PUERTO RICO
INNOVATION &
TECHNOLOGY
SERVICE

PRITS-SOP-0007-OPE

Procedimiento para informar incidentes de Ciberseguridad

Procedure for Reporting Information Security Incidents

- Aplicación: N/A
  Application: N/A

- Sistema
  System: N/A

Tabla de Contenido

1. Propósito

El propósito de este Procedimiento Operativo Estándar (POE) es establecer los procesos para reportar de manera rápida y efectiva los incidentes de ciberseguridad que puedan comprometer la información o los sistemas de información del Gobierno. Para facilitar la notificación y documentación de cualquier evento que resulte en una violación de leyes, procedimientos o políticas de seguridad, así como aquellos que representen una amenaza o riesgo. PRITS ha desarrollado una sección específica en la herramienta PRITS Service Desk donde se podrán realizar los reportes; alternativamente, podrán enviar los reportes por correo electrónico. Este proceso permite la comunicación rápida de incidentes, la recopilación de datos relevantes para análisis posteriores, el seguimiento de actividades en curso, la identificación de las partes involucradas y el desarrollo de planes de acción.

2. Alcance

Los lineamientos descritos en este POE son aplicables a los empleados de informática y tecnología de la información de la Rama Ejecutiva del Gobierno de Puerto Rico, 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.

3. Roles y responsabilidades

Según establece la Ley Núm. 40 de 2024, conocida como "Ley de Ciberseguridad del estado Libre Asociado de Puerto Rico", todas las agencias gubernamentales tienen la

obligación de reportar cualquier sospecha de incidente de ciberseguridad a la Oficina de Evaluación de Incidentes Cibernéticos (OEIC), adscrita a PRITS. Esta coordinación entre la agencia afectada y la OEIC permitirá gestionar el incidente, tomar medidas inmediatas para aislarlo, mitigar su impacto, colaborar con las agencias locales y federales involucradas, resolver el incidente y documentar el proceso.

Rol	**Responsabilidades**
Empleados de las agencias	Todos los empleados de las agencias gubernamentales, sin importar su puesto o nivel jerárquico, deberán reportar de manera inmediata cualquier sospecha de incidente de ciberseguridad a la Oficina de Informática, o su equivalente dentro de su agencia.
Oficina de Informática de las agencias, o su equivalente	Reportar a la OEIC cualquier evento que pueda representar una amenaza para la seguridad de la información de su agencia.
Proveedores de servicios contratados de las agencias	Los proveedores de servicios contratados que brindan servicios de tecnología de la información y comunicaciones están obligados a notificar tanto a PRITS como a la agencia contratante dentro de un plazo máximo de cuarenta y ocho (48) horas desde la detección del incidente o amenaza que comprometa datos, software, firmware, servicios confidenciales del gobierno, o información de cualquier persona natural o jurídica. Esta responsabilidad de reporte se extiende a todos los proveedores que utilicen o accedan a cualquier recurso de tecnología de la información perteneciente a una agencia gubernamental, gestionen sistemas de tecnología de la información (ya sean automatizados o manuales) bajo la administración de una agencia, operen estos sistemas en representación de una agencia, o manejen sistemas de información privados que contengan datos gubernamentales.
Agencias	Cada agencia establecerá procesos claros y eficientes para la notificación de incidentes de ciberseguridad a su oficina de informática, o su equivalente, tanto por parte de los empleados como de los proveedores de servicios contratados. Las agencias

Rol	Responsabilidades
	deberán asegurar la correcta comunicación y capacitación para que todas las partes conozcan sus roles y responsabilidades.

4. Abreviaciones, acrónimos, definiciones y significados

Abreviación / Acrónimo	Significado
CISO	Principal Oficial de Seguridad Cibernética *(Chief Information Security Officer)* del Gobierno
IIP	Información de identificación personal
IP	Protocolo de internet *(Internet protocol)*
IPS	Información protegida de salud
OEIC	Oficina para la Evaluación de Incidentes Cibernéticos
OPI	Oficial Principal de Informática
POE	Procedimiento operativo estándar
PRITS	Puerto Rico Innovation and Technology Service
TI	Tecnología de la información

Término	Definición
Acceso	La capacidad o los medios necesarios para leer, escribir, modificar o comunicar datos/información o utilizar cualquier recurso del sistema.
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.
Agencia u organismo gubernamental	Incluye todas las entidades y organismos que componen la Rama Ejecutiva del Gobierno de Puerto Rico y sus municipios. Esto incluye, pero no se limita a cualquier departamento, junta,

Término	Definición
	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, independientemente de cómo se denomine.
Ciberataque	Uso de un código no autorizado o malicioso en un sistema de información o el uso de otro mecanismo digital, como un ataque de denegación de servicios, con el propósito interrumpir o afectar las operaciones de un sistema de información o comprometer la confidencialidad, disponibilidad, o integridad de información digital almacenada en, procesada por, o que transita a través de un sistema de información.
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 su disponibilidad, integridad, autenticidad, confidencialidad y no repudio.
Código malicioso (*malicious code*)	(*Ransomware/malware/virus/worms*) 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 los datos, 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.
Confidencialidad	Preservar las restricciones de acceso y divulgación, incluyendo los medios para proteger la privacidad e información confidencial.
Contraseña	Cadena de caracteres (letras, números y otros símbolos) utilizada para autenticar una identidad o para verificar la autorización de acceso a sistemas y recursos protegidos.
Cuenta comprometida de Office 365 (*Office 365 compromised account*)	Ocurre cuando alguien roba o tiene acceso no autorizado a las credenciales de Office 365 (por ejemplo, nombre, contraseña o PIN).
Datos	Cualquier secuencia de uno o más símbolos a los que se les da significado mediante actos específicos de interpretación.

Término	Definición
Datos confidenciales	Información que, si se divulga, podría causar daños significativos a la organización. Este nivel incluye datos personales, registros financieros y otros documentos sensibles.
Datos restringidos	Información de máxima sensibilidad cuya divulgación podría causar daños severos a la organización o a individuos. Incluye secretos comerciales, información sobre investigación y desarrollo y datos altamente sensibles de clientes.
Gestión de incidente	Todos los procedimientos administrativos, físicos y técnicos aplicados para la investigación y mitigación ante la sospecha o el reporte de un incidente; incluyendo las notificaciones de violación o brechas a las partes o individuos impactados por el incidente, según aplicables por las regulaciones federales y locales.
Gobierno	Es el Estado Libre Asociado de Puerto Rico.
Impacto	Magnitud del daño que se puede esperar como resultado de las consecuencias de la divulgación, modificación o destrucción no autorizadas de la información, pérdida de esta, o por la indisponibilidad del sistema de información.
Incidente o incidente de seguridad de la información	Suceso que (i) pone en riesgo real o inminente, sin autoridad, la integridad, confidencialidad o disponibilidad de la información, sistema o proceso o un recurso de información; o (ii) representa un uso indebido de un recurso de información o 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. Para propósitos de este documento, los términos 'incidente', 'incidente cibernético', 'incidente de seguridad de la información' e 'incidente de ciberseguridad' se utilizarán indistintamente.
Infraestructura crítica	Servicios, sistemas, recursos 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.

Término	Definición
Ingeniería social	(*Phishing/spoofing/vishing*) 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.
Municipio(s)	Cualquiera de los 78 municipios de Puerto Rico. Para propósitos de esta política se utilizarán los términos Municipio(s) y Agencia indistintamente.
Oficial Principal de Informática (OPI)	Individuo responsable de la gestión y supervisión de la infraestructura y operaciones tecnológicas de una agencia gubernamental.
Pérdida o robo de dispositivos o medios digitales (*loss or theft of device or media*)	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.
Phishing	Técnica de ingeniería social donde los atacantes utilizan la comunicación electrónica, como correos electrónicos, mensajes de texto o sitios web falsos, para engañar a las personas y obtener información confidencial, como contraseñas, datos financieros o información personal.
Principal Oficial de Seguridad Cibernética (CISO) del Gobierno	Líder encargado de establecer las medidas de seguridad adecuadas para evitar el acceso no autorizado, divulgación, uso, daño, degradación y destrucción de la información electrónica, sus sistemas e infraestructura crítica. También será responsable de reducir el riesgo, el impacto y el costo de los ciberataques al establecer un marco con requisitos mínimos de seguridad de las tecnologías de la información (TI), definir roles y responsabilidades y establecer los estándares para proteger la información.
Principio de Privilegios Mínimos *(Least Privilege Principle*)	Cada módulo (proceso, usuario, o programa, dependiendo del tema) solo puede acceder a la información y recursos necesarios para su propósito legítimo.

