PR iTS cyber security

PUERTO RICO INNOVATION & TECHNOLOGY SERVICE

ESTÁNDARES PARA LA SEGURIDAD CIBERNÉTICA

V1.0

Para la Rama Ejecutiva del Gobierno de Puerto Rico

Según establecido por el Puerto Rico Innovation and Technology Service por virtud de la Ley 75-2019.

Título:	**Estándares para la Seguridad Cibernética**		
Aprobado por:	Enrique A. Völckers Nin		10/29/2021
Jefe responsable:	N'gai Oliveras Arroyo	Revisado:	10/29/2021
Oficina responsable:	Oficina *de Ciberseguridad*, Puerto Rico Innovation and Technology Service (PRITS)	Contacto:	soc@prits.pr.gov

Contenido

1. Trasfondo

La Política para la Seguridad Cibernética del Gobierno de Puerto Rico establece un marco con medidas de seguridad mínimas, define roles y responsabilidades e instaura los estándares para proteger la información gubernamental. Con estos fines, los requisitos técnicos aquí presentados fueron diseñados para respaldar la política y delinear los principios y procedimientos para proteger los sistemas y activos de información.

2. Definiciones

Para este documento, los siguientes términos tendrán el significado que se establece a continuación:

2.1 *"Acceso no autorizado"* – ocurre cuando una persona obtiene acceso lógico o físico sin aprobación o consentimiento a una red de infraestructura crítica, sistema, datos, aplicación u otro recurso de tecnología de la información del gobierno.

2.2 "Activos sensitivos" – significa información, equipo o medios donde la pérdida, mal uso, acceso o modificación no autorizados pudieran afectar adversamente los intereses del Gobierno de Puerto Rico y/o la privacidad de los ciudadanos.

2.3 *"Agencia"* – significa cualquier junta, organismo, junta examinadora, 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.

2.4 "Arquitectura de confianza cero" (zero trust arquitecture, en inglés) – significa un plan de seguridad cibernética de una agencia, que, ante una red considerada comprometida, es diseñado para minimizar la incertidumbre en la aplicación de políticas precisas de acceso con privilegios mínimos y abarca las relaciones de los componentes y la planificación del flujo de trabajo.

2.5 *"Autenticación"* – significa una medida de seguridad diseñada para 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.

2.6 "Autenticación multifactorial" (MFA) – significa un sistema de autenticación que utiliza dos o más factores distintos para una autenticación exitosa. La autenticación multifactorial se puede realizar utilizando un autenticador multifactorial o mediante una combinación de autenticadores que proporcionan diferentes factores. Los factores de autenticación son:

i. Algo que sepa (por ejemplo, contraseña / número de identificación personal (PIN),
ii. Algo que tenga (por ejemplo, dispositivo de identificación criptográfica, "token"),
iii. Algo que eres (por ejemplo, biométrico).

2.7 *"Autorización"* – significa el proceso de otorgar a un usuario privilegios de acceso a la información o a un sistema de información.

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

2.9 *"Credenciales"* – el nombre de usuario y la contraseña únicos que se proporcionan a cada usuario autorizado para acceder a los recursos y aplicaciones de los sistemas de información del gobierno.

2.10 *"Cuenta administrativa"* – significa una cuenta de usuario con privilegios elevados destinada a realizar tareas legítimas de administración, como la instalación de actualizaciones y software de aplicación, la administración de cuentas de usuario, la configuración de aplicaciones y la modificación al sistema operativo (SO), entre otros.

2.11 *"Disponibilidad"* – significa garantizar el acceso y el uso oportuno y confiable a la información.

2.12 *"Infraestructura crítica"* – se refiere a los servicios, sistemas y activos esenciales, ya sean físicos o virtuales, cuya incapacidad o destrucción tendría repercusiones perjudiciales en la seguridad cibernética, la salud, la economía, la seguridad de Puerto Rico o cualquier combinación de esos asuntos.

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

2.14 *"Datos"* – significa información registrada, independientemente de la forma o el medio en el que está registrada.

