PR iTS cyber security

PUERTO RICO INNOVATION & TECHNOLOGY SERVICE

Gobierno de Puerto Rico

Política TI-PRITS-007

Política de gestión de acceso, identidad y credenciales

V 1.0

Agencias y Municipios del Gobierno de Puerto Rico

PR iTS

Título	Política de gestión de acceso, identidad y credenciales	
Número:	POLÍTICA TI-PRITS-007	
Aprobado por:	Antonio Ramos Guardiola Principal Ejecutivo de Innovación e Información	24/01/2024
Jefe Responsable	Poincaré Diaz Peña Principal Oficial de Seguridad Cibernética	Revisado: 24/01/2024
Oficina responsable:	Oficina para la Evaluación de Incidentes Cibernéticos	*Contacto:* support@prits.pr.gov

Contenido

1. DESCRIPCIÓN

La gestión de identidades, credenciales y accesos (ICAM, por sus siglas en inglés) consiste en un marco de procesos, políticas y tecnologías que facilita la gestión de identidades electrónicas o digitales. De esta forma, se controla el acceso de los usuarios a información crítica dentro de la organización.

El marco de ICAM permite a los administradores de tecnología de la información (TI) asignar y eliminar privilegios de acceso, ya sea de forma individual, grupal o basada en roles. También posibilita administrar las bases de datos de identidades de usuarios y sus privilegios de acceso, además de registrar la información de inicio de sesión. Entre los sistemas de ICAM se incluyen el inicio de sesión única, autenticación multifactorial y la administración de acceso privilegiado.

Estas tecnologías facilitan almacenar de forma segura los datos de identidad y perfil de usuarios. A su vez, incorporan controles para garantizar que se compartan estrictamente los datos necesarios y relevantes. Un ICAM adecuado reduce la probabilidad de comprometer la confidencialidad, disponibilidad e integridad de los datos de las agencias.

2. BASE LEGAL

Esta política se emite al amparo del artículo 6 de la Ley Núm. 75-2019, mejor conocida como "*Ley de Puerto Rico Innovation and Technology Service (PRITS)*"; de los artículos 4, 5, 6 (e) de la Ley Núm. 151-2004, según enmendada, conocida como la "*Ley de Gobierno Electrónico*" y de los artículos 5 y 14 de la Ley Núm. 40-2024, conocida como "*Ley de Ciberseguridad del Estado Libre Asociado de Puerto Rico"*.

La Ley Núm. 75, *supra*, creó PRITS con el propósito de establecer y promover la política pública sobre la elaboración, el manejo, desarrollo, la coordinación e integración interagencial efectiva de la infraestructura tecnológica e informática del Gobierno de Puerto Rico. Además, el artículo 6 de esta ley otorga a PRITS la responsabilidad de crear e implementar planes estratégicos, políticas, estándares y una arquitectura integrada para las tecnologías de información y telecomunicaciones del Gobierno. Asimismo, este artículo establece que PRITS será el promotor de la implementación de la disciplina en las mejores prácticas en el manejo de proyectos y publicar guías y directrices a esos efectos. PRITS también tiene la responsabilidad de establecer e implementar políticas y aplicaciones de seguridad en el Gobierno para el uso de Internet y la red interagencial.

Por otra parte, el artículo 4 de la Ley Núm. 151, *supra*, otorga a PRITS la autoridad de administrar sistemas de información, establecer normas y procedimientos para el uso de tecnologías de información a nivel gubernamental, asesorar a las agencias, desarrollar transacciones electrónicas gubernamentales y garantizar su funcionamiento correcto, así como evaluar y asesorar en sistemas de procesamiento e interconexión para facilitar la coordinación interagencial. Con este propósito, PRITS tiene la facultad para establecer políticas de seguridad a nivel gubernamental sobre el acceso, uso, clasificación y custodia de los sistemas de información según lo estipulado en el artículo 6, inciso (e). De igual modo, podrá establecer políticas dirigidas a garantizar la privacidad y protección de la información personal con relación al uso del

Internet conforme al artículo 6, inciso (f). Corresponde a las agencias cumplir con lo dispuesto en la Ley 151, las políticas de manejo de información y los estándares tecnológicos relativos a la Informática emitidos por PRITS, y comunicar las mismas de manera rápida y efectiva a su personal según lo establecido en el artículo 7, incisos (g) y (h) de la ley antes citada.