Término	Definición
PRITS	Puerto Rico Innovation and Technology Service, Oficina de la Rama Ejecutiva encargada de implantar, desarrollar y coordinar la política pública del Gobierno sobre la innovación, información y tecnología, según lo dispuesto por la Ley 75 de 2019.
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.
Ransomware	(i) Significa un ciberataque, que incluye una amenaza de utilizar un código no autorizado o malicioso en un recurso de información, o una amenaza de utilizar otro mecanismo digital, como un ataque de denegación de servicios, con el propósito interrumpir o afectar las operaciones de un Recurso de información o comprometer la confidencialidad, disponibilidad, o integridad de información digital almacenada en, procesada por, o que transita a través de un recurso de información, con el fin de exigir un pago por rescate; y (ii) no incluye un evento en el cual el pago sea exigido por una entidad del Gobierno Federal, una investigación de seguridad bona fide, un pago legítimo de servicios por respuesta a un incidente o como respuesta a una invitación hecha por el dueño u operador del sistema de información a terceros para identificar vulnerabilidades en el sistema de información.
Recurso de información	Información y los recursos relacionados, como, por ejemplo, personal, equipos, programas, y tecnología de la información, entre otros.
Seguridad informática o seguridad de la información	Conjunto de controles, salvaguardas y otras medidas que toma una organización para proteger la información en cualquier formato. Esto implica la protección de los activos de informática, incluyendo la información, independientemente de si los activos están interconectados.
Sistema de información	Conjunto discreto de recursos de información para la recopilación, procesamiento, mantenimiento, uso, intercambio, difusión o disposición de información.

Término	Definición
Spoofing	Técnica en la que atacantes se hacen pasar por otra persona o dispositivo confiable con el objetivo de obtener acceso no autorizado a sistemas o redes, o para manipular a las víctimas para que revelen información confidencial.
Tecnología de la información	Para una agencia, significa 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. 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.
Violación de datos (*data breach*)	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.

5. Adiestramiento

Las agencias implementarán un programa de capacitación y educación en ciberseguridad para todos los empleados y proveedores de servicios contratados, con el fin de familiarizarlos con sus roles, responsabilidades y los procedimientos a seguir para reportar incidentes o potenciales incidentes de seguridad de la información. Los proveedores de servicios contratados recibirán una orientación inicial dentro de los

primeros 30 días de su contratación, y todos los empleados y proveedores recibirán capacitaciones periódicas al menos una vez al año o según sea necesario.

6. Referencias

Número de identificación	Título	Versión
PRITS-POL-0001	Política de Clasificación de Datos del Gobierno de Puerto Rico	1.0
PRITS-POL-002	Política de Respuesta a Incidentes de Seguridad de la Información	1.0
N/A	Incident Response Process for Compromised Office 365 Accounts	1.0
Ley Núm. 40-2024	Ley de Ciberseguridad del Estado Libre Asociado de Puerto Rico	N/A

7. Importante

Este Procedimiento Operativo Estándar (SOP) reemplaza cualquier carta circular, memorando, orden administrativa, comunicación escrita o instrucción previa que presente cualquier nivel de incompatibilidad con los lineamientos establecidos en este documento, en la medida en que se presente dicha incompatibilidad.

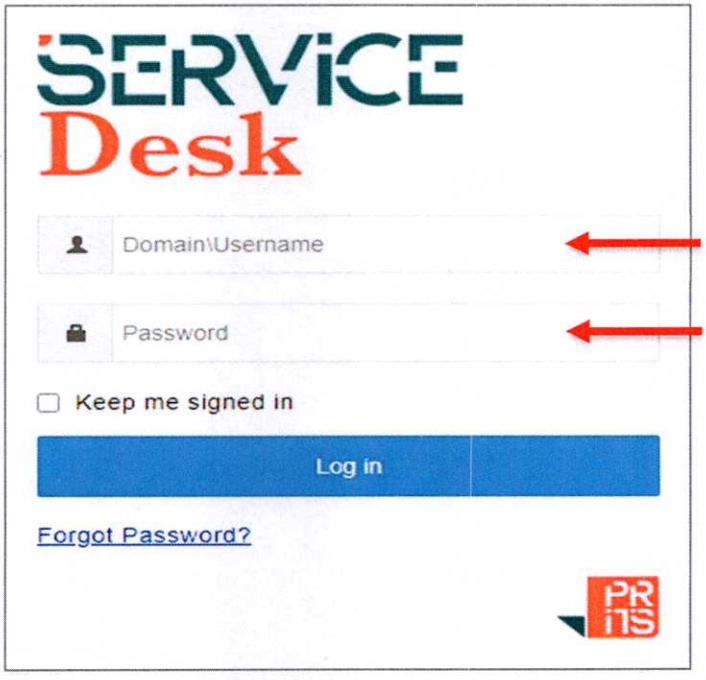
8. Procedimiento

8.1 Informe de un incidente de seguridad de la información a través de PRITS Service Desk

8.1.1 Inicio de sesión

8.1.1.1 El usuario accede a la página web https://support.prits.pr.gov/.
8.1.1.2 Ingresa el nombre de usuario y contraseña en los campos correspondientes.
8.1.1.3 El usuario selecciona la opción de "*Log in*" para acceder a su cuenta.

8.1.1.4 Si el usuario ha olvidado la contraseña, selecciona la opción de "*Forgot password?*".

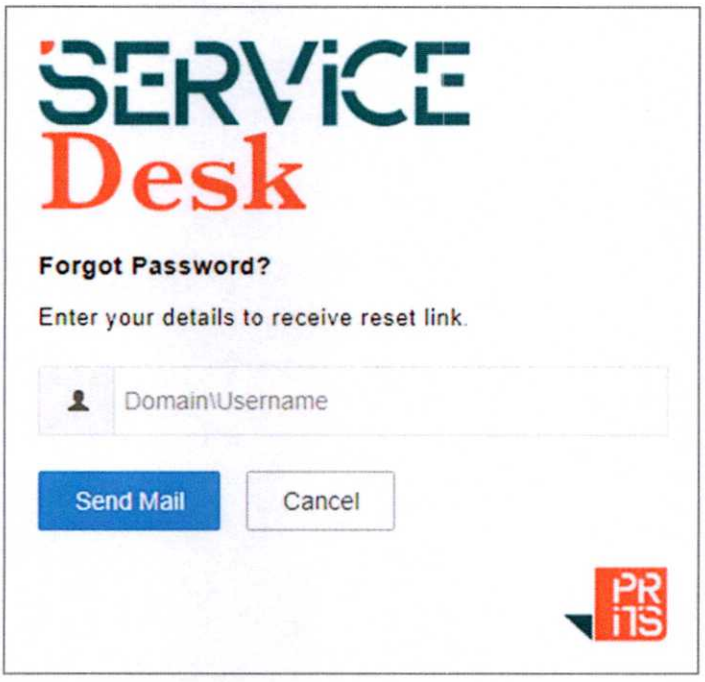


8.1.1.4.1 El usuario ingresa su nombre de usuario en el campo designado y selecciona "*Send mail*".

8.1.1.4.2 El sistema enviará un correo electrónico con un enlace para restablecer la contraseña a la dirección de correo electrónico asociada.

8.1.1.4.3 Para cancelar el proceso y regresar a la pantalla de inicio de sesión, el usuario selecciona "*Cancel*".

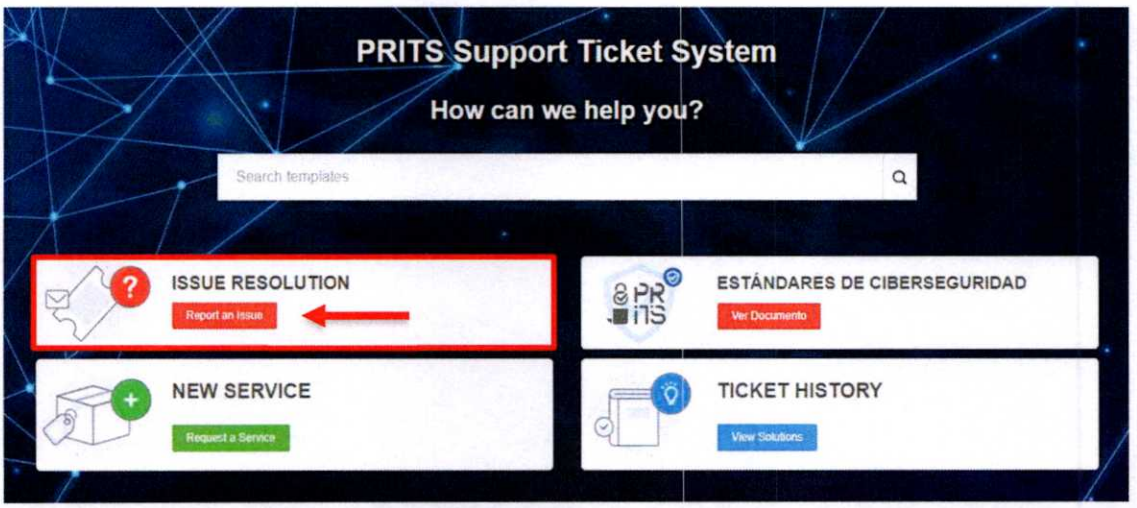
Este espacio se ha dejado intencionalmente en blanco.