2.15 *"Dispositivo móvil"* – significa cualquier dispositivo de computación móvil como un teléfono inteligente, otros teléfonos celulares, tableta, lector electrónico, dispositivo de medios portátil, dispositivo de computación portátil o cualquier otro dispositivo móvil con capacidad para almacenamiento de datos y conexión de red.

2.16 *"Cifrado"* – significa un procedimiento criptográfico en el que el texto sin formato se convierte a un formato de texto cifrado para evitar que cualquier persona, excepto el destinatario previsto, lea dichos datos.

2.17 “Cuenta de usuario estándar” – significa una cuenta de usuario con privilegios limitados para tareas generales.

2.18 *“Equipo”* – significa 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.

2.19 *“Firewall”* – significa una entrada que, siguiendo una política de seguridad local, limita el tráfico de comunicación de datos hacia y desde una de las redes conectadas para proteger los recursos del sistema de esa red contra las amenazas de la otra red.

2.20 “Firmware” - significa software y datos almacenados en hardware en una memoria de solo lectura (ROM, en inglés) o memoria programable de solo lectura (PROM, en inglés), de manera que los programas y datos no se pueden escribir o modificar durante la ejecución de los programas.

2.21 *“Gobierno”* – significa la Rama Ejecutiva del Gobierno de Puerto Rico.

2.22 *“Incidente”* o *“incidente de seguridad de la información”* – significa un suceso que (i) pone en riesgo real o inminente, sin autoridad legal, la integridad, confidencialidad o disponibilidad de la información o un sistema de información; o (ii) representa una violación o amenaza inminente de violación de la ley, políticas de seguridad, procedimientos de seguridad, políticas de uso aceptable o prácticas estándar de seguridad informática.

2.23 “Información de Identificación Personal” (IIP) significa cualquier representación de información que es legible sin la necesidad de una clave criptográfica especial para acceder a ella, permite o facilita el rastreo de la identidad de un individuo, incluyendo el nombre o la primera inicial y el apellido paterno de un individuo combinado con otra información que está vinculada o que se puede vincular a un individuo específico, como:

- Número de Seguro Social
- Número de licencia de conducir, tarjeta electoral u otra identificación oficial
- Números de cuentas bancarias o financieras de cualquier tipo, con o sin claves de acceso que puedan habérsele asignado
- Nombres de usuario y claves de acceso a sistemas informáticos públicos o privados
- Información médica protegida por la Ley HIPAA
- Información contributiva
- Evaluaciones laborales

2.24 “Información protegida de salud” (IPS) – significa cualquier representación de información que es legible sin la necesidad de una clave criptográfica especial para acceder a ella, contiene al menos el nombre de una persona o la primera inicial, y el apellido paterno combinado con información médica protegida por la Ley HIPAA, que incluye información demográfica, historial médico, resultados de análisis y laboratorio, afecciones de salud mental, información de seguros

o cualquier otro dato que los profesionales de la salud recopilan para identificar a una persona y determinar la atención adecuada.

2.25 "Integridad" – significa proteger la información contra la modificación o destrucción indebida, incluyendo garantizar el no repudio y la autenticidad de la información.

2.26 *"Malware"* – significa un software diseñado para obtener acceso no autorizado a un sistema de información y/o interrumpir, comprometer o dañar el funcionamiento de un sistema, al realizar una función o proceso no autorizado que afecta la confidencialidad, integridad o disponibilidad de un sistema de información.

2.27 "PRITS" – significa el Puerto Rico Innovation and Technology Service.

2.28 "Programa" o "software" – se refiere a los programas informáticos y datos asociados que pueden escribirse o modificarse dinámicamente durante su ejecución.

2.29 *"Recursos de información"* – significa información y los recursos relacionados, como, por ejemplo, personal, equipo y tecnología de la información.

2.30 *"Seguridad de la información"* – significa proteger la información y los sistemas de información para prevenir el acceso, utilización, divulgación, interrupción, modificación o la destrucción no autorizada que impida su confidencialidad, integridad y disponibilidad.

2.31 *"Sistema de información"* – significa un conjunto discreto de recursos de información para la recopilación, procesamiento, mantenimiento, uso, intercambio, difusión o disposición de información.

