Autoridad del Distrito del Centro de Convenciones del Gobierno de Puerto Rico

REGLAMENTO DE NORMAS Y CONTROLES PARA EL USO, ADMINISTRACIÓN Y ADQUISICIÓN DE LOS SISTEMAS TECNOLÓGICOS DEL DISTRITO DEL CENTRO DE CONVENCIONES

04 de marzo de 2021

AUTORIDAD DEL DISTRITO DEL CENTRO DE CONVENCIONES DE PUERTO RICO

La Autoridad del Distrito del Centro de Convenciones de Puerto Rico (en adelante, "Autoridad"), es una corporación pública e instrumentalidad gubernamental con personalidad jurídica propia,[1] creada para servir como "… entidad responsable, por sí misma o mediante contrato con terceros, de mejorar, desarrollar, administrar y operar la propiedad y las mejoras localizadas en el Distrito [del Centro de Convenciones de Puerto Rico]".[2] En esencia, la Autoridad fue concebida para apoyar el uso del centro de convenciones, comercio y exhibiciones, por parte de grupos y convenciones nacionales e internacionales en el Distrito.[3]

> Al atraer visitantes del exterior mediante el desarrollo de un adecuado centro de convenciones, comercio y exhibiciones y de las facilidades de apoyo adecuadas, se espera estimular considerablemente el desarrollo económico en industrias relacionadas al turismo como lo son las industrias de transportación, hoteles, restaurantes, recreación, diversión y establecimientos de ventas al detal. Al estimular dichas industrias de servicios se promoverá a su vez el desarrollo económico general del gobierno de Puerto Rico, se fomentará el desarrollo y la inversión privada y se proveerán nuevas y mejores oportunidades de empleo, proveyendo así beneficios importantes para el bienestar general de los puertorriqueños.[4]

Las responsabilidades delegadas a la Autoridad y que nos honramos día a día en cumplir, constituyen propósitos públicos de tal importancia para el beneficio general del Pueblo de Puerto Rico, la industria de hospitalidad y el gobierno, que la propia Ley Habilitadora dispone que el ejercicio de las facultades y los derechos conferidos en ese estatuto, constituyen el desempeño de <u>funciones esenciales de gobierno</u>.[5]

Este Reglamento se adopta con el propósito de establecer las normas y controles para el uso, administración y adquisición de los sistemas tecnológicos, a seguir por la Autoridad del Distrito del Centro de Convenciones del Gobierno de Puerto Rico. Mediante este, se persigue establecer los controles internos necesarios para garantizar, razonablemente, la seguridad y confiabilidad de los sistemas de información tecnológicos de la Autoridad del Distrito del Centro de Convenciones del Gobierno de Puerto Rico, así como la integridad y disponibilidad de los datos y la continuidad de las operaciones en caso de emergencias. Además, se busca asegurar la efectividad de los procesos

---

[1] Artículo 1.05, Ley 351-2000, según enmendada, conocida como "Ley del Distrito del Centro de Convenciones de Puerto Rico"**.**

[2] Exposición de Motivos, Ley 351-2000, *supra*.

[3] *Id*. El Coliseo de Puerto Rico "José Miguel Agrelot" está adscrito al Distrito, el cual también incluye el "*Ribas Dominicci Executive Airport*".

[4] *Id*.

[5] Subrayado nuestro. Artículo 6.01, Ley 351-2000, *supra*.

utilizados en la planificación, el desarrollo y la implementación de los proyectos tecnológicos, así como la adquisición, el control y la disposición de los equipos.

CAPÍTULO I. INTRODUCCIÓN

Artículo 1.1- Título

Este Reglamento se conocerá como "Reglamento de normas y controles para el uso, administración y adquisición de los sistemas tecnológicos del Distrito del Centro de Convenciones".

Artículo 1.2.- Base legal

Se promulga este Reglamento de conformidad con lo dispuesto en la Ley 351-2000, según enmendada, conocida como "Ley del Distrito del Centro de Convenciones de Puerto Rico"; y la Ley 38-2017, según enmendada, conocida como "Ley de Procedimiento Administrativo Uniforme del Gobierno de Puerto Rico" (L.P.A.U).

Artículo 1.3.- Propósito

La política pública vigente en cuanto a el uso, administración y adquisición de sistemas tecnológicos en el Gobierno de Puerto Rico, es la de "… crear un nuevo andamiaje de gobierno innovador, atemperado a las exigencias del siglo XXI y capaz de valerse de la tecnología avanzada, para cumplir con las expectativas de la ciudadanía y con los estándares modernos de gobernanza efectiva. Esto responde a que está probado que la innovación en los desarrollos tecnológicos y en la programación informática promueve la eficiencia gubernamental y un manejo más apropiado de los recursos humanos y físicos, lo que se traduce en un desarrollo económico de Puerto Rico positivo".[6]

Ciertamente, "[l]a incorporación oportuna de la tecnología a los programas y servicios del gobierno es un valioso instrumento para reducir el tiempo de gestión y los costos de operación, y para hacer más accesibles los servicios que se prestan a los ciudadanos". Pero ello, a la vez, "…requiere una inversión de recursos considerable, en el desarrollo, la adquisición, la implementación, la seguridad y el mantenimiento de los sistemas de información, y en la contratación de servicios profesionales de asesoría técnica en sistemas [tecnológicos]. La inversión de fondos públicos en tecnología de información debe planificarse, de manera que se obtengan los beneficios esperados en un tiempo razonable".[7]

Mediante este Reglamento se persigue establecer los controles internos necesarios para garantizar, razonablemente, la seguridad y confiabilidad de los sistemas

[6] Exposición de Motivos, Ley 75-2019.
[7] "Normas Generales Sobre la Implantación de Sistemas, Compra de Equipos y Programas y Uso de la Tecnología de Información para los Organismos Gubernamentales', Carta Circular 140-16 de la Oficina de Gerencia y Presupuesto de 7 de noviembre de 2016, Págs. 2-3.

de información tecnológicos de la Autoridad del Distrito del Centro de Convenciones del Gobierno de Puerto Rico, así como la integridad y disponibilidad de los datos y la continuidad de las operaciones en caso de emergencias.

Artículo 1.4.- Jurisdicción y alcance

Las disposiciones de este Reglamento aplicarán a todos los procesos relacionados a el uso, administración y adquisición de los sistemas tecnológicos de la Autoridad del Distrito del Centro de Convenciones. Asimismo, aplicará a todo empleado o funcionario de la Autoridad del Distrito del Centro de Convenciones, a los miembros de su Junta de Directores y a toda persona natural o jurídica que administre o utilice los sistemas tecnológicos del Distrito del Centro de Convenciones, incluyendo a contratistas.

Artículo 1.5.- Interpretación

Las disposiciones de este Reglamento se interpretarán de manera integrada con lo dispuesto en la Ley 351-2000, según enmendada, conocida como “Ley del Distrito del Centro de Convenciones de Puerto Rico”; Ley Núm. 151-2004, según enmendada, conocida como “Ley de Gobierno Electrónico”; “Ley para la Competencia Justa en Servicios de Telecomunicaciones, de Información y Televisión por Paga en Puerto Rico”, Ley 80-2017; Ley 75-2019, conocida como “Ley de la Puerto Rico Innovation and Technology Service (PRITS)”; la Ley Núm. 5 del 8 de diciembre de 1955, conocida como “Ley de Administración de Documentos Públicos de Puerto Rico”, según enmendada; la Ley 38-2017, según enmendada, conocida como “Ley de Procedimiento Administrativo Uniforme del Gobierno de Puerto Rico” (L.P.A.U); y cualesquiera otras leyes, reglamentos, Órdenes Ejecutivas u otras normas vigentes que se adopten al amparo de dichas leyes, tales como, sin que se entienda como una limitación, los siguientes, cuando apliquen:

a. Recopilación de datos sobre la inversión de fondos públicos en equipos y sistemas de información computadorizados sin obtener los beneficios esperados, Informe Especial TI-17-02 de la Oficina del Contralor de 31 de agosto de 2016; y

b. Carta Circular 2020-3 y *Proposal Evaluation Guidelines* (PEG) PRITS-001, de la "*Puerto Rico Innovation and Technology Service*” (PRITS).

Artículo 1.6.- Definiciones

Las palabras o frases usadas en este Reglamento serán interpretadas según el contexto y significado aceptado por el uso común y corriente. Las voces usadas en el tiempo presente incluyen también el futuro; las usadas en singular incluyen el plural, el

plural incluye el singular y, las usadas en el género masculino incluyen el femenino, salvo los casos en que tal interpretación resulte ilógica.

Todo término utilizado para referirse a una persona o a un puesto es sin alusión a género.

Cuando se utilice el término “días” y esté relacionado a un término de tiempo, el mismo será interpretado como días calendario, salvo expresión en contrario.

A los fines de este Reglamento, las siguientes palabras y frases tendrán el significado que se expresa a continuación:

1. **“Acceso”** - Proceso por el cual se proporciona o controla el acceso de usuarios a los recursos de un sistema tecnológico. En una red, es el medio para garantizar la seguridad del sistema que requiere que los usuarios proporcionen un nombre de registro de entrada y una contraseña. Se le llama “acceso remoto" cuando es por medio de una línea de servicio telefónico, Internet o sistema inalámbrico; medio de conexión a otra computadora o a una red.

2. **“Administrador de la Red”** - Persona designada por el Director Ejecutivo que tiene a su cargo la red de comunicación de la Autoridad del Distrito del Centro de Convenciones.

3. **“Antivirus”** - Programa diseñado para detectar y eliminar virus informáticos de una o más computadoras y/o un sistema y/o subsanar daños causados por estos.

4. **“Archivo”** - Documento u acopio de información grabado en un disco, disco compacto, cinta magnética o cualquier otro medio electrónico de almacenamiento, y que se identifica como una unidad mediante un nombre único.

5. **“Autoridad”** - Autoridad del Distrito del Centro de Convenciones del Gobierno de Puerto Rico, creada mediante la Ley 351-2000, según enmendada.

6. **“Barrera de protección de acceso (*Firewall*)”** - Programa informático que controla el acceso de una computadora a la red y de elementos de la red a la computadora, por motivos de seguridad, con el propósito de evitar el acceso y la entrada y salida de archivos, programas y documentos no autorizados, entre otros.

