Hon. Jorge R. Rivera Rueda
Presidente

ORDEN ADMINISTRATIVA CEE-26-006-OA

ASUNTO: APROBACIÓN Y ADOPCIÓN DEL REGLAMENTO NÚM. CEE-008-RA SOBRE LAS NORMAS PARA EL USO DE LOS SISTEMAS DE INFORMACIÓN, DE INTERNET Y DEL CORREO ELECTRÓNICO DE LA COMISIÓN ESTATAL DE ELECCIONES.

En ejercicio de las facultades que me confiere el Artículo 3.8 de la Ley Núm. 58-2020, según enmendada, conocida como "Código Electoral de Puerto Rico de 2020", y en virtud de la Orden Administrativa CEE-25-001-OA, según enmendada, se emite la presente Orden Administrativa para aprobar y adoptar formalmente el Reglamento Núm. CEE-008-RA sobre las Normas para el Uso de los Sistemas de Información, de Internet y del Correo Electrónico de la Comisión Estatal de Elecciones.

Este reglamento establece las normas y controles para el uso adecuado, seguro y responsable de los sistemas de información, el acceso a Internet y el correo electrónico institucional de la Comisión Estatal de Elecciones. Su propósito es proteger la confidencialidad, integridad y disponibilidad de la información y de los recursos tecnológicos de la Comisión, garantizando su utilización exclusivamente para fines oficiales. Además, define las responsabilidades de los usuarios y las medidas de seguridad necesarias para prevenir accesos no autorizados, incidentes de seguridad y el uso indebido de los sistemas institucionales.

El Reglamento entrará en vigor y será de cumplimiento obligatorio a partir de la fecha de esta Orden Administrativa, y permanecerá vigente hasta que sea enmendado, derogado o sustituido conforme a derecho.

En San Juan, Puerto Rico, hoy 30 de junio de 2026.

Hon. Jorge R. Rivera Rueda
Presidente

PO Box 195552
San Juan, PR 00919-5552
presidencia@cee.pr.gov
787-777-8675

www.ceepur.org

Reglamento Núm. CEE-008-RA sobre las Normas para el uso de los Sistemas de Información, de Internet y del Correo Electrónico de la Comisión Estatal de Elecciones de Puerto Rico

Aprobado: 30 de junio de 2026

COMISIÓN ESTATAL
DE ELECCIONES DE
PUERTO RICO

TABLA DE CONTENIDO

I: DISPOSICIONES GENERALES

1.1 – Descripción

La Comisión Estatal de Elecciones (en adelante, la "Comisión"), define y detalla esta Política sobre el uso aceptable de la información que se maneja a través de los sistemas de información, así como sus herramientas de Internet y correo electrónico, en aras de proteger al usuario y a la agencia de situaciones que pongan en peligro los sistemas y la información en sus servidores.

1.2 – Título

Esta política se conocerá como las *Normas para el Uso de los Sistemas de Información, de Internet y del Correo Electrónico de la Comisión Estatal de Elecciones*.

1.3 – Base Legal

Estas Normas se promulgan en virtud y de conformidad con las disposiciones de los Artículos 3.8 (3) y 14.4 de la Ley Núm. 58-2020, según enmendada, conocida como "Código Electoral de Puerto Rico de 2020".

1.4 – Propósito

El propósito de esta política es fijar las normas fundamentales que deben regir los controles básicos a ser establecidos por el personal de la Comisión de manera que se garantice el uso adecuado de los recursos relativos a los sistemas de información.

1.5 – Aplicabilidad

Estas normas serán aplicables a todo el personal de la Comisión y a sus contratistas mientras utilicen los sistemas de información y demás recursos tecnológicos de la Comisión.

1.6 – Interpretación

Las disposiciones de estas normas se interpretarán según el contexto y el significado por el uso común y corriente.