Complementando estas leyes, la Ley Núm. 40, *supra*, establece un marco legal para fortalecer la seguridad cibernética en el Gobierno de Puerto Rico, enfocándose en la protección de datos gubernamentales y la infraestructura crítica contra amenazas digitales. Para dirigir esta encomienda, esta ley creó la Oficina para la Evaluación de Incidentes Cibernéticos y el cargo del Principal Oficial de Seguridad Cibernética (CISO), bajo la supervisión del Principal Ejecutivo de Innovación e Información del Gobierno (PEII) de PRITS. Así también, la ley establece políticas públicas y estándares de ciberseguridad centrados en mantener la confidencialidad, integridad y disponibilidad de la información gubernamental, mejorar la seguridad de redes e infraestructuras críticas, y fortalecer las capacidades para prevenir y responder a amenazas cibernéticas. Además, la ley promueve la protección de la privacidad de los ciudadanos y el cumplimiento de normativas básicas de ciberseguridad del Gobierno de los Estados Unidos. Finalmente, introduce sanciones para aquellas entidades gubernamentales y proveedores de servicios que incumplan con las normativas de PRITS.

3. PROPÓSITO

La política de gestión de acceso, identidad y credenciales tiene como propósito establecer los requisitos y lineamientos para la administración de **identidades digitales** en el Gobierno de Puerto Rico. Esta política define los controles que rigen la emisión, mantenimiento, auditoría y evaluación de riesgos de todas las identidades digitales, tanto de individuos como de sistemas que acceden a redes, sistemas de información y datos gubernamentales.

4. ALCANCE

Las disposiciones de esta política son aplicables a la Rama Ejecutiva, incluyendo todo departamento, junta, dependencia, comisión, negociado, oficina, agencia, administración u organismo, subdivisión política, corporaciones públicas y municipios. De igual forma aplica a cualquier persona natural o jurídica que haga negocios o tenga contratos con el Gobierno de Puerto Rico, incluyendo, de forma no exhaustiva, a las personas privadas que desempeñan funciones y servicios públicos, pero solamente con respecto a las funciones y servicios públicos desempeñados; a todo ejercicio de administración pública o privada en el que se hubieren dedicado o invertido fondos o recursos públicos ya sea directa o indirectamente, o sobre la cual se hubiere ejercido la autoridad de cualquier servidor público, en cuanto a los datos que se generan como producto de tales actividades.

5. DEFINICIONES

5.1 **Acceso no autorizado —** ocurre cuando una persona, grupo, código, programa, aplicación o cualquier otra entidad o proceso informático obtiene acceso lógico, digital o físico sin aprobación o consentimiento a una red de infraestructura crítica, sistema, datos, aplicación, "*data room*" u otro recurso de tecnología de la información del Gobierno o cuando se obtiene acceso o se intenta obtener acceso a información o recursos que no son necesarios para cumplir con su trabajo y o función, siguiendo el Principio de Privilegios Mínimos.

5.2 **Activos de información —** cualquier dato, información, o recurso relacionado con la información que tiene valor para una organización.

5.3 **Agencia —** todas las entidades y organismos que componen la Rama Ejecutiva del Gobierno de Puerto Rico y los municipios. Esto incluye, pero no se limita a cualquier departamento, junta, dependencia, comisión, negociado, oficina, agencia, administración, organismo, subdivisión política, y corporaciones públicas. También, comprende el conjunto de funciones, cargos y puestos que constituyen toda la jurisdicción de una autoridad nominadora de estas agencias y municipios independientemente de cómo se le denomine.

5.4 **Autenticación —** medida de seguridad diseñada para proteger un sistema de información y verificar la identidad de un usuario, proceso o dispositivo. A menudo, es un requisito previo para permitir el acceso y proteger los recursos en un sistema de información.

5.5 **Autorización —** proceso de otorgar a un usuario privilegios de acceso a la información o a un sistema de información siguiendo el principio de privilegio mínimo.