2.32 *"Tecnología de la Información"* (TI)

2.32.1 Para una agencia, significa cualquier sistema interconectado o subsistema de equipo utilizado en la adquisición, almacenamiento, análisis, evaluación, manipulación, manejo, movimiento, control, visualización, conmutación, intercambio, transmisión o recepción automática de datos o información por la agencia 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;

2.32.2 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.

3. Requisitos Técnicos

3.1 Internet

3.1.1 Está prohibido el uso de Internet para realizar actos ilícitos, incluido el acceso a sitios web con contenido ilegal, obsceno, de odio, difamatorio, indecente, objetable o inapropiado.

3.1.2 Las agencias establecerán controles para evitar el uso inadecuado del internet y una política de seguridad para al menos bloquear el acceso a sitios web con contenido pornográfico.

3.1.3 Se establecerán controles de autenticación, autorización, confidencialidad, integridad y monitoreo para proteger la información y los sistemas en aquellos casos en los que sea necesario acceder a la red interna desde fuera de las instalaciones de la agencia.

3.1.4 Se utilizará un "firewall" para controlar la comunicación con el internet desde dentro de la agencia.

3.1.5 Se establecerán los controles necesarios (por ejemplo, cifrado) para garantizar la confidencialidad de los datos sensibles en reposo y en tránsito en redes no seguras (por ejemplo, Internet, redes inalámbricas).

3.1.6 Las conexiones remotas a la red del gobierno se realizarán únicamente a través de una red privada virtual (VPN, en inglés) exclusivamente para uso oficial cuando las tareas relacionadas con el trabajo sean necesarias. Para el uso de la aplicación VPN, se establecerá un acuerdo que incluya una autorización de administrador de datos y un reconocimiento de las siguientes responsabilidades.

3.1.6.1 Proteger la información del gobierno evitando el acceso de usuarios no autorizados a las redes internas del gobierno a través del VPN.

3.1.6.2 Mantenimiento de parches y certificaciones de seguridad del sistema.

3.1.6.3 Asegurarse de que no haya información no cifrada y altamente confidencial almacenada en el dispositivo.

3.2 Software y Aplicaciones

3.2.1 Todo programa de aplicación desarrollado, por una agencia o mediante contrato con un tercero, para brindar servicios a los ciudadanos a través de Internet o facilitar las operaciones internas de la agencia, deberá asegurar que considera los siguientes elementos mínimos de seguridad para su implementación.

3.2.1.1 La integración de las mejores prácticas de seguridad para evitar accesos no autorizados y/o maliciosos a través del internet.

3.2.1.2 El uso de un firewall que controla el acceso al programa desde el internet.

3.2.1.3 Si el servicio a brindarse maneja datos sensibles, se deberá incluir e instalar en una red alternativa un sistema de prevención/detección de intrusiones para permitir el acceso controlado desde Internet y a la red interna para un intercambio de datos limitado y monitoreado.

3.2.1.4 Se deberá realizar una evaluación de vulnerabilidad antes de que la aplicación se ponga en producción y su certificación se incluirá como parte de la entrega de los servicios o productos.

3.2.2 Cualquier agencia que acepte pagos con tarjeta de crédito en sus portales a través de un motor de pago deberá cumplir con los estándares de seguridad de datos de la industria de tarjetas de pago (PCI DSS, en inglés). Además, la agencia deberá enviar los informes de cumplimiento requeridos por el proveedor de la cuenta o aplicación.

3.3 Autenticación multifactorial

Para garantizar las mejores prácticas de ciberseguridad, el uso de autenticación multifactorial (MFA, en inglés) será obligatorio para el siguiente tipo de usuarios:

- Todas las cuentas administrativas de TI.
- Cuentas de usuario del personal ejecutivo, directores y cualquier otro personal que administre información confidencial, IPS y/o IIP.
- Empleados que trabajan de forma remota.
- Contratistas y proveedores de servicios externos.

3.4 Servicios Contratados

3.4.1 Los contratos con terceros incluirán medidas para salvaguardar los activos sensibles. Los contratistas recopilarán y mantendrán información relevante para la prevención, detección, respuesta e investigación de la seguridad cibernética en todos los sistemas de información sobre los cuales tienen control u operan en nombre de las agencias.

3.4.2 Los proveedores de servicios externos de tecnología de la información y comunicaciones compartirán información y notificarán de inmediato al PRITS y a la agencia contratante cuando descubran un incidente de seguridad cibernética o un incidente potencial que pueda poner en riesgo los datos, productos de software y servicios confidenciales del gobierno.

3.4.3 Para cualquier contrato de servicios de ciberseguridad, el proveedor de servicios externo presentará a la Oficina Principal de Seguridad de la Información del gobierno informes mensuales sobre el estado de la ciberseguridad de los sistemas de información y los activos administrados en nombre de la agencia. Estos informes incluirán la información que se detalla a continuación.

- Las amenazas detectadas, los actores de amenazas y las vulnerabilidades.
- Las acciones de respuesta y remediación.
- El número total de incidentes de seguridad de la información que se informaron al PRITS a través de la plantilla para el Informe de Incidentes de Ciberseguridad.

3.4.4 Los proveedores cuyos servicios estén relacionados con la ciberseguridad o cuyos servicios requieran que información sensible de los ciudadanos resida en sus sistemas, deberán contar con una certificación de seguridad válida conocida como SOC 2 o ISO/IEC 27001. El PRITS tiene la autoridad única para solicitar esto o certificaciones adicionales en función de los productos o servicios a ser entregados.

3.4.5 La agencia será responsable de determinar cuándo un contratista o un tercero requiere acceso a una aplicación o sistema de información en particular, y cualquier otro aspecto del entorno de TI de la agencia. Una solicitud de privilegios de acceso será evaluada por el Oficial Principal de Informática o el personal de TI designado por éste, antes de otorgar acceso. El acceso será limitado en alcance y tiempo, de acuerdo con los servicios a ser prestados por el contratista, y será modificado o revocado cuando corresponda.

3.4.6 Si es necesario para llevar a cabo los servicios contratados, cada individuo tercero deberá tener una cuenta única establecida para ellos en el directorio activo, incluidas las credenciales de inicio de sesión. Se prohíben las cuentas genéricas o globales con credenciales de inicio de sesión compartidas.

3.5 Controles Adicionales de TI

3.5.1 Las agencias instalarán controles automáticos para la detección de programas no deseados (por ejemplo, virus, *adware*, *spyware*, *malware*, *ransomware*) y la prevención de eventos o actividades de intrusión que puedan afectar la seguridad de la información. Microsoft Defender AV será la primera opción para proteger los activos gubernamentales. El uso de otros productos antivirus deberá obtener la aprobación previa del PRITS. Los productos y servicios proporcionados por Kaspersky Lab están prohibidos.

3.5.2 Los sistemas de TI del gobierno se utilizarán estrictamente para realizar asuntos gubernamentales.

3.5.3 Las instalaciones y activos de procesamiento de información (por ejemplo, servidores, armarios de cableado para redes, conexiones telefónicas, áreas de impresión para datos sensitivos o

confidenciales) deberán estar alojados en áreas seguras, protegidas con un perímetro de seguridad apropiado y controles para evitar el acceso no autorizado y daños.

3.5.4 La información confidencial (por ejemplo, IIP, IPS) no quedará expuesta ni desprotegida bajo ninguna circunstancia. Deberá estar encriptada en todos sus estados (es decir, en tránsito y en reposo).

3.5.5 Los usuarios no deberán usar la misma contraseña para múltiples cuentas (por ejemplo, cuentas de correo electrónico personales y laborales, cuentas de sitios web, etc.).

3.5.6 Los usuarios evitarán abrir y ejecutar archivos de fuentes desconocidas o no confiables. Deberán validar con el personal de TI de su agencia antes de descargar y ejecutar archivos de sitios web no gubernamentales.

3.5.7 Los privilegios de acceso de los usuarios se reevaluarán periódicamente. El acceso empleará el principio de privilegio mínimo, permitiendo a los usuarios autorizados acceder solo a los datos y aplicaciones que son necesarios para realizar sus tareas y funciones.

