



Estado Libre Asociado de Puerto Rico Oficina del Contralor

Yesmín M. Valdivieso
Contralora

**Carta Circular
OC-16-16**

Año Fiscal 2015-2016
9 de febrero de 2016

Alcaldes, presidentes de las legislaturas municipales y
legisladores municipales¹

**Asunto: Evaluación de los controles de los sistemas de
información computadorizados de los municipios²**

Estimados señores y señoras:

La incorporación de la tecnología a los programas y a los servicios del Gobierno es un valioso instrumento para reducir el tiempo de administración y los costos de operación. Además, hace accesible los servicios que presta el Gobierno a los ciudadanos. Sin embargo, esto requiere una inversión considerable de recursos para el desarrollo, la adquisición, la implementación, la contratación de servicios, y la seguridad y el mantenimiento de los sistemas de información. Esta inversión de fondos públicos en tecnología de información requiere planificación para que se obtengan los beneficios esperados en un tiempo razonable. También deben establecerse los controles necesarios para mantener una operación eficiente de los sistemas de información computadorizados.

ymu
Mediante el *Memorando Circular 2015-03* del 27 de febrero de 2015, el Comisionado de Asuntos Municipales informó a los municipios sobre la eliminación del Sistema Uniforme de Contabilidad Mecanizado (SUCM), y sobre la necesidad de firmar contratos de servicios profesionales para la implementación de los nuevos sistemas de contabilidad. Este proceso conlleva la inversión de recursos para adquirir equipos, servicios profesionales y nuevas tecnologías basadas en servicios en la nube, entre otros. Por otra parte, los municipios han incursionado en el uso de nuevas tecnologías como las páginas en Internet, las redes sociales y las aplicaciones móviles para mejorar la accesibilidad de la información y de los servicios provistos a los ciudadanos.

¹ Las normas de la Oficina prohíben el discrimen, entre otros motivos, por orientación sexual e identidad de género. Para propósitos de esta *Carta Circular*, se deberá entender que todo término utilizado para referirse a una persona o puesto se alude a ambos géneros.

² Esta comunicación se emite al amparo del Artículo 14 de la *Ley Núm. 9 del 24 de julio de 1952*, según enmendada, conforme se detalla en la Certificación sometida por esta Oficina ante la Comisión Estatal de Elecciones el 1 de febrero de 2016, número CEE-C-16-099.

La División de Auditorías de Tecnología de Información de la Oficina del Contralor efectuará una evaluación de los controles de los sistemas de información computadorizados de los municipios. Esto, con el propósito de verificar las operaciones relacionadas con estos sistemas y promover la implementación de las mejores prácticas para la adquisición y la operación eficiente y segura de los sistemas de información computadorizados en los municipios.

Esta *Carta Circular* tiene el propósito de anunciarles que la evaluación de los controles de los sistemas de información computadorizados de los municipios se realizará en marzo de 2016. Los siete componentes establecidos por la Oficina para la evaluación son:

- **Administración de la seguridad de los sistemas de información computadorizados** - Permite al municipio lograr la exactitud, la integridad y la protección de todos los procesos y los recursos de sistemas de información computadorizados. Esto, de modo que se minimicen los errores, el fraude y la pérdida de la información que interconecta al municipio con sus clientes, proveedores y otras partes interesadas.
- **Continuidad de los servicios** - Asegura que todas las operaciones críticas que el municipio realiza a través de los sistemas de información computadorizados estarán disponibles para sus ciudadanos, usuarios, clientes, proveedores, y otras entidades pertinentes. Incluye un gran número de tareas diarias como la administración de proyectos, la preparación y el mantenimiento de los respaldos, el control de los cambios y el apoyo a los usuarios (*helpdesk*). La continuidad no se implementa cuando ocurre un desastre, sino que hace referencia a todas aquellas actividades que se llevan a cabo diariamente para mantener el servicio y facilitar la recuperación, en caso de que ocurra una emergencia.
- **Seguridad física y controles ambientales** - Minimiza el riesgo de daños e interferencias en la información y en las operaciones del municipio. El establecimiento de perímetros de seguridad y áreas protegidas facilita la implementación de controles de protección sobre las instalaciones de procesamiento de información crítica o confidencial del municipio que eviten el acceso físico no autorizado. Además, los controles sobre los factores ambientales (internos o externos) permiten garantizar el funcionamiento correcto de los equipos de procesamiento y minimizar las interrupciones del servicio.
- **Control de acceso lógico** - Involucra todas aquellas medidas establecidas por el municipio para la administración de las cuentas de los usuarios y de los administradores de los recursos de tecnología de información. Esto, con el propósito de minimizar los riesgos de seguridad asociados con la operación cotidiana del uso de la tecnología de información. Los principales objetivos de la seguridad lógica son: restringir el acceso a los programas y a los archivos, y limitar el acceso de los usuarios para que sólo vean y accedan lo necesario, de acuerdo con sus funciones y responsabilidades.
- **Control de las computadoras y de los equipos computadorizados** - Incluye los controles sobre el equipo (servidores, computadoras, computadoras portátiles, tabletas, equipo de comunicación, entre otros), y los programas que permiten el almacenamiento, el recibo, la transmisión y el procesamiento de la información del municipio.

