasos en el Registro de Corporaciones, el Archivo de Corporaciones y el área de Informes Anuales de la División de Corporaciones.

En febrero de 2009, durante la Convención Nacional de Secretarías de Estados, el Secretario advino en conocimiento del servicio especializado de plataforma[9] en línea que ofrecía una compañía. Luego de evaluar la propuesta presentada por esta, el Secretario determinó contratarla para agilizar y mejorar los servicios corporativos provistos, hasta entonces, por personal del Departamento. Durante el proceso, no se evaluaron propuestas adicionales.

El 16 de diciembre de 2009, mientras se negociaba el contrato con la compañía, se aprobó la *Ley 164-2009, Ley General de Corporaciones*[10] *(Ley)*, según enmendada. Esta *Ley*, entre otras cosas, establecía:

- los derechos a cobrar por la radicación de documentos corporativos
- la distribución de los fondos generados a una cuenta especial del Departamento de Estado y al Fondo General.

Durante los primeros 5 años de vigencia de la *Ley*, el 40% de las cantidades recaudadas por concepto de la radicación de documentos corporativos ingresaría en una cuenta especial del Departamento. Estos fondos se utilizarían para actualizar y mejorar los servicios

[9] Equipos y programas computadorizados que permiten la prestación de los servicios.

[10] Esta derogó la *Ley 144-1995*.

provistos por la División de Corporaciones, y sufragar parte de los costos de digitalización y mecanización del Registro de Corporaciones. El restante 60% ingresaría al Fondo General. Al cumplirse el término de 5 años, la *Ley* dispone que el 100% de las cantidades recaudadas ingresarán al Fondo General.

El 18 de diciembre de 2009 el Departamento formalizó el contrato 2010-000051 con la compañía. Este estaría vigente por cinco años a un costo estimado de $4,914,532.

En el contrato se establecían, entre otras, las siguientes disposiciones:

- Todos los honorarios por transacción asociados al uso de la aplicación y al servicio prestado por la compañía, serán cobrados y remitidos al Departamento por la compañía. En caso de que el contrato fuese enmendado, y la compañía no fuera responsable del cobro y la remisión de estos honorarios, entonces la compañía se reserva el derecho de suspender el acceso y el uso del sistema al Departamento, cuando queden deudas pendientes con la compañía que excedan los 30 días. En cuyo caso, el Departamento no responsabilizaría a la misma por la suspensión del servicio. **[Artículo 3.8.1]**

- Cualquiera de las partes puede terminar el contrato por causa de una violación contractual material, mediante notificación escrita a la otra con 30 días consecutivos de anticipación. La notificación debe establecer en detalle la causa del incumplimiento. Esto con el propósito de darle a la parte que incumplió la oportunidad de remediar la situación. De no subsanarse el incumplimiento, se dará por terminado el contrato. Terminado el contrato, el Departamento no tendrá derecho a utilizar el servicio. Además, si el contrato se termina previo a lo estipulado, el Departamento acuerda que la compañía recibirá todos los honorarios pendientes de pago hasta la fecha de la terminación. **[Artículo 3.8.3]**

- El Departamento podía cancelar el contrato si el Gobernador del Estado Libre Asociado de Puerto Rico que estaba al momento de la firma del mismo no era reelecto en las elecciones generales de 2012. En este caso, el Departamento podía ejercer su derecho a cancelar mediante notificación escrita a la compañía, en un período de 180 días consecutivos posterior a la toma de posesión del nuevo Gobernador. Luego de esto, la cancelación no es posible. **[Artículo 3.8.5]**

- Como resultado del modelo de costo por transacción, el Departamento acuerda y entiende que la cancelación del contrato, previo a la fecha de expiración, causaría daños sustanciales que no permitirían a la compañía recuperarlos. Es por esto, que las partes acordaron establecer que el Departamento pagaría $200,000 a la compañía por concepto de daños por la terminación temprana del contrato. Esta cantidad no se consideraría una cláusula penal y sería pagadera dentro de diez días de la fecha de efectividad de la cancelación o terminación del contrato. **[Artículo 3.10]**

Los honorarios por transacciones procesadas, entre otros cargos por servicios pagaderos a la compañía contratada, se estipularon en el Anejo 2, *Services Transactional Fees and Payment Processing Schedule*, del contrato. Además, en este se estipuló que los recaudos corporativos procesados mediante la aplicación en línea serían depositados en una cuenta separada creada por la compañía contratada. Al final de cada mes, de esta cuenta se deducirían todos los cargos por servicio, tales como: bancarios, de procesamiento y los asociados con las tarjetas de crédito, entre otros. El detalle de los recaudos corporativos y de los costos de procesamiento asociados se incluirían en el informe *Monthly Transaction Report*[11] *(Informe)*.