8.1.2 Informar el incidente en *PRITS Support Ticket System*

8.1.2.1 Después de iniciar sesión, el usuario localiza la sección "*Issue Resolution*".

8.1.2.2 Selecciona la opción, "*Report an Issue*".



8.1.2.3 Accede la pantalla de catálogo de incidentes.

8.1.2.4 Dentro del catálogo, el usuario selecciona "*Cybersecurity Incident Report*" y completa el formulario con la información requerida para la evaluación inicial del incidente.

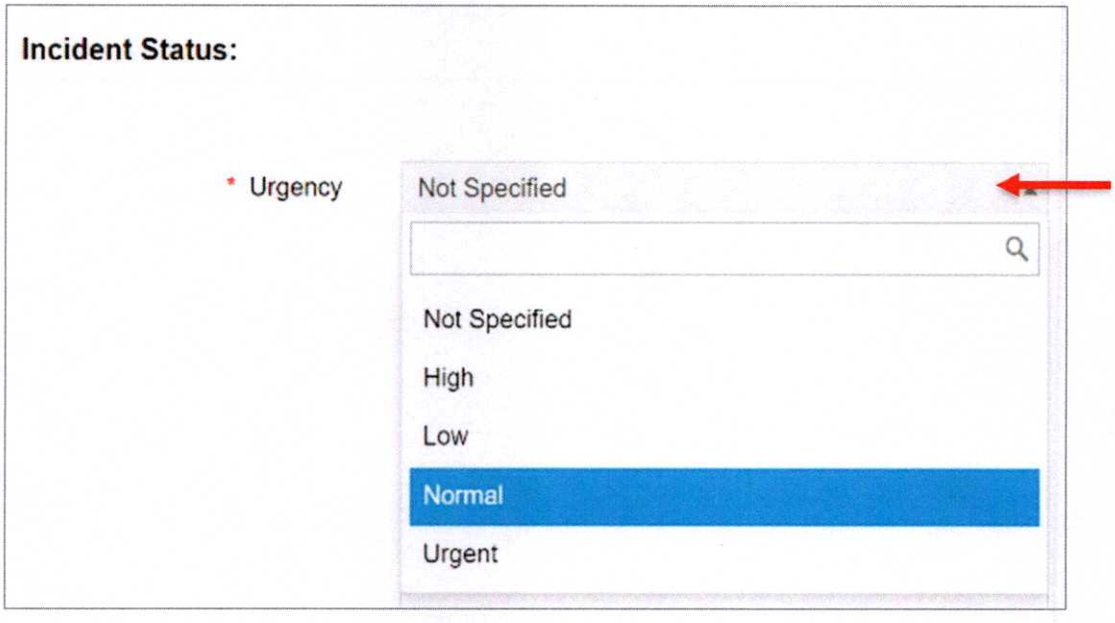
8.1.3 Completar el formulario

8.1.3.1 Estatus del incidente

8.1.3.1.1 En la sección "*Incident Status*", el usuario selecciona el nivel de urgencia (*urgent, high, normal, low*) que mejor refleje la gravedad del incidente, basado en los siguientes criterios:

Niveles de urgencia	Descripción
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.
High (alta)	El incidente está causando una degradación significativa de servicios para un grupo específico de usuarios, representa una violación seria de seguridad o pérdida de datos sensibles, afecta sistemas importantes, pero no críticos, o tiene el potencial de escalar rápidamente a nivel urgente si no se atiende de inmediato.

Niveles de urgencia	Descripción
Normal	El incidente tiene efectos menores en un pequeño grupo de usuarios, no causa la interrupción de los servicios o representa amenaza para los datos o la seguridad de la red.
Low (baja)	El incidente tiene poco o ningún impacto o afecta sólo a unos pocos usuarios.



8.1.3.2 Información de contacto

En la sección "*Contact Information*" (información de contacto), el usuario completa los siguientes campos:

8.1.3.2.1 *Agency Info Sec Contact*

Nombre completo del individuo designado como punto de contacto para asuntos de seguridad cibernética en la agencia.

8.1.3.2.2 *Contact phone*

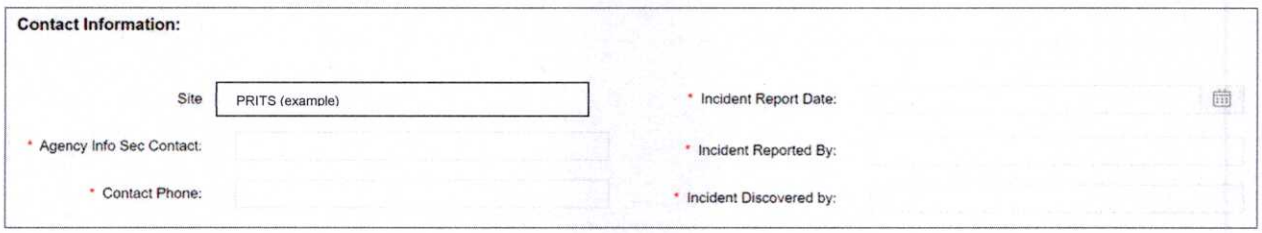
Número de teléfono de la persona de contacto.

8.1.3.2.3 *Incident Report Date*

Selecciona la fecha del reporte formal utilizando el ícono de calendario.

8.1.3.2.4 *Incident Reported By*
Nombre completo de la persona que reporta el incidente. Esta persona puede o no ser la misma que detectó inicialmente el incidente.

8.1.3.2.5 *Incident Discovered By*
Nombre de la persona que detectó el incidente inicialmente. Esta persona es la primera en detectar cualquier anomalía, fallo o vulnerabilidad en el sistema o proceso. Puede tratarse de un miembro del equipo técnico, un empleado o cualquier otro individuo que interactúe con el sistema o área afectada.



8.1.3.3 Resumen del incidente
En la sección "*Incident Summary*", el usuario incluye:

8.1.3.3.1 *Subject*
Título descriptivo del incidente.

8.1.3.3.2 *Date*
Fecha y hora exactas del incidente, siempre y cuando esta información sea conocida. En caso de que solo se disponga de una estimación, el usuario registra la hora aproximada más cercana a la ocurrencia del incidente.

8.1.3.3.3 *Description*
Descripción detallada del incidente, incluyendo, pero sin limitarse a:

- Impacto inicial, incluyendo los efectos inmediatos del incidente sobre las operaciones, datos o usuarios.
- Acciones iniciales para mitigar el incidente.

- Estado actual del incidente (activo, contenido o resuelto).

La descripción del incidente debe ser objetiva y basada en hechos verificables. Si alguna información relevante aún no ha sido confirmada, el usuario debe indicar explícitamente la falta de datos en el informe.

8.1.3.3.4 *Type of incident*

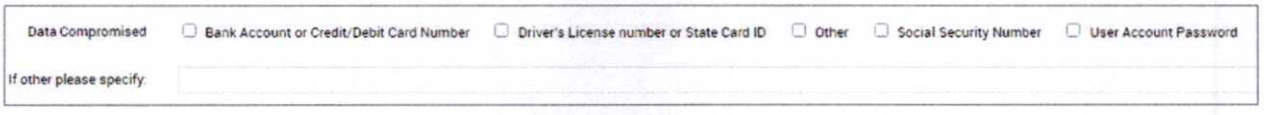
La categoría del incidente:

8.1.3.3.4.1 *Data Breach*

Exposición no autorizada de datos confidenciales o restringidos.

En la sección "*Compromised Data*", el usuario especifica el tipo de datos comprometidos:

- *Bank Account or Credit/Debit Card Number* (Número de cuenta bancaria o tarjeta de crédito/débito)
- *Driver's License Number or State Card ID* (Número de licencia de conducir o identificación estatal)
- *Social Security Number* (número de seguro social)
- *User Account Password* (contraseña de cuenta de usuario)
- *Other* (otro)
  - Si el usuario selecciona la opción "*Other*", detalla el tipo de dato comprometido en el campo correspondiente.



8.1.3.3.4.2 *Loss or theft of device or media*

Pérdida o robo un dispositivo o medio de almacenamiento que contiene información importante.

8.1.3.3.4.3 *Malicious Code* (*Ransomware/Malware/Virus/Worms*)
Presencia de software malicioso que compromete la seguridad del sistema.

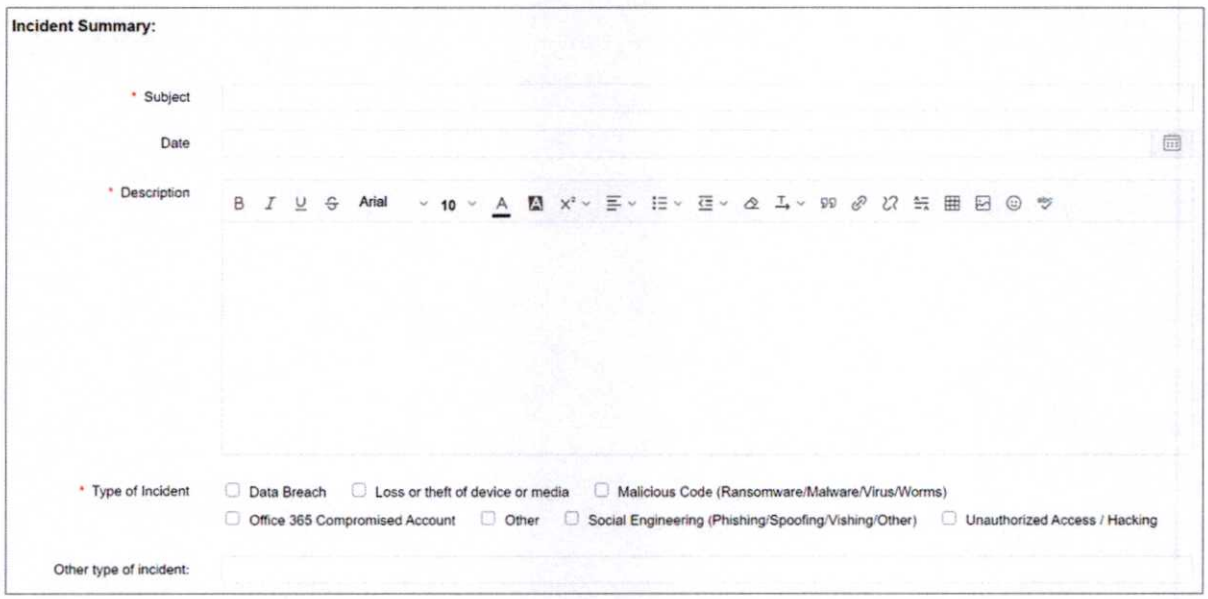
8.1.3.3.4.4 *Office 365 Compromised Account*
Cuenta de Office 365 comprometida, pudiendo resultar en el acceso no autorizado a los datos de la cuenta afectada.
Si el incidente involucró una cuenta de Office 365 comprometida, el usuario revisa la lista de verificación de recuperación de cuenta proporcionada y marca las casillas correspondientes a los pasos ya completados. Para obtener instrucciones detalladas, el usuario consulta el documento titulado "Proceso de Respuesta a Incidentes: Cuentas Comprometidas Office 365"

Office 365 Recover Account Checklist	
	☐ 1. Change Password
	☐ 2. Revoke Access Token
	☐ 3. Remove suspicious Forwading addresses
	☐ 4. Disable any suspicious Inbox Rules
	☐ 5. Verify delegated permissions in users mailbox (Send As, On Behalf)
	☐ 6. Verify mailbox folders permissions
	☐ 7. Verify additional PRITS recommendations section.

8.1.3.3.4.1 *Other*
El incidente no encaja en ninguna de las categorías disponibles y el usuario proporciona una descripción detallada en el campo correspondiente, junto a "*Other type of incident*".

8.1.3.3.4.2 *Social Engineering (Phishing/Spoofing/Vishing/Other)*
Uso de tácticas de manipulación psicológica para obtener información o acceso, por ejemplo, *phishing* o *spoofing*.

8.1.3.3.4.3 *Unauthorized Access/Hacking*
Acceso no autorizado a sistemas, datos o redes.



8.1.3.4 Información adicional
En la sección "*Additional Information*", el usuario proporciona detalles específicos del incidente que no se han detallado en secciones anteriores, incluyendo, si corresponde:

8.1.3.4.1 *Systems / Applications Affected*
Nombres de los sistemas y/o aplicaciones que han sido comprometidos o impactados por el incidente. Esto incluye cualquier *software* crítico para las operaciones que haya sido afectado.

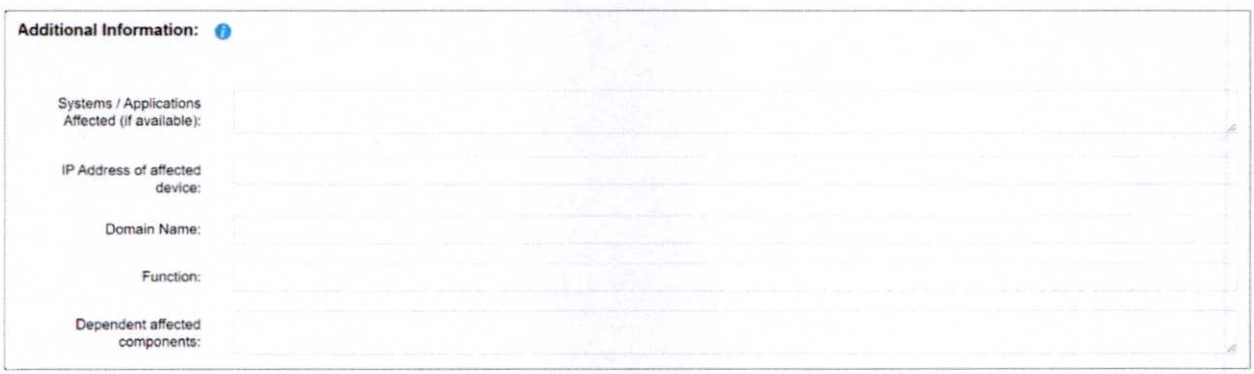
8.1.3.4.2 *IP Address of affected device*

Direcciones IP de los dispositivos que han sido vulnerados o comprometidos durante el incidente.

8.1.3.4.3 *Domain Name*
Nombre del dominio afectado.

8.1.3.4.4 *Function*
Rol o función de los sistemas o dispositivos comprometidos dentro de la red o infraestructura de la organización, por ejemplo, servidores de bases de datos, dispositivos de almacenamiento, sistemas de autenticación, etc.

8.1.3.4.5 *Dependent affected components*
Sistemas, aplicaciones o dispositivos que están vinculados o interconectados con los sistemas comprometidos y que, debido a esa dependencia, también podrían verse impactados de manera directa o indirecta.



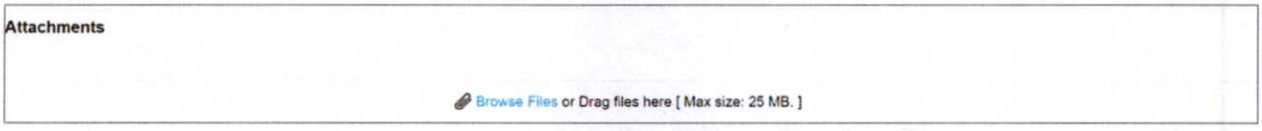
8.1.3.5 Adjuntar archivos
Para adjuntar archivos o capturas de pantalla al reporte, el usuario utiliza la sección "*Attachments*". Se ofrecen dos opciones:

8.1.3.5.1 *Browse Files*
8.1.3.5.1.1 El usuario selecciona "*Browse Files*".
8.1.3.5.1.2 Se abre un explorador de archivos.
8.1.3.5.1.3 El usuario buscar y selecciona el archivo deseado.

8.1.3.5.1.4 El usuario presiona el botón "*Open*" para iniciar la carga.

8.1.3.5.2 *Drag files*

8.1.3.5.2.1 El usuario arrastra y suelta los archivos directamente en el área designada



("*Drag files here*").

Al finalizar la carga exitosa, el nombre del archivo se mostrará en la lista de archivos adjuntos. El usuario debe considerar que el tamaño máximo permitido para cada archivo es de 25 MB.

8.1.3.6 Revisión a final y envío

8.1.3.6.1 El usuario realiza una revisión exhaustiva de toda la información ingresada y verifica que todos los datos sean correctos y completos.

8.1.3.6.2 El usuario hace clic en "*Add request*" para enviar el informe.

8.1.3.6.3 El usuario recibirá un correo electrónico de confirmación que incluye un número de boleto, el cual sirve como referencia para futuras consultas o actualizaciones.

8.2 Notificación alterna por correo electrónico

El usuario que no tiene acceso al PRITS Service Desk, podrá informar el incidente de seguridad de la información enviando un correo electrónico a support@prits.pr.gov. Este correo electrónico deberá incluir toda la información requerida en el formulario del Service Desk, según se detalla en este documento, incluyendo, el estatus y resumen del incidente, los datos de contacto, información adicional relevante y cualquier archivo que pueda ayudar a evaluar la situación.

8.3 Actualización de información de un incidente

En caso de descubrir nueva información relacionada con un incidente previamente reportado, el usuario notificará inmediatamente a la Oficina para la Evaluación de Incidentes Cibernéticos enviando un correo electrónico a support@prits.pr.gov. Este correo electrónico debe incluir el número de boleto original y toda la información adicional relevante, como detalles técnicos actualizados, el impacto del incidente y cualquier otra novedad que pueda ayudar a resolver el caso de manera más efectiva.

9. Documentación

No aplica.

Este espacio se ha dejado intencionalmente en blanco.

10. Purpose

This Standard Operating Procedure (SOP) aims to establish processes for quick and effective reporting of cybersecurity incidents that may compromise the government's information or information systems. To facilitate the notification and documentation of any event that results in a violation of laws, procedures, or security policies, as well as those that pose a threat or risk, PRITS has developed a specific section in the PRITS Service Desk tool where users can submit their reports; alternatively, they can send reports by email. This process enables rapid communication of incidents, the collection of relevant data for subsequent analysis, the tracking of ongoing activities, the identification of involved parties, and the development of action plans.

11. Scope

The guidelines outlined in this SOP apply to computer and information technology employees of the Government of Puerto Rico Executive Branch, including any department, board, dependency, commission, bureau, office, agency, administration or organism, political subdivision, public corporations, and municipalities. It also applies to any natural or legal person who does business or has contracts with the Government of Puerto Rico, including, but not limited to, private persons performing public functions and services, but only with respect to the public functions and services performed; to any exercise of public or private administration in which public funds or resources have been dedicated or invested, either directly or indirectly, or over which the authority of any public servant has been exercised, concerning to the data generated as a result of such activities.

12. Roles and Responsibilities

As established by Law No. 40 of 2024, known as the "Commonwealth of Puerto Rico Cybersecurity Act," all government agencies are required to report any suspected cybersecurity incident to the Cyber Incident Evaluation Office (OEIC), attached to PRITS. This coordination between the affected agency and the OEIC will allow for incident management, immediate measures to isolate it, mitigation of its impact, collaboration with involved local and federal agencies, resolution of the incident, and documentation of the process.

Role	Responsibilities
Agency Employees	All government agency employees, regardless of their role or rank, must immediately report any suspected cybersecurity incident to their agency's IT office or equivalent.
Agency IT Office, or its equivalent	Report to the OEIC any event that could threaten the information security of its agency.
Agency contracted service providers	Contracted service providers that provide information and communications technology services must notify both PRITS and the contracting agency within a maximum period of forty-eight (48) hours from the detection of an incident or threat that compromises data, software, firmware, confidential government services, or information of any natural or legal person. This reporting responsibility extends to all providers that use or access any information technology resource belonging to a government agency, manage information technology systems (whether automated or manual) under the administration of an agency, operate these systems on behalf of an agency, or handle private information systems that contain government data.
Agencies	Each agency shall establish clear and efficient processes for the notification of cybersecurity incidents to its IT office or its equivalent by both employees and contracted service providers. Agencies shall ensure proper communication and training so that all parties are aware of their roles and responsibilities.

14. Abbreviations, Acronyms, Definitions, and Meanings

Abbreviation / Acronym	Meaning
CIO	Chief Information Officer
CISO	Chief Information Security Officer of the Government
IP	Internet protocol
IT	Information technology
OEIC	Office for the Evaluation of Cyber Incidents (*Oficina para la Evaluación de Incidentes Cibernéticos*)
PHI	Protected health information
PII	Personally Identifiable Information

Abbreviation / Acronym	Meaning
PRITS	Puerto Rico Innovation and Technology Service
SOP	Standard operating procedure

Term	Definition
Access	The ability or means necessary to read, write, modify, or communicate data/information or use any system resource.
Agency or government organism	Includes all entities and agencies that comprise the Executive Branch of the Government of Puerto Rico and its municipalities. This includes, but is not limited to, any department, board, dependency, commission, bureau, office, agency, administration, organism, political subdivision, and public corporations. It also encompasses the set of functions, positions, and posts that constitute the entire jurisdiction of an appointing authority of these agencies, regardless of how it is denominated.
Chief Information Officer (CIO)	Individual responsible for managing and overseeing a government agency's technology infrastructure and operations.
Chief Information Security Officer (CISO)	Leader in charge of establishing appropriate security measures to prevent unauthorized access, disclosure, use, damage, degradation, and destruction of electronic information, its systems, and critical infrastructure. Will also be responsible for reducing the risk, impact, and cost of cyberattacks by establishing a framework with minimum information technology (IT) security requirements, defining roles and responsibilities, and setting the standards to protect information.
Computer security or information security	Set of controls, safeguards, and other measures an organization takes to protect information in any format. This involves protecting computing assets, including information, regardless of whether the information assets are interconnected.
Confidential data	Information that, if disclosed, could cause significant harm to the organization. This level includes personal data, financial records, and other sensitive documents.
Confidentiality	Preserve restrictions on access and disclosure, including means to protect privacy and confidential information.
Contracted service provider	Entity, whether a natural or legal person, public or private, that provides services such as networks, applications, programs,

Term	Definition
	infrastructure, or security means through continuous and regular support, as well as active management services either at the facilities of an Agency, at the Agency's data processing center (hosting), or at a third-party data processing center.
Critical Infrastructure	Essential services, systems, resources, and assets, whether physical or virtual, whose incapacity or destruction would have detrimental impacts on cybersecurity, health, the economy, the security of Puerto Rico, or any combination of these matters.
Cyberattack	The use of unauthorized or malicious code in an information system or another digital mechanism, such as a denial-of-service attack, with the intent to disrupt or affect its operations or compromise the confidentiality, availability, or integrity of digital information stored, processed, or in transit by an information system.
Cybersecurity	Prevention of damage, protection, and restoration of computers, systems, and/or electronic communications services, including the information contained therein, to guarantee their availability, integrity, authenticity, confidentiality, and non-repudiation.
Data	Any sequence of one or more symbols that are given meaning by specific acts of interpretation.
Data breach	Loss of control, compromise, disclosure, and/or unauthorized acquisition, or any similar event in which: an unauthorized person accesses or potentially could access Personally Identifiable Information (PII) or Protected Health Information (PHI), or an authorized user accesses PII or PHI for purposes other than those authorized.
Gobierno	Is the Commonwealth of Puerto Rico.
Impact	The magnitude of the harm that can be expected as a result of the consequences of unauthorized disclosure, modification, or destruction of information, loss of information, or unavailability of the information system.
Incident management	All administrative, physical, and technical procedures applied for investigating and mitigating the suspected or reported incident, including notifications of violations or breaches to the parties or individuals impacted by the incident, as applicable under federal and local regulations.

Term	Definition
Incident or Information Security Incident	An event that (i) poses an actual or imminent risk, without authorization, to the integrity, confidentiality, or availability of information, system, or process, or an information resource; or (ii) represents a misuse of an information resource or an actual or imminent threat of a violation of law, security policies, security procedures, acceptable use policies, or standard computer security practices. For purposes of this SOP, the terms 'incident', 'cyber incident', 'information security incident', and shall be used interchangeably.
Information resource	Information and related resources, such as personnel, equipment, software, information technology, and more.
Information system	A discrete set of information resources for the collection, processing, maintenance, use, exchange, dissemination, or disposition of information.
Information Technology (IT)	For an agency, means any interconnected system, or resource, or subsystem of equipment used in the acquisition, storage, analysis, evaluation, manipulation, handling, movement, control, display, switching, exchange, destruction, transmission, or automatic reception of data or information, if the equipment is used by the agency directly or by a third party under a contract with the agency that requires the use (i) of that equipment; or (ii) of such equipment to a significant extent for the provision of a service or the supply of a product. It includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by a computer's central processing unit, software, firmware, and similar procedures and services (including support services), and related resources.
Least Privilege Principle	Each module (process, user, or program, depending on the context) should only have access to the information and resources necessary to fulfill its legitimate purpose.
Loss or theft of device or media	Occurs when an employee, contractor, or other authorized person loses possession, through misplacement or misappropriation by someone, of a government-owned IT equipment, device, or media that can be used to access confidential data, the government network, accounts, or poses a threat to information security.

