PUERTO RICO
INNOVATION &
TECHNOLOGY
SERVICE

**PRITS-POL-0002**

# Política de respuesta a incidentes de seguridad de la información

*Information Security Incident Response Policy*

- Aplicación: N/A
  *Application: N/A*

- Sistema
  *System: N/A*

## Tabla de Contenido

## 1. Descripción

La Política de Respuesta a Incidentes de Seguridad de la Información establece un marco integral para el Programa de Respuesta a Incidentes Cibernéticos (PRIC) del Puerto Rico Innovation and Technology Service (PRITS). Esta política define los lineamientos, procedimientos y responsabilidades esenciales para la detección eficaz, respuesta oportuna y recuperación eficiente ante incidentes que puedan comprometer la integridad, confidencialidad o disponibilidad de los activos de información de PRITS y las entidades gubernamentales que sirve.

Fundamentada en las mejores prácticas, incluyendo el Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST, en inglés), esta política enfatiza la importancia de la preparación proactiva, la asignación clara de roles y responsabilidades, y la mejora continua de las capacidades de respuesta a incidentes como pilares fundamentales para mantener un entorno digital seguro y resiliente.

## 2. Base Legal

Esta política se emite al amparo de la Ley Núm. 75-2019, conocida como "Ley de Puerto Rico Innovation and Technology Service (PRITS)" y la Ley Núm. 40-2024, conocida como "Ley de Ciberseguridad del Estado Libre Asociado de Puerto Rico".

La Ley Núm. 75-2019, *supra*, creó al PRITS para establecer y promover la política pública sobre la evaluación, manejo, desarrollo, coordinación e integración interagencial efectiva de la infraestructura tecnológica e informática del Gobierno de Pico. Además, el artículo 6 de la Ley 75-2019, *id.*, otorga a PRITS la responsabilidad de crear e implementar planes estratégicos, políticas, estándares y una arquitectura integrada para las tecnologías de información y telecomunicaciones del Gobierno. Asimismo, establece que PRITS será el promotor de la disciplina en las mejores prácticas en el manejo de proyectos tecnológicos y publicar guías y directrices a esos efectos.

La Ley Núm. 40-2024, *supra*, establece un marco legal para fortalecer la seguridad cibernética en el Gobierno de Puerto Rico, enfocándose en la protección de datos gubernamentales y la infraestructura crítica contra amenazas digitales. La ley establece la política pública, jurisdicción y estándares centrados en mantener la confidencialidad,

integridad y disponibilidad de la información gubernamental, mejorar la seguridad de redes e infraestructuras críticas, así como el fortalecimiento de las capacidades para prevenir y responder a amenazas cibernéticas. Además, promueve la protección de la privacidad de los ciudadanos y el cumplimiento de normativas básicas de ciberseguridad del Gobierno de los Estados Unidos. Finalmente, incluye disposiciones para imponer sanciones a la Rama Ejecutiva del Gobierno, los municipios y sus respectivos proveedores de servicios contratados que incumplan con las normativas correspondientes.

Con esta política reafirmamos el cumplimiento con otros preceptos estatutarios, entre ellos la Ley Núm. 151-2004, según enmendada, conocida como "Ley de Gobierno Electrónico". Esta política se fundamenta en las Leyes 75-2019 y 40-2024, por lo que, cualquier referencia a otras leyes se entenderá como una referencia y no deberá interpretarse como una base legal para la aplicabilidad y jurisdicción de esta normativa.

## 3. Propósito

El propósito de esta política es fortalecer la postura de ciberseguridad de PRITS y del Gobierno de Puerto Rico, estableciendo un enfoque estructurado y eficaz para el manejo de incidentes. Los objetivos específicos de esta política son:

- Establecer expectativas claras y medibles para la creación, mantenimiento, supervisión y mejora continua de las capacidades de respuesta a incidentes.

- Definir y asignar roles, responsabilidades y niveles de autoridad específicos para el manejo de incidentes, garantizando una respuesta coordinada y eficaz ante cualquier incidente de ciberseguridad.

- Proporcionar un marco de referencia alineado con estándares internacionales reconocidos, como el NIST CSF 2.0 y NIST SP.800-61r2, para guiar las prácticas de respuesta a incidentes y facilitar la interoperabilidad con otras entidades gubernamentales y de seguridad.

- Fomentar una cultura de conciencia y preparación en materia de ciberseguridad, promoviendo la detección temprana, la notificación rápida y la respuesta eficaz ante potenciales amenazas.