El 5 de febrero de 2010 la Subsecretaria de Estado formalizó la Enmienda A del Contrato. Esto, con el propósito de delegar a la

[11] El informe es provisto al Departamento con el nombre de *Summary Transaction Report*.

compañía contratada la compra del equipo computadorizado que utilizarían para la implantación del servicio en línea. El costo del equipo adquirido ascendió a $64,200.

El 15 de marzo de 2010 se implantó, en ambiente de producción, el *Portal de Servicios Corporativos en Línea (Portal)* para efectuar búsquedas de las corporaciones registradas en el Departamento y para la radicación electrónica de los informes anuales[12]. El acceso al *Portal* está disponible, mediante el enlace https://prcorpfiling.f1hst.com, en la página en Internet del Departamento. En abril de 2010 se implantó el servicio electrónico de pago de derechos anuales de las compañías de responsabilidad limitada; en octubre de 2010 la solicitud de los certificados de cumplimiento corporativo *(good standing)*; y en mayo de 2011 la creación de nuevas corporaciones.

Del 28 de diciembre de 2010 al 25 de octubre de 2011, se formalizaron las enmiendas B[13], C[14] y D[15] del Contrato con el propósito de que la compañía contratada proveyera al Departamento servicios relacionados con el procesamiento y la digitalización de documentos anteriores[16] *(back file services)*. Los costos asociados a estas enmiendas ascendían a $5,809,365.

En el inciso 3 del Anejo 2 del contrato 2010-000051, según enmendado, se establecía que la compañía contratada proveería al Departamento, al final de cada mes, un informe con el total de

---

[12] El sistema en línea inició con el procesamiento de los informes anuales correspondientes al año 2009. Los ciudadanos interesados en presentar los informes corporativos de años previos debían radicarlos, personalmente, en el Departamento.

[13] Sustituyó el Anejo 2 del contrato para disponer un costo adicional de $1,756,504.

[14] Modificó los costos de los servicios incluidos en la Enmienda B para establecer una cuantía máxima de $3,750,549 ($1,756,504 por los costos establecidos en la enmienda B y $1,994,045 por costos adicionales correspondientes a documentos identificados que no fueron incluidos en el estimado inicial de la Enmienda B).

[15] Sustituyó los Anejos 1, 2 y 3 de la Enmienda C para incluir trabajos relacionados con el Registro de Marcas por $2,058,816.

[16] Estos eran los informes anuales correspondientes a los años del 2006 al 2009.

transacciones. Este informe incluiría el total de recaudos en la cuenta creada por la compañía contratada e información de todas las deducciones aplicables asociadas al uso del sistema.

Además, en el mismo inciso se establecía que cualquier reclamación relacionada con la información presentada en el informe de transacciones, debía ser notificada por el Departamento a la compañía contratada dentro de los 10 días de recibido el mismo. Esto, con el propósito de que ambas partes identificaran y resolvieran cualquier diferencia que causase la reclamación.

Del 1 de enero al 30 de noviembre de 2011, el total de recaudos por derechos corporativos ascendió a $9,886,743. De estos, $6,869,327[17] (69%) ingresaron directamente a la cuenta creada por la compañía contratada, y $3,017,416 (31%) se recaudaron mediante la emisión de comprobantes de pago[18] del Departamento de Hacienda.

La Oficial de Preintervenciones de la Oficina de Finanzas[19] del Departamento era la persona responsable de reconciliar las transacciones corporativas que se procesaban a través del *Portal*. Para esto, utilizaba los informes contenidos en un CD-R que enviaba mensualmente la compañía contratada.