5.6 **Ciberseguridad —** prevención de daños a, protección y restauración de computadoras, sistemas y/o servicios de comunicación electrónica, incluyendo la información contenida en ellos para garantizar la disponibilidad, integridad, autenticidad, confidencialidad y no repudio.

5.7 **Confidencialidad —** significa preservar las restricciones de acceso y divulgación, incluyendo los medios para proteger la privacidad personal e información confidencial.

5.8 **Credenciales —** atributos únicos que se proporcionan a cada usuario autorizado para acceder los recursos y aplicaciones de los sistemas de información.

5.9 **Cuenta administrativa —** cuenta de usuario con privilegios completos destinada a realizar tareas de administración legítimas como la instalación de actualizaciones y programas, administración de cuentas de usuario, modificación del sistema operativo ("OS", en inglés) y configuración de aplicaciones, entre otros.

5.10 **Cuenta compartida —** cuenta que tiene un nombre de usuario y contraseña que se comparte entre dos o más personas. Las cuentas compartidas no incluyen cuentas con firmas múltiples ("*multi-signature*" o "*multi-sig*", en inglés) donde cada individuo posee credenciales únicas para coordinar el acceso a una sola cuenta.

5.11 **Datos —** cualquier secuencia de uno o más símbolos a los que se les da significado mediante actos específicos de interpretación e información registrada, independientemente de la forma o el medio en el que se graban los datos.

5.12 **Disponibilidad —** significa garantizar el acceso y el uso oportuno y confiable de la información.

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

5.14 **Integridad —** significa proteger la información contra la modificación o destrucción indebida, incluyendo garantizar el no repudio y la autenticidad de la información.

5.15 **Principio de Privilegios Mínimos —** cada módulo (proceso, usuario, o programa, dependiendo del tema) solo puede acceder a la información y recursos necesarios para su propósito legítimo.

5.16 **Proveedor de servicios contratados —** entidad, ya sea persona natural o jurídica, pública o privada que provee servicios como redes, aplicaciones, programas, infraestructura o medios de seguridad mediante el soporte continuo y habitual, así como servicios de administración activa ya sea en las instalaciones de una Agencia, en el centro de procesamiento de datos de la Agencia (hosting), o en el centro de procesamiento de datos de un tercero.

5.17 **Sistema de información —** conjunto discreto de recursos de información para la recopilación, procesamiento, mantenimiento, uso, intercambio, difusión o disposición de información.

5.18 **Oficial Principal de Información de una agencia (OPI) —** empleado responsable de la gestión y supervisión de la infraestructura tecnológica y manejo de datos de una agencia.

5.19 **Tecnología de la Información (TI) —** cualquier sistema o recurso interconectado o subsistema de equipo utilizado en la adquisición, almacenamiento, análisis, evaluación, manipulación, manejo, movimiento, control, visualización, conmutación, intercambio, destrucción, transmisión o recepción automática de datos o información, si el equipo es utilizado por la agencia directamente o por un tercero bajo un contrato con la agencia que requiere el uso (i) de ese equipo; o (ii) de ese equipo en una medida significativa para la prestación de un servicio o el suministro de un producto. Además, incluye computadoras, equipos auxiliares (incluidos periféricos de imágenes, dispositivos de entrada, salida y almacenamiento necesarios para la seguridad y vigilancia), equipos periféricos diseñados para ser controlados por la unidad central de procesamiento de una computadora, software, firmware y procedimientos y servicios similares (incluyendo servicios de apoyo) y recursos relacionados.

6. POLÍTICA

Las agencias están obligadas a implementar los procedimientos necesarios que aseguren el cumplimiento de los requisitos aquí establecidos. Dichos procedimientos deben estar diseñados para garantizar que tanto las personas como los sistemas obtengan únicamente el acceso necesario a los recursos para realizar sus tareas y funciones específicas. Esto permitirá reforzar la postura de ciberseguridad gubernamental,

protegiendo efectivamente los activos de información contra amenazas internas y externas, al tiempo que se resguarda la confidencialidad, integridad y disponibilidad de los datos.

7. PROCESOS REQUERIDOS

7.1 Control de Acceso

El acceso a información se basará en el principio de la "necesidad de conocer" y el privilegio mínimo. Los usuarios tendrán el nivel mínimo requerido para sus funciones gubernamentales legítimas luego de obtener las autorizaciones correspondientes.

7.1.1 Los controles de acceso se implementarán cuando el propietario de un recurso tecnológico (por ejemplo, sistemas, aplicaciones, datos) requiera restringir el acceso a un grupo limitado de usuarios o asignar diferentes niveles de acceso. Recursos ampliamente disponibles (por ejemplo, acceso a Internet, *software* de oficina, etc.) podrán no necesitar controles de acceso.

7.1.2 Los derechos de acceso se otorgarán a los usuarios en roles y responsabilidades. Si estas cambian, se modificarán los accesos de forma inmediata y prioritaria.

7.1.3 El acceso a datos confidenciales deberá ser documentado adecuadamente.

7.1.4 Los controles de acceso podrán utilizarse para separar funciones y limitar el nivel de acceso y acciones de un usuario.

7.1.5 Los controles de acceso podrán ser proporcionados por el sistema operativo, integrados al recurso o en una solución de un proveedor de servicios.

7.1.6 Se revisarán periódicamente las configuraciones y controles de acceso para garantizar su alineación con las necesidades y autorizaciones vigentes.

7.1.7 Cada agencia deberá mantener un listado actualizado que identifique las cuentas administrativas. Este listado incluirá los administradores principales y secundarios de cada sistema con estos privilegios. Este listado podrá ser utilizado por el Administrador de Sistemas y el OPI. Así también, se dispone que la Oficina de Recursos Humanos será custodio de dicho listado y la hará disponible a la persona designada en caso de emergencias.

7.2 Gestión de cuentas

7.2.1 Deberá existir separación de funciones, de modo que la solicitud, autorización y administración de accesos se realicen por personas distintas.

7.2.2 Los propietarios de los recursos de información serán responsables de la evaluación y aprobación de las solicitudes de acceso.

7.2.3 La creación de cuentas de usuario y las modificaciones de accesos deberán documentarse y/o registrarse adecuadamente.

7.2.4 Las cuentas que no se hayan accedido durante el periodo de tiempo establecido por PRITS serán deshabilitadas.

7.2.5 Las agencias deberán contar con documentación e instrucciones formales para la autorización y gestión de cuentas con privilegios de administrador o acceso especial. Esto incluye la creación, asignación, uso y eliminación de dichas cuentas con capacidades elevadas.

7.2.6 Las agencias deberán proporcionar una cuenta de usuario a cada persona que trabaje para el proveedor de servicios que requiera acceso para el manejo de los sistemas de información del Gobierno, incluyendo, pero sin limitarse a, manejo de bases de datos y servidores, configuración de aplicaciones, entre otros, según la normativa establecida por PRITS.

7.2.7 El OPI o empleado designado se encargará de manejar los accesos de los proveedores de servicios que interaccionan con los sistemas de información de la agencia. Los accesos se limitarán a los privilegios mínimos necesarios para provisión de los servicios acordados.

7.2.8 Los administradores de sistemas u otra persona designada deberán entregar el listado de cuentas bajo su responsabilidad cuando lo solicite PRITS, así como proveer la información para atender investigaciones de incidentes de ciberseguridad.

7.3 Cuentas

7.3.1 *General*

7.3.1.1 Todas las cuentas tendrán un identificador único (“*username*”) provisto por la Oficina de Informática, verificando que no existan duplicados.

7.3.1.2 Todas las cuentas deberán tener una expiración de contraseña con excepción de las cuentas administrativas o cuentas raíz (“*root access accounts*”) que seguirán el proceso de rotación de contraseñas establecido por PRITS.

7.3.1.3 No se permitirán cuentas compartidas.

7.3.1.4 Los empleados no podrán tener cuentas de correo electrónico activas en más de una agencia a la vez.

7.3.2 Administrativas

7.3.2.1 Las credenciales de cuentas administrativas o con privilegios elevados sólo podrán ser usadas por un (1) administrador en el ejercicio de sus funciones. No se compartirán excepto en el estricto cumplimiento de procedimientos de cambio de control, recuperación ante desastres y/o continuidad de operaciones gubernamentales.