## 4. Alcance

Las disposiciones de esta política son aplicables a 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[1]. De igual forma aplica a cualquier persona natural o jurídica que haga negocios o tenga contratos con el Gobierno de Puerto Rico, incluyendo, de forma no exhaustiva, a las personas privadas que desempeñan funciones y servicios públicos, pero solamente con respecto a las funciones y servicios públicos desempeñados; a todo ejercicio de administración pública o privada en el que se hubieren dedicado o invertido fondos o recursos públicos ya sea directa o indirectamente, o sobre la cual se hubiere ejercido la autoridad de cualquier servidor público, en cuanto a los datos que se generan como producto de tales actividades.

## 5. Abreviaciones, acrónimos, definiciones y significados

| **Abreviación / Acrónimo** | **Significado** |
|---|---|
| CISO | Principal Oficial de Seguridad Cibernética *(Chief Information Security Officer)* del Gobierno |
| CSIRT | Equipo de Respuesta a Incidentes de Seguridad Informática *(Computer Security Incident Response Team)* |
| DDoS | Denegación de servicio distribuido *(distributed denial of service)* |
| IDS | Sistema de detección de intrusiones *(intrusion detection system)* |
| IIP | Información de identificación personal |
| IoT | Internet de las cosas *(internet of things)* |

[1] Véase, artículo 2 de la Ley 40-2024.

| **Abreviación / Acrónimo** | **Significado** |
|---|---|
| KPI | Indicador clave de desempeño *(key performance indicator)* |
| NIST | Instituto Nacional de Estándares y Tecnología *(National Institute of Standards and Technology)* |
| OEIC | Oficina para la Evaluación de Incidentes Cibernéticos |
| OPI | Oficial Principal de Informática |
| PEII | Principal Ejecutivo de Información e Innovación del Gobierno de Puerto Rico |
| PRIC | Programa de Respuesta a Incidentes Cibernéticos |
| 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. |
| 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, 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. |

| Término | Definición |
|---|---|
| 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. |
| 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. |
| Datos | Cualquier secuencia de uno o más símbolos a los que se les da significado mediante actos específicos de interpretación. |
| Denegación de servicio distribuido | Técnica de denegación de servicio que utiliza numerosos *hosts* para realizar el ataque. |
| 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. |
| HIPAA | Ley de Portabilidad y Responsabilidad del Seguro Médico de 1996; una ley federal que requirió al Departamento de Salud y Servicios Humanos federal establecer estándares regulatorios para proteger la privacidad y seguridad de la información de salud identificable individualmente. |
| 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. |

| Término | Definición |
|---|---|
| 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 esta Política, los términos 'incidente', 'incidente de seguridad de la información' se utilizarán indistintamente. |
| Información de identificación personal (IIP) | Es cualquier representación de información que es legible sin la necesidad de una clave criptográfica especial para acceder a ella o facilita el rastreo de la identidad de un individuo, incluyendo el nombre o la primera inicial y apellido paterno de un individuo combinado con otra información que está vinculada o que se debe vincular a un individuo específico, como:<br>- Número de Seguro Social<br>- Número de licencia de conducir, tarjeta electoral u otra identificación oficial<br>- Números de cuentas bancarias o financieras de cualquier tipo, con o sin claves de acceso que puedan habérsele asignado<br>- Nombres de usuario y claves de acceso a sistemas informáticos públicos o privados<br>- Información médica protegida por la Ley HIPAA<br>- Información contributiva<br>- Evaluaciones laborales |
| 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. |
| Municipio(s) | Cualquiera de los 78 municipios de Puerto Rico. Para propósitos de esta política se utilizarán los términos municipio(s) y agencia(s) indistintamente. |

| Término | Definición |
|---|---|
| Oficial Principal de Informática (OPI) | Individuo responsable de la gestión y supervisión de la infraestructura y operaciones tecnológicas de una agencia gubernamental. |
| 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. |
| 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<br>(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. |

| Término | Definición |
|---|---|
| Recurso de información | Información y los recursos relacionados, como, por ejemplo, personal, equipos, programas y tecnología de la información, entre otros. |
| Riesgo | Toda circunstancia o hecho razonablemente identificable que tenga un posible efecto adverso en la seguridad de las redes y recursos de información. |
| 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. |
| *Software* | Programas informáticos y datos asociados que pueden escribirse o modificarse dinámicamente durante su ejecución. |
| Tecnología de la información (TI) | 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.<br>Incluye computadoras, equipos auxiliares (incluidos periféricos de imágenes, dispositivos de entrada, salida y almacenamiento necesarios para la seguridad y vigilancia), equipos periféricos diseñados para ser controlados por la unidad central de procesamiento de una computadora, *software*, *firmware* y procedimientos y servicios similares (incluyendo servicios de apoyo) y recursos relacionados. |

# 6. Política

## 6.1 Programa de Respuesta a Incidentes Cibernéticos (PRIC)

PRITS desarrollará, implementará y mantendrá un Programa de Respuesta a Incidentes Cibernéticos (PRIