PR iTS cyber security

PUERTO RICO INNOVATION & TECHNOLOGY SERVICE

Guía para Informar INCIDENTES DE CIBERSEGURIDAD

Para las Agencias de la Rama Ejecutiva del Gobierno de Puerto Rico

Según establecido por PRITS en virtud de la Ley 75-2019

PR iTS

Tabla de Contenido

Introducción

En virtud de la Ley 75-2019, se creó el Puerto Rico Innovation and Technology Service (PRITS) para establecer y promover la política pública sobre la preparación, gestión, desarrollo, coordinación e integración interagencial efectiva de la innovación e infraestructura tecnológica y tecnología de la información del Gobierno de Puerto Rico. Las responsabilidades de PRITS incluyen el desarrollo de un marco de ciberseguridad y establecer e implementar las políticas, aplicaciones, procesos y procedimientos que garanticen controles gubernamentales de seguridad efectivos para los sistemas de información, archivos electrónicos, el uso de Internet y la red interagencial.

Para obtener la información crítica relacionada con los incidentes de ciberseguridad, PRITS ha desarrollado una sección para informar incidentes de ciberseguridad en la herramienta PRITS ServiceDesk. Ésta permitirá a los usuarios notificar y documentar todos los eventos de ciberseguridad que hayan resultado en un incidente que represente una violación de las leyes, procedimientos y políticas de seguridad, o que sea una amenaza o haya puesto en riesgo la información o los sistemas de información del Gobierno. Este informe será esencial para recopilar información relevante para un posterior análisis basado en los datos históricos proporcionados, las actividades que se están llevando a cabo, las partes involucradas y los planes de acción futuros.

Definiciones

Para propósitos de esta guía, los siguientes términos tendrán el significado que se establece a continuación:

1. *Agencia* – 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. *Data breach (violación de datos)* – significa la pérdida de control, compromiso, divulgación y/o adquisición no autorizada, o cualquier suceso similar en el que: una persona que no sea un usuario autorizado accede o potencialmente pueda acceder Información de Identificación Personal (IIP) o Información Protegida de Salud (IPS), o un usuario autorizado accede a IIP o IPS para fines distintos a los autorizados.

3. *Gobierno* – Significa el Gobierno de Puerto Rico.

4. *Incidente* – significa cualquier suceso que (i) pone en riesgo real o inminente, sin autoridad legal, la integridad, confidencialidad o disponibilidad de 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 o políticas de uso aceptable.

5. *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, incluye el nombre o la primera inicial y el apellido paterno de un individuo combinado con otra información, y que está vinculado o es vinculable a un individuo específico como:

   (a) Número de Seguro Social

   (b) Número de Licencia de Conducir, Tarjeta Electoral u otra Identificación

   (c) Números de cuentas bancarias o financieras de cualquier tipo, con o sin las claves de acceso que puedan habérsele asignado

   (d) Nombres de usuario y claves de acceso a sistemas informáticos públicos o privados

   (e) Información médica protegida por la Ley HIPAA

   (f) Información contributiva

   (g) Evaluaciones laborales

6. *Información Protegida de Salud (IPS)* – significa cualquier representación de información que sea legible sin la necesidad de una clave criptográfica especial para acceder a ella, que contenga al menos el nombre o la primera inicial de una persona y el apellido paterno combinado con información médica protegida por la Ley de Portabilidad y Responsabilidad de Seguros de Salud (HIPAA), incluyendo información demográfica, historial médico, resultados de análisis y laboratorio, condiciones de salud mental, información del seguro o cualquier otro dato que los profesionales de la salud recopilen para identificar a una persona y determinar la atención adecuada.

7. *Integridad de la información* – significa proteger la información contra la modificación o destrucción indebida y garantizar el acogimiento y la autenticidad de la información.

8. *Loss or theft of device or media (pérdida o robo de dispositivos o medios digitales)* – ocurre cuando un empleado, contratista u otra persona autorizada pierde la posesión, por extravío o apropiación indebida por parte de alguien, de un equipo, dispositivo o medio de tecnología de la información del gobierno que se puede utilizar para acceder a datos confidenciales, la red del gobierno, cuentas o representan una amenaza para la seguridad de la información.

9. *Malicious code* (ransomware/malware/virus/worms) (*código malicioso*) – significa un grupo arbitrario de letras, números o símbolos organizados como un conjunto de instrucciones para una computadora que busca comprometer o dañar la confidencialidad, integridad o disponibilidad de computadoras, sistemas de información o comunicaciones, redes, infraestructura física o virtual controlada por computadoras o sistemas de información, o la información que reside en los mismos.

10. *Office 365 compromised account (cuenta comprometida de Office 365)* – ocurre cuando alguien roba o tiene acceso no autorizado a las credenciales de Office 365 (por ejemplo, nombre, contraseña o PIN).

11. *PRITS* – significa el Puerto Rico Innovation and Technology Service.

12. *Recursos de información* – significa la información y sus recursos relacionados, como personal, equipo, fondos y tecnología de la información.

13. *Seguridad de la información* – significa proteger la información y los sistemas de información del acceso no autorizado, la utilización, la divulgación, la interrupción, la modificación o la destrucción para proporcionar (i) confidencialidad, lo que significa preservar las restricciones autorizadas de acceso y divulgación, incluidos los medios para proteger la privacidad personal y la información de propiedad; (ii) integridad, que significa protegerse contra la modificación o destrucción indebida de la información, e incluye garantizar el acogimiento y la autenticidad de la información; y (iii) disponibilidad, lo que significa asegurar el acceso y uso oportuno y confiable de la información.

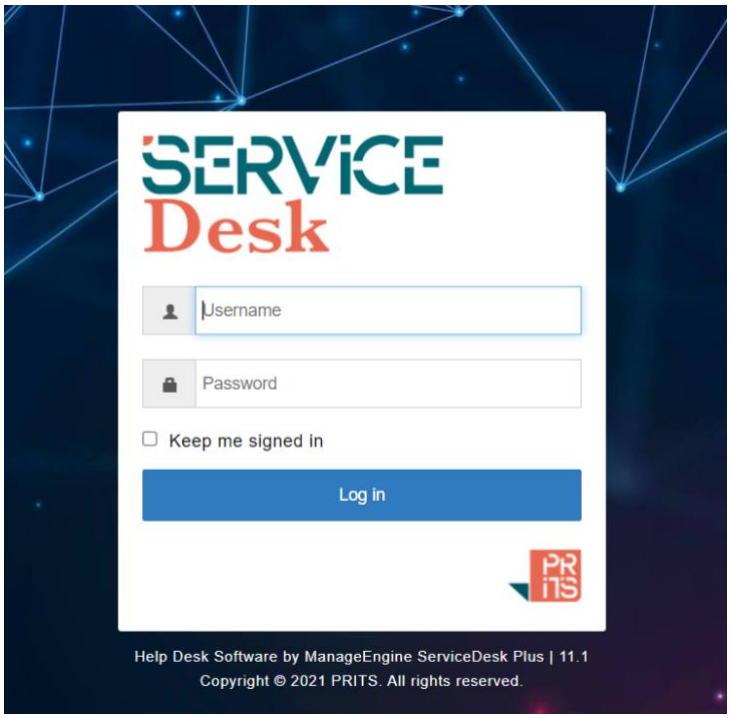
14. *Social engineering (phishing/spoofing/vishing/other)* (*Ingeniería social*) – significa el acto o intento de engañar a una persona para que revele información confidencial (por ejemplo, contraseña) o para realizar ciertas acciones que pueden usarse para obtener acceso no autorizado, cometer fraude, atacar sistemas o redes, descargar y ejecutar archivos que parecen ser benignos, pero en realidad son maliciosos, entre otros.

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

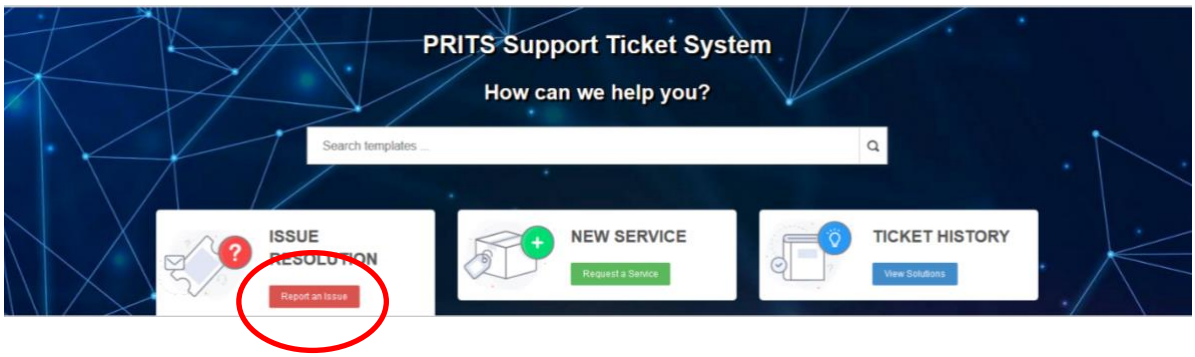
16. *Unauthorized access / Hacking (Acceso no autorizado / Hacking)* – ocurre cuando una persona obtiene acceso lógico o físico sin aprobación o consentimiento a una red, sistema, datos, aplicación u otro recurso de tecnología de la información.

Instrucciones

1. Inicie sesión en su cuenta de usuario de ServiceDesk mediante el enlace [support.prits.pr.gov.](support.prits.pr.gov)

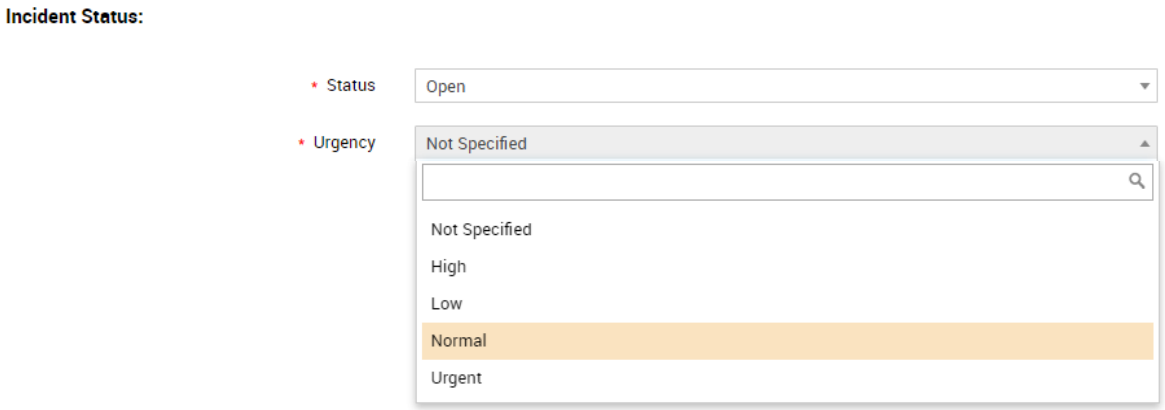


2. Seleccione *Report an Issue (reportar un problema)*.



3. Seleccione la opción *Cybersecurity Incident Report (informe de incidente de ciberseguridad)*.

4. En la sección de *Incident Status (estatus del incidente),* seleccione la urgencia del incidente.



La urgencia se basa en los siguientes criterios:

(a) *Low (baja)*
El incidente tiene poco o ningún impacto o afecta sólo a unos pocos usuarios.

(b) *Normal*
El incidente tiene efectos menores en un pequeño grupo de usuarios, no causa la interrupción de los servicios o representa una pequeña amenaza para los datos o la seguridad de la red.

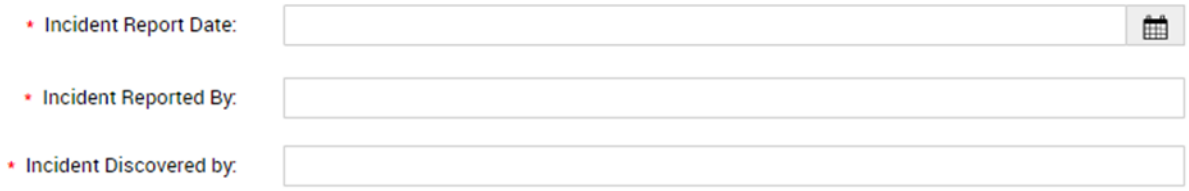
(c) *High (alta)*
Es probable que el incidente afecte a un pequeño grupo de usuarios, interrumpa servicios no esenciales e involucre violaciones de seguridad de la red o de los datos.

(d) *Urgent (urgente)*
El incidente está causando la degradación de servicios vitales para una gran cantidad de usuarios, constituye una violación grave de la seguridad o los datos de la red, afecta equipos o servicios de misión crítica o daña la confianza del público en la agencia.

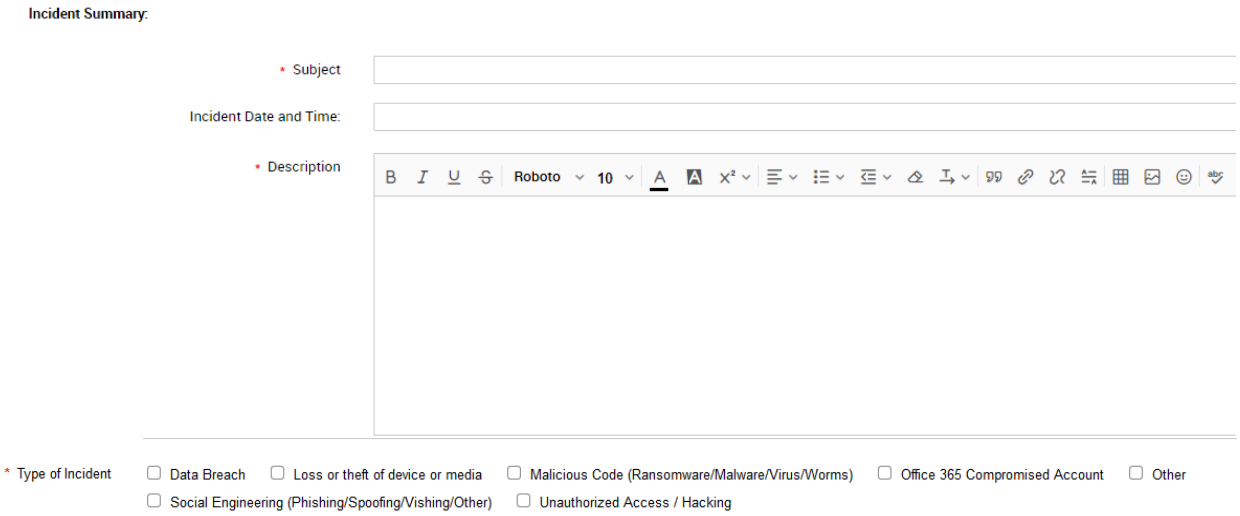
5. En la sección de *Contact Information (información de contacto),* incluya (a) el nombre y número de teléfono del punto de contacto de la agencia a cargo de la seguridad cibernética; y (b) la fecha en que se informó el incidente, el nombre de la persona que lo informó y el nombre de la persona que descubrió el incidente.