7. **“Base de datos”** - Conjunto almacenado de datos relacionados, necesarios para satisfacer las necesidades de procesamiento y recuperación de información.

8. **“Cinta magnética”** - tipo de medio o soporte de almacenamiento de documentos, datos, audios o videos, que se graba en pistas sobre una banda plástica con un material magnetizado.

9. **“Computadora”** - Máquina electrónica capaz de almacenar información y tratarla automáticamente mediante operaciones matemáticas y lógicas controladas por programas informáticos.

10. **“Contraseña o clave (*Password*)”** - Código secreto que se introduce en una máquina para poder accionar un mecanismo o para acceder a ciertas funciones informáticas; herramienta de seguridad empleada para identificar a los usuarios autorizados de un programa o de una red y para determinar sus privilegios como “solo lectura”, “lectura y escritura”, “descargue de archivos” o “copiado de archivos”, entre otros.

11. **“Contratista o consultor”** - Cualquier persona natural o jurídica o grupo de personas que establecen una relación contractual con la Autoridad del Distrito del Centro de Convenciones para la prestación de servicios tecnológicos.

12. **“Contrato”** - Pacto o convenio suscrito entre partes competentes que se obligan proveerle a la Autoridad del Distrito del Centro de Convenciones bienes o servicios tecnológicos, independientemente de que sean no personales o profesionales y consultivos.

13. **“Control de acceso”** - Proceso por el cual se controla el acceso físico o lógico a los recursos de un sistema tecnológico, solicitándole a los usuarios que proporcionen un nombre de registro de entrada y una contraseña.

14. **“Copias de reserva (Resguardos / Réplicas / *Backups*)**” - Equipo, datos o procedimientos disponibles para utilizar en la eventualidad de una falla o pérdida de los archivos y programas en uso.

15. **“Correo electrónico (*Email*)”** - sistema de correspondencia que permite el intercambio de mensajes entre usuarios que estén conectados a una red informática, pero ubicados en distintas computadoras.

16. **“Descargue”** o **“*Download/Upload* (*Downloading Internet*)"** - Proceso de transferir un archivo o información de una computadora a la propia por medio de una línea de transmisión o sistema inalámbrico Wifi.

17. **“Desconectarse o salir del sistema (*Log off*)”** - Proceso con el que se termina de manera metódica la conexión con un sistema de computadora o un dispositivo periférico.

18. **“Director Ejecutivo”** – principal oficial ejecutivo de la Autoridad del Distrito del Centro de Convenciones del Gobierno de Puerto Rico, nombrado por la Junta

de Gobierno de la Autoridad, conforme a las disposiciones del Artículo 2.01(e) de la Ley 351-2000, según enmendada.

19. **"Director de Oficina"** - Cualquier director de una oficina, dependencia o programa de la Autoridad del Distrito del Centro de Convenciones.

20. **"Director de Tecnología de Información"** – Empleado, funcionario o contratista de la Autoridad del Distrito del Centro de Convenciones, designado como tal por el Director Ejecutivo de la Autoridad del Distrito del Centro de Convenciones.

21. **"Disco Compacto (CD o DVD)"** - Es un disco óptico utilizado para almacenar datos en formato digital, consistentes en cualquier tipo de información (audio, imágenes, vídeo, documentos y otros datos).

22. **"Disco duro (*Hard disk*)"** - Disco con una gran capacidad de almacenamiento de datos informáticos que se encuentra insertado permanentemente en la unidad central de procesamiento de una computadora.

23. **"Disco Externo"** – También conocido como "disco duro portátil", es una unidad de disco duro que es fácil de instalar y transportar de una computadora a otra, sin necesidad de consumir constantemente energía eléctrica o batería o algún otro recurso.

24. **"Distrito"** o **"Distrito del Centro de Convenciones de Puerto Rico"** – zona comprendida dentro del área geográfica delineada en un mapa conservado en las oficinas corporativas de la Autoridad, y que consiste en toda la propiedad inmueble poseída o adquirida por la Autoridad que sea afín con los propósitos de la Ley 351-2000, según enmendada. Incluye el Centro de Convenciones Pedro Rosselló González, el Coliseo de Puerto Rico "José Miguel Agrelot" y el área donde enclava el Aeropuerto de Isla Grande, conocido como "Ribas Dominicci Executive Airport".

25. **"Documento"** - Todo papel, folleto, fotografía, fotocopia, película, microfilme, cinta magnetofónica, mapa, dibujo, plano, cinta magnética, disquete, disco compacto digital, video y cualquier otro material leído por máquina de carácter informativo, sin importar su forma o características físicas.

26. **"Documento de computadora"** - Archivo que contiene trabajos creados por un usuario de computadora.

27. **"Emergencia u urgencia"** - Aquella situación que ocasione unas necesidades públicas inesperadas, imprevistas, urgentes e inaplazables en la Autoridad, que requieran una acción inmediata por estar en peligro la vida, la salud o la seguridad de los funcionarios, empleados o visitantes; por estar en peligro de afectarse o suspenderse las actividades en la Autoridad o dañarse o perderse

propiedad pública; aquella situación en que el Director Ejecutivo su representante autorizado determine que la oportunidad para adquirir los artículos, materiales o equipos pueda perderse, afectando adversamente el buen funcionamiento de la Autoridad; y cualquier otra situación en la que, de no actuarse con la premura y diligencia necesaria, se pudieran afectar los mejores intereses de la Autoridad. Cuando por causa de una emergencia fuera menester realizar un proceso expedito de adquisición de bienes y servicios, se fundamentarán por escrito las razones que así obligan a proceder.

28. **"Empleado"** - Cualquier persona que ocupe un cargo o esté empleada en la Autoridad y no sea un funcionario contratista.

29. **"Estación de trabajo"** - Un terminal o una computadora que utiliza un usuario para acceder a los sistemas de información computarizados de la Autoridad.

30. **"Equipo"** - Todo material de utilidad en un espacio o lugar que por su uso y naturaleza no se deteriore, gaste o consuma con facilidad (no fungible).

31. **"Funcionario"** - Cualquier persona que dirija o administre una oficina o programa de la Autoridad y que por consiguiente participe activamente en la toma de decisiones y en la elaboración de la política pública relacionada con la administración de la Autoridad, o aquella que colabora sustancialmente en la formulación de la política pública, o que asesora directamente o preste servicios directos al Director Ejecutivo.

32. **"Identificación del usuario (*User ID*)"** - Cadena de caracteres que autentica al usuario ante una computadora (*user*) y una contraseña (*password*).

33. **"Internet" –** Red informática descentralizada de alcance global**;** sistema de redes interconectadas mediante distintos protocolos que ofrece una gran diversidad de información, servicios y recursos, como, por ejemplo, el acceso a archivos de hipertexto a través de la web.

34. **"Intranet"** - grupo local de redes de área (LAN's) que se han conectado por medio de un protocolo común de comunicaciones.

35. **"Junta" o "Junta de Gobierno"** – la Junta de Gobierno de la Autoridad, establecida en el Artículo 2.01 de la Ley 351-2000, según enmendada.

36. **"Lenguaje de programación"** - Lenguaje artificial, compuesto por un vocabulario fijo y un conjunto de reglas que se pueden utilizar para crear instrucciones que una computadora debe seguir.

37. **"Ley 351" o "Ley de la Autoridad"** - "Ley del Distrito del Centro de Convenciones de Puerto Rico", Ley 351-2000, según enmendada.

38. **“Manufacturero”** - Compañía o empresa que fabricó los equipos tecnológicos utilizados por la Autoridad o equipos que pudieran ser utilizados por esta.

39. **“Menú”** - Despliegue en pantalla que detalla las opciones y los comandos disponibles.

40. **“Modem”** - Equipo que adapta un terminal o una computadora a una red de telecomunicación, que convierte las señales digitales en señales moduladas y analógicas necesarias para transmitir a través de una línea telefónica.

41. **“Oficina de Tecnología e Informática”** - Oficina que tiene a su cargo los sistemas de información computarizada de la Autoridad.

42. **“Programa de computadora (*Software*)”** - Utilidades o aplicaciones expresados en un lenguaje de programación; grupo de instrucciones que procesa datos en una computadora.

43. **“Proveedor”** - Cualquier individuo u organización cualificada que someta cotizaciones de precios por bienes o servicios tecnológicos no personales y que haya provisto o pueda proveer los mismos a satisfacción de la Autoridad.

44. **“Red”** - Conjunto de enlace de comunicaciones y los equipos y demás dispositivos que lo componen.

45. **“Red de Área Local (LAN) o *LAN on Premises*** - Computadoras portátiles y de otros tipos, así como cualquier otro equipo, enlazadas dentro de un área limitada, mediante comunicación de alto desempeño para que los usuarios puedan intercambiar información, compartir equipos periféricos y extraer programas y datos almacenados en una computadora dedicada, llamada servidor.

46. **Servicio en la Nube - *Cloud Services*"** - Los servicios en la Nube ofrecen conexión a la red a través de Internet, ofreciendo los mismos servicios. WAN (*Wide Area Network*), MAN (*Metropolitan Area Network*), *Campus Network* (Conjunto de Edificios Interconectados).

47. **“Representante autorizado"** - La persona en quien el Director Ejecutivo haya delegado por escrito una función o tarea.

48. **“Seguridad de datos”** - Conjunto de controles que protegen la información computadorizada o impresa contra sabotaje, contra el acceso no autorizado o contra el uso indebido.

49. **“Servidor (físico o virtual) o en la Nube”** - La computadora que almacena en su disco duro los programas de aplicación y los archivos de datos de todas las estaciones de trabajo de la red.

50. **“Sistemas de información (físico o virtual)”** - Conjunto de datos ordenados, equipos, aplicaciones y programas computarizados de la Autoridad, así como de las comunicaciones efectuadas mediante dichos equipos y demás recursos relacionados en los previos o en la Nube mediante servicios rentados.

51. **“Sistema operativo”** - Programa maestro de control que dirige a la computadora y actúa para la asignación y el control del intercambio de información.

52. **“Solicitud de Compras y Servicios”** - Documento que prepara el Director de Oficina en el que se solicita la adquisición de equipos o de servicios no personales.

53. **“Supervisor inmediato”** - Todo aquel funcionario o empleado a quien uno o más funcionarios o empleados responden directamente.

54. **“Periférico” (*Peripheral*)"** - Dispositivo o equipo externo a la unidad central de procesamiento, tal como una impresora o una unidad de disco o cinta, que se conecta a una computadora y es controlado por esta.

55. **“Redes Sociales” -** plataformas informáticas diseñadas para albergar comunidades virtuales de individuos interconectados que comparten contenido, información, archivos, fotos, audios, videos, etc., tales como Facebook, Twitter, Instagram, entre otros.

56. **“Telecomunicaciones”** - La trasmisión a distancia de datos de información por medios electrónicos y/o tecnológicos.

57. **“Terminal"** - Dispositivo para enviar y recibir datos de computadoras, mediante líneas de transmisión, compuesto de un teclado y un monitor que se emplea, por lo general, en un sistema multiusuario.

58. **“Transmisión (*streaming*)”** - Transmisión (*cast*) utilizando el sistema de red de telecomunicaciones de la Autoridad para escuchar música o transmitir videos vía Wifi a través de cualquier aplicación local o en la nube para difundirla.

59. **“Unidades de energía y acondicionamiento de voltaje (UPS)”** - Equipo o batería capaz de suministrar energía de forma continua a una computadora y sus periféricos en caso de interrupción de la energía eléctrica, y que también les provee cierta estabilidad al flujo eléctrico que reciben.

60. **“Usuario”** - Persona que utiliza un sistema de computadoras y sus programas de aplicaciones en el trabajo para efectuar tareas y producir resultados.

61. **“Virus”** - Programa diseñado intencionalmente para simular o sabotear transacciones o registros, que se copia a sí mismo, para lo cual se une a otros programas y efectúa operaciones no deseadas y en ocasiones dañinas. Son programas maliciosos diseñados para diseminar y replicarse desde una computadora a otra por media de enlaces de telecomunicaciones o al compartir archivos computarizados.

CAPÍTULO II. AUTORIZACIÓN DE ACCESO

Artículo 2.- Autorización requerida

a. Para utilizar los sistemas computadorizados de la Autoridad, todo usuario deberá contar con la autorización escrita del Director de Oficina. En esta se indicarán los archivos, programas, etc., que el usuario podrá acceder y utilizar.

b. Tras recibir la capacitación y orientación en la Oficina de Capital Humano, el usuario firmará la aceptación del uso de los sistemas de la Autoridad en el formulario utilizado para dicho propósito y se guardará récord del mismo, el cual expresará lo siguiente:

> "Cumpliré con los términos consignados en los reglamentos y órdenes administrativas vigentes y aplicables a los usuarios sobre normas y controles para la administración y uso de los sistemas tecnológicos de la Autoridad, copia de los cuales me ha sido suministrada para mi debido conocimiento. Entiendo, además, que el acceso a los sistemas de información electrónica de la Autoridad está restringido a su utilización de acuerdo con esta política en todo momento y que el uso indebido podrá resultar en la cancelación de este privilegio, así como en medidas disciplinarias, sanciones civiles y penales.”

c. En la pantalla del sistema, se advertirá al usuario sobre las normas principales para el uso de este, mediante el texto siguiente:

> "La Autoridad del Distrito del Centro de Convenciones del Gobierno de Puerto Rico promueve el uso de sistemas de información electrónica, Internet y correo electrónico a los usuarios de la Autoridad únicamente como recurso para las investigaciones, educación o comercio sobre asuntos oficiales que cumplan con los objetivos de la Autoridad exclusivamente.
>
> Uso del Recurso:

A. Todo acceso y uso está limitado exclusivamente a propósitos oficiales. Se prohíbe el uso del sistema para llevar a cabo negocios o asuntos personales.

B. La Autoridad del Distrito del Centro de Convenciones del Gobierno de Puerto Rico se reserva el derecho de registrar, revisar y auditar el uso de todos los sistemas de acceso y la información contenida en cualquiera de sus aplicaciones, con o sin notificación previa, aun cuando la data estuviera almacenada bajo un código personal del empleado.

Entendimiento:

Cumpliré con los términos consignados en los reglamentos y órdenes administrativas vigentes y aplicables a los usuarios sobre normas y controles para la administración y uso de los sistemas computadorizados de la Autoridad del Distrito del Centro de Convenciones del Gobierno de Puerto Rico, copia de los cuales me han sido suministrados para mi debido conocimiento."

CAPÍTULO III. CONDICIONES, LIMITACIONES Y NORMAS APLICABLES AL USO DE LOS SISTEMAS TECNOLÓGICOS

Artículo 3.1.- Sobre información confidencial

Se prohíbe que un usuario divulgue a terceros información confidencial de la Autoridad obtenida de los sistemas tecnológicos de esta o que divulgue cualquier tipo de información a persona alguna que debido a la naturaleza de sus funciones, deberes o tareas, no debe tener conocimiento o acceso a la misma.

Se entenderá por información confidencial aquella interna de la Autoridad relacionada con sus operaciones incluyendo, pero sin limitarse a, información sobre recursos humanos, finanzas o contabilidad de la Autoridad, planes o estrategias de mercadeo o de promoción o planes de desarrollo.

Artículo 3.2.- Sobre el uso con fines no públicos

Se prohíbe el uso de los sistemas de computadoras y comunicaciones de la Autoridad para propósitos no oficiales, personales, ya sea de recreo, para manejo de un negocio o asunto privado del usuario o para la utilización y envío de mensajes en cadena.

De igual forma, se prohíbe el uso de los recursos electrónicos o tecnológicos de la Autoridad para tener acceso a compras, juegos, concursos, encuestas, páginas de entretenimiento o cualquier otro servicio ajeno a las funciones de la Autoridad.

El uso de redes sociales está prohibido, además, para la divulgación de información, comunicados, itinerarios de eventos, fotos o cualquier opinión no autorizada por el Director Ejecutivo o el funcionario en quien este delegue para propósitos oficiales.

Artículo 3.3.- Sobre políticas de discrimen y hostigamiento sexual

Existirá una prohibición absoluta y una política de cero tolerancia a la utilización de las computadoras o del sistema de correspondencia electrónica para crear, redactar, editar o enviar mensajes o documentos:

1. de contenido discriminatorio por razón de raza, color, nacimiento, origen, condición social, sexo, orientación sexual, ideas políticas o religiosas, discapacidad física o mental o cualquier otro motivo prohibido por ley; o

2. que puedan ser catalogados como hostigamiento sexual.

Asimismo:

a. Se prohíbe la divulgación, por cualquier medio de los sistemas tecnológicos de la Autoridad, de cualquier tipo de opinión, inclusive personal, con relación raza, color, nacimiento, origen, condición social, sexo, orientación sexual, ideas políticas o religiosas o discapacidad física o mental.

b. Estará prohibido el acceso, manejo o transmisión de cualquier tipo de material erótico, obsceno, profano u ofensivo a través del sistema de computadoras o del sistema de comunicación electrónica de la Autoridad, incluyendo mensajes, comentarios o escritos que puedan violar las políticas sobre discrimen y hostigamiento sexual de la Autoridad.

c. Se prohíbe que se utilicen protectores de monitores (*screen savers*, *backgrounds* o *wallpapers*) con fotos de personas, artistas, modelos, deportistas, de calendarios o cualquier otra imagen que pueda resultar poco seria u ofensiva. Solo se podrán utilizar protectores de monitores uniformes establecidos o autorizados por el Director Ejecutivo.

Artículo 3.4.- Sobre correo electrónico (e-mail)

a. El sistema de correo electrónico es una herramienta de comunicación y será utilizado exclusivamente para propósitos oficiales de la Autoridad.

b. El sistema de correo electrónico no podrá ser utilizado para fines privados que incluyen, pero no se limitan a, asuntos personales, actividades comerciales, asuntos políticos o político-partidistas; actividades ilegales, ilícitas, no éticas o no profesionales; actividades que afecten la imagen y reputación de la Autoridad y sus integrantes, envío de cartas o mensajes en cadena, chistes o mensajes de índole sexual o de mal gusto.

c. Para la conservación del uso del papel y el medioambiente, la comunicación escrita entre oficinas de la Autoridad y/o entidades de gobierno con dirección de correo electrónico oficial, se remitirá, preferiblemente, por medio del correo electrónico con mecanismo con acuse de recibo electrónico, como primera opción.

d. Todo correo electrónico llevará el siguiente mensaje al final de cada comunicación, en español e inglés como sigue:

"AVISO DE CONFIDENCIALIDAD

Esta comunicación y cualquier archivo transmitido con ella puede contener información que es confidencial, privilegiada o privada bajo la ley aplicable. Se utilizará solamente para el uso de la persona o entidad a la cual se dirige. Si usted no es el destinatario intencional, se le notifica por la presente que cualquier uso, diseminación o copia de esta comunicación está prohibido estrictamente. Si usted ha recibido esta comunicación por error, por favor notifique de ello al remitente. Gracias por su cooperación.

CONFIDENTIALITY NOTE

This communication and any files transmitted with it may contain information that is confidential, privileged and/or exempt from disclosure under applicable law. It is intended solely for the use of the individual or entity to which it is addressed. If you are not the intended recipient, you are hereby notified that any use, dissemination or copying of this communication is strictly prohibited. If you have received this communication in error, please notify the sender. Thank you for your cooperation."

e. Solo se podrán utilizar las cuentas de correo electrónico provistas por la Autoridad para propósito de comunicaciones/funciones oficiales.

f. Para maximizar los recursos del servicio del correo electrónico, el Director de la Oficina de Tecnología e Informática podrá asignar un límite de espacio para almacenar los mensajes electrónicos mediante una cuota mensual de consumo.

g. El correo electrónico deberá ser utilizado para facilitar las tareas rutinarias de envío y recibo de información, divulgación de nominas y procedimientos, notificación de reuniones y otros asuntos oficiales relacionados.

h. Se prohíbe el envío interno o externo a otras personas de copia de un mensaje de correspondencia electrónica recibido sin el conocimiento o consentimiento del remitente original, a menos que estas deban o les corresponda estar enteradas de tales mensajes (*need to know basis*) para propósitos estrictamente oficiales y no se adjudiquen la autoría del mensaje de correspondencia electrónica del remitente original.

i. Se prohíbe leer, revisar o interceptar cualquier tipo de comunicación electrónica de la Autoridad o de cualquier otra persona o entidad, sin el consentimiento expreso del remitente y del destinatario de la comunicación.