Term	Definition
Malicious code	(Ransomware/malware/virus/worms) Arbitrary group of letters, numbers, or symbols organized as a set of instructions for a computer that seeks to compromise or damage the confidentiality, integrity, or availability of computers, information systems, or communications, networks, physical or virtual infrastructure controlled by computers or information systems, or the information that resides therein.
Municipality(-ies)	Any of the 78 municipalities of Puerto Rico. For purposes of this SOP, the terms Municipality(-ies) and Agency(-ies) will be used interchangeably.
Office 365 compromised account	Occurs when someone steals or has unauthorized access to Office 365 credentials (for example, name, password, or PIN).
Password	A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify authorization to access protected systems and resources.
Phishing	Social engineering technique where attackers use electronic communication, such as emails, text messages, or fake websites, to deceive individuals and obtain confidential information, like passwords, financial data, or personal information.
PRITS	Puerto Rico Innovation and Technology Service, Executive Branch Office in charge of implementing, developing, and coordinating the Government's public policy on innovation, information, and technology, as provided by Act 75 of 2019.
Ransomware	(i) Means a cyberattack, which includes a threat to use unauthorized or malicious code on an information resource or a threat to use another digital mechanism, such as a denial-of-service attack, to interrupt or affect the operations of an Information resource or compromise the confidentiality, availability, or integrity of digital information stored in, processed by, or that transits through an information resource, in order to demand a ransom payment; and (ii) does not include an event in which payment is required by a Federal Government entity, a bona fide security investigation, a legitimate payment for incident response services, or as a response to an invitation made by the owner or operator of the information system to third parties to identify vulnerabilities in the information system.

Term	Definition
Restricted data	Highly sensitive information whose disclosure could cause severe damage to the organization or individuals. Includes trade secrets, research and development information, and highly sensitive customer data.
Social engineering	(Phishing/spoofing/vishing) Act or attempt to deceive a person into revealing confidential information (e.g., password) or to perform certain actions that can be used to gain unauthorized access, commit fraud, attack systems or networks, download and execute files that appear to be benign but are actually malicious, among others.
Spoofing	A technique where attackers impersonate a trusted person or device to gain unauthorized access to systems or networks, or to manipulate victims into revealing confidential information.
Unauthorized access	Occurs when a person, group, code, program, application, or any other computing entity or process obtains logical, digital, or physical access without approval or consent to a critical infrastructure network, system, data, application, data room, or other government information technology resource; or when access is obtained or attempted to be obtained to information or resources that are not necessary to perform their job or function, following the Principle of Least Privilege.

13. Training

Agencies will implement a cybersecurity training and education program for all employees and contracted service providers. The goal is to familiarize everyone with their roles, responsibilities, and procedures for reporting security incidents or potential security threats. Contracted service providers will receive initial onboarding within the first 30 days of their employment, and all employees and providers will undergo regular training at least annually or as needed.

14. References

Identification Number	Title	Version
PRITS-POL-0001	Data Classification Policy of the Government of Puerto Rico	1.0
PRITS-POL-002	Information Security Incident Response Policy	1.0
N/A	Proceso de Respuesta a Incidentes: Cuentas Comprometidas Office 365	1.0
Law No. 40-2024	Commonwealth of Puerto Rico Cybersecurity Act	N/A

15. Important

This Standard Operating Procedure (SOP) replaces any circular letter, memorandum, administrative order, written communication, or previous instruction that is inconsistent with the guidelines outlined in this document.

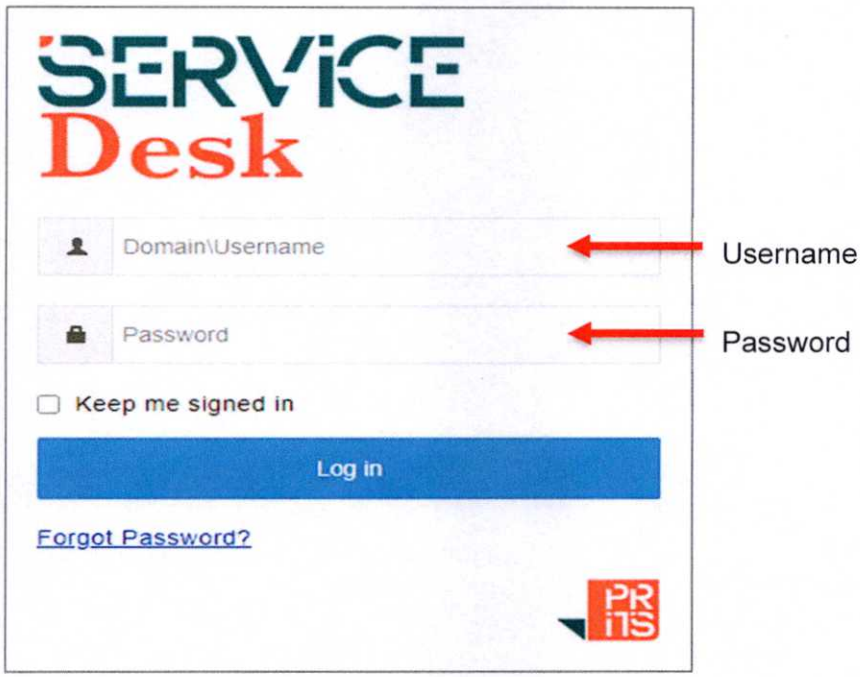
16. Procedure

16.1 Reporting Information Security Incidents through the PRITS Service Desk

16.1.1 Log in

16.1.1.1 The user accesses the webpage https://support.prits.pr.gov/.
16.1.1.2 Enters the username and password in the corresponding fields.
16.1.1.3 The user selects the "Log in" option to access their account.
16.1.1.4 If the user has forgotten their password, they select the "Forgot password?" option.

This space has been intentionally left blank.