(a)

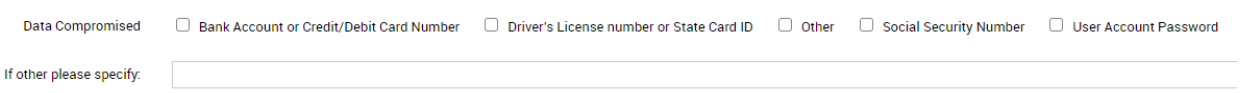
(b)



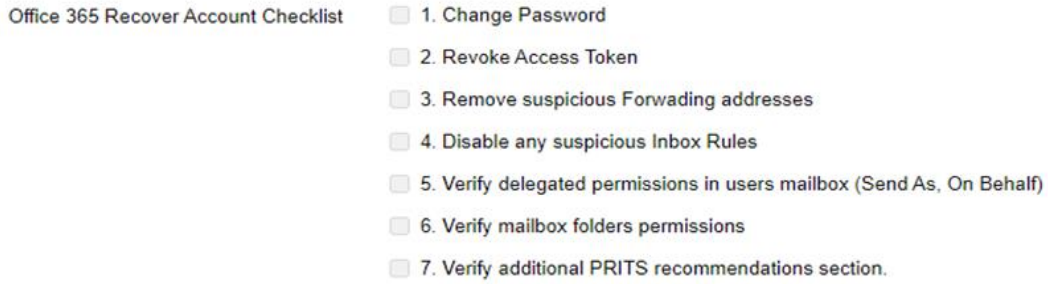
6. En la sección de *Incident Summary (resumen del incidente),* ingrese el tema del incidente, la descripción del evento, la fecha y hora en que ocurrió (si está disponible) y el tipo de incidente.



(a) Si el tipo de incidente fue una *Data Breach (violación de datos)*, complete la sección *Compromised Data (datos comprometidos)* y seleccione el tipo de datos que se sospecha que se han visto afectados. Si los datos comprometidos no se presentan entre las opciones, especifique en el espacio provisto.



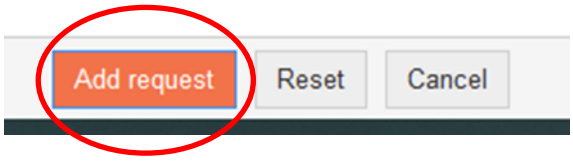
(b) Si el tipo de incidente fue una *cuenta comprometida de Office 365 (Office 365 Compromised Account)*, revise la lista para la recuperación de la cuenta. Marque las casillas correspondientes a los pasos que ya han sido completados. Para obtener más detalles sobre éstos, refiérase al documento "Proceso de respuesta a incidentes: buzones de cuentas comprometidas de usuario Office 365".



7. En la sección de *Additional Information (información adicional)*, incluya cualquier información complementaria disponible. De no haber disponibilidad de ésta, los espacios se pueden dejar en blanco.

8. Para respaldar la documentación del incidente, se pueden adjuntar archivos o capturas de pantalla adicionales en la sección de *Attachments (adjuntos).*

9. Para completar el proceso de notificación de incidentes, haga clic en *Add request (agregar solicitud)*.



Mantenimiento del Documento

El Oficial de Innovación e Información (OII) del Gobierno de Puerto Rico, o personal designado por éste, tendrá la autoridad para realizar cualquier cambio a este documento. Esta guía se revisará periódicamente a medida que evolucionen los procedimientos de tecnología e innovación. Se podrían esperar revisiones recurrentes a corto y mediano plazo a medida que PRITS continúe incorporando requisitos y refinando los criterios basados en (1) mejores prácticas y estándares reconocidos, (2) la integración de herramientas para optimizar el proceso, y (3) a medida que se analiza y atiende la retroalimentación de los usuarios.

Historial de Revisión

Fecha	*Descripción del cambio*	*Aprobado por*
8/30/21	Versión inicial	Nannette Martínez, CTO