j. Se prohíbe que los usuarios se suscriban a listas de correo electrónico o que participen en grupos de noticias (*newsgroups*) que divulguen información o mensajes ajenos a las funciones y deberes de la Autoridad.

k. No se podrán crear o enviar archivos mediante correo electrónico que excedan la capacidad de la cuota del usuario en el servidor.

l. Está terminantemente prohibido que cualquier usuario envíe mensajes o documentos a todo el personal a la vez o en cadena mediante el correo electrónico. Se exceptúa de esta prohibición la difusión de mensajes o documentos con autorización expresa del Director Ejecutivo o documentos de uso común que sean difundidos por el Director de Tecnología de Información o el Administrador de la Red.

m. Se prohíbe el uso del correo electrónico para uso personal. Se entiende por uso personal, sin que se entienda como una limitación, a peticiones, recolectas, anuncios, propaganda comercial, anuncios de eventos, artículos o propiedad para la venta o alquiler, o cualquier mensaje que resulte en beneficio personal.

n. Queda prohibido el uso del correo electrónico para actividades como mensajes en cadena, mensajes raciales, obscenos, pornográficos, sugestivos o amenazantes, distribución de mensajes comerciales, la propagación de virus, la presentación de mensajes a nombre de otra persona, real o ficticia, mensajes anónimos y mensajes de libelo o contenido difamatorio, entre otros. La Autoridad no será responsable por la transmisión de este tipo de mensajes.

o. Se dispone que los usuarios del sistema de correo electrónico de la Autoridad prestarán atención particular y cuidado al enviar sus mensajes a grandes audiencias y evitarán repetir los mismos "a manera de recordatorio". La practica correcta del envío de mensajes es limitar el envío de estos al grupo de personas más pequeño posible. Únicamente en situaciones extraordinarias, el Director Ejecutivo y los administradores del sistema serán los autorizados para enviar mensajes oficiales a grandes audiencias.

p. Los usuarios del sistema se asegurarán de que, al enviar contestaciones a los mensajes, dirijan las mismas a las personas deseadas y no a un grupo de personas, (*Reply To All*).

q. Cada usuario será responsable por la confidencialidad y seguridad de su contraseña o (*password*), la cual será individual y no deberá ser compartida o divulgada en ninguna circunstancia. Si el usuario sospecha que su contraseña ha sido divulgada, capturada o compartida, deberá cambiarla inmediatamente.

r. Está prohibido acceder a otra cuenta o computadora de otro usuario con una contraseña ajena, así como acceder a documentos que se encuentren en los archivos del correo electrónico de dicho usuario. Dicha acción constituye, además, una violación al *Federal Electronic Communications Privacy Act*, según enmendada, 18 U.S.C. Sec. 2510.

s. Se prohíbe la interceptación o acceso a correspondencia electrónica de carácter confidencial y la remisión de esta a un tercero sin la autorización del remitente. Se entiende por comunicación confidencial cualquier mensaje de esta naturaleza entre remitente y destinatario, dentro de sus funciones en la Autoridad. Sin embargo, existen circunstancias específicas en este Reglamento, mediante las cuales la Autoridad, a través de los administradores del sistema, podrá acceder a dichos archivos electrónicos para salvaguardar la integridad del sistema de correo electrónico y asegurar el cumplimiento de las leyes y normas aplicables.

t. Los administradores del sistema protegerán la confidencialidad de los documentos y comunicaciones enviadas a través del correo electrónico de la Autoridad. Cualquier inspección de dichos archivos, o cualquier acción basada en dicha inspección, deberá estar regida por las disposiciones establecidas en este Reglamento.

u. El correo electrónico no podrá ser utilizado para violar o incitar a la violación de las leyes y reglamentos estatales o federales, así como de normas o políticas de la Autoridad referentes al hostigamiento sexual o a cualquier discrimen prohibido por ley o reglamento.

Artículo 3.4.1- Recibo de mensajes externos no deseados ni solicitados

Todo usuario del sistema computadorizado de la Autoridad será responsable de comunicar a su supervisor inmediato o al Director de Oficina para la cual labora, así como a la Oficina de Tecnología e Informática, el recibo vía correo electrónico (*E-mail*), de mensajes externos no deseados ni solicitados, con el propósito de que se tomen las medidas pertinentes para que dichas transmisiones no vuelvan a ocurrir. Todo correo sospechoso deberá ser reportado inmediatamente a las oficinas antes indicadas, para ser contrarrestados o intervenidos. No deberán abrirse correos electrónicos desconocidos o sospechosos.

Artículo 3.4.2- Confidencialidad de la información en correo electrónico

La Autoridad no garantizará a los usuarios del sistema del correo electrónico la confidencialidad de la información almacenada o enviada a través del sistema. Existen una serie de circunstancias en las cuales los administradores del sistema, conforme a los deberes y poderes dispuestos en este Reglamento, y siempre que no exista conflicto con las funciones asignadas a otras oficinas de la Autoridad, podrán válidamente acceder a dichos archivos electrónicos y divulgar la información allí contenida. Estas circunstancias incluyen, pero no se limitan, a:

a. La realización de alguna investigación administrativa, identificar la vulnerabilidad de algún mecanismo de seguridad o mantener la integridad o estado óptimo de operación del sistema de correo electrónico.

b. El Director el Director de Oficina para el cual el usuario labora o los auditores de la Autoridad, según sea el caso, podrán autorizar cualquier investigación en los archivos de un usuario, siempre que tenga motivos fundados para sospechar que la investigación revelará evidencia que demuestre que el usuario ha violado este Reglamento o cualquier ley o reglamentación aplicable. La investigación estará limitada razonablemente al ámbito de búsqueda o al asunto que generó la sospecha.

c. Monitoreo del uso del sistema de correo electrónico y otros sistemas computadorizados relacionados, para determinar si las políticas de la Autoridad han sido violadas, así como cualesquiera leyes o reglamentos aplicables; y monitoreo del uso del correo electrónico y otros sistemas computadorizados relacionados, cuando sea necesario, para que la Autoridad pueda proveer sus servicios o proteger sus derechos y propiedades.

Artículo 3.5.- Sobre el uso de la Internet/Intranet

Artículo 3.5.1.- Sobre el uso del Internet

a. Solo tendrán acceso a la Internet aquellos usuarios autorizados por su supervisor inmediato y cuyas funciones requieran su uso. Tal supervisor deberá solicitar dicho acceso por escrito.

b. El servicio de Internet se utilizará como un instrumento para la búsqueda de información oficial del gobierno estatal o federal, universidades, organizaciones, corporaciones y compañías privadas, entre otras, relacionadas con las funciones de la Autoridad y las encomiendas que se les asignan a sus funcionarios y empleados.

c. Los usuarios no deberán revelar a ninguna persona su contraseña. Cada usuario será responsable por las transacciones efectuadas en su cuenta o con su contraseña.

d. El sistema llevará un registro de las páginas visitadas en el Internet para propósitos de auditorías.

e. Todo usuario deberá desconectarse o salir del sistema una vez termina de utilizar el Internet.

Será responsabilidad del Administrador de la Red asegurarse de que los usuarios del sistema estén debidamente autorizados y que una vez tengan acceso, solo puedan acceder los menús y las opciones para los cuales se les han concedido derechos de acceso.

Las políticas sobre el uso de la Internet serán revisadas periódicamente en caso de que necesiten ser actualizadas por normas aplicables vigentes o que surjan nuevas tecnologías o necesidades, únicas y particulares de la Autoridad. Se incorporan y se hacen formar parte de este Reglamento todos los documentos, memorandos, instrucciones, manuales o políticas que se notifiquen de tiempo en tiempo y que sean pertinentes al uso de las computadoras en la Autoridad.

Artículo 3.5.2.- Sobre el uso del Intranet

a. Los servicios de Intranet se le proveerán a todos los usuarios autorizados a utilizar la red.

b. El servicio de Intranet se utilizará para comunicar información sobre las operaciones de la Autoridad; acceso a formularios de uso común; modelos de cartas; directorio de empleados y funcionarios de la Autoridad; noticias y artículos de interés general y actividades oficiales.

c. Los usuarios no deberán revelar a ninguna persona su contraseña. Cada usuario será responsable por las transacciones efectuadas en su cuenta o con su contraseña.

d. El sistema llevará un registro de las páginas visitadas en el Intranet para propósitos de auditorías.

e. Todo usuario deberá desconectarse o salir del sistema una vez termina de utilizar el Intranet.

Será responsabilidad del Administrador de la Red asegurarse de que los usuarios del sistema estén debidamente autorizados y que una vez tengan acceso, solo puedan acceder los menús y las opciones para los cuales se les han concedido derechos de acceso.

Las políticas sobre el uso de la Intranet serán revisadas periódicamente en caso de que necesiten ser actualizadas por normas aplicables vigentes o que surjan nuevas tecnologías o necesidades, únicas y particulares de la Autoridad. Se incorporan y se hacen formar parte de este Reglamento todos los documentos, memorandos, instrucciones, manuales o políticas que se notifiquen de tiempo en tiempo y que sean pertinentes al uso de las computadoras en la Autoridad.

Artículo 3.6.- Sobre otros recursos

Las normas antes mencionadas sobre el uso y auditorías serán de igual aplicación para los otros recursos de la red de comunicaciones electrónicas e Internet, tales como el WWW, FTP, Chat, YouTube, Facebook, Facebook Live, Instagram, entre otros medios de comunicación digital.

Se permitirá el uso de programas de charlas (*chats*) y *streaming* de audio o video, sujeto a la autorización escrita del Director Ejecutivo y exclusivamente para fines oficiales de la Autoridad. La autorización del Director Ejecutivo será innecesaria cuando el desempeño de los deberes del cargo o funciones que el usuario realiza en la Autoridad conlleva la utilización de tales medios.

CAPÍTULO IV. NORMAS SOBRE TITULARIDAD Y DERECHOS

Artículo 4.- Sobre titularidad y derechos

a. Toda computadora, servicios asociados tanto internos como externos, el sistema de correspondencia electrónica (e-mail), la red de comunicaciones electrónicas, el acceso a la Internet y los documentos y programas que existen en lo mismos, son propiedad de la Autoridad y solo podrán utilizarse para propósitos lícitos, prudentes, responsables y dentro de las funciones o poderes de la Autoridad.

b. Toda información, dato, obra literaria o de arte, 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 Autoridad, será propiedad de la Autoridad, aunque la información, dato, obra literaria o de arte, escrito, documento, programa, acción, privilegio o patente, derecho de autor o cualquier otro derecho, haya surgido mediante el esfuerzo personal del usuario.

c. La información contenida en las computadoras de la Autoridad, los servicios asociados tanto internos como externos, los mensajes de correspondencia electrónica (e-mails), información de la red de comunicaciones electrónicas 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 Autoridad.

d. Se prohíbe el uso de programas o recursos en los sistemas computadorizados de la Autoridad para los cuales no exista una licencia o autorización de uso válida a nombre de la Autoridad.

e. Se prohíbe copiar programas de cuya licencia es dueña la Autoridad para instalarlos en otras computadoras sin la autorización por escrito del Director Ejecutivo de la Autoridad.

f. Se prohíbe instalar programas en las computadoras de la Autoridad sin la autorización por escrito del Director Ejecutivo o del Director de Tecnología e Informática.

g. Se prohíbe acceder a propiedad intelectual (*copyrighted information*) que viole los derechos do autor o utilizar la misma sin el permiso debido del autor.

h. Está prohibido transferir a las estaciones de trabajo aplicaciones de pizarras de boletines electrónicos o de otra fuente que provea servicios en línea. Solo se podrán efectuar dichas transferencias con la autorización expresa y por escrito del Administrador de la Red, quien a su vez deberá obtener la autorización del Director de Tecnología de Información.

i. Ningún usuario estará autorizado para duplicar aplicaciones o instalar aplicaciones que han sido duplicadas en violación a los derechos de propiedad intelectual del manufacturero. Los infractores estarán sujetos a acciones disciplinarias según la reglamentación aplicable, incluyendo terminación en el empleo o procesamiento criminal o civil conforme al derecho vigente.
j. Todo lo contenido en las computadoras, email o cualquier equipo tecnológico y/o de comunicaciones propiedad de la Autoridad, es propiedad exclusiva de la Autoridad y como tal, la Autoridad, puede usar, auditar, disponer y compartir con los entes que entienda necesario. Esto incluye, pero no se limita a procedimientos civiles y penales en corte, procedimientos administrativos, auditorías y servicios de mantenimiento de los sistemas, entre otros. Este derecho pertenece única y exclusivamente a la Autoridad y no a sus empleados.

CAPÍTULO V. NORMAS SOBRE SEGURIDAD

Artículo 5.- De aplicación general

a. El uso de un código de acceso (*password*), no impedirá que se audite el sistema ni significará que el usuario albergue expectativa alguna de intimidad con relación a la información almacenada en la computadora que tenga asignada o en

cualquier otra. Las contraseñas deberán ser mantenidas en estricta confidencialidad y administrarse conforme a las disposiciones sobre medidas de seguridad consignadas en este Reglamento.

Todo empleado, funcionario o contratista debidamente autorizado para utilizar las computadoras o sistemas tecnológicos de la Autoridad, deberá haber aceptado previamente las condiciones, normas y limitaciones contenidas en este Reglamento. Esa aceptación se documentará.

b. La Autoridad se reserva el derecho de auditar, vigilar y fiscalizar los sistemas de correspondencia electrónica y todos los servicios computadorizados para garantizar que su propiedad sea utilizada únicamente para los propósitos y gestiones relacionados con asuntos oficiales. Estas auditorias serán realizadas periódicamente o al azar o cuando exista una investigación sobre una situación en particular. Por estas circunstancias, el personal de la Autoridad no tendrá derecho a la intimidad con relación a cualquier información, documento o mensaje creado, recibido o enviado a través del sistema de correo electrónico (e-mail) de la Autoridad.

c. A ningún usuario se le permitirá acceso ni podrá invocar comandos de los sistemas operativos de la red, excepto al personal que administra y opera la red y a los auditores de la Autoridad. Ello, de manera que se eviten daños accidentales o intencionales y el uso inapropiado del sistema.

d. Se prohíbe el envío fuera de la Autoridad de documentos electrónicos o mensajes que contengan información confidencial por medio del correo electrónico (e-mail), a menos de que estos sean dirigidos para fines estrictamente oficiales y los usuarios cuenten con la autorización previa correspondiente de sus respectivos supervisores. En caso de que se trate de usuarios que necesiten laborar con relación a tales mensajes o documentos con información confidencial, estos podrán remitirse internamente mediante el uso de sus respectivos correos electrónicos asignados para propósitos oficiales.

e. Se prohíbe el envío de mensajes de correo electrónico o de cualquier otro tipo entre el personal, funcionarios o contratistas de la Autoridad y personas que no laboren en esta, en los cuales se divulguen, comenten o expresen hechos, opiniones o cualquier tipo de información relacionada a situaciones, controversias, problemas, malentendidos, funcionamiento, políticas, personas o cualquier otra situación o asunto interno de la Autoridad, que puedan poner en entredicho la reputación o imagen de la Autoridad. Esta disposición aplicará aun cuando se trate de información quo no sea de naturaleza confidencial.

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

g. Se prohíbe codificar, cifrar, asignar contraseñas o modificar de alguna manera la información, mensajes de correo electrónico o archivos propiedad de la Autoridad, con el propósito de impedir que alguien pueda leerlos, entenderlos o utilizarlos o con el propósito de falsificar o alterar el nombre del usuario, la fecha de creación o de modificación o cualquier otra información que se utilice regularmente para identificar la información, mensajes o archivos, si no se obtiene previamente el consentimiento por escrito del Director Ejecutivo.

En el caso de que por razones de seguridad se permita codificar, asignar contraseñas o modificar alguna información a fines de evitar que otras personas puedan leerla, la Autoridad estará facultada para decodificar la misma o restituirla a su condición original, y el usuario será responsable de proveer todos los datos necesarios para lograr el acceso a la información o archivo.

h. Se prohíbe la modificación de los parámetros o de la configuración de las computadoras de la Autoridad para proveerle la capacidad de recibir llamadas telefónicas o cualquier otro tipo de acceso o conexión remota que permita intrusiones no autorizadas a la red de la Autoridad.

i. Se prohíbe el uso de discos portátiles externos personales, USB, Micros SD o cualquier otro medio de almacenaje de información) sin que haya sido autorizado y verificado como libre de virus por el sistema de protección electrónica de antivirus en la red de la Autoridad.

j. Ningún usuario está autorizado a instalar o utilizar aplicaciones de juegos electrónicos en las computadoras de la Autoridad. Tampoco podrá transferir (*download*) a su estación de trabajo, juegos de pizarras de boletines electrónicos (*electronic bulletin boards*), o redes sociales, programas u otros servicios que puedan contaminar con virus y comprometer el ancho de banda u otras amenazas a los sistemas de información de la Autoridad.

k. Todos los archivos que se creen en las computadoras de la Autoridad deberán ser guardados en el directorio asignado a cada usuario con el propósito de que puedan protegerse mediante los mecanismos de resguardo (*backup*) existentes.

l. Todo usuario autorizado a utilizar la red deberá validar su identidad mediante una clave de identificación como usuario (barrera de protección de acceso**)**. Las contraseñas deberán ser complejas, memorizadas y debidamente aseguradas por los usuarios. Estas no deberán guardarse en forma impresa en etiquetas o papeles pegados a la estación de trabajo, debajo del teclado o en algún otro lugar visible o de fácil acceso por otros usuarios o personas no autorizadas.

m. Todo usuario autorizado utilizará una contraseña que constará de un mínimo de echo (8) caracteres; y que estará compuesta par una combinación de caracteres alfabéticos (letras mayúsculas y/o minúsculas) y numéricos.

n. La contraseña para utilizar la red será válida por un periodo de noventa (90) días y antes de finalizar el periodo, el sistema le notificará que deberá cambiar su contraseña. Las contraseñas expiradas no podrán volver a utilizarse dentro de un término de un (1) año u once (11) veces (11 *passwords* consecutivos). A partir de su fecha de expiración, la cuenta quedará deshabilitada. Si el usuario no hace el cambio de contraseña durante dicho término, el sistema le negará acceso. En esta eventualidad, el usuario deberá solicitarle al Administrador de la Red que le brinde acceso mediante una contraseña nueva.

o. Solamente tendrán derecho a utilizar los sistemas de información de la Autoridad los funcionarios y empleados de esta, así como a aquellas personas autorizadas. A los contratistas de la Autoridad se les podrá permitir el uso limitado de estos cuando por la naturaleza del contrato y los servicios a prestarse sea conveniente a la Autoridad. También se podrá permitir el uso limitado a aquellas personas autorizadas, por escrito, por el Director Ejecutivo.

p. Los Directores de Oficina solicitarán el acceso a la red y a los sistemas de información para el personal bajo su supervisión cuyas funciones requieran utilizar dichos recursos.

   La solicitud se hará mediante un formulario para estos propósitos, que la Oficina de Tecnología e Informática tendrá la responsabilidad de mantener debidamente archivados con las debidas autorizaciones.

q. Como mecanismo para evitar que personas no autorizadas logren acceso a los sistemas de información de la Autoridad, los usuarios que hayan olvidado su contraseña tendrán tres (3) intentos consecutivos para registrar la contraseña correcta. Luego de tres (3) intentos consecutivos, el sistema denegará el acceso, por lo cual tendrán que comunicarse con el Administrador de la Red para identificarse y que se puedan desbloquear sus respectivas cuentas.

r. Si un usuario fuere a dejar su estación de trabajo inactiva por un periodo mayor de diez (10) minutos, el sistema automáticamente bloqueará la pantalla, requiriendo el sistema que entre nuevamente su contraseña para continuar su trabajo. De esta forma, se evitará dejar dicha estación expuesta a personas no autorizadas que puedan tener acceso al sistema mientras el usuario no esté en estación de trabajo.

s. Todo Director de Oficina será responsable de la integridad de la información que se mantiene en los directorios asignados a las oficinas que dirigen. Esta responsabilidad conlleva, entre otros:

   1. que se verifique periódicamente la integridad de los archivos que se mantienen en el directorio de trabajo asignado; y

2. que se notifique inmediatamente al Director de Tecnología e Informática, así como al Director de Capital Humano, por medio electrónico, del disfrute prolongado de licencia o el traslado o el relevo o cese de funciones de algún usuario. Ello, para que se inactive la cuenta de acceso, -según corresponda.

   También se notificará inmediatamente a los referidos directores de algún cambio en las funciones de un usuario para las cuales no requerirá acceso a los sistemas de información, al correo electrónico e Internet, entre otros, para que se modifique el alcance de su acceso. Los cambios de funciones u oficinas afectan los accesos a los archivos, por lo que estos estarán limitados por la función que realizará un usuario.

t. Todo movimiento de equipo de computadoras de la Autoridad fuera de los predios del Distrito del Centro de Convenciones de Puerto Rico requerirá la autorización del Director de la Oficina de Propiedad, quien podrá utilizar personas contratadas para dicha labor con la supervisión del personal de la Oficina de Propiedad, y se coordinará con la Oficina de Tecnología e Informática. Está prohibido todo movimiento de equipo de computadoras por parte de personas ajenas a la Oficina de Propiedad, con la previa evaluación del personal de la Oficina de Tecnología e Informática respecto a servicio en garantía, reparación o disposición.

u. Está prohibido fumar, comer o ingerir bebidas, en el área de los servidores o próximo a las computadoras, los terminales o las estaciones de trabajo (incluyendo *racks* de comunicaciones, cuartos de comunicaciones, estantes de *switches*, etc.); colocar equipos electrónicos tales como radios o plantas o tiestos sobre las computadoras; y tapar el panel de ventilación de estas. Tampoco está permitido mantener químicos volátiles, tales como alcohol, pegamentos o solventes industriales en las áreas inmediatas a dichos equipos. Los directores de oficinas serán responsables de que se cumpla con esta norma.

CAPÍTULO VI. PROCEDIMIENTOS DE QUERELLAS Y DISCIPLINARIOS

Artículo 6.1- Querella

Cualquier usuario funcionario, empleado, contratista o cualquiera otra persona que reciba un mensaje a través o desde el sistema tecnológico de la Autoridad, o que sea testigo de cualquier acción por otro funcionario, empleado, contratista o cualquiera otra persona, que esté prohibido según las leyes y reglamentos estatales o federales o este Reglamento, someterá una querella ante la Oficina de Recursos Humanos si el remitente de dicho mensaje, o la persona que lleva a cabo dicha acción, fuere algún empleado, funcionario, contratista o Director de Oficina de la Autoridad. En la

eventualidad de que el remitente del referido mensaje, o la persona que lleva a cabo dicha acción, fuere otra persona, la querella será sometida ante los auditores de la Autoridad para su consideración.

Artículo 6.2- Medidas disciplinarias, civiles o criminales

Se tomarán las medidas disciplinarias, civiles o criminales que correspondan contra los usuarios que violen estas políticas o abusen del acceso a los sistemas tecnológicos de la Autoridad, según sea el caso. Respecto a medidas disciplinarias, estas podrán ser tan severas como el despido inmediato, de conformidad con el Reglamento de Normas de Conducta y Acciones Correctivas de Disciplina de la Autoridad del Distrito del Centro de Convenciones de Puerto Rico 2019, según enmendado.

Artículo 6.3- Reserva de derecho

La Autoridad se reserva el derecho de someter acusaciones criminales por las actuaciones que constituyan delito federal o estatal, aunque no estén expresamente prohibidas por las condiciones de uso consignadas en este Reglamento.

CAPÍTULO VI. DIRECTOR DE LA OFICINA DE TECNOLOGÍA E INFORMÁTICA

Artículo 6.- Deberes y facultades

El Director de la Oficina de Tecnología e Informática administrará el sistema de computadoras, redes, servicios tecnológicos internos y las redes de información computadorizada de la Autoridad.

El Director, además, tendrá los siguientes deberes y facultades:

a. Se asegurará de que los empleados y funcionarios de la Autoridad cumplan con las disposiciones de este Reglamento y llevará a cabo los trámites requeridos para que se tomen las medidas disciplinarias que apliquen, conforme a las leyes y los reglamentos, Órdenes Ejecutivas u otras normas vigentes que se adopten al amparo de estas.

b. Se asegurará de divulgar este Reglamento y cualquier enmienda al mismo, así como cualesquiera normas o procedimientos adicionales que haya formulado para regir las operaciones tecnológicas de la Autoridad, a través del sistema de

correo electrónico o por cualquier otro medio disponible, a todos los usuarios presentes y futuros del sistema de la Autoridad.

c. Velará por que a los empleados o usuarios concernidos se les divulgue o adiestre, según corresponda, en cuanto a las políticas, normas y procedimientos necesarios, entre otros, para:

    1. administrar la seguridad y las operaciones de los sistemas de información tecnológicos;

    2. detectar, reportar y responder a incidentes de seguridad;

    3. controlar el acceso a los sistemas de información;

    4. controlar el uso de las cuentas de acceso a la red, al correo electrónico, a Internet, y a las aplicaciones de la Autoridad;

    5. administrar las cuentas de acceso, incluyendo su creación y mantenimiento, y la asignación de los privilegios definidos, según las funciones realizadas por cada usuario;

    6. preparar las copias de reserva de la información almacenada en los sistemas de la Autoridad; y

    7. administrar los equipos computadorizados y las licencias de los programas, para asegurar el control efectivo de las mismos.

d. Desarrollará un programa efectivo de concienciación y divulgación a los usuarios sobre las normas y los procedimientos para la seguridad de la información establecidos en la Autoridad; y orientará sobre la importancia de salvaguardar la información y utilizarla correctamente. Como parte del referido programa, se incluirá la evidencia del compromiso de los usuarios con el cumplimiento de estas normas, la instalación de pantallas de advertencia en las computadoras, y el adiestramiento al personal administrativo, al personal técnico de sistemas de información y a los usuarios.

e. Atenderá con premura toda querella formal o informal que se haya presentado, según lo dispuesto en este Reglamento.

f. Podrá válidamente acceder a los archivos electrónicos de los usuarios, específicamente en las circunstancias dispuestas en este Reglamento, particularmente las relacionadas con la confidencialidad y privacidad de los archivos.

g. Divulgará, cuando el usuario obtenga acceso al sistema, el mensaje cuyo texto so consigna en el Artículo 2, inciso (b) de este Reglamento.

h. Evaluará las compras de equipo tecnológico y de sistemas a implantarse que afecten a la red de computadoras de la Autoridad, y realizar los estudios de necesidad y justificación de las solicitudes de compras y servicios o de contratos de servicios profesionales relacionados con tecnología, conforme a las disposiciones de este Reglamento.

i. Preparará un informe de análisis de riesgos de los sistemas de información computadorizados de la Autoridad. Dicho informe, entre otras cosas, identificará los activos y vulnerabilidades, y las amenazas a las que estén expuestos los referidos sistemas.

j. Uniformará las operaciones de los sistemas de la Autoridad, y establecerá un programa de administración de seguridad (Plan de Seguridad), en el que establecerá las estrategias necesarias para protegerlos, de manera que permita identificar oportunamente errores o irregularidades.

Además, velará que se realicen evaluaciones periódicas para asegurar el funcionamiento del plan de seguridad.

k. Desarrollará un programa efectivo de concienciación y divulgación a los usuarios sobre las normas y los procedimientos para la seguridad de la información establecidos en la Autoridad; y orientará sobre la importancia de salvaguardar la información y utilizarla correctamente. Como parte del referido programa, se incluirá la evidencia del compromiso de los usuarios con el cumplimiento de estas normas, la instalación de pantallas de advertencia en las computadoras, y el adiestramiento al personal administrativo, al personal técnico de sistemas de información y a los usuarios.

l. Velará que en la Oficina de Tecnología e Informática se activen las opciones correspondientes con la pantalla de políticas de auditoría, de manera que se pueda mantener un rastro de los eventos realizados en los sistemas computadorizados, cuando sea solicitado o se estime el período necesario.

m. Se asegurará de que se documente el proceso para la solicitud, autorización y modificación de las cuentas de acceso creadas en los sistemas de información computadorizada; y de que los privilegios que se asignen a dichas contraseñas, respondan a la necesidad que tienen los funcionarios o empleados de acceder a determinada información para realizar sus funciones.

n. Velará que se cumpla con el proceso establecido en la Autoridad para remover las cuentas de acceso una vez los usuarios cesen labores o dejen de realizar las funciones para las que se les otorgaron estas. Ello incluye la notificación inmediata al encargado de la administración de los sistemas del cese o la modificación en las funciones de los usuarios, para lo cual habrá un proceso

efectivo de comunicación entre la Oficina de Capital Humano, el área u oficina en que trabaja el usuario y la Oficina de Tecnología e Informática.

o. Velará que haya respaldos de la información almacenada en los sistemas computadorizados de la Autoridad; y se asegurará de que el personal interno o externo contratado para ello por la Autoridad, prepare periódicamente el respaldo de la información de los sistemas, conforme a su nivel de criticidad, y remita una copia de estos a un lugar externo.

Además, se preparará un informe periódico sobre tales gestiones relacionadas con los respaldos de la información almacenada.

p. Establecerá los controles necesarios para asegurarse de que los equipos que se mantienen en el área principal de procesamiento y en los cuartos de comunicación, estén protegidos contra accesos no autorizados y posibles daños causados por condiciones ambientales y físicas que puedan afectar su disponibilidad y rendimiento.

q. Realizará las gestiones necesarias para identificar un centro alterno que cuente con la infraestructura y los equipos necesarios para restaurar las operaciones críticas de la Autoridad, en caso de que ocurra una emergencia. Se asegurará de que dicho centro no esté expuesto a los mismos riesgos que el área principal de procesamiento de la Autoridad.

r. Velará que en la Oficina de Tecnología e Informática se mantengan y revisen, periódicamente, los registros de los accesos a la red, al correo electrónico, a Internet y a las aplicaciones.

s. Se asegurará de que exista una segregación adecuada de las funciones realizadas por el personal, relacionadas con las operaciones críticas y confidenciales de la Autoridad. En la eventualidad de que no se cuenten con los recursos necesarios para mantener una segregación adecuada, se coordinarán controles compensatorios, tales como supervisión y utilización y revisión de registros de auditoría que permitan mitigar el riesgo.

t. Se asegurará de que se identifiquen alternativas costo-efectivas para recomendar al Director Ejecutivo un plan de continuidad de negocios. Este plan deberá incluir planes para la recuperación de desastres y la continuidad de las operaciones de los sistemas de información computadorizados utilizados por la Autoridad, particularmente los de la misión critica. Una vez el plan sea preparado y aprobado, se asegurará de que se realicen pruebas periódicas y se divulgue a los empleados y usuarios concernidos.

u. Administrará las bases de datos de forma efectiva para asegurarse de que cuenten con los controles de entrada, procesamiento y salida de datos, que provean un flujo de datos completo, exacto y oportuno de la información.

v. Velará que los empleados o usuarios que tengan la custodia de la información o las bases de datos de la aplicación principal de la Autoridad se aseguren de que en estas se hayan establecido controles de validación efectivos que permitan mantener la integridad y disponibilidad de dicha información.

w. Recomendará al Director Ejecutivo las normas y procedimientos que estime necesarios o convenientes para regir las operaciones computadorizadas de la Autoridad -incluyendo, pero no limitado a- procedimientos para el manejo de incidentes de seguridad, que incluyan, entre otras cosas, una estrategia documentada para atenderlos, un equipo de respuesta y la documentación de las actividades relacionadas con los mismos, adicionales a los contenidos en este Reglamento.

x. Ejercerá todos aquellos poderes y deberes necesarios y convenientes para implantar las disposiciones de este Reglamento.