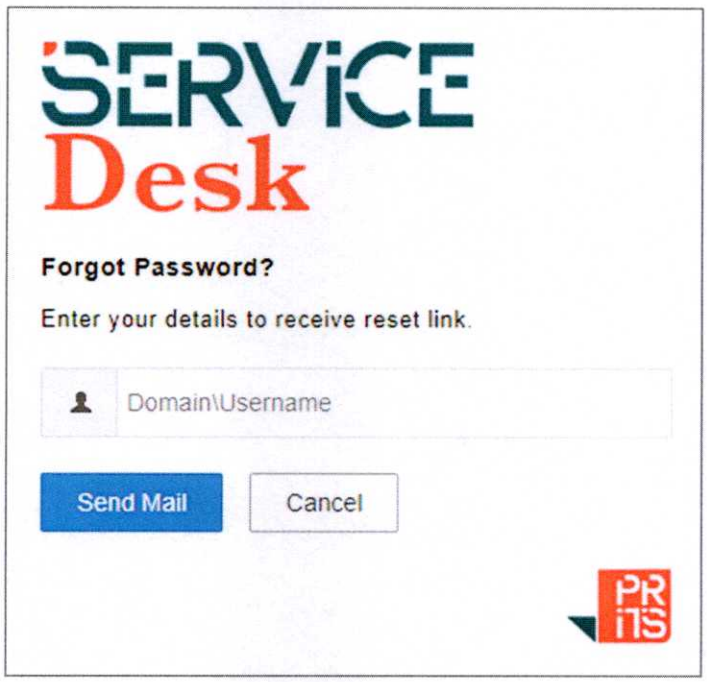


16.1.1.4.1 The user enters their username in the designated field and selects "Send mail."

16.1.1.4.2 The system will send an email with a password reset link to the associated email address.

16.1.1.4.3 To cancel the process and return to the login screen, the user selects "Cancel."

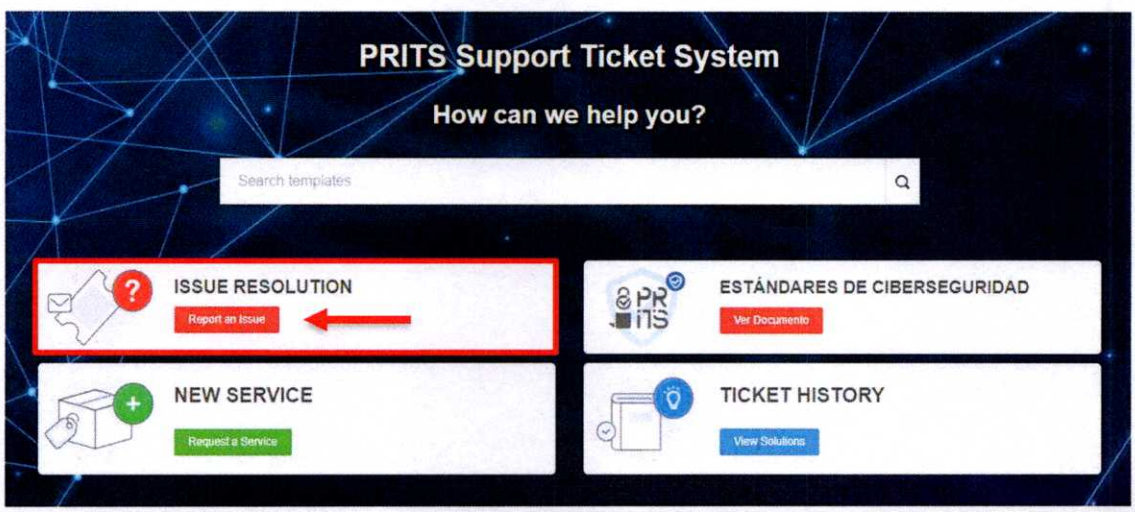
This space has been intentionally left blank.



16.1.2 Reporting an Information Security Incident in the PRITS Support Ticket System

16.1.2.1 After logging in, the user locates the "Issue Resolution" section.

16.1.2.2 Selects the option "Report an Issue."



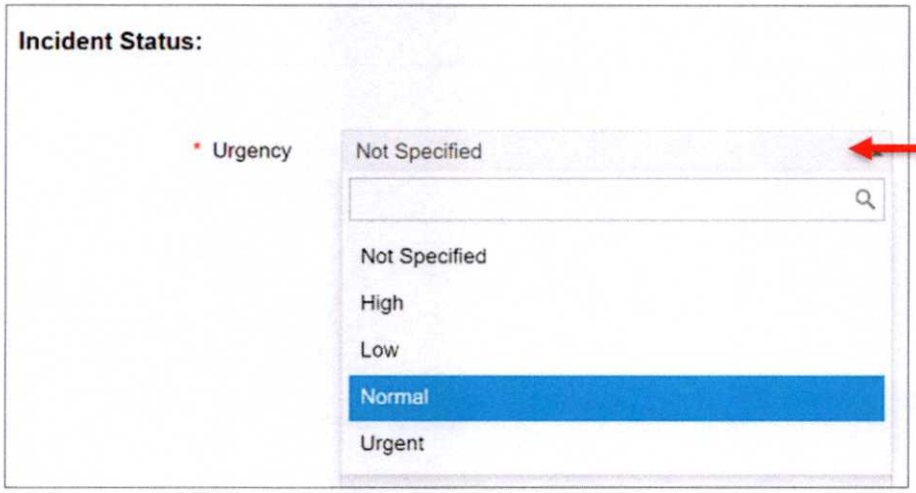
16.1.2.3 Access the incident catalog screen.
16.1.2.4 Within the catalog, the user selects "Cybersecurity Incident Report" and completes the form with the required information for the initial incident assessment.

16.1.3 Complete the form

16.1.3.1 Incident Status
16.1.3.1.1 In the "Incident Status" section, the user selects the urgency level (urgent, high, normal, low) that best reflects the severity of the incident based on the following criteria:

Urgency Levels	Description
Urgent	The incident is causing the degradation of vital services for a large number of users, constitutes a serious violation of network security or data, affects mission-critical equipment or services, or damages the public's trust in the agency.
High	The incident is causing a significant degradation of services for a specific group of users, represents a serious security breach or loss of sensitive data, affects important but non-critical systems, or has the potential to quickly escalate to an urgent level if not addressed immediately.

Urgency Levels	Description
Normal	The incident has minor effects on a small group of users, does not cause service interruption, and does not threaten data or network security.
Low	The incident has little to no impact or affects only a few users.



16.1.3.2 Contact Information
In the "Contact Information" section, the user completes the following fields:

16.1.3.2.1 *Agency Info Sec Contact*
Full name of the individual designated as the agency's point of contact.

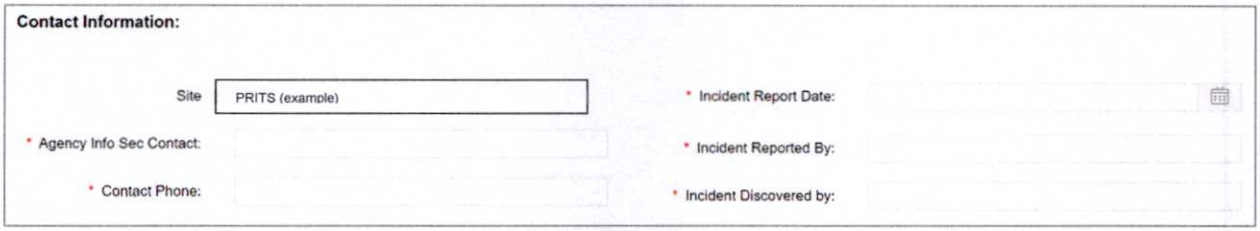
16.1.3.2.2 *Contact phone*
Phone number of the contact person.

16.1.3.2.3 *Incident Report Date*
Select the date of the formal report using the calendar icon.

16.1.3.2.4 *Incident Reported By*
Full name of the person reporting the incident. This person may or may not be the same person who initially detected the incident.

16.1.3.2.5 *Incident Discovered By*

Name of the person who initially detected the incident. This person is the first to detect any anomaly, failure, or vulnerability in the system or process. This could be a technical team member, an employee, or any other individual who interacts with the affected system or area.



16.1.3.3 Incident Summary

In the "Incident Summary" section, the user includes:

16.1.3.3.1 *Subject*

A descriptive title for the incident.

16.1.3.3.2 *Date*

If known, the exact date and time of the incident. If only an estimate is available, the user records the approximate time closest to when the incident occurred.

16.1.3.3.3 *Description*

A detailed description of the incident is provided, including but not limited to:

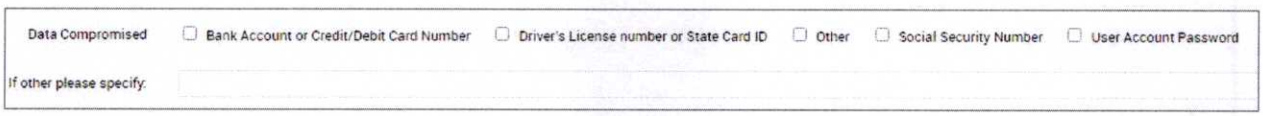
- Initial impact, including the immediate effects of the incident on operations, data, or users.
- Initial actions taken to mitigate the incident.
- Current status of the incident (active, contained, or resolved).

The incident description should be objective and based on verifiable facts. If any relevant information has not yet been confirmed, the user must explicitly indicate the lack of data in the report.

16.1.3.3.4 *Type of Incident*
The category of the incident:

16.1.3.3.4.1 *Data Breach*
Unauthorized exposure of confidential or restricted data.
In the "Compromised Data" section, the user specifies the type of data compromised:

- Bank Account or Credit/Debit Card Number
- Driver's License Number or State Card ID
- Social Security Number
- User Account Password
- Other
  If the user selects "Other," they must detail the type of compromised data in the corresponding field.



16.1.3.3.4.2 *Loss or theft of device or media*
Loss or theft of a device or storage medium containing important information.

16.1.3.3.4.3 *Malicious Code (Ransomware/Malware/Virus/ Worms)*
Presence of malicious software that compromises system security.

16.1.3.3.4.4 Office 365 Compromised Account
Compromised Office 365 account, which may result in unauthorized access to the affected account's data.

If the incident involved a compromised Office 365 account, the user reviews the provided account recovery checklist and checks the boxes corresponding to the steps already completed. For detailed instructions, the user consults the "Incident Response Process: Compromised Office 365 Accounts" document.