7.3.2.2 Las personas con cuentas administrativas se abstendrán de abusar sus privilegios y los utilizarán estrictamente para sus funciones.

7.3.2.3 Las personas con cuentas administrativas deberán utilizar la cuenta con el mínimo nivel de privilegios necesario para realizar sus tareas (por ejemplo, cuenta de usuario en lugar de cuenta de administrador).

7.3.2.4 Si un sistema tiene un solo administrador, deberán existir procedimientos de custodia de contraseñas para el acceso durante emergencias.

7.3.3 Proveedor de servicios

7.3.3.1 Los proveedores de servicios deberán utilizar la cuenta provista bajo el dominio del Gobierno para la prestación de los servicios a las agencias. No se aceptarán cuentas de entidades externas al Gobierno.

7.3.3.2 Cada cuenta de un proveedor de servicios o contratistas cumplirá con todas las políticas gubernamentales aplicables.

7.3.3.3 La actividad de acceso de proveedores de servicios deberá ser monitoreada y registrada en casos de soporte o acceso remoto.

7.3.3.4 Las cuentas de un proveedor de servicios que se utilizan para mantenimiento deberán estar deshabilitadas, excepto cuando se vaya a realizar mantenimiento autorizado. Esto aplicará cuando el equipo de mantenimiento de un proveedor de servicios se conecta a la red gubernamental y a su vez tiene otra conexión, ya sea a través de una línea telefónica, una línea alquilada u otro medio.

7.4 Autenticación

7.4.1 Se requerirá el uso de contraseñas para autenticar las identidades de los usuarios, especialmente al iniciar sesión. Todas las cuentas y dispositivos que requieren contraseñas deberán tener autenticación multi-factorial (MFA, en inglés). Esto implica un método de

autenticación adicional a la contraseña, como, por ejemplo, un token físico o sistema biométrico.

7.4.2 Se utilizarán contraseñas únicas para cada sistema. El sistema "*single-sign on*" no se considera como una contraseña bajo esta política.

7.4.3 Las contraseñas cumplirán con los requisitos de administración, expiración, longitud, complejidad y rotación establecidos por PRITS.

7.4.4 Las contraseñas se clasificarán como confidenciales y no deberán mostrarse, transmitirse, ni almacenarse en un texto claro que pueda ser visto por terceros, incluyendo, pero sin limitarse a, equipo y dispositivos electrónicos. Estas deberán cifrarse durante su transmisión y almacenamiento en todos los componentes del sistema.

7.4.5 Las contraseñas iniciales, por ejemplo, aquellas asignadas por los administradores de TI al crear una cuenta o durante el restablecimiento de la contraseña, deberán establecerse en un valor único por usuario y cambiarse inmediatamente después del primer uso.

7.4.6 Antes de instalar un sistema en la red, las contraseñas predeterminadas proporcionadas por el proveedor deberán cambiarse inmediatamente y las cuentas predeterminadas innecesarias deberán eliminarse o deshabilitarse.

7.4.7 Los empleados y terceros con acceso a sistemas de información gubernamentales tienen el deber de mantener la confidencialidad de sus credenciales. En caso de pérdida, compromiso o robo de estas credenciales, deberán notificarlo inmediatamente a la Oficina de Informática de la respectiva agencia.

7.4.8 Las contraseñas comprometidas se cambiarán de inmediato.

7.4.9 No se evadirán controles de autenticación con *scripts* o contraseñas codificadas.

7.4.10 Los usuarios no deberán eludir la entrada de las credenciales por medio de contraseñas almacenadas en aplicaciones, *scripts* incrustados o contraseñas codificadas en *software* del usuario. Se podrán hacer excepciones para aplicaciones específicas (como respaldo automatizado) con la aprobación del OPI.

7.4.11 Las credenciales destinadas a grupos, como las empleadas para reuniones virtuales, serán para el uso exclusivo de los miembros que cuenten con autorización previa.