9 de febrero de 2016

- **Control de las aplicaciones** - Asegura, mediante controles automatizados (realizados por el sistema), el procesamiento completo y preciso de los datos desde la entrada hasta la salida. Estos controles garantizan que los datos estén completos, sean exactos, sean válidos, y aseguren la confidencialidad y la disponibilidad de los mismos.
- **Proceso de adquisición de los sistemas de contabilidad** - Permite la adquisición e implementación de una solución tecnológica de infraestructura capaz de conectarse con otros sistemas y adaptarse a nuevas necesidades de procesamiento. Esto, para mejorar la capacidad operacional, productividad y ejecución de los servicios en el municipio.

El procedimiento para realizar la evaluación de los controles de los sistemas de información computadorizados de los municipios es el siguiente:

1. Al 18 de febrero de 2016 o antes, el Alcalde deberá enviar una certificación que indique el nombre, teléfono y correo electrónico del funcionario asignado para coordinar y entregar la información a los auditores. Favor remitir la información a la Sra. Lourdes Díaz Valcárcel, Directora de la División de Auditorías de Tecnología de Información, al correo electrónico: ldiaz@ocpr.gov.pr.
2. El funcionario designado deberá preparar un expediente digital que incluya los documentos solicitados en el *Anejo, Solicitud de Información Criterios para la Evaluación de los Controles de los Sistemas de Información Computadorizados en los Municipios*, necesarios para evaluar los siete componentes de control. Favor de incluirlos en formato *pdf*. Los documentos deben estar certificados como copia fiel y exacta de los mantenidos en los registros del municipio. Además, deberán estar disponibles para examen durante la visita de nuestros auditores en marzo de 2016.
3. Nuestros auditores coordinarán la visita, mediante llamada telefónica o correo electrónico al funcionario contacto asignado.
4. Los auditores de la Oficina del Contralor efectuarán una evaluación de los controles de sistemas de información computadorizados que les permitirá determinar si el municipio cumple, cumple sustancialmente o no cumple con los controles que requiere el campo de la tecnología de información, para cada uno de los siete componentes mencionados. El resultado³ de las evaluaciones efectuadas por nuestros auditores se dará a conocer mediante la publicación de un informe especial.

Les exhortamos a que impartan las instrucciones pertinentes a los funcionarios y a los empleados correspondientes para que recopilen la información solicitada, la cual está relacionada con los controles necesarios para la operación eficiente y segura de los sistemas de información computadorizados.

³ Este resultado es independiente del resultado de auditorías en proceso o que realicemos en el futuro sobre los sistemas de información computadorizados de los municipios.



Carta Circular OC-16-16

Página 4

9 de febrero de 2016

Estamos a sus órdenes para ofrecerles cualquier información. De considerarlo necesario, pueden comunicarse a la División de Auditorías de Tecnología de Información al (787) 754-3030, extensiones 2502 y 2503.

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

Cordialmente,


Yesmín M. Valdivieso

Anejo

c Comisionado de Asuntos Municipales



Estado Libre Asociado de Puerto Rico

Anejo

OFICINA DEL CONTRALOR

San Juan, Puerto Rico

SOLICITUD DE INFORMACIÓN

**Criterios para la Evaluación de los Controles de los
Sistemas de Información Computadorizados de los Municipios**

**COMPONENTE 1 - ADMINISTRACIÓN DE LA SEGURIDAD DE LOS SISTEMAS DE
INFORMACIÓN**

<u>Referencia</u>	<u>Documentos</u>
A.	Certificación que indique quién es el encargado de la administración de los sistemas de información computadorizados.
B.	Copia de las normas que requieran un análisis de los riesgos, al menos, cada dos años o cuando ocurra un cambio significativo.
C.	Copia del informe de análisis de riesgos.
D.	Copia del documento dónde el alcalde y la legislatura municipal expresen la política sobre la seguridad de los sistemas de información computadorizados.
E., F.	Copias de las políticas, las normas o los procedimientos aprobados para reglamentar lo siguiente: • La adquisición de los equipos computadorizados • El control de los equipos computadorizados (identificación, registro, asignación y disposición)¹ • La administración y el control de los accesos físicos a las áreas donde están localizados los equipos computadorizados • La configuración de la seguridad de los sistemas de información computadorizados (servidores y equipos) • El uso y la revisión de registros de auditoría o de seguridad • La solicitud y la autorización para la creación, modificación y cancelación de las cuentas de acceso a los sistemas de información computadorizados • El uso de contraseñas complejas para acceder a los sistemas de información computadorizados • El uso autorizado de los sistemas de información computadorizados (Internet, correo electrónico, redes sociales, equipos y aplicaciones) • La instalación de programas autorizados • El uso de programas para evitar la propagación de virus y de <i>malwares</i> • El manejo de incidentes de seguridad • El uso y la divulgación de la información

¹ Este documento será utilizado para evaluar los componentes I.E.2. y 5.G.

- El respaldo de la información
 - La distribución, retención, y disposición de los documentos (físicos y electrónicos) generados por los sistemas de información computadorizados
 - La capacitación y educación continua a los empleados sobre la seguridad
 - La responsabilidad de los empleados de proteger los servicios y recursos informáticos (equipos, programas y datos) del municipio
 - Las sanciones por incumplir con las políticas establecidas.
- G. Copia de la documentación relacionada con:
- La divulgación de las políticas, las normas o los procedimientos aprobados sobre la seguridad de los sistemas de información computadorizados
 - Las advertencias sobre las políticas y normas para el uso y la seguridad de los sistemas de información computadorizados instaladas en los equipos computadorizados
 - Los adiestramientos ofrecidos sobre la seguridad de la información a los usuarios, a los contratistas, al personal técnico a cargo de los sistemas de información computadorizados y a la gerencia.
- H., I. Copias de los últimos tres informes de auditorías relacionados con los sistemas de información computadorizados.

COMPONENTE 2 - CONTINUIDAD DE LOS SERVICIOS

- A. Copia del plan escrito y aprobado por el alcalde y la legislatura municipal para recuperar las operaciones del municipio en caso de una emergencia.
- B. Certificación que indique los apartados del plan donde se consideran los sistemas de información computadorizados del municipio.
- C. Copias de los acuerdos para restablecer las operaciones de los sistemas computadorizados en un centro alternativo.
- D. Certificación que indique la persona responsable de realizar los respaldos y la frecuencia de la preparación de los mismos.
- E. Copia del acuerdo para mantener los respaldos en un lugar externo.
- F. Copia del registro de los respaldos realizados durante el 2015 en el que se identifique el lugar de almacenamiento (municipio y lugar externo).
- G. Copias de los acuerdos de servicios en la nube (*cloud computing*). Identifique en los mismos las cláusulas que garanticen la seguridad y disponibilidad de la información cuando:
- Ocurren emergencias en las instalaciones del proveedor de servicio en la nube
 - Ocurre la terminación o se rescinde del servicio en la nube.

COMPONENTE 3 - SEGURIDAD FÍSICA Y CONTROLES AMBIENTALES

- A. Certificación que explique dónde está localizada la instalación de procesamiento y el equipo de comunicación principal del municipio, y las medidas que se han establecido para asegurar estas áreas y el equipo, para reducir el riesgo de amenazas naturales.
- B. Certificación que explique las medidas que se han establecido para evitar el acceso no autorizado a la instalación de procesamiento y al equipo de comunicación principal.
- C. Certificación que indique si las instalaciones principales de procesamiento del municipio cuentan con generadores eléctricos, *UPS*, *surge protectors*, extintores de incendio y detectores de humo.