Las palabras y frases utilizadas en este Reglamento se interpretarán según el contexto aceptado por el uso común y corriente; las usadas en el presente incluye el futuro; el

número singular incluye el plural; y las usadas en el género masculino incluyen también al femenino y el neutro, salvo en los casos que tal interpretación resulte absurda.

1.7 – Definiciones

1. **Acceso no autorizado** – ocurre cuando una persona obtiene acceso lógico o físico sin aprobación o consentimiento a una red de infraestructura crítica, sistema, datos, aplicación u otro recurso de tecnología de la Comisión.
2. **Antivirus** - programa que protege a los sistemas de los ataques de virus conocidos.
3. ***Antispam*** – programa que detecta correos electrónicos no deseados y prohíbe la entrada de estos al manejador de correos electrónicos.
4. **Archivo** – grupo de registro de datos que se almacena en algún medio interno o externo a un sistema de información.
5. ***Chat*** – intercambio de mensajes electrónicos a través de internet que permite establecer una conversación entre dos o más personas de forma escrita, visual y/o verbal.
6. **Cifrado – (*encrypted*)** – significa un procedimiento criptográfico en el que el texto sin formato se convierte a un formato de texto cifrado para evitar que cualquier persona, excepto el destinatario previsto, lea dichos datos.
7. **Contraseña** - secuencia de caracteres que se utiliza para comprobar que el usuario que está requiriendo acceso a un sistema es realmente ese usuario.
8. **Equipo** – cualquier propiedad tangible y duradera de la Comisión 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 de la Comisión.
9. ***Firewall*** - significa una entrada que, siguiendo una política de seguridad local, limita el tráfico de comunicación de datos hacia y desde una de las redes conectadas para proteger los recursos del sistema de esa red contra las amenazas de la otra red.
10. **Incidente de Seguridad de la Información** – evento o conjunto de eventos que compromete o tiene el potencial de comprometer la confidencialidad, integridad o

disponibilidad de la información, los sistemas de información, las redes, los equipos o los servicios tecnológicos de la Comisión.

11. **Lenguaje discriminatorio** - expresiones que podrán percibirse como ofensivas, ya sea por razones de raza, sexo, origen, nacionalidad, orientación sexual, edad, impedimento, religión o ideales políticos.
12. **Oficina** – división, área, departamento, dependencia, organismo o unidad, conformado según la estructura organizacional de la Comisión.
13. ***Phishing*** **-** técnica fraudulenta utilizada para obtener información confidencial mediante correos electrónicos, mensajes o sitios web que aparentan ser legítimos.
14. **Programa o *Software*** – se refiere a los programas informáticos y datos asociados que pueden escribirse o modificarse dinámicamente durante la ejecución.
15. **Sistema de información** – conjunto discreto de recursos de información para la recopilación, procesamiento, mantenimiento, uso, intercambio, difusión o disposición de información.
16. ***Spam*** – correo electrónico no solicitado que por lo general no guarda relación con las funciones del destinatario.
17. ***Streaming*** - en informática y telecomunicaciones, transferencia continua de datos a través de internet que permite a un usuario acceder a transmisiones audiovisuales en directo o en diferido, sin necesidad de descargar previamente el contenido en el dispositivo.
18. **Usuario** - empleado de la Comisión o contratista que tiene acceso autorizado a los sistemas.
19. **Virus** - programa malicioso que, al ejecutarse, replica su código con el fin de hacerle daño a la computadora donde reside.

II: USO DE LOS SISTEMAS DE INFORMACIÓN DE LA COMISIÓN

2.1 – Normas Generales

1. Los sistemas de información son herramientas de trabajo que la Comisión le provee a sus empleados y contratistas.
2. Los sistemas de información, sus programas, aplicaciones y archivos electrónicos son propiedad de la Comisión, por lo que solo pueden ser utilizados para fines estrictamente oficiales y legales. Este sistema de información debe constar en el inventario de la Comisión y ser revisado anualmente constatándolo en documento oficial.
3. El Presidente de la Comisión o su representante autorizado, supervisará y restringirá conforme a estas normas y las leyes y reglamento aplicables el contenido de su sistema de información accesible a los usuarios. Además, se reservará el derecho de limitar o prohibir el acceso de los usuarios a los sistemas de información cuando se violen estas normas o leyes y reglamentos aplicables.
4. Ningún dispositivo personal podrá conectarse a la red institucional o almacenar información oficial sin autorización previa de la Oficina de Sistemas de Información y Procesamiento Electrónico (en adelante, "OSIPE"). De autorizarse, la Comisión no será responsable por daños a equipos o archivos personales de los usuarios causados por fallas en el sistema de información de la Comisión.
5. El Presidente podrá actuar e imponer medidas correctivas y acciones disciplinarias sobre aquellos empleados que por negligencia o a propósito alteren, dañen, modifiquen o eliminen el sistema de información de la Comisión y/o incumplan o violenten estas normas.
6. La Comisión tendrá los derechos de programación, desarrollados internamente o adquiridos, así como toda la información que se genere, resida o se desarrolle en sus sistemas de información o redes, salvo se establezca lo contrario en un contrato.

7. La Comisión avisará a todos sus usuarios al acceder al sistema de información que el mismo es propiedad de la Comisión y que se compromete a utilizarlo conforme a las normas establecidas.
8. Los sistemas de información y las herramientas asociadas, como el correo electrónico y la Internet, solo podrán ser utilizados por personal debidamente autorizado. El uso de tales recursos constituye un privilegio otorgado con el propósito de agilizar los trabajos de la agencia y no es un derecho.
9. La información desarrollada, transmitida o almacenada en los sistemas de información de la Comisión es propiedad de la agencia, por lo que les aplican todas las disposiciones legales aplicables a los documentos públicos, con excepción de aquellos documentos que por disposición de ley, reglamento o medida aplicable sean considerados para todos los fines privados y/o privilegiados o generados como parte de labores ordinarias. La divulgación de tal información sin autorización está estrictamente prohibida. La alteración fraudulenta de cualquier documento en formato electrónico conllevará las sanciones aplicables a la alteración fraudulenta de documentos públicos.
10. Los documentos generados o contenidos en los sistemas de información de la Comisión serán parte de los expedientes oficiales de la entidad. La destrucción de tales documentos electrónicos estará sujeta a las sanciones aplicables a la destrucción de documentos públicos, excepto en casos que dichos documentos sean considerados privados y/o privilegiados, o aquellos cuyo decomiso o destrucción sea ordenado por ley, reglamento o medida aplicable.
11. Los usuarios de los sistemas de información están obligados a respetar los derechos de propiedad intelectual de los autores de las obras, programas, aplicaciones u otros, manejadas o accedidas a través de dicho sistema.
12. Los programas y recursos utilizados en los sistemas de información de la Comisión deben tener su correspondiente licencia vigente o autorización de uso para poder

ser utilizados. Dichos programas solo podrán ser instalados por personal autorizado a tales efectos. Además, no podrán instalarse programas sin la previa autorización de la OSIPE.

13. Los programas y aplicaciones contenidos en los sistemas de información no podrán reproducirse sin autorización o ser utilizados para fines ajenos a las funciones o poderes de la Comisión.
14. La OSIPE será responsable de implementar medidas de seguridad como: claves secretas (contraseñas), controles de acceso a los servidores y sistemas para auditar su uso, la integridad y la seguridad de los datos y comunicaciones que se envían. Los usuarios de los sistemas deberán cumplir con todas las normas de uso y las relativas a la seguridad de la información emitidas por la Comisión. Cada usuario será individualmente responsable por el manejo adecuado de los códigos de acceso o contraseñas asignadas.
15. La correspondiente asignación de códigos de acceso no impedirá que el uso de los sistemas de información sea auditado por el personal autorizado de la Comisión a tales fines, con el propósito de garantizar el uso apropiado de los recursos. Dicha autorización solamente podrá ser concedida por el Presidente o su representante autorizado, motu proprio o a solicitud de parte debidamente justificada. Asimismo, los usuarios no deben tener expectativa de privacidad alguna con relación a la información almacenada en su computadora o que sea emitida o comunicada a través de los sistemas de información de la Comisión, excepto en aquellos casos que la información sea considerada privilegiada y/o privada por ley, reglamento o medida adoptada.
16. El acceso no autorizado a información o a una cuenta ajena, obtenido mediante la modificación de privilegios de acceso o la interceptación de información en cualquier otra manera está prohibido, por lo que tal conducta se castigará conforme

a la legislación local y federal vigente y a las normas aplicables que rigen la conducta de los empleados.

2.2 – Normas Aplicables al Uso de Internet

1. Los sistemas de comunicación y acceso a la Internet son propiedad de la Comisión y deberán ser utilizados exclusivamente como una herramienta de trabajo conforme a las normas que rigen el comportamiento del personal de la entidad y nunca con fines no oficiales o para actividades personales o con fines de lucro.
2. Los usuarios que tengan acceso al Internet no tienen expectativa de privacidad interna alguna con relación al uso y los accesos realizados a través de la Internet. La Comisión se reserva el derecho a intervenir y auditar los accesos realizados por los usuarios a través de su sistema de información, el acceso a la Internet y el contenido de lo accedido.
3. La Comisión no se responsabiliza por la validez, calidad, contenido o corrección de la información contenida en la Internet.
4. La publicación de información de la Comisión a través del Internet será previamente autorizada por el Presidente de la Comisión o su representante autorizado.

2.3 – Normas Aplicables al Uso del Correo Electrónico Institucional

1. El sistema de correo electrónico es propiedad de la Comisión y es parte íntegra de sus sistemas de información, por lo que la misma se reserva el derecho absoluto de intervenir, auditar e investigar para constatar el uso adecuado del mismo.
2. Los usuarios de las cuentas de correo electrónico no tienen expectativa de privacidad alguna con relación a la información contenida en dichas cuentas. Las cuentas están sujetas a auditorías y revisiones sin previo aviso por el personal de la Comisión autorizado por el Presidente o su representante autorizado a tales efectos.
3. El correo electrónico podrá utilizarse únicamente para propósitos oficiales relativos a las funciones de la Comisión. Se prohíbe el uso de éste para asuntos no oficiales

o actividades personales con o sin fines de lucro o en menoscabo de la imagen de la Comisión o sus empleados. Los usuarios deberán velar por el cumplimiento de las normas aplicables al comportamiento de los empleados de la Comisión al momento de utilizar el correo electrónico.

4. No se debe utilizar el correo personal para comunicaciones/funciones oficiales, excepto en caso de contratistas externos que tengan su propio correo electrónico asociado con sus servicios o por autorización expresa del Presidente o su representante autorizado.
5. Solo la OSIPE como administradora del servidor de correo electrónico estará autorizada a incorporar los criterios de acceso a cuentas de correo conforme al perfil del usuario.
6. La OSIPE dispondrá de una lista de emisores no deseados con la cual se deberá filtrar todo correo no deseado.
7. Las cuentas de correo electrónico de cada usuario serán válidas hasta que finalice la relación laboral o contractual adquirida con la Comisión, según sea el caso.
8. El usuario deberá notificar a la OSIPE si requiere una ampliación temporal al criterio del tamaño del buzón electrónico, cuando requiere enviar o recibir un correo electrónico sobre el límite asignado.
9. El usuario deberá notificar a la OSIPE si requiere una ampliación temporal para enviar o recibir correos electrónicos que contengan archivos con extensiones restringidas o sobre el límite asignado.
10. La OSIPE podrá realizar la ampliación o extensión de las secciones 2.3(8) y 2.3(9) siempre y cuando se tenga la capacidad para realizarlo sin que el sistema se vea afectado.
11. Los correos electrónicos entrantes se tratarán a través de un sistema de antivirus y *antispam*, previo a que el usuario tenga acceso al contenido de estos.

12. La OSIPE se asegurará de que los usuarios cuenten con un sistema de depuración de buzones con el cual periódicamente se eliminen aquellos correos que se encuentran en desuso.

2.4– Normas Aplicables a los Nombres de Usuarios y Contraseñas

1. Los usuarios están prohibidos de compartir sus contraseñas y medios de acceso sin la debida autorización.
2. La OSIPE notificará a los usuarios para que cambien sus contraseñas al menos cada cuarenta y cinco (45) días.
3. Las contraseñas deberán ser seguras y difíciles de descifrar.
4. El sistema de la Comisión requiere el uso de dos contraseñas distintas antes de que se permita reutilizar la primera contraseña a un usuario.
5. El sistema tendrá un término de siete (7) días contados a partir del cambio de contraseña para que el sistema le permita al usuario cambiarla nuevamente.
6. Se requerirá un mínimo de seis (6) caracteres alfanuméricos en las contraseñas.

2.5– Creación de Perfiles de Acceso a la Red y a los Sistemas de Información

El Director de Recursos Humanos notificará a la OSIPE la información del personal de la Comisión al cual requiera la creación de un perfil de acceso a la red y a los sistemas de información. La OSIPE agrupará los usuarios conforme a las clases del Plan de Clasificación y Retribución de la Comisión. En el caso de los contratistas de la Comisión, el Presidente o su representante autorizado notificará a la OSIPE la información del contratista al cual desea se le cree un perfil con acceso a la red y a los sistemas de información de la Comisión. De igual forma, el Director de Recursos Humanos, el Presidente o su representante autorizado podrán notificar a la OSIPE si se requiere la modificación de algún perfil.

2.6 – Cierre de Perfiles de Acceso a la Red y a los Sistemas de Información

El Director de Recursos Humanos será responsable de notificar por escrito a la OSIPE los nombres completos de los empleados que han cesado funciones en la Comisión para que estos puedan deshabilitar los perfiles. El Presidente o su representante autorizado

notificará lo propio cuando se trate de contratistas. La OSIPE tendrá un término de treinta (30) días para deshabilitar los perfiles que le fueron notificados desde la notificación.

2.7 – Acceso a la Red y a los Sistemas de Información

Todo acceso a la red y a los sistemas de información de la Comisión serán solicitados a la OSIPE por el Presidente, su representante autorizado o por el Director de Recursos Humanos mediante la Hoja de Autorización de Acceso a la Red y Uso de Sistema de Información. En la misma se indicará la clase del empleado o si es un contratista y la oficina a la cual pertenece el usuario. La Hoja de Autorización de Acceso a la Red y Uso de Sistema de Información deberá ser firmada por el supervisor inmediato del empleado o en caso de ser un contratista por el Director de Asuntos Legales o su representante autorizado. Los accesos estarán regidos por el perfil de acceso previamente creado. Los accesos que se otorguen a contratista se regirán conforme al perfil de acceso creado de acuerdo con las tareas encomendadas a cada contratista.

2.8 – Limitación de Acceso a la Red y a los Sistemas de Información

La OSIPE notificará al Presidente de la Comisión, inmediatamente de que advenga en conocimiento de una amenaza a la seguridad de la red o de los propios sistemas de información. La OSIPE limitará, aislará o bloqueará el acceso a la red y a los sistemas de información de la Comisión, previa autorización del Presidente, hasta tanto se resuelva o cese la amenaza o se imparta alguna otra instrucción.

