OFICINA DEL CONTRALOR ELECTORAL

Número: 9809

Fecha: 21 de octubre de 2026

Aprobado: Rosachely Rivera Santana
Secretaria de Estado
Departamento de Estado

REGLAMENTO NÚM. 50

REGLAMENTO PARA EL USO DE LOS SISTEMAS DE INFORMACIÓN DE LA OFICINA DEL CONTRALOR ELECTORAL

Aprobado 22 de septiembre de 2026

TABLA DE CONTENIDO

TÍTULO I – DISPOSICIONES PRELIMINARES 1

Sección 1.1 – Título 1

Sección 1.2 – Autoridad 1

Sección 1.3 – Declaración de propósitos y resumen ejecutivo 1

Sección 1.4 - Análisis de Costo-Beneficio 1

Sección 1.5 – Definiciones 2

Sección 1.5 – Aplicabilidad 3

TÍTULO II – TITULARIDAD Y DERECHOS 3

Sección 2.1 – Disposición General 3

TÍTULO III – NORMAS PARA EL USO DE LOS SISTEMAS DE INFORMACIÓN 4

Sección 3.1 – Asignación de Equipos y Autorización de Acceso 4

Sección 3.2 – Seguridad 4

Sección 3.3 – Protección y cuidado de equipos 6

Sección 3.4 – Disposición de los equipos 6

Sección 3.5 – Internet, mensajería y correo electrónico 6

Sección 3.6 – Repositorio de datos 7

TÍTULO IV – AUDITORÍAS 8

Sección 4.1 - Facultad de Auditoría, Monitoreo y Acceso Institucional 8

TÍTULO V – MEDIDAS DISCIPLINARIAS 8

Sección 5.1 - Investigación Administrativa y Medidas Disciplinarias 8

TÍTULO VI – DISPOSICIONES FINALES 8

Sección 6.1 – Cláusula de salvedad 8

Sección 6.2 – Enmiendas 8

Sección 6.3 – Exclusión 8

Sección 6.4 – Vigencia 9

Sección 6.5 – Derogación 9

Sección 6.6 – Distribución 9

GOBIERNO DE PUERTO RICO
OFICINA DEL CONTRALOR ELECTORAL
REGLAMENTO PARA EL USO DE LOS SISTEMAS DE INFORMACIÓN DE LA OFICINA DEL CONTRALOR ELECTORAL

TÍTULO I – DISPOSICIONES PRELIMINARES

Sección 1.1 – Título

Este Reglamento se conocerá como "Reglamento para el uso de los Sistemas de Información de la Oficina del Contralor Electoral".

Sección 1.2 – Autoridad

Este Reglamento se adopta y promulga al amparo de las facultades conferidas al Contralor Electoral por los Artículos 3.003A, 3.006 y 3.007 de la Ley Núm. 222-2011, según enmendada, conocida como la "Ley para la Fiscalización del Financiamiento de Campañas Políticas en Puerto Rico", y de conformidad con la Ley Núm. 151-2004, según enmendada, conocida como la "Ley de Gobierno Electrónico"; la Ley Núm. 75-2019, según enmendada, conocida como la "Ley de la Puerto Rico Innovation and Technology Service" (PRITS); la Ley Núm. 40-2024, según enmendada, conocida como la "Ley de Ciberseguridad del Estado Libre Asociado de Puerto Rico"; y la Carta Circular Núm. 2023-004 de PRITS, titulada "Normas Generales que Deben Seguir las Agencias al Establecer sus Controles y Procedimientos, de Manera que se Atiendan Adecuadamente los Recursos, las Adquisiciones e Implementación de Soluciones o Tecnología Nueva, así como el Uso y Manejo de los Sistemas de Información y el Manejo de Cambios en los Proyectos de Tecnología".

Sección 1.3 – Declaración de propósitos y resumen ejecutivo

Los sistemas de información computadorizados de la Oficina del Contralor Electoral (OCE) son una parte vital de las herramientas operacionales de la Oficina. Su integridad y buen funcionamiento son necesarios como herramienta de todos los empleados para realizar sus funciones de manera eficiente y efectiva. Por tanto, su uso adecuado es vital para las operaciones diarias de la OCE. El conocimiento de los empleados y la orientación adecuada a cada uno de los empleados es importante para lograr este objetivo. Este reglamento obedece a esta necesidad.