COMPONENTE 4 - CONTROL DE ACCESO LÓGICO

- A. Certificación que indique el formulario, o método alternativo, utilizado por el municipio para documentar la autorización de acceso a la red, a Internet, al correo electrónico y a las aplicaciones principales del municipio.
Lista certificada del personal con acceso a la red, a Internet, al correo electrónico y a las aplicaciones principales del municipio, que incluya los usuarios con privilegios de acceso remoto. Esta debe indicar el nombre del empleado, nombre de usuario, división, puesto que ocupa, sistema utilizado y nivel de acceso (leer, modificar y escribir).
- B. Copia del formulario de solicitud de acceso o de cualquier otra documentación utilizada para solicitar los accesos.
- C. Copias de las notificaciones sobre la separación de empleados o de empleados en licencias prolongadas, referidas al encargado de los sistemas de información durante el último año.
- D., E. y F. Impresión de pantalla de la configuración de los servidores principales y de las aplicaciones principales (que, al menos, muestre la configuración de las contraseñas, de las políticas de auditoría y de seguridad).
- G. Impresión de pantalla de las herramientas para controlar el tráfico entre las redes internas y externas.
- H. Certificación que identifique las cláusulas del acuerdo de servicios en la nube (*cloud computing*) para la administración de las cuentas de acceso.

COMPONENTE 5 - CONTROL DE LAS COMPUTADORAS Y LOS EQUIPOS COMPUTADORIZADOS

- A. Certificación que explique cómo se identifican las computadoras y los equipos periféricos en el municipio y los códigos que componen el número de propiedad asignado.
- B. Copia del inventario de los equipos computadorizados (servidores, computadoras, dispositivos móviles, equipos de comunicación, entre otros).
Incluya una certificación con el nombre del sistema utilizado por el municipio para mantener el inventario del equipo computadorizado.

- C. Copia del inventario de las licencias de los programas instalados en cada servidor, computadora y dispositivo móvil.
- D. Copia del diagrama esquemático de la red que incluya todos los equipos y conexiones (*servidores, switches y wireless access points*).
- E. Copia de la documentación sobre revisiones efectuadas a los accesos a Internet, las computadoras y los dispositivos móviles para verificar el uso adecuado de estos.
- F. Impresión de pantalla de las herramientas para protección de virus y *malware*.
- G. Copias de las notificaciones sobre las pérdidas de equipos computadorizados, informadas a la Oficina del Contralor durante los años fiscales 2013-14 y 2014-15.
Certificación sobre la *Notificación de Pérdidas o Irregularidades en el Manejo de Fondos o Bienes Públicos a la Oficina del Contralor* durante los años fiscales 2013-14 y 2014-15.

COMPONENTE 6 - CONTROL DE APLICACIONES

- A. Certificación que indique si el sistema de contabilidad utilizado por el municipio permite el registro de todas las transacciones contables, tales como: recaudaciones, nómina, patente, desembolsos y propiedad. Además, indique las transacciones que no se pueden registrar en el sistema y explique cómo mantienen el registro de estas.
- B. Certificación que indique que los cheques, los comprobantes de desembolso y las órdenes de compra, procesados manualmente al 31 de diciembre de 2015, fueron registrados en el sistema de contabilidad. En caso de no estar actualizados, explique las razones para esto.
- C. Copia de la reconciliación bancaria de diciembre de 2015 realizada en el sistema de contabilidad. En caso de no poder proveer la misma, incluya una certificación que explique las razones para esto.
- D. Copias de los informes generados por el sistema de contabilidad a diciembre de 2015:
 - Informe Mensual de Ingresos y Gastos (4A)
 - Conciliaciones Bancarias
 - Inventario Físico de la Propiedad
 - Registro de Inversiones
 - Presupuesto Municipal
 - Liquidaciones PresupuestariasCertificación que explique los informes que no produce el sistema y que son necesarios para el municipio.
- E. Copia del último *Single Audit* realizado que incluya el *Management Letter*.
Certificación que explique las gestiones realizadas por el municipio para corregir los reparos comentados en el *Single Audit* que están relacionados con la confiabilidad de los registros contables en el sistema.
- F. Impresión de pantalla que evidencie la configuración para que se produzcan los registros de transacciones (*audit trail*) y de seguridad.

COMPONENTE 7 - PROCESO DE ADQUISICIÓN DE SISTEMAS DE CONTABILIDAD

- A.1 Copia del estudio de necesidad y viabilidad realizado por el municipio para adquirir el sistema de contabilidad, o en su lugar, estudio de viabilidad realizado por el municipio para seleccionar entre los proveedores de los sistemas de contabilidad recomendados por la OCAM.
- A.2 Certificación que indique el nombre y puesto del administrador de proyecto designado durante el proceso de implementación del sistema de contabilidad.
- A.3 Copia de la documentación relacionada con los adiestramientos ofrecidos a los empleados para el uso del sistema de contabilidad.
- A.4 Certificación que identifique las cláusulas del acuerdo de servicios en la nube (*cloud computing*) para requerir la entrega de documentación del sistema de contabilidad.