2.9 – Medidas de Seguridad

Los sistemas de información de la Comisión no se utilizarán para la creación o distribución de ningún material que se considere inapropiado, irrespetuoso, ofensivo, amenazante, abusivo, difamatorio, ilegal, sexista, racista, sexualmente explícito, fraudulento o discriminatorio contra otros. Del mismo modo, está prohibido el uso del Internet para realizar actos ilícitos, incluido el acceso a sitios web con contenido ilegal, obsceno, odioso, difamatorio, indecente, objetable o inapropiado.

En ninguna circunstancia la información confidencial quedará expuesta ni desprotegida.

Los usuarios deben evitar abrir y ejecutar archivos de fuentes desconocidas o no confiables. En caso de recibir algún archivo que entiendan proviene de una fuente desconocida o desconfiable deberán referir el asunto al personal de la OSIPE para validar el mismo antes de descargar y ejecutar los archivos.

No se instalará ningún programa (*software*) en los dispositivos y equipos de la Comisión sin la aprobación de la OSIPE. Solo se instalarán programas debidamente autorizados y con licencia. Se prohíbe el uso de programas no autorizados, sin licencia o copiados ilegalmente.

2.10 – Responsabilidades de los Empleados y Contratistas

1. Actuar de forma profesional y responsable en el desempeño de sus funciones y den a conocer cualquier actividad o evento sospechoso, accidental o intencional que comprometa la integridad, disponibilidad y/o confidencialidad de la información.
2. El incumplimiento de la política y lo planteado en estas normas puede resultar en una medida correctiva o acción disciplinaria en caso de los empleados o la cancelación de contratos en caso de los contratistas.
3. Actuar con precaución y cuidado al utilizar cualquier sistema de información, servicio o plataforma tecnológica para evitar la divulgación no autorizada o inadvertida de información sensible, confidencial o personal.
4. Ser cauteloso con los mensajes y tecnologías sospechosos que podrían tener la intención de atraer a un usuario a un incidente cibernético malicioso.
5. Usar los sistemas de información de la Comisión sólo para tareas oficiales relacionadas con la agencia que correspondan a las funciones y responsabilidades del usuario.
6. Mantener las contraseñas secretas y seguras. Los usuarios no se apropiarán, divulgarán o utilizarán las credenciales de inicio de sesión de alguien sin la autorización previa del Presidente o su representante autorizado.

7. Cada usuario se considerará responsable de todos los actos que se registren en su cuenta. Por tal razón, los usuarios deben asegurar sus cuentas y desconectar o cerrar las mismas una vez terminen de utilizarlas para evitar el acceso o uso de terceros.
8. El usuario tomará las precauciones adecuadas y necesarias para evitar daños, pérdidas o robos de cualquier dispositivo o equipo gubernamental emitido para su uso.
9. El usuario informará de inmediato al supervisor y al personal de OSIPE si un dispositivo o equipo se ha perdido, robado o comprometido (ya sea una sospecha o se haya confirmado).
10. Los usuarios deberán de abstenerse de abrir correos electrónicos de dudosa procedencia o contenido.

2.11 – Responsabilidades de los Directores y de la OSIPE

Los directores de las oficinas de la Comisión serán responsables de hacer cumplir estas normas y de informar a la OSIPE cualquier irregularidad.

La OSIPE será responsable de monitorear e informar al Presidente o su representante autorizado sobre el cumplimiento de estas normas o cualquier irregularidad ocurrida.

La OSIPE será responsable de bloquear el acceso de los usuarios a páginas de Internet con contenido discriminatorio, pornográfico, religioso, de entretenimiento, juegos, *streaming*, así como cualquier otra página de internet cuyo contenido no esté relacionado con las funciones oficiales de la Comisión. de la Comisión.

2.12 – Prohibiciones Generales

1. Añadir, modificar o eliminar componentes de los sistemas de información, excepto empleados o contratistas designados para estos propósitos.
2. Interceptar o tener acceso a información que ha sido restringida o se considera privilegiada o confidencial sin la debida autorización.

3. Utilizar los sistemas de información, redes o servicios de correo electrónico para otros propósitos que no sea cumplir con las funciones oficiales.
4. Prestar u otorgar un *software* cuya licencia sea propiedad de la Comisión.
5. Permitir el uso de los programas informáticos o *softwares* de la Comisión a personas ajenas a esta, excepto cuando medie autorización para esto.
6. Instalar, copiar, utilizar o distribuir software de propiedad personal en las computadoras o redes de la Comisión.
7. Usar medios de almacenaje de la Comisión para guardar información personal o no autorizada.
8. Establecer conexiones no autorizadas a redes externas.
9. Cambiar o alterar los parámetros de configuración de comunicación sin autorización.
10. Utilizar los sistemas de información de la Comisión para enviar, recibir o crear mensajes o documentos o divulgar opiniones de contenido discriminatorio por razón de raza, color, sexo, género, orientación sexual, nacimiento, origen o condición social, ideas políticas o religiosas e impedimentos físico o mental.
11. Enviar, recibir o crear mensajes o documentos cuyo contenido pueda ser catalogado como de hostigamiento sexual o laboral, según tipificado por la ley o reglamentos aplicables.
12. Descargar e instalar programas de Internet u otras redes sin aprobación previa.

2.13– Prohibiciones Específicas del Uso de la Red

1. La transmisión de información o realización de actos que infrinjan o amenacen con violentar las reglas, visión y misión de la Comisión o que vayan en contra de la ley, la moral y el orden público.
2. Fines personales o de lucro.
3. La circulación de información difamatoria de cualquier tipo ya sea contra entidades o personas.

4. El desarrollo de actividades que produzcan la congestión de la red mediante el envío de información, mensajes o programas concebidos para tal fin. Por ejemplo, este tipo de actividad podrá ser *streaming* de audio o video, o programas de chat no autorizados previamente.
5. La destrucción, manipulación, apropiación o modificación que no esté debidamente autorizada de la información de otros usuarios que circula por la red.
6. La obtención y el uso de cuentas ajenas.
7. Compartir contraseñas u otro tipo de información que permite que otros usuarios o personal no autorizado pueda acceder al sistema de la Comisión.
8. La conexión, desconexión o reubicación de equipos sin autorización previa.
9. Acceder a páginas de internet de índole discriminatorio, pornográfico, religioso, de entretenimiento, juegos, *streaming*, así como cualquier otra página de internet que no corresponda a las funciones inherentes de la Comisión.
10. El uso de *streaming*, chat o redes sociales para propósitos personales, diversión o entretenimiento está prohibido. No obstante, se podrá autorizar su uso siempre y cuando sea para propósitos educativos o de informar al electorado.

2.14 – Acceso a la Red para Uso de Entidades Gubernamentales y Contratistas

La Comisión podrá brindar acceso al Internet a agencias gubernamentales y/o entidades contratadas que así los soliciten a la Oficina del Presidente. Una vez autorizado por el Presidente, la OSIPE se asegurará de brindar el acceso y conexión al Internet de forma directa, separada y aislada de los sistemas de información de la Comisión.

2.15 – Auditorías

Los datos e información producida, transmitida o almacenada en cualquier sistema de información será propiedad de la Comisión y estará accesible para ser examinada, auditada y utilizada en trámites oficiales por funcionarios autorizados de la Comisión.

La OSIPE podrá auditar los sistemas de información sin previo aviso con el aval del Presidente o su representante autorizado. Se exceptúan de estas auditorías la Oficina del

Presidente, las oficinas de los Comisionados Electorales y ciertas oficinas que están revestidas de confidencialidad política, elemento esencial e indispensable del balance político que sostiene el sistema electoral.

Los directores de oficinas, los Comisionados Electorales y la Oficina del Presidente podrán solicitar a la OSIPE auditoría por conducto del Presidente para sus respectivas oficinas, de considerarlo necesario.