Este Reglamento tiene el propósito de establecer el uso de los sistemas de información, con el fin de asegurar la integridad y exactitud de la propiedad e información de la Oficina, protegiéndola contra la divulgación, modificación y la destrucción no autorizada o accidental.

Los equipos de computadoras, los programas (*software*), así como la información contenida en los sistemas de información son propiedad de la Oficina del Contralor Electoral.

Sección 1.4 - Análisis de Costo-Beneficio

La Oficina del Contralor Electoral certifica que la adopción de este Reglamento no representa un impacto fiscal adicional para el erario.

Sección 1.5 – Definiciones

Las palabras y frases usadas en este Reglamento se interpretarán según el contexto en que sean usadas y tendrán el significado aceptado por el uso común y corriente. Los siguientes términos usados en este Reglamento tendrán el significado que a continuación se expresa:

1. "**Contralor Electoral**" – Oficial ejecutivo de la Oficina del Contralor Electoral.

2. "**Correo electrónico**" – Servicio de transmisión de mensajes a través de una red, también denominado *e-mail*.

3. "**División**" – División de Apoyo Tecnológico, dependencia de la Oficina del Contralor Electoral, cuyo personal es responsable de la instalación, mantenimiento y actualización de los equipos electrónicos, servicios, aplicaciones y materiales relativos a los servicios de sistemas de información, independientemente de su localización.

4. "**Equipo**" – cualquier propiedad tangible, y duradera del gobierno relacionada con las tecnologías de la información y la comunicación, que es útil para llevar a cabo las funciones de comunicación o manejar la información.

5. "**Internet**" – Red informática mundial, descentralizada, formada por la conexión directa entre computadoras u ordenadores mediante un protocolo especial de comunicación.

6. "**Oficial Principal de Informática**" (OPI) – empleado nombrado por el Contralor Electoral ante la oficina Puerto Rico Innovation & Technology Service (PRITS), responsable de la gestión y supervisión de la infraestructura tecnológica y manejo de datos. El OPI es el director de la División de Apoyo Tecnológico de la OCE.

7. "**Oficina**" u "**OCE**" – Oficina del Contralor Electoral.

8. "**MFA**" o "**Multi Factor Authentication**" – método de autenticación adicional a la contraseña, como un token físico o sistema biométrico.

9. "**Resguardo**" – Mecanismo para salvaguardar la información con el fin de prevenir alguna pérdida, también denominado *backup*.

10. "**Repositorio de datos**" – Área reservada o clasificación de espacios que se utilizan para almacenar información y agrupar datos.

11. "**Servicios en la nube**" – Servicios e información obtenidos a través de la internet.

12. "**Sistema de Información**" – Uso y manejo de la información en los equipos electrónicos que se utilizan como herramienta de trabajo en la Oficina.

13. "**Usuario**" – Empleado de la Oficina del Contralor Electoral, contratista o visitante que está autorizado al uso de los sistemas de información.

14. "**Virus**" – Programa de computadora cuyo propósito es dañar aplicaciones, datos y el equipo electrónico donde se instale.

15. "**VPN**" o "***Virtual Private Network***" – Método para proveer acceso remoto y seguro a la red de la Oficina a través de internet.

Sección 1.5 – Aplicabilidad

Las disposiciones de este Reglamento aplican a los empleados, contratistas, y visitantes de la Oficina que utilicen equipos en las facilidades de la Oficina del Contralor Electoral, en asuntos oficiales fuera de la Oficina y en accesos remotos vía VPN.

TÍTULO II – TITULARIDAD Y DERECHOS

Sección 2.1 – Disposición General

La Oficina cuenta con acceso a computadoras, redes, servicios electrónicos internos y a la red Internet. Al hacer uso de estos equipos electrónicos y de los servicios asociados, los usuarios acatarán las siguientes normas:

a. Los equipos, servicios asociados tanto internos como externos, el sistema de correspondencia electrónica (*e-mail*), mensajería instantánea, telefonía, internet y los documentos y programas, son propiedad de la Oficina del Contralor Electoral y sólo podrán ser utilizados para propósitos lícitos, prudentes, responsables y dentro de las funciones inherentes a la Oficina y los mejores intereses del Gobierno de Puerto Rico.

b. Toda información, dato, escrito, documento, programa, acción, privilegio, patente, derecho de autor o cualquier otro derecho que surja, se cree o modifique mediante el uso de una de las computadoras de la Oficina será propiedad de la agencia, aunque la información, dato, escrito, documento, programa, acción, privilegio, patente, derecho de autor o cualquier otro derecho haya surgido mediante el esfuerzo personal del usuario.