La Directora de Finanzas de la compañía contratada preparaba los informes que recibía el Departamento. Además, esta notificaba al *Support Desk Staff* de la compañía contratada sobre las transacciones rechazadas *(declined transactions)* por el sistema electrónico de pago

[17] En los informes mensuales *Summary Transaction Report*, provistos por la compañía, las transacciones eran segregadas de acuerdo al método de pago utilizado al momento de procesarlas. Una transacción cuyo costo fue sufragado mediante el uso de dos o más métodos de pago (tarjeta de crédito, ACH, *voucher*) era incluida igual número de veces en el informe. Debido a esto, nuestros auditores no pudieron determinar el número de transacciones procesadas durante dicho período, a excepción del mes de abril, cuyos informes fueron provistos para examen por la Oficina de Finanzas del Departamento.

[18] Estos eran los derechos corporativos cuyo pago se efectuaba en una colecturía del Departamento de Hacienda, quién le emitía un comprobante de pago.

[19] Esta estaba adscrita a la Secretaría de Administración del Departamento.

del banco y de aquellas que fueron canceladas a solicitud del cliente, para que estos realizaran los ajustes correspondientes en la base de datos del sistema.

Junto al CD-R, la compañía contratada enviaba un cheque del sobrante de los recaudos corporativos cobrados, luego de haber descontado los cargos correspondientes a sus honorarios.

El 22 de junio de 2011 la compañía contratada preparó el CD-R correspondiente a abril de 2011. Este contenía, entre otros informes, el *April 2011 Summary Transaction Report*, el cual reveló que la compañía contratada cobró $4,318,135 (59%) de los $7,288,307 recaudados por concepto de transacciones corporativas. El detalle de las transacciones asociadas a estos recaudos se incluyó en el informe *Payment & Invoice Item*.

El examen realizado de los informes contenidos en el CD-R, reveló que el informe *Payment & Invoice Item* no incluía el detalle de 3,541 recibos de una serie de 52,757 recibos. De los 3,541 recibos no incluidos, 880 se identificaron en el informe de transacciones declinadas o rechazadas por los bancos, 17 estaban incluidos en 2 informes de transacciones de pago acreditado, cancelado o devuelto, y los restantes 2,644 no estaban incluidos en ninguno de los informes contenidos en el CD-R.

b. La Oficial de Preintervenciones no tenía acceso a un informe en pantalla, a través del área de Administración del *Portal*, que incluyera el detalle de todas las radicaciones y las solicitudes electrónicas que generaban recaudos a través del *Portal*. Esto, con el propósito de corroborar oportunamente la veracidad y la exactitud de los informes de transacciones procesadas provistos por la compañía contratada, y de los ajustes realizados por esta.

Criterio

Las situaciones comentadas son contrarias a lo establecido en la *Política TIG-011, Mejores Prácticas de Infraestructura Tecnológica de la Carta Circular 77-05, Normas sobre la Adquisición e Implantación de los*

Sistemas, Equipos y Programas de Información Tecnológica para los Organismos Gubernamentales, aprobada el 8 de diciembre de 2004 por la Directora de la Oficina de Gerencia y Presupuesto. En esta se dispone que las agencias deberán establecer metodologías para asegurar la integridad y la confiabilidad de los datos producidos y almacenados en sus sistemas. Estos datos son vitales para la toma de decisiones tanto para la agencia como para el desarrollo de estrategias que benefician los servicios ofrecidos por el Gobierno del Estado Libre Asociado de Puerto Rico.

Efectos

Las situaciones comentadas restaban confiabilidad al procesamiento de las transacciones corporativas registradas. Además, impidieron al Departamento ejercer un control adecuado sobre estas transacciones, al no contar con la información necesaria para realizar una reconciliación completa, correcta y oportuna. Esto, a su vez, podría propiciar que el Departamento no reciba los ingresos que le corresponden, entre otros efectos adversos.

Causa

Las situaciones comentadas se debían a que el Secretario Auxiliar de Servicios no había requerido a la compañía contratada proveer la información necesaria que le permitiera, en coordinación con la Secretaria Auxiliar de Administración, establecer los mecanismos de control para que la Oficina de Finanzas del Departamento realice una reconciliación efectiva de los recaudos corporativos.