2.16 – Privacidad

La Comisión respetará la privacidad de los usuarios, pero se reserva el derecho de inspeccionar el uso de los sistemas de información cuando haya sospecha de violaciones a las leyes federales, estatales o sus propias normas y reglamentos. De igual forma, la Comisión podrá inspeccionar el uso de los sistemas de información cuando haya una situación de emergencia o una amenaza a la seguridad de la red o los sistemas de información.

La Comisión hará un esfuerzo razonable para notificar al usuario concernido antes de tener acceso a los archivos que inspeccionará. La Comisión podrá acceder a los archivos en caso de que no se logre la notificación al usuario.

2.17 – Notificación y Manejo de Incidentes de Seguridad de la Información

Todo empleado o contratista que tenga conocimiento, sospecha o evidencia de un incidente de seguridad de la información deberá notificarlo inmediatamente a su supervisor y a la OSIPE.

Se considerarán incidentes de seguridad de la información, entre otros:

1. Accesos no autorizados o intentos de acceso a sistemas, aplicaciones, cuentas o información de la Comisión.
2. Pérdida, robo o extravío de equipos, dispositivos móviles, medios de almacenamiento o credenciales de acceso.
3. Infecciones o sospechas de infecciones por virus, *malware* u otros programas maliciosos.

4. Correos electrónicos, mensajes o comunicaciones sospechosas relacionadas con intentos de fraude, phishing o suplantación de identidad.
5. Divulgación, alteración, destrucción o acceso no autorizado a información confidencial, sensitiva o de uso oficial.
6. Cualquier situación que pueda afectar la confidencialidad, integridad o disponibilidad de los sistemas de información o de los datos de la Comisión.

La OSIPE notificará al Presidente de la Comisión o a su representante autorizado y recomendará las medidas correctivas correspondientes.

La OSIPE evaluará el incidente reportado y adoptará las medidas técnicas y administrativas necesarias para contener, mitigar, documentar y corregir la situación, así como para preservar cualquier evidencia que pueda ser necesaria para fines administrativos, civiles o criminales.

Ningún empleado o contratista intentará investigar, contener o remediar por cuenta propia un incidente de seguridad sin la coordinación de la OSIPE, salvo aquellas medidas inmediatas necesarias para proteger la información o los equipos de daños mayores.

La OSIPE se asegurará de que todo incidente de seguridad sea documentado y conservado conforme a los procedimientos internos de la Comisión y a las disposiciones legales y reglamentarias aplicables.

III: DISPOSICIONES FINALES

3.1 – Acciones Disciplinarias

Cualquier violación a estas normas será causa para el inicio de un proceso administrativo en contra del usuario que podría conllevar medidas correctivas o acciones disciplinarias en conformidad con la normativa vigente en la Comisión. De ser ese el caso, la Oficina de Asuntos Legales, con la asistencia de la OSIPE realizará una evaluación e investigación de

la situación y someterá un informe con los hallazgos y recomendaciones al Presidente de la Comisión para su debida evaluación.

3.2 – Cláusula de Salvedad

Si cualquier capítulo, artículo, sección, inciso o párrafo de estas Normas fuera declarada inconstitucional, inválida o nula por un tribunal de jurisdicción competente, las disposiciones restantes de las Normas continuarán vigentes.

3.3 – Cláusula Derogatoria

Estas Normas dejan sin efecto las *Normas para el Uso de los Sistemas de Informática*, aprobado el 23 de abril de 2015, así como cualquier otra norma emitida previamente relacionada específicamente a los asuntos regulados en estas Normas.

3.4 – Vigencia

Estas Normas entrarán en vigor inmediatamente después de su aprobación.

3.5 – Aprobación

Aprobado en San Juan, Puerto Rico, el 30 de junio de 2026.

Hon. Jorge R. Rivera Rueda
Presidente