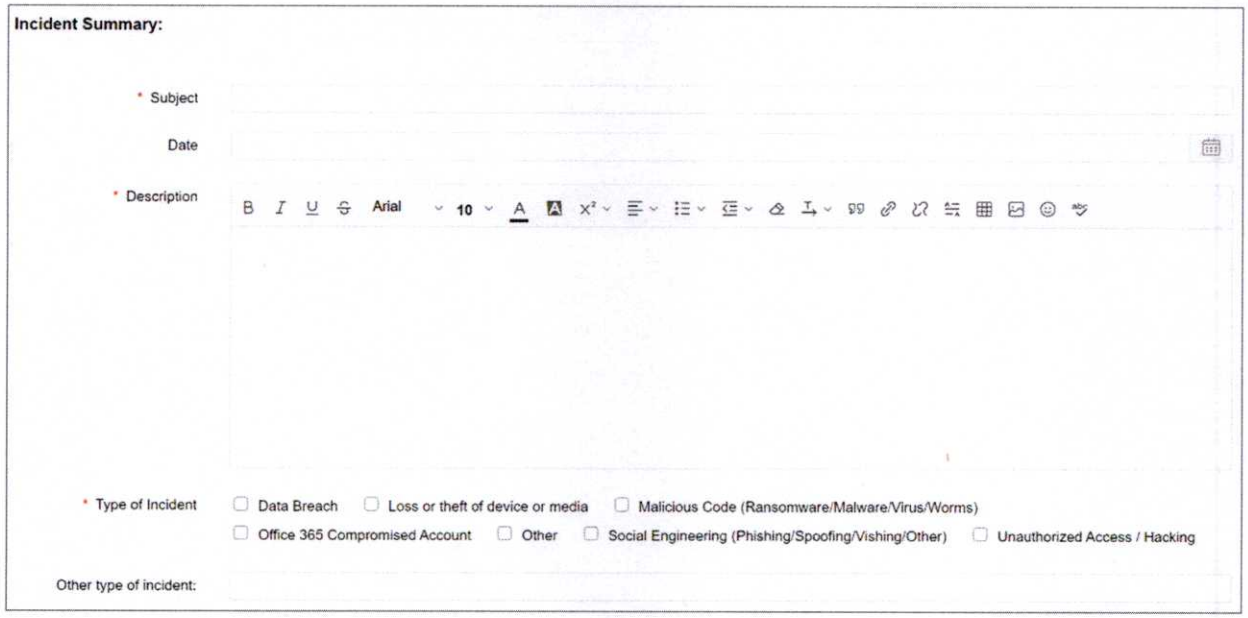
Office 365 Recover Account Checklist	
	☐ 1. Change Password
	☐ 2. Revoke Access Token
	☐ 3. Remove suspicious Forwading addresses
	☐ 4. Disable any suspicious Inbox Rules
	☐ 5. Verify delegated permissions in users mailbox (Send As, On Behalf)
	☐ 6. Verify mailbox folders permissions
	☐ 7. Verify additional PRITS recommendations section

16.1.3.3.4.5 *Other*
If the incident does not fit into any of the previous categories, this option is selected, and a detailed description is provided in the corresponding field next to "Other type of incident."

16.1.3.3.4.6 *Social Engineering (Phishing/Spoofing/Vishing/Other)*
The incident involves the use of psychological manipulation tactics to obtain information or access, such as phishing or spoofing attacks

16.1.3.3.4.7 *Unauthorized Access/Hacking*

An unauthorized third party has gained access to systems, data, or networks.



16.1.3.4 Additional Information

In the "Additional Information" section, the user provides specific details about the incident that have not been detailed in previous sections, including, if applicable:

16.1.3.4.1 *Systems / Applications Affected*

Names of the systems and/or applications that have been compromised or impacted by the incident. This includes any software critical to operations that have been affected.

16.1.3.4.2 *IP Address of affected device*

IP addresses of the devices that have been compromised or vulnerable during the incident.

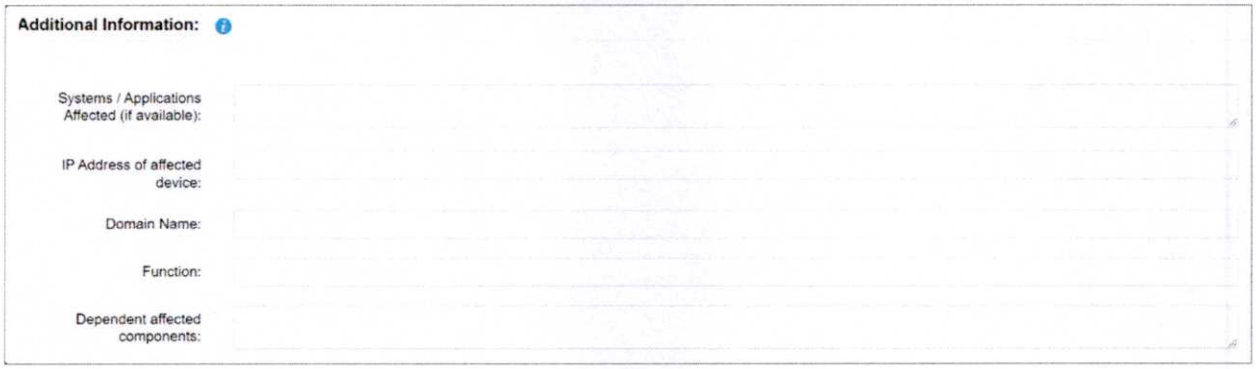
16.1.3.4.3 *Domain Name*

Name of the affected domain.

16.1.3.4.4 *Function*

Role or function of the compromised systems or devices within the organization's network or infrastructure, for example, database servers, storage devices, authentication systems, etc.

16.1.3.4.5 *Dependent affected components*
Systems, applications, or devices that are linked or interconnected with the compromised systems and that, due to this dependency, could also be impacted directly or indirectly.

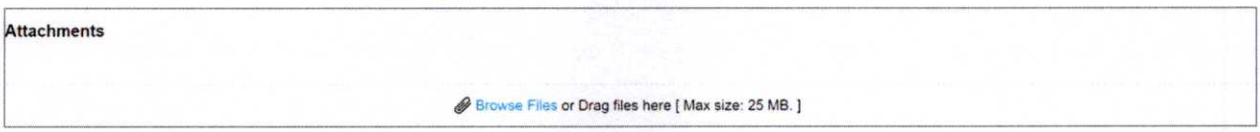


16.1.3.5 Attach Files
To attach files or screenshots to the report, the user uses the "Attachments" section. Two options are offered:

16.1.3.5.1 *Browse Files*
- 16.1.3.5.1.1 The user selects "Browse Files."
- 16.1.3.5.1.2 A file explorer opens.
- 16.1.3.5.1.3 The user searches for and selects the desired file.
- 16.1.3.5.1.4 The user presses the "Open" button to start the upload.

16.1.3.5.2 *Drag files*
- 16.1.3.5.2.1 The user drags and drops the files directly into the designated area ("Drag files here").

The file name will be displayed in the attached file list upon successful upload.

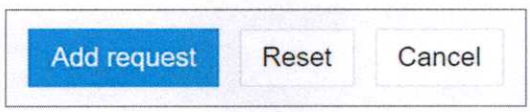


16.1.3.6 Final Review and Submission

16.1.3.6.1 The user thoroughly reviews all entered information and verifies that all data is correct and complete.

16.1.3.6.2 The user clicks "Add request" to submit the report.

16.1.3.6.3 The user will receive a confirmation email that includes a ticket number, which serves as a reference for future inquiries or updates.



16.2 Alternative Email Notification

Users who do not have access to the PRITS Service Desk may report information security incidents by emailing support@prits.pr.gov. This email must include all the information required in the Service Desk form, as detailed in this document, including incident status and summary, contact information, relevant additional information, and any files that may assist in assessing the situation.

16.3 Incident Information Update

If new information regarding a previously reported incident is discovered, the user shall immediately notify the Office for the Evaluation of Cyber Incidents by emailing support@prits.pr.gov. This email must include the original ticket number and all relevant additional information, such as updated technical

details, the impact of the incident, and any other new developments that may assist in resolving the case more effectively.

17. Documentation

Does not apply.

Firmas de aprobación / *Approval Signatures*

Posición /Title	**Acción realizada / *Action Taken***	**Nombre en letra de Molde / *Print Name***	**Firma / *Signature***	**Fecha / *Date***
Principal Oficial de Tecnología / *Chief Technology Officer*	Revisado por / *Revised by*	Roberto Clausell Rivera		13/nov/2024
Principal Ejecutivo de Información e Innovación / *Chief Information and Innovation Officer*	Aprobado por / *Approved by*	Antonio Ramos Guardiola		13/nov/2024

Historial de Revisiones / *Revision History*

Versión / *Version*	**Fecha / *Date***	**Autor / *Author***	**Descripción de cambios / *Change Description***