7.4.12 Cuando se utilicen otros mecanismos de autenticación, como *tokens* de seguridad, tarjetas inteligentes, certificados, u otros, cada deberá asignarse a un solo usuario. Además, se

deberán implementar controles físicos o lógicos para garantizar que sólo el usuario previsto tenga acceso.

7.4.13 Los *tokens* físicos de seguridad deberán devolverse a solicitud de la agencia o al finalizar la relación con ésta. También deberán revocarse de inmediato las credenciales asociadas a los mismos. Los *tokens* que pertenecen a dispositivos o sistemas acreditados deberán desacreditarse de inmediato al finalizar la relación con la agencia.

7.5 Acceso Remoto

Se considera acceso remoto, cualquier tipo de conexión establecida con las redes internas de la agencia desde ubicaciones externas. Esto incluye, pero no se limita a, conexiones desde el hogar, escuelas, universidades, hoteles, aeropuertos, cafeterías, oficinas satélites, así como a través de dispositivos inalámbricos y otros medios similares.

Todo trabajo realizado para una agencia mediante acceso remoto de cualquier tipo estará cubierto por esta sección. Esto incluye, pero no se limita a, el uso del correo electrónico, navegación web y otras aplicaciones de la agencia utilizada a través de internet.

7.5.1 El acceso remoto se otorgará a los empleados según sea necesario y con la aprobación del OPI. El Oficial administrará el acceso de forma centralizada, utilizando medidas de seguridad sólidas, como el cifrado y autenticación.

7.5.2 Los usuarios con acceso remoto deberán asegurar que su conexión sea tan segura como dentro de la agencia. El uso de conexiones remotas para funciones gubernamentales será monitoreado para identificar el uso adecuado y actividades inusuales o sospechosas.

7.5.3 Los usuarios autorizados recibirán instrucciones y responsabilidades sobre el acceso remoto. El acceso remoto debe realizarse de forma adecuada, ética y responsable.

7.5.4 Este acceso y/o conexión serán monitoreados para identificar cuentas o computadoras comprometidas y patrones de uso inusuales u otra actividad sospechosa.

7.5.5 El acceso remoto a los activos de información deberá registrarse. Las tecnologías que permiten el acceso remoto, como *firewalls*, plataformas web, etc., deberán estar configurados para guardar los registros generados por este tipo de conexión.

7.5.6 El mantenimiento remoto de los activos de la agencia deberá aprobarse, registrarse y realizarse de manera que se evite el acceso no autorizado.

7.6 Gestión de dispositivos

7.6.1 El acceso a la red de la agencia deberá incluir un procedimiento de inicio de sesión seguro.

7.6.2 Las computadoras se configurarán para bloquearse automáticamente tras un período de inactividad determinado por PRITS.

7.6.3 Cada sesión de usuario permanecerá activa hasta que se realice un cierre de sesión manual o tras el tiempo máximo de inactividad determinado por PRITS.

7.7 Concienciación sobre la política, comunicación y capacitación

Las agencias serán responsables de proveer a los empleados, contratistas y proveedores de servicios externos acceso a esta política, así como capacitaciones, talleres u orientaciones periódicas.

7.7.1 *Empleados nuevos*

El Departamento de Recursos Humanos de cada agencia deberá garantizar que los empleados y funcionarios recién nombrados accedan, lean y comprendan esta política, así como los requisitos asociados aplicables a sus responsabilidades. Esto deberá hacerse antes de que se le otorgue acceso a una cuenta o a los recursos de información de la agencia.

7.7.2 *Empleados existentes*

El Departamento de Recursos Humanos, en colaboración con el OPI o el empleado designado por la autoridad nominadora establecerán los procedimientos para garantizar que los empleados y funcionarios con acceso a cuentas o recursos de información reciban, lean y cumplan con los requisitos de esta política que sean aplicables a sus respectivas áreas de responsabilidad. El Departamento de Recursos Humanos en colaboración con el OPI o empleado designado por la autoridad nominadora, deberán establecer los procedimientos para garantizar que los empleados y funcionarios con acceso a cuentas o recursos de información reciban, lean y cumplan con los requisitos de la política que sean aplicables a sus respectivas áreas de responsabilidad.