3.5.8 Los programas de aplicación y la información tendrán controles de acceso que incluirán mecanismos de autenticación y autorización.

3.5.9 Todos los mecanismos de autenticación incluirán una contraseña de no menos de ocho (8) caracteres, que incluya una combinación de números, letras y caracteres especiales.

3.5.10 Todas las contraseñas de las cuentas administrativas se cambiarán al menos cada cuatro (4) meses y todas las de cuentas de usuario estándar se cambiarán al menos cada seis (6) meses.

3.5.11 No se instalará ningún software en dispositivos y equipos de TI del gobierno a menos que lo apruebe el Oficial Principal de Informática (OPI) de la agencia o el personal de TI autorizado por éste. Solo se instalará software debidamente aprobado y con licencia. Se prohíbe cualquier software no autorizado, sin licencia o copiado ilegalmente.

3.5.12 La disposición de todo el equipo con información sensitiva debe realizarse con métodos seguros, de tal manera que no se pueda acceder a los datos una vez que el equipo se encuentre fuera de las instalaciones de la agencia.

3.5.13 Si un dispositivo o equipo de TI del gobierno se pierde o es robado, la Oficina de Informática de la agencia tomará las medidas apropiadas para borrar de forma remota, cuando sea posible, cualquier dato alojado en dicho hardware. Además, la Oficina de Informática de la agencia deberá completar un Informe de Incidente de Ciberseguridad para notificar al PRITS sobre la situación y la posible seguridad de la información en riesgo.

3.5.14 El uso de equipo fuera de las instalaciones de la agencia requerirá la autorización previa del Oficial Principal de Informática de la agencia o el personal de TI designado por éste. Las

agencias establecerán los controles y monitoreo necesarios para asegurar que el equipo que ha estado fuera de la agencia se esté utilizando legítimamente para cumplir con las obligaciones gubernamentales del personal autorizado y que el uso externo del equipo no represente un riesgo para los sistemas de la agencia. Esto incluye la evaluación del equipo y la realización de auditorías al conectarse a los sistemas o redes de la agencia.

3.5.15 Se requerirá la aprobación previa del Oficina de Informática de la agencia para las reubicaciones y transferencias de equipos.

3.5.16 El acceso a las instalaciones de los sistemas de información (por ejemplo, servidores, áreas de almacenaje de equipo) estará controlado de manera que solo el personal autorizado pueda accederlos.

En consonancia con la creciente complejidad y sofisticación del entorno de amenazas cibernéticas, se exhorta a las agencias a desarrollar un plan para implementar la Arquitectura de Confianza Cero de una manera coordinada para prevenir, detectar, evaluar y remediar incidentes cibernéticos.

3.6 Dispositivos Móviles

3.6.1 Controles Generales para Dispositivos Móviles Propiedad del Gobierno

Para evitar actividades maliciosas, violaciones de datos y otros incidentes de seguridad de la información, se tomarán las siguientes medidas para el uso adecuado de los dispositivos móviles.

3.6.1.1 Todos los dispositivos móviles se registrarán en la Oficina de Informática de la Agencia antes de ser asignados a empleados específicos. Esta Oficina mantendrá una lista de los dispositivos móviles asignados y las aplicaciones de software y utilidades instaladas antes de ser entregadas al usuario.

3.6.1.2 Los dispositivos móviles se utilizarán solo para tareas oficiales legítimas relacionadas con los roles y responsabilidades de los empleados.

3.6.1.3 Los usuarios no realizarán modificaciones en el hardware o software instalados, incluyendo las reconfiguraciones, sin la aprobación de la Oficina de Informática.

3.6.1.4 Según sea necesario, la Oficina de Informática podrá establecer mecanismos de auditoría para acceder y utilizar sin previo aviso con fines de investigación y detección de posibles infracciones y/o uso indebido.

3.6.1.5 Los usuarios instalarán, sólo de las tiendas de aplicaciones oficiales, exclusivamente aquellas aplicaciones necesarias para realizar asuntos gubernamentales. Las fuentes de aplicaciones confiables incluyen el Company Portal, Google Play Store, Apple Store

y Microsoft Store. Las aplicaciones de cualquier otra fuente están prohibidas y no deben usarse.