Comentarios de la gerencia

En la carta del Secretario, este indicó, entre otras cosas, lo siguiente:

> Esta es una situación que habíamos detectado en el proceso de administración del Servicio en Línea y para el cual hemos comenzado a evaluar la adopción de un mecanismo de control que nos permita monitorear y conciliar las transacciones y la facturación de los servicios en línea. En el Departamento de Estado ya se han comenzado los procesos necesarios para llevar a cabo una conciliación efectiva del servicio contratado. [*sic*]

Véanse las recomendaciones de la 1 a la 2.b.

Hallazgo 2 - Faltas de control relacionadas con las cuentas de acceso creadas en el área de Administración del Portal

Situaciones

a. El Secretario Auxiliar de Servicios del Departamento era el responsable de autorizar la creación de las cuentas de acceso que se otorgaban al área de Administración del *Portal*. A estas cuentas se le asignaba uno de los siguientes privilegios:

- acceso de consulta *(read-only)*
- creación y modificación de comprobantes de pagos e ingreso de informes anuales previos
- edición de la información básica corporativa.

El examen realizado el 22 de febrero de 2011 de 45 cuentas con acceso al área de Administración del *Portal* y de los privilegios otorgados a estas, reveló las siguientes faltas de control:

1) El Secretario Auxiliar de Servicios no contaba con una lista completa y correcta de las cuentas creadas. En su lugar, certificó la existencia de 17 de estas, de las cuales a 5 (29%) las identificó incorrectamente.

2) El Especialista en Tecnología Cibernética y nueve empleados de la compañía contratada tenían asignadas cuentas de acceso con privilegio para crear y modificar comprobantes de pagos e ingresar informes anuales previos, tareas que no eran compatibles con las funciones ejercidas por estos usuarios.

3) El Gerente de Proyecto de la compañía contratada y su ayudante tenían asignado cuentas de acceso con privilegio de edición de la información básica corporativa. Esto les permitiría modificar la clase y el tipo de corporación, lo cual, a su vez, determina el importe de honorarios que descuenta la compañía contratada de los recaudos corporativos.

Criterios

La situación comentada en el **apartado a.1)** es contraria a lo establecido en el Artículo 2.3 del contrato, en el cual se establece que el Departamento será responsable, entre otros, por el uso de las cuentas de acceso.

Las situaciones comentadas en el **apartado a.2) y 3)** son contrarias a lo establecido en la *Política TIG-003, Seguridad de los Sistemas de Información* de la *Carta Circular 77-05*. En esta 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. Además, se establece que la información y los programas de aplicación utilizados en las operaciones de la agencia deberán tener controles de acceso para su utilización, de manera que solamente el personal autorizado pueda ver los datos que necesita, o usar las aplicaciones (o parte de las aplicaciones) que necesita.

En la *Política* también se dispone que las entidades gubernamentales deberán establecer controles adecuados en sus sistemas de información computadorizados para garantizar la confidencialidad, la integridad y la disponibilidad de la información. Conforme a dicha *Política* y como norma de sana administración, es necesario que se establezca la supervisión de las tareas conflictivas como control. El objetivo primordial de dichas medidas de control es disminuir la probabilidad de que se cometan errores o irregularidades.

Además, en esta *Política* se establece que la seguridad de los sistemas de información, aun cuando el manejo y el control de parte o de todos los procesos han sido delegados a un tercero, son responsabilidad de las agencias.

Efecto

Las situaciones comentadas pueden propiciar errores o irregularidades relacionados con el procesamiento de los comprobantes de pago o con la información corporativa, sin que estos puedan detectarse con prontitud, con los consiguientes efectos adversos para el Departamento.

Causas

Las situaciones comentadas obedecen, principalmente, a que el Secretario Auxiliar de Servicios no había desarrollado, ni remitido para la consideración del Secretario, las normas y los procedimientos necesarios para controlar el proceso de creación, modificación o eliminación de cuentas con acceso al *Portal*, particularmente al área de Administración, y de los privilegios otorgados a la base de datos corporativa.