CAPÍTULO VII. NORMAS APLICABLES A LA ADQUISICIÓN DE TECNOLOGÍA

Artículo 7.1- Normas de aplicación general sugeridas por la Oficina del Contralor

A tenor con el Informe Especial TI-17-02, “Recopilación de datos sobre la inversión de fondos públicos en equipos y sistemas de información computadorizados sin obtener los beneficios esperados”, de 31 de agosto de 2016, de la Oficina del Contralor de Puerto Rico:

> La incorporación oportuna de la tecnología a los programas y servicios del gobierno es un valioso instrumento para reducir el tiempo de gestión y los costos de operación, y para hacer más accesibles los servicios que se prestan a los ciudadanos. Sin embargo, en toda institución, mantenerse al día sobre los adelantos tecnológicos, requiere una inversión de recursos considerable. Anualmente las entidades gubernamentales invierten millones de dólares en el desarrollo, la adquisición, la implementación, la seguridad y el mantenimiento de los sistemas de información, y en la contratación de servicios profesionales de asesoría técnica en sistemas computadorizados. La inversión de fondos públicos en tecnología de información debe planificarse, de manera que se obtengan los beneficios esperados en un tiempo razonable, y que se pueda cumplir con la política gubernamental de interconexión entre los sistemas de información computadorizados de las entidades gubernamentales.

Los proyectos relacionados con la tecnología de información, generalmente, involucran distintas fases durante su ciclo vital. Por ejemplo, el ciclo vital de un sistema computadorizado comienza con el análisis de las necesidades y termina cuando se remplaza por un nuevo sistema o se determina que este deja de ser necesario. En términos generales, el ciclo vital de un proyecto tecnológico consta de las siguientes fases:

1. Análisis y planificación
2. Desarrollo y pruebas
3. Implementación
4. Operaciones
5. Conservación y control de cambios.

Cada una de estas fases conlleva la implementación de controles y métodos de seguridad, así como la adquisición de servicios. También se recomienda, en cada etapa, establecer un proceso de revisión de calidad de los productos. Aunque cada caso se debe examinar en su contexto, se sugiere que se establezca una metodología de desarrollo para los sistemas de información. De esta manera se obtendrán resultados de forma rápida, se identificarán los requerimientos específicos de los usuarios y se reducirá el riesgo de la inversión.

Es importante que, durante las diferentes etapas del desarrollo de los sistemas, se requiera la participación de los auditores internos. Esto, para el desarrollo y la implementación de controles adecuados mediante la identificación y evaluación de las exposiciones de los riesgos, y contribuyan al mejoramiento de los sistemas de gestión de riesgos y control.

También los auditores internos deben evaluar las exposiciones de riesgo relacionadas con el gobierno, las operaciones y los sistemas de información, en cuanto a lo siguiente:

1. Confiabilidad e integridad de la información financiera y operativa
2. Eficacia y eficiencia de las operaciones
3. Protección de activos
4. Cumplimiento de las leyes, los reglamentos y los contratos.

Se recomienda, además, designar un funcionario, con la preparación necesaria, como Administrador de Proyecto que será responsable de dirigir, coordinar y supervisar el personal responsable del mismo. Este servirá de enlace entre los usuarios, el personal técnico y la gerencia. Esto debe hacerse de forma ponderada, de acuerdo con la inversión y la magnitud de cada proyecto.

Los funcionarios principales de cada entidad gubernamental son responsables del cuidado, la protección, la conservación y el uso adecuado

de los fondos públicos bajo su dominio, control o custodia. Además, cada entidad también tiene la responsabilidad de establecer controles adecuados para proteger los mismos.

Artículo 7.2- Facultades de la *Puerto Rico Innovation and Technology Service* (PRITS)

La Ley 75-2019, creó la *Puerto Rico Innovation and Technology Service* (PRITS), con el propósito de establecer y promover la política pública sobre la elaboración, manejo, desarrollo, coordinación e integración inter agencias efectiva de la innovación y de la infraestructura tecnológica e informática del Gobierno de Puerto Rico. Véase, además, la Ley Núm. 151-2004, según enmendada, conocida como "Ley de Gobierno Electrónico".

De conformidad con el inciso el Artículo 6 de la Ley 75-2019, PRITS, por "[s]er la Oficina de la Rama Ejecutiva encargada de implantar, desarrollar y coordinar la política pública del Gobierno sobre la innovación, información y tecnología", tiene la facultad de "[r]evisar, evaluar y aprobar cualquier proyecto de creación, implantación, modificación, migración y actualización de las bases de datos, innovación, información y tecnología a ser adoptadas por las agencias".

Además, el Artículo 15 de la referida ley establece que "[l]a *Puerto Rico Innovation and Technology Service* tendrá la facultad de revisar, evaluar y aprobar cualquier proyecto de creación, implantación, modificación, migración y actualización de las bases de datos, innovación, información y tecnología a ser adoptadas por las agencias. La *Puerto Rico Innovation and Technology Service* emitirá por escrito las recomendaciones y los estándares que correspondan, según sea el caso, para que los proyectos de bases de datos, innovación, información y tecnología de las agencias cumplan con los propósitos de esta Ley y remitirá dicha comunicación al jefe de agencia y al Oficial Principal de Informática de ésta. Las agencias tendrán que diseñar, desarrollar, adoptar e implantar sus proyectos de base de datos, innovación, información y tecnología a tenor con los parámetros y las especificaciones que establezca la *Puerto Rico Innovation and Technology Service*. Asimismo, dicha Oficina deberá evaluar y aprobar cualquier contratación de servicios o compra de equipo por parte de las agencias a ser utilizado o destinado para un proyecto de base de datos, innovación, información y tecnología".

De hecho, en el Artículo 14 de la Ley 75-20199, expresamente se dispone que "[n]inguna propuesta de desarrollo de las tecnologías de información y comunicación o contrato para la prestación de servicios de las tecnologías de información y comunicación por cualquier Agencia será otorgada sin la revisión y los comentarios previos de la *Puerto Rico Innovation and Technology Service*".

La propia Ley 75-2019, en su Artículo 3, define el término "agencia" como "cualquier junta, cuerpo, tribunal examinador, comisión, corporación pública, oficina,

división, administración, negociado, departamento, autoridad, funcionario, empleado, persona, entidad o cualquier instrumentalidad de la Rama Ejecutiva del Gobierno de Puerto Rico". Por tanto, la *Puerto Rico Innovation and Technology Service* tiene injerencia y jurisdicción sobre los proyectos de creación, implantación, modificación, migración y actualización de las bases de datos, innovación, información y tecnología a ser adoptados por la Autoridad.

Artículo 7.2.1- Evaluación de contratos de servicios tecnológicos

A tenor con las disposiciones del inciso (j) del Artículo 13 de la Ley 75-2019, la *Puerto Rico Innovation and Technology Service*, tiene la facultad para evaluar todo contrato de servicios relativo a las tecnologías de información y comunicación a ser suscrito por la agencia, en lo relacionado al cumplimiento con las disposiciones y los propósitos de la Ley 75-2019, así como con la reglamentación que se adopte, previo a que se le remita el contrato en cuestión a PRITS para su consecuente revisión y análisis

A base de lo expuesto, el Director de Tecnología de Información tendrá la responsabilidad de comunicar a PRITS cualquier asunto de interés que haya identificado al evaluar un contrato relativo a las tecnologías de información y comunicación, lo cual incluye pero no se limita, a irregularidades o disposiciones que van o podrían ir en contravención con la Ley 75-2019 y su reglamentación.

Artículo 7.2.2- Procedimiento para la evaluación de contratos de servicios tecnológicos

El procedimiento para la evaluación de toda solicitud de revisión, evaluación y aprobación de todo proyecto, compra, subasta, requerimiento de propuesta, contrato o cualquier método establecido para la adquisición de bienes y/o servicios relacionados en todo o en parte a los sistemas de información o que impacte los centros de datos ("data centers"), servicios de nube, sistemas de telefonía, infraestructura de redes, equipos y servicios de seguridad informática, digitalización de trámites y servicios, plataformas de datos, páginas y portales web, aplicaciones móviles, servicios, aplicaciones y sistemas de informática en general, y cualquier otro cubierto por la Ley 75-20199 o que requiera la intervención de la PRITS, de la Autoridad, será el siguiente:

1. El Director de Tecnología de Información, tras identificar la necesidad del bien o servicio correspondiente, completará la versión vigente del Formulario PRITS-001 de la *Puerto Rico Innovation and Technology Service* y lo remitirá, acompañado de toda la información complementaria correspondiente, al siguiente correo electrónico: **solicitudes@prits.pr.gov.**

2. Deberá incluir propuestas, si alguna. No será necesario contar con propuestas para presentar la solicitud. De contar con propuestas, el Director de Tecnología de Información unirá a la solicitud su opinión y recomendación

para cada una de ellas y recomendación debidamente fundamentada. Dicha opinión y recomendación deberá ser específica, detallando las necesidades, presupuesto y alternativas de la Autoridad. Toda opinión no fundamentada, generalizada o pro-forma se tendrá por no puesta.

3. La solicitud será firmada y certificada por el Director de Tecnología de Información y por el Director Ejecutivo, quienes certificarán la veracidad de la solicitud y necesidad del bien o bienes y/o servicio o servicios.

4. De aprobarse la solicitud, PRITS remitirá una certificación que tiene que hacerse formar parte del expediente de la solicitud de la Autoridad. El documento de aprobación emitido por PRITS formará parte de los documentos a presentar en el sistema de Procesamiento de Contratos (PCo) y/o en el de Procesamientos de Planteamientos (PP), según aplique. A su vez, formará parte del expediente del Contrato u Orden de Compra, independientemente exista un contrato de selección múltiple.

5. La aprobación de PRITS contendrá las limitaciones y exigencias que el Principal Ejecutivo de Innovación e Información del Gobierno de Puerto Rico (PEII), o su delegado, establezca y condicione en dicha aprobación, las cuales incluyen, pero no se limitan a:

    a. La aprobación se limita una sola instancia de adquisición o contratación, que no podrán ser segmentadas o fragmentadas sin la previa aprobación de PRITS. Tampoco podrá entenderse que constituye una autorización para una orden de cambio en la adquisición o contratación sin previa solicitud y aprobación de la PRITS.

    b. En caso de que la solicitud contenga cualquier información incorrecta, falsa, inexactitud o tergiversación, sea intencional o no, la aprobación se entenderá revocada inmediatamente. En caso de que la Autoridad adviniera en conocimiento de cualquier variación, información incorrecta, falsa, inexactitud o tergiversación en la solicitud, lo informará inmediatamente a PRITS y detendrá la gestión, adquisición o contratación objeto de la solicitud, en cuyo caso PRITS podrá autorizar una enmienda a la solicitud o en su discreción solicitar que se presente una nueva solicitud de recomendación y aprobación.

    c. La aprobación tendrá un periodo de vigencia que establecerá PRITS de conformidad con la envergadura de la adquisición o contratación propuesta. Con posterioridad a la vigencia establecida, se podrá brindar una extensión a petición justificada de la Autoridad. De iniciarse la gestión la aprobada objeto de la solicitud vigente y no completarse en el término informado en la solicitud, la Autoridad deberá informar de dicha dilación y su justificación a PRITS. PRITS se reserva el derecho de proporcionar observaciones adicionales a su entera discreción y modificar o revocar la

aprobación de obtener información adicional, que no estuviera disponible al momento de evaluación de PRITS.

6. Sólo se considerarán las solicitudes debidamente completadas y acompañadas de la información pertinente sometidas a través del correo electrónico antes señalado.

7. En caso de que la Autoridad obtenga la recomendación y aprobación de PRITS para la celebración de subasta o solicitud de propuesta (RFP), esta no podrá ser utilizada *ipso facto* para suscribir el contrato u orden de compra resultante del proceso de licitación. Es de conocimiento general que podrá haber variantes en cuanto a múltiples aspectos con posterioridad a una convocatoria a subasta o solicitud de propuesta. Ante esto, una vez culminado el proceso de licitación, de haber variación alguna entre el contenido de la Forma PRITS-001 (y cualquier condición de aprobación) y sus anejos con el contrato u orden de compra a celebrarse con el licitador agraciado, la Autoridad tendrá la obligación de notificar de dichos cambios a PRITS.

   La Autoridad no suscribirá contrato o emitirá orden de compra hasta tanto reciba la aprobación de PRITS a los cambios propuestos a la Forma PRITS-001, *so pena* de nulidad al amparo del Artículo 14 de la Ley-75. Para notificar cambios la Autoridad deberá enviar a PRITS, mediante el correo electrónico: solicitudes@prits.pr.gov, el Formulario PRITS-001 e identificarlo como enmienda. PRITS considerará la enmienda propuesta o remitirá a la Autoridad a un nuevo trámite de conformidad con la sección 5(b), anterior (dependiendo si la variación es sustancial).

8. PRITS se reserva el derecho de requerir toda la información necesaria para proceder con la evaluación.

Artículo 7.3- Contratación de servicios de telecomunicaciones y/o de información se hará mediante subasta

La “Ley para la Competencia Justa en Servicios de Telecomunicaciones, de Información y Televisión por Paga en Puerto Rico”, Ley 80-2017, regula la participación de las entidades gubernamentales y sus subsidiarias en el mercado de ofrecimiento de servicios de telecomunicaciones en el Gobierno de Puerto Rico. En su Artículo 6, inciso (b), dicha ley ordena que “toda agencia, departamento, corporación pública, municipio, corporación municipal y subdivisión política del Gobierno que contrate servicios de telecomunicaciones y/o servicios de información tales como: servicios de voz, centros de data (data centers), VOIP, banda ancha, cable televisión, celulares, IPTV y DBS, entre otros, así como equipos y programación para servicios de información y de telecomunicaciones, tendrá que hacerlo siempre mediante subasta asegurándose que

tanto las entidades privadas como gubernamentales que ofrezcan los servicios lo hagan en una base justa y en igualdad de condiciones y oportunidades".

CAPÍTULO VII. INFORMES, EXPEDIENTES E INTERVENCIONES FISCALES

Artículo 7.1.- Informe anual

Anualmente, al finalizar cada año fiscal, el Director Ejecutivo someterá a la Junta de Directores un informe sobre el uso, administración y adquisición de los recursos tecnológicos de la Autoridad.

Artículo 7.2.- Examen o inspección de expedientes y documentos originales

Todo archivo, expediente o documento, electrónico o no, relacionado con los procedimientos dispuestos en este Reglamento, será custodiado por la Oficina de Tecnología e Informática, constituirá información oficial y estará sujeto a examen por la Oficina del Inspector General y la Oficina del Contralor de Puerto Rico, quienes podrán examinar los documentos antes indicados conforme a sus itinerarios de intervenciones.

Artículo 7.3.- Término de conservación

Los archivos, expedientes y documentos, electrónicos o no, se conservarán por lo menos seis (6) años o hasta que hayan sido objeto de una intervención de la Oficina del Contralor de Puerto Rico, lo que ocurra primero. Disponiéndose, que los expedientes y documentos originales de propuestas objeto de señalamientos en los informes de intervención del Contralor se conservarán hasta tanto se tome acción final sobre los mismos.

Independientemente de lo dispuesto en el párrafo anterior, los expedientes y documentos originales de propuestas que se encuentren en proceso de investigación o pendientes de acción judicial, serán conservados hasta tanto se resuelva finalmente la investigación o el caso judicial.

CAPÍTULO VIII. DISPOSICIÓN DE APLICACIÓN GENERAL

Artículo 8.- Aceptación de las normas de acceso y uso

Todo empleado, funcionario, contratista de la Autoridad o persona autorizada para tener acceso a los sistemas tecnológicos de esta, suscribirá un documento en el que certifique haber leído estas normas y estar conforme con ellas, previo a que se le autorice el uso o acceso al sistema de comunicaciones electrónicas de la Autoridad.

CAPÍTULO IX. DISPOSICIONES TRANSITORIAS

Artículo 9.1.-Documentos vigentes

Todos los formularios, órdenes, cartas circulares, memorandos o documentos interpretativos, que gobiernan el uso, administración y adquisición de los sistemas tecnológicos, emitidos por la Autoridad del Distrito del Centro de Convenciones del Gobierno de Puerto Rico, que estén vigentes al momento de entrar en vigor ese Reglamento -en la medida que no sean contrarios a las disposiciones de este- continuarán vigentes hasta tanto sean enmendados, derogados o sustituidos.

Cualquier formulario, orden, carta circular, memorando o documento interpretativo, que sea inconsistente con las disposiciones de este Reglamento, carecerá de validez y eficacia.

Artículo 9.2.-Contratos

Cualquier contrato relacionado a el uso, administración y adquisición de los sistemas tecnológicos otorgado por la Autoridad válido al momento de entrar en vigor este Reglamento, continuará vigente. A su expiración, cualquier nueva contratación será manejada y tramitada conforme a las disposiciones de este Reglamento.

CAPÍTULO X. DISPOSICIONES FINALES

Artículo 10.1. – Derogación

Se deroga el Reglamento para la Administración de Sistema de Tecnología de Información de la Autoridad del Distrito del Centro de Convenciones del Gobierno de Puerto Rico V2.0, de 19 de agosto de 2010.

Artículo 10.2.- Enmiendas

Este Reglamento podrá ser enmendado en virtud de cualquier ley, norma o reglamento, federal o estatal, aplicables.

Artículo 10.3.- Interpretación

El Director Ejecutivo de la Autoridad del Distrito del Centro de Convenciones del Gobierno de Puerto Rico interpretará toda controversia o duda que surja sobre la interpretación de este Reglamento.

Artículo 10.4.- Divulgación

Copia de este Reglamento se entregará a todos los empleados o funcionarios de la Autoridad que sean usuarios o intervengan directa o indirectamente con el uso, administración y adquisición de los sistemas tecnológicos del Distrito del Centro de Convenciones del Gobierno de Puerto Rico. La Autoridad mantendrá evidencia de dicha entrega y divulgación y orientará sobre el contenido y aplicación de este.

Artículo 10.5.- Prohibición de discrimen

En la implantación de las disposiciones de este Reglamento, no se discriminará por razón de raza, color, nacimiento, origen, condición social, sexo, orientación sexual, ideas políticas o religiosas.

Artículo 10.6.- Separabilidad

Si cualquier inciso, Artículo o parte de este Reglamento fuese declarado inconstitucional o nulo por un tribunal con jurisdicción y competencia, tal declaración no afectará, menoscabará o invalidará las restantes disposiciones y partes de este Reglamento, sino que su efecto se limitará al inciso, Artículo o parte específica declarado inconstitucional o nulo.

Artículo 10.7 – Vigencia

Este Reglamento comenzará a regir treinta (30) días después de su después de su presentación en el Departamento de Estado de Puerto Rico, a tenor con la Ley Núm. 38-2017, según enmendada, conocida como “Ley de Procedimiento Administrativo Uniforme del Gobierno de Puerto Rico” (L.P.A.U), y aplicará a todos los procedimientos que sean iniciados a partir de su vigencia.

Aprobado por la Junta de Gobierno de la Autoridad del Distrito del Centro de Convenciones del Gobierno de Puerto Rico en San Juan, Puerto Rico, hoy ___ de _____ de 2021.

APROBADO:

Director Ejecutivo
Autoridad del Distrito del Centro de Convenciones

Presidente Junta de Directores
Autoridad del Distrito del Centro de Convenciones

Secretario Junta de Directores
Autoridad del Distrito del Centro de Convenciones