3.6.1.6 Todos los usuarios de dispositivos móviles emplearán medidas de seguridad física razonables, ya sea que el dispositivo esté en uso o sea transportado. Los dispositivos no deben dejarse desatendidos.

3.6.1.7 Cuando se utilizan dispositivos móviles para acceder a información confidencial, se tendrá especial cuidado para garantizar que la información a la que se accede no se vea comprometida (por ejemplo, personas no autorizadas que ven información en la pantalla).

3.6.1.8 El software se mantendrá con las actualizaciones más actualizadas y aprobadas.

3.6.1.9 Se prohíben los dispositivos liberados (“rooted”) o con "jailbreak".

3.6.1.10 Las capacidades de red, por ejemplo, Bluetooth y comunicación de campo cercano (NFC, en inglés) se desactivarán cuando no estén en uso.

3.6.1.11 Se evitarán las redes no seguras y las redes Wi-Fi públicas con problemas de seguridad. Los dispositivos no se conectarán a redes no seguras o no confiables a través de conexiones inalámbricas, de radio, Bluetooth o USB mientras estén acoplados, emparejados o conectados a las redes o dispositivos de la agencia.

3.6.1.12 Los dispositivos estarán protegidos con fuertes controles de seguridad, como contraseñas, datos biométricos o códigos de acceso (PIN, en inglés). Se prohíbe la divulgación de las credenciales de inicio de sesión.

3.6.1.13 Los usuarios configurarán cada dispositivo para que se bloquee automáticamente cuando esté inactivo.

3.6.1.14 Las opciones de autorellenar o autocompletar en los navegadores web no se utilizarán para recuperar automáticamente las credenciales de inicio de sesión (es decir, nombre de usuario y/o contraseñas).

3.6.1.15 Al acceder a información o utilizar cuentas, los usuarios deberán cerrar sesión y desconectarse al final de ésta.

3.6.1.16 La Oficina de Informática de la agencia podrá instalar software de seguridad adicional, administrar políticas de seguridad, redes, aplicaciones y acceso a datos más estrictos utilizando soluciones tecnológicas adecuadas, incluyendo controles remotos.

3.6.1.17 Los usuarios notificarán inmediatamente a la Oficina de Informática de la agencia en las siguientes circunstancias.

- El dispositivo se pierde o es robado. Se podrá solicitar información específica, como información, cuentas y aplicaciones susceptibles de acceso no autorizado.
- Se sospecha que el dispositivo está o ha sido atacado con malware, virus o cualquier otro ataque cibernético.
- Existe un problema de seguridad con respecto a los datos confidenciales o la información de las agencias.

3.7 Evaluación Periódica de Ciberseguridad

Según sea requerido por PRITS, las agencias realizarán periódicamente evaluaciones de ciberseguridad, que incluyen, entre otras, la evaluación de amenazas y vulnerabilidades, controles de TI existentes e inventario de activos de TI, etc. Los usuarios garantizarán actualizaciones periódicas de los sistemas operativos y aplicaciones primarias (por ejemplo, navegadores web, software de productividad, clientes de correo electrónico y software de seguridad).

3.8 Informes

3.8.1 Informe de Incidente de Ciberseguridad

Una vez que se descubre un incidente o amenaza de seguridad de la información, la agencia notificará inmediatamente al PRITS y enviará el Informe de Incidente de Ciberseguridad que incluirá la información descrita en la Guía para Informar Incidentes de Ciberseguridad.

3.8.2 Informes Mensuales

Las agencias que no son monitoreadas por PRITS deberán enviar informes mensuales de ciberseguridad, con una breve descripción de los puntos finales, ataques, vulnerabilidades críticas, detecciones de malware, intentos fallidos de autenticación y conexiones denegadas. Según sea necesario, los PRITS pueden requerir información adicional.

Historial de Revisiones

Los estándares para la seguridad cibernética pertenecen y son mantenidos por la Oficina del Principal Oficial de Ciberseguridad del Gobierno de Puerto Rico adscrita a PRITS.

Fecha	*Descripción del cambio*	*Revisado por*	*Aprobado por*