Cuando un empleado asume nuevas funciones o cambia de puesto, el OPI deberá asegurarse de que su acceso se ajuste adecuadamente a sus responsabilidades actuales, eliminando o modificando cualquier acceso innecesario de acuerdo con su nuevo nombramiento o designación, o responsabilidades.

7.7.3 *Separación o ausencias prologadas*

En situaciones de separación, desvinculación del servicio o ausencia prolongada de un empleado o funcionario, el Departamento de Recursos Humanos deberá notificar de inmediato al OPI.

En caso de separación o desvinculación del servicio, el OPI deberá restringir la cuenta y los accesos de manera inmediata.

En casos de ausencias prolongadas, el OPI y la autoridad nominadora tendrán discreción para permitir el acceso si consideran que es necesario para la agencia.

7.7.4 *Contratistas y terceros*

Los vendedores, suplidores, socios, contratistas, proveedores de servicios y otros terceros con acceso a los sistemas de información del Gobierno deberán cumplir con los requisitos aplicables aquí presentados. La agencia será responsable de establecer los procesos necesarios para informar al OPI o el empleado designado por éste sobre cualquier cambio o terminación de relación con terceros de modo que los accesos sean manejados o eliminados de forma adecuada.

8. SANCIONES

Si alguna agencia o cualquiera de sus funcionarios y empleados incumpliese con lo dispuesto en esta política, se le podrá imponer, previa notificación y oportunidad de ser oída, una multa no menor de cincuenta (50) dólares ni mayor de cien (100) dólares diarios por incidente o por cada día que incumpla con los estándares y principios de ciberseguridad aquí establecidos. Además, cuando medie obstrucción, negligencia, mala fe, temeridad o negativa caprichosa en el manejo o reporte de un Ciberataque, la PRITS podrá imponer a la agencia empleados o funcionarios, previa notificación y oportunidad de ser oída, una multa no menor de mil (1,000) dólares ni mayor de cinco mil (5,000) dólares por cada violación.

Si se identifica a un servidor público responsable de esta conducta, PRITS, en coordinación con la Oficina de Administración y Transformación de los Recursos Humanos (OATRH) y con la autoridad nominadora correspondiente, ordenará, previa notificación y oportunidad de ser oído, la anotación de la determinación en el expediente de personal del servidor público. De dicha acción culminar en el despido de dicho servidor público, el mismo no podrá ser contratado por una agencia o contratista del gobierno, ni como empleado, ni bajo una relación como contratista o subcontratista por un periodo de cinco (5) años.

Si se identifica a un proveedor de servicios responsable de esta conducta, le aplicarán sanciones monetarias conforme hasta un tope de la cuantía contratada, más cualquier otra contractual y por daños causados, incluyendo penalidades establecidas por leyes locales y federales aplicables. Además, ni ese proveedor de servicios o cualquier entidad que tenga un número significante de la misma gente podrá ser contratado por una agencia o contratista del Gobierno, ni como subcontratista por un periodo de cinco (5) años.

9. CERTIFICACIÓN DE CUMPLIMIENTO Y SOLICITUD DE EXENCIONES

Las agencias dispondrán de un término de seis (6) meses para finalizar todos los procedimientos necesarios a fin de cumplir con lo establecido en esta política. En o antes de la fecha de vencimiento, el OPI o la autoridad nominadora deberán certificar ante el CISO el cumplimiento de esta política a través del correo electrónico: cumplimientocyber@prits.pr.gov.

Cuando el cumplimiento de esta política no sea factible, técnicamente posible o se requiera una desviación, la agencia, a través del OPI o la persona designada por la autoridad nominadora, presentará una justificación escrita al CISO al correo electrónico antes descrito. Esta justificación será evaluada, y la decisión se comunicará por escrito a la agencia.

10. CLÁUSULA DEROGATORIA

Esta política deja sin efecto cualquier otra carta circular, memorando, orden administrativa, políticas, normativas, comunicación escrita o instrucción anterior que en todo o en parte sea incompatible con ésta, hasta donde existiera tal incompatibilidad.

11. VIGENCIA

Esta política tendrá vigencia inmediata.