c. La información contenida en el equipo electrónico, los servicios asociados tanto internos como externos, los mensajes de correspondencia electrónica (*e-mail*), información de la Intranet o la Internet y los documentos y programas existentes no podrán ser reproducidos o utilizados para fines ajenos a las funciones y poderes de la Oficina. Cualquiera de esta

información podrá ser examinada o utilizada por el Contralor Electoral, el OPI, o su personal autorizado.

d. Se prohíbe el uso de programas o recursos para los cuales no exista una licencia o autorización de uso válido a nombre de la Oficina. La División velará por el licenciamiento de los productos y registrará las licencias en sus respectivas compañías.

e. Se prohíbe hacer copias de programas de computadora adquiridos por la Oficina. Se prohíbe acceder a, o utilizar, propiedad intelectual (*copyrighted information*) que viole derechos de autor.

f. Se prohíbe instalar programas en las computadoras que no hayan sido adquiridos por la Oficina, sin la autorización previa del OPI.

g. Se prohíbe el uso de los sistemas de información y comunicaciones de la Oficina para propósito personal, de recreo, para manejo de un negocio o asunto privado del usuario, o para el recibo y envío de mensajes en cadena, para tener acceso a compras, juegos, concursos, encuestas, páginas de entretenimiento o cualquier otro asunto o servicio no oficial o ajeno a las funciones de la Oficina.

h. Todo archivo o programa ajeno a las funciones y deberes de la Oficina será removido o eliminado de los equipos electrónicos inmediatamente se detecte la existencia de este.

TÍTULO III – NORMAS PARA EL USO DE LOS SISTEMAS DE INFORMACIÓN

Sección 3.1 – Asignación de Equipos y Autorización de Acceso

La División recomendará y asignará equipos electrónicos a las áreas de la OCE, de acuerdo con sus necesidades, funciones y encomiendas, tomando en consideración las limitaciones presupuestarias de la Oficina. Cada director será responsable de completar el formulario de acceso a los sistemas de información de la OCE, donde se establecerán los servicios y el horario autorizado para cada empleado.

Sección 3.2 – Seguridad

Para garantizar la seguridad y protección de los equipos del sistema de información, se cumplirá con las siguientes normas:

1. Cada computadora deberá mostrar una notificación electrónica al usuario indicando que está accediendo los sistemas de información propiedad de la Oficina del Contralor Electoral y que está obligado a usar la misma en cumplimiento con las normas establecidas.

2. Cada usuario deberá establecer y mantener en estricta confidencialidad su contraseña de acceso. Los requisitos de seguridad aplicables, incluidos su composición, extensión, vigencia, expiración, reutilización y frecuencia de cambio, serán determinados y divulgados periódicamente por el OPI, conforme a las políticas administrativas y a las mejores prácticas de seguridad vigentes. De sospechar que su contraseña ha sido revelada por inadvertencia o descuido, deberá notificar inmediatamente a su supervisor inmediato y a la División para tomar las medidas correspondientes de seguridad. En caso de renuncia o separación de funciones, el OPI o el encargado desactivará la clave de acceso de ese usuario para todos los servicios de la OCE.

3. Todos los usuarios tendrán autenticación MFA para garantizar y validar la autenticidad de los accesos a los sistemas de información de la OCE.

4. Se prohíbe el uso de computadoras, dispositivos o equipos personales para realizar trabajos oficiales, salvo que dicho uso sea autorizado por el OPI o resulte necesario para acceder a los sistemas implementados o utilizados por la OCE a los fines de cumplir con las funciones de trabajo presencial o remoto, conforme a la reglamentación vigente, las políticas de seguridad aplicables y los acuerdos autorizados entre las partes.

5. Se prohíbe modificar los privilegios de acceso a las redes internas o externas para obtener acceso no autorizado a dichos recursos.

6. No se podrá modificar la información archivada propiedad de la Oficina con el propósito de impedir que alguien pueda leerla, entenderla o usarla. Tampoco se podrá alterar el nombre del usuario u otra información que se utilice regularmente para identificar la información, mensajes o archivo. En caso de que algún usuario asigne contraseñas o codifique la información a fines de evitar que otras personas puedan leerla, éste proveerá a la División todos los datos para lograr acceso a los archivos al momento de su creación.

7. Se prohíbe modificar los parámetros y configuración adoptados por la División en las computadoras y otros equipos de la Oficina.

8. Todos los archivos que se creen en las computadoras deben ser guardados en el directorio asignado a cada usuario y oficina con el fin de protegerlos mediante los mecanismos de resguardo existentes. Se realizará resguardo a los archivos que residan en las computadoras siempre que estén ubicados en los directorios asignados por la División y los archivos cumplan con las políticas de almacenamiento de los servicios en la nube.

Sección 3.3 – Protección y cuidado de equipos

1. Ningún usuario realizará tareas de instalación de equipo, programas, ni de reparación. Solamente el personal autorizado de la División podrá instalar, configurar o reparar los equipos.

2. La División será responsable de la configuración, seguridad y cumplimiento de todos los equipos, así como de las claves de acceso, para garantizar la seguridad e integridad de los datos y sus componentes.

3. Cuando el usuario detecte problemas en el funcionamiento del sistema, deberá notificarlo rápidamente a la División para que se proceda a revisar el equipo, corregir la falla o se refiera para reparación, según el caso.

4. Ningún usuario llevará alimentos ni bebidas a las áreas de trabajo donde los equipos de computadoras estén localizados.

5. Cualquier movimiento de equipos deberá ser coordinado con el personal de la División y el empleado encargado de la propiedad de la OCE.

6. Con el fin de lograr la mayor uniformidad y compatibilidad entre equipos, previo a la adquisición de computadoras, redes, servicios electrónicos internos y programas deberá contarse con el asesoramiento de la División.

7. Al finalizar la jornada laboral, los usuarios deberán retirar sus claves de acceso de las computadoras, desconectar cualquier dispositivo portátil (*pen drive*) y apagar todos los equipos en su área de trabajo.

8. En caso de emergencia cada usuario es responsable de tomar las medidas necesarias para proteger el equipo que tenga asignado.

Sección 3.4 – Disposición de los equipos

El proceso de disposición de equipo debe efectuarse de conformidad con la reglamentación aplicable y en coordinación con el Encargado de la Propiedad de la OCE. Durante este proceso deben utilizarse métodos tales como *overwriting*, *degaussing* o la destrucción física del medio para remover toda la información oficial grabada y garantizar su confidencialidad. Si el equipo no tiene uso futuro en la Oficina, se puede donar o transferir a otra entidad gubernamental.

Sección 3.5 – Internet, mensajería y correo electrónico

1. Ningún empleado podrá reclamar interés propietario o expectativa razonable de intimidad sobre comunicaciones transmitidas por la Internet o correo electrónico. La Oficina tendrá

acceso a los mensajes electrónicos e información de páginas visitadas por los empleados en cualquier momento y los mismos serán considerados parte de los expedientes de la Oficina.

2. Se prohíbe bajar información de la Internet que sea ajena a las funciones oficiales del empleado, sin la debida autorización del OPI o de la persona que este designe a cargo del sistema de información.

3. Se prohíbe acceder y almacenar información oficial en equipos y cuentas de correo electrónico distintos a los equipos y cuentas oficiales provistas por la Oficina.

4. El usuario deberá mantener la correspondencia electrónica de manera que se pueda utilizar al máximo el espacio asignado por el servicio de mensajería y de la computadora.

5. Se prohíbe el envío fuera del sistema de información de la OCE de documentos o mensajes que contengan información confidencial. La prohibición no aplicará cuando la información se envíe a un contratista de la Oficina para que este cumpla con una encomienda oficial, en cuyo caso, este será responsable de mantener su confidencialidad.

6. Se prohíbe el envío de información en los cuales se divulguen, comenten o expresen hechos, opiniones, situaciones o asuntos internos, que puedan poner en entredicho la reputación y la imagen de la Oficina.

7. Se prohíbe a terceras personas leer, revisar, interceptar, modificar o destruir cualquier tipo de comunicación oficial y confidencial de la Oficina, sin el consentimiento expreso del remitente y del destinatario de la comunicación.

8. Se prohíbe a los usuarios el suscribirse a listas de correo electrónico o que participen en foros y redes sociales que divulguen información o mensajes ajenos a las funciones y deberes de la Oficina sin la debida autorización.

9. Se prohíbe la reproducción maliciosa o voluntaria de virus, envío de correo que no sea oficial, envío de material ofensivo, ilegal o pornográfico o de cualquier otra índole no autorizada.

Sección 3.6 – Repositorio de datos

Los empleados tendrán áreas reservadas o repositorio de datos en el sistema de información o los servicios en la nube de la OCE. La División reservará estas áreas de acuerdo con las necesidades del empleado, la división y la capacidad del sistema.

Cada uno de los repositorios de datos será usado única y exclusivamente por la oficina o dependencia a la que está asignada. La División controlará el acceso a los repositorios de datos mediante restricción de accesos en las cuentas de usuarios, de forma que los usuarios sólo podrán entrar a las

áreas que les han sido asignadas. Estos procedimientos de restricción de acceso le garantizarán al usuario que nadie podrá acceder, ver, copiar o imprimir los documentos en su librería sin su autorización. El contenido del repositorio de datos será responsabilidad exclusiva de su usuario.

TÍTULO IV – AUDITORÍAS

Sección 4.1 - Facultad de Auditoría, Monitoreo y Acceso Institucional

La Oficina se reserva el derecho a auditar, vigilar y fiscalizar todos los servicios computadorizados para garantizar que su propiedad sea utilizada sólo para propósitos y gestiones relacionadas con el trabajo. Estas auditorías se realizarán periódicamente, al azar o cuando exista una investigación sobre una situación en particular. El Contralor Electoral podrá contratar auditores externos para realizar auditorías comprensivas de los sistemas de información computadorizada sin previo aviso a los usuarios.

El personal de la Oficina no tiene expectativa de intimidad sobre cualquier información, documento, mensaje creado, recibido o enviado a través del sistema de correo electrónico de la OCE, incluyendo contenido de carácter personal, ni sobre información almacenada en equipos o servicios provistos por la Oficina.

TÍTULO V – MEDIDAS DISCIPLINARIAS

Sección 5.1 - Investigación Administrativa y Medidas Disciplinarias

El incumplimiento con las disposiciones de este Reglamento estará sujeto a investigación administrativa y/o la imposición de las medidas disciplinarias correspondientes, a discreción del Contralor Electoral, según las disposiciones del "Reglamento de personal de la Oficina del Contralor Electoral".

TÍTULO VI – DISPOSICIONES FINALES

Sección 6.1 – Cláusula de salvedad

Si cualquier título, artículo, inciso, parte, párrafo o cláusula de este Reglamento fuere declarado inconstitucional o nulo por un tribunal de jurisdicción competente, la sentencia a tal efecto dictada no afectará ni invalidará el resto de este Reglamento.

Sección 6.2 – Enmiendas

Este Reglamento podrá enmendarse, en cualquier momento en que así se estime conveniente, en beneficio de una mayor efectividad en la implementación de la Ley 222.

Sección 6.3 – Exclusión

Por disposición de los Artículos 3.003A (dd) y 12.004 de la Ley 222, este Reglamento está exento de cumplir con el proceso de reglamentación dispuesto en la Ley de Procedimiento Administrativo Uniforme, Ley 38-2017, según enmendada.

Sección 6.4 – Vigencia
Este Reglamento tendrá vigencia a partir de su aprobación.

Sección 6.5 – Derogación
Queda expresamente derogado el Reglamento Núm. 25, Reglamento para el Uso de los Sistemas de Información de la Oficina del Contralor Electoral. Asimismo, queda derogada cualquier disposición contenida en reglamentos, cartas circulares u órdenes administrativas de la OCE que sea incompatible con el presente Reglamento, exclusivamente en cuanto alcance dicha incompatibilidad.

Toda referencia al derogado Reglamento Núm. 25, Reglamento para el Uso de los Sistemas de Información de la Oficina del Contralor Electoral, contenida en cualquier reglamento, carta circular, orden administrativa, determinación o cualquier otro documento oficial de la OCE, se entenderá hecha al Reglamento Núm. 50, Reglamento para el Uso de los Sistemas de Información de la Oficina del Contralor Electoral.

Sección 6.6 – Distribución
Copia de este reglamento será distribuido a cada empleado de forma electrónica y cada empleado deberá firmar una declaración de recibo y de haber leído su contenido. La División de Apoyo Tecnológico mantendrá un archivo de evidencia de distribución y recibo del reglamento por los empleados.

En San Juan, Puerto Rico a 22 de septiembre de 2026.

Walter Vélez Martínez
Contralor Electoral