Además, las situaciones comentadas en el **apartado a.2) y 3)** se debían a que el Departamento no contaba con las herramientas de monitorear necesarias para ejercer una supervisión efectiva sobre las cuentas de acceso y los privilegios otorgados a estas, y de las transacciones realizadas por los usuarios, según se comentó en el **Hallazgo 1-b.**

Comentarios de la gerencia

En la carta del Secretario, este indicó, entre otras cosas, lo siguiente:

> Entendemos y aceptamos el señalamiento, por lo que hemos impartido instrucciones al Secretario Auxiliar para analizar las cuentas de acceso y limitar las mismas a las áreas estrictamente compatibles con las funciones ejercidas por los usuarios. [*sic*]

Véanse las recomendaciones 2.c., y 3.a. y b.

Hallazgo 3 - Faltas de control relacionadas con la información corporativa y los documentos digitalizados que se accedían a través del Portal

Situaciones

a. En la enmienda B del contrato 2010-000051 se estableció que la compañía proveería al Departamento los servicios de *back file services*. Esto, con el propósito de actualizar el Registro de Corporaciones.

   En la Sección 4.14 de la propuesta de esta enmienda se estableció que la compañía contratada importaría los datos y las imágenes periódicamente. El Departamento debía proveer al Gerente de Proyecto de la compañía contratada, dentro de 30 días consecutivos, una lista de errores o de información no incluida en el Registro de Corporaciones conforme a la revisión realizada por la entidad

gubernamental. Los costos asociados a cualquier error identificado durante este período serían deducidos como porcentaje del total de registros incluidos en los entregables[20]. Al concluir los 30 días, los datos e imágenes incluidos en el sistema serían aceptados como correctos, por lo que cualquier esfuerzo adicional de la compañía contratada para corregir los datos, sería considerado una orden de cambio.

El 14 de enero de 2011 la compañía contratada inició el proyecto de convertir a formato digital, aproximadamente, 10,000,000 páginas. Para llevar a cabo este proyecto, la compañía subcontrató a otras dos compañías. Estas serían responsables de la extracción, la preparación, la digitalización de los expedientes, y de la entrada de datos e indexación de los documentos que se incluirían en la base de datos.

En diciembre de 2011 la compañía contratada emitió un correo electrónico a los clientes[21] del Departamento para que, durante el período del 15 de diciembre de 2011 al 14 de enero de 2012, revisaran la información contenida en los expedientes corporativos incluidos en el *Portal*.

Un examen realizado el 6 y 9 de marzo de 2012 de varios de estos expedientes, reveló las siguientes faltas de control:

1) Ciento diecisiete expedientes examinados incluían, en el campo Nombre Corporación, información que no correspondía a un nombre corporativo.

2) Doce corporaciones mantenían 2 o 3 expedientes activos, bajo números de registros distintos. Esto, en lugar de tener sólo uno.

[20] Por ejemplo: si se radican 10,000 informes anuales en el primer mes del proyecto de documentos anteriores procesados, y el Departamento determina que 100 de estos documentos contienen errores, la compañía diferirá el pago de 1% del costo facturado hasta que los registros sean corregidos.

[21] Estos eran los que tenían una dirección de correo electrónico válida registrada en el sistema.

3) Los documentos digitalizados de tres corporaciones activas se incluyeron en los expedientes corporativos digitalizados de otras tres compañías. Los documentos eran: certificados de incorporación, informes anuales, entre otros.

4) No se incluyó detalle del propósito ni el nombre de los incorporadores de dos corporaciones activas. Además, una de estas tampoco contenía el detalle de la fecha de inscripción. En su lugar, el *Portal* tenía registrado frases como *No Disponible* y *No hay registros en el archivo*. Esto, a pesar de que los expedientes corporativos digitalizados contenían tal información.

Criterios

Las situaciones comentadas en el **apartado a.1) y 2)** son contrarias a lo establecido en la Sección 4.14 de la propuesta del contrato 2010-000051B, *Key Assumption*. En esta se establece que el Departamento debía informar a la compañía, dentro de 30 días consecutivos, una lista específica de errores en los datos o imágenes incluidos en los expedientes corporativos. Además, se establece que al Departamento determinar que ciertos documentos o datos no cumplen con los estándares definidos, la compañía deducirá hasta un 1% del total facturado por este concepto.

Las situaciones comentadas en el **apartado a.** son contrarias a lo establecido en la *Política TIG-011*. En esta se dispone que los datos e información que las agencias mantienen son vitales para la toma de decisiones tanto para la agencia como para el desarrollo de estrategias que benefician los servicios ofrecidos por el Gobierno del Estado Libre Asociado de Puerto Rico. Esto implica que las agencias deben establecer metodologías para asegurar la integridad y la confiabilidad de los datos producidos y almacenados, incluidos mecanismos de depuración y de validación de datos previo a la digitalización de los expedientes corporativos. Esto, con el propósito de que la aplicación funcione apropiadamente de acuerdo con los propósitos para la cual fue adquirida, y apoye la estrategia de Gobierno, sus metas y objetivos.

Efectos

Las situaciones comentadas en el **apartado a.1) y 2)** le impide al Departamento contar con información completa y correcta sobre las corporaciones realmente activas, la cual le permita ejercer un control administrativo eficaz sobre los honorarios que correspondía pagarle a la compañía contratada.

Las situaciones comentadas en el **apartado a.3) y 4)** crearon el ambiente propicio para que el Departamento no obtuviera el beneficio de recibir descuentos en los honorarios cobrados por la compañía contratada por concepto de errores identificados durante el proceso de digitalización de expedientes corporativos. Además, pudo propiciar que se emitieran o denegaran certificados de cumplimiento *(good standing)* que no correspondían, con los consiguientes efectos adversos.

Causas

Las situaciones comentadas en el **apartado a.1) y 2)** se deben a que el Secretario Auxiliar de Servicios no estableció un proceso para requerir la depuración de la información contenida en el *legacy*[22], la cual se utilizó para nutrir la nueva base de datos corporativa.

Las situaciones comentadas en el **apartado a.3) y 4)** denotan que el Secretario Auxiliar de Servicios no estableció un mecanismo de control para que personal del Registro de Corporaciones del Departamento se asegurase de la corrección e integridad de la información contenida en los expedientes corporativos digitalizados por la compañía contratada, de modo que estos se identificaran e informaran, dentro del período estipulado en el contrato.

Comentarios de la gerencia

En la carta del Secretario, este indicó, entre otras cosas, lo siguiente:

> Esta situación es una que nos preocupa grandemente por la importancia de la información para las transacciones comerciales en Puerto Rico. Debido a la importancia de este asunto, hemos impartido instrucciones para realizar una monitoria que nos

[22] Aplicación desarrollada internamente en *MS Access*, en el año 2004.

> permita determinar los errores y establecer las medidas necesarias para corregir la información y garantizar la confiabilidad de la información en los expedientes digitalizados del Departamento. [*sic*]

Véase la Recomendación 3.c.

Hallazgo 4 - Deficiencias relacionadas con la continuidad de las operaciones relacionadas con las bases de datos corporativas del Departamento

Situaciones

a. El Departamento mantenía la información corporativa en dos bases de datos independientes. Una de estas estaba localizada en un servidor externo que custodiaba la compañía contratada, y la otra en un servidor interno del Departamento.

   La base de datos externa se actualizaba mediante el registro y el procesamiento de datos que ocurría a través del *Portal*, y mediante modificaciones directas a la base de datos. Entre otras, la que ocurría cada 10 minutos, mediante un proceso de transferencia de datos que provenía del *legacy* para actualizar la base de datos externa. Sin embargo, el *legacy* no era actualizado. En el *legacy* se mantenían las enmiendas corporativas, los cambios de nombres y de agentes residentes, y las fusiones corporativas que, a la fecha de nuestro examen, aún no se registraban a través del *Portal*.

   El examen de las estrategias para la continuidad de las operaciones relacionadas con las bases de datos corporativas, reveló las siguientes deficiencias:

   1) El contrato 2010-000051, ni otro documento provisto para examen de nuestros auditores, indicaban los parámetros aceptables, establecidos por el Departamento, como tiempo de recuperación[23] (*RTO*, por sus siglas en inglés) y tolerancia a la

[23] Indica cuánto tiempo puede emplear el personal de sistemas de información para volver a poner la aplicación en línea después de ocurrir un desastre.

pérdida[24] (*RPO*, por sus siglas en inglés) de las bases de datos corporativas, en caso de interrupciones. En su lugar, el contrato indicaba que los datos se restaurarían tan pronto fuera posible.

2) El Departamento no tenía un plan detallado de los sistemas y del proceso de respaldo implementado por la compañía contratada. En su lugar, contaba con el documento *PRPROD SQL Backup Plan*, el cual era un itinerario de respaldo que carecía de lo siguiente:

   - El nombre de la aplicación utilizada para el respaldo de los datos y programas
   - El detalle del proceso de respaldo que realizaban
   - El requerimiento de realizar pruebas periódicas.

3) El Departamento no conservaba una copia recurrente del respaldo externo preparado por la compañía contratada. En su lugar, se proveyó en el contrato que al concluir la vigencia del mismo, y hasta un año posterior, la compañía contratada proveería al Departamento una copia de la base de datos.

4) Al 22 de febrero de 2012, el Departamento no tenía un plan de continuidad ni de recuperación de operaciones propio, como medida de control adicional al *PRPROD SQL Backup Plan* que proveyó la compañía contratada. Esto, con el propósito de asegurar la continuidad de los servicios corporativos provistos en línea, una vez culmine el contrato.

Criterio

Las situaciones comentadas son contrarias a la *Política TIG-003* de la *Carta Circular 77-05*. En esta se establece que las entidades gubernamentales deberán desarrollar un plan de continuidad de negocios

[24] Expresa la cantidad de datos que una aplicación puede llegar a perder antes de que ello resulte en repercusiones negativas para la entidad.

que incluya para la recuperación de desastres y la continuidad de las operaciones. Esto implica el desarrollo de estrategias claras y definidas que incluya los aspectos mencionados en el **Hallazgo**.

Efectos

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 ciudadanos y a los usuarios del sistema. Además, de ocurrir una emergencia, podría dar lugar a la pérdida de información corporativa, lo que podría atrasar el proceso de reconstrucción de archivos y el pronto restablecimiento y la continuidad de las operaciones normales del Registro de Corporaciones.

Causas

Las situaciones comentadas se debían, en parte, a que el Secretario Auxiliar de Servicios no había desarrollado estrategias claras y definidas para la continuidad de las operaciones relacionadas con el Registro de Corporaciones, desde que se negoció el contrato. Además, la situación comentada en el **apartado a.4)** se debía a que el Secretario no había impartido directrices al Secretario Auxiliar de Servicios para que preparara un plan que le permita al Departamento asegurar la continuidad del servicio corporativo provisto en línea, una vez finalizado el contrato.

Comentarios de la gerencia

En la carta del Secretario, este indicó, entre otras cosas, lo siguiente:

> Como parte de la evaluación del contrato del Servicio de Plataforma en Línea se han impartido instrucciones específicas para que se de cumplimiento a la Política TIG-003 que requiere la adopción de mecanismos de seguridad en los Sistemas de Información del Gobierno y específicamente establecer y adoptar los mecanismos necesarios para la continuidad y recuperación de las operaciones del Departamento. [*sic*]

Véanse las recomendaciones 2.d. y e., y 3.d. y e.

RECOMENDACIONES

Al Secretario de Estado

1. Asegurarse de que el Secretario Auxiliar de Servicios y la Secretaria Auxiliar de Administración establezcan las medidas de control necesarias sobre el proceso de reconciliación mensual. Este debe basarse en la designación de un empleado del Departamento con la función de supervisar oportunamente los informes remitidos por la compañía contratada, para asegurarse de que la información contenida en estos está completa y correcta. Además, el empleado designado debe tener acceso directo a la base de datos corporativa para monitorear el historial de modificaciones, de modo que el Departamento se asegure de que recibe los recaudos corporativos correspondientes. **[Hallazgo 1]**

2. Imparta instrucciones al Secretario Auxiliar de Servicios para que se asegure de que la compañía contratada:

    a. Provea, al final de cada mes, un informe que incluya el total de recibos generados por el sistema, incluso los que corresponden a transacciones rechazadas, anuladas, canceladas o en suspenso. **[Hallazgo 1-a.]**

    b. Permita el acceso a una cuenta con privilegio de consulta en el área de Administración del *Portal* para examinar todas las transacciones remitidas para procesamiento. Esto le permitiría al Departamento la detección temprana de errores e inconsistencias en la información provista por la compañía contratada. **[Hallazgo 1-b.]**

    c. Provea acceso a un informe o pantalla que refleje el historial de modificaciones realizadas directamente a la base de datos corporativa. Estos deberán incluir, entre otros, información relacionada con la fecha y el nombre del usuario que generó la modificación, y la justificación para esto. **[Hallazgo 2-a.2) y 3)]**

    d. Revise el *Plan de Respaldo Sistema de Producción SQL (PRPROD SQL Backup Plan)* para que este detalle, entre otras

cosas: la aplicación utilizada para el respaldo de los datos y de los programas; el proceso de respaldo realizado para la continuidad del servicio del servicio corporativo provisto en línea; la documentación que se mantiene del movimiento del archivo de respaldo; y del proceso de pruebas realizadas por la compañía contratada. **[Hallazgo 4-a.2)]**

e. Prepare y remita al Departamento una copia recurrente del respaldo *(backup)* de la base de datos corporativa. **[Hallazgo 4-a.3)]**

3. Imparta instrucciones al Secretario Auxiliar de Servicios para que:

a. Redacte y remita, para la consideración del Secretario, las normas y los procedimientos necesarios para la creación, el mantenimiento y el control de las cuentas con acceso al área de Administración del *Portal*. **[Hallazgo 2-a.1)]**

b. Evalúe los deberes y las responsabilidades de los usuarios, internos y externos, que tienen cuentas con acceso al área de Administración. Una vez realizada la evaluación, realice las gestiones necesarias para: **[Hallazgo 2-a.2) y 3)]**

1) Eliminar los privilegios que no correspondan, según las funciones realizadas por los usuarios.

2) Documentar la justificación y la autorización de los privilegios otorgados.

c. Establezca una estrategia para validar el contenido de los expedientes corporativos digitalizados. Esto, con el propósito de asegurar que en ellos exista información completa, correcta y confiable. Además, tome las medidas necesarias para que no se repitan situaciones como las comentadas en el **Hallazgo 3**.

d. Realice un análisis para determinar los parámetros aceptables para el Departamento en cuanto al tiempo de recuperación *(RTO)* y de tolerancia a la pérdida de datos corporativos *(RPO)*. **[Hallazgo 4-a.1)]**

e. Establezca un plan de continuidad propio que le permita recuperar, restaurar, responder y reanudar prontamente las operaciones corporativas provistas por la compañía contratada, incluido en el caso del cese del servicio provisto por la misma. **[Hallazgo 4-a.4)]**

AGRADECIMIENTO

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

Oficina del Contralor

Por: Yasmín M. Valdivieso

ANEJO 1

DEPARTAMENTO DE ESTADO

SISTEMAS DE INFORMACIÓN COMPUTADORIZADOS

INFORMES PUBLICADOS

INFORME	FECHA	CONTENIDO DEL INFORME
TI-13-09	27 nov. 12	Examen de los controles internos establecidos para la administración del programa de seguridad y la continuidad del servicio del Departamento.
TI-14-03	24 oct. 13	Examen del contrato de servicios profesionales y consultivos para la implantación del Sistema de Información de las Juntas Examinadoras (SIJE).

ANEJO 2

DEPARTAMENTO DE ESTADO

SISTEMAS DE INFORMACIÓN COMPUTADORIZADOS

FUNCIONARIOS PRINCIPALES DE LA ENTIDAD

DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Sr. Kenneth McClintock Hernández	Secretario de Estado	1 sep. 11	9 mar. 12
Lcda. Vanessa Viera Rabelo	Subsecretaria de Estado	1 sep. 11	9 mar. 12
Lcdo. Eduardo Arosemena Muñoz	Secretario Auxiliar de Servicios	1 sep. 11	9 mar. 12
CPA Marlene Smith Bermúdez	Secretaria Auxiliar de Administración	1 sep. 11	9 mar. 12

MISIÓN

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

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

PRINCIPIOS PARA LOGRAR UNA ADMINISTRACIÓN PÚBLICA DE EXCELENCIA

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

QUERELLAS

Las querellas sobre el mal uso de la propiedad y de los fondos públicos pueden presentarse, de manera confidencial, personalmente o por teléfono al (787) 754-3030, extensión 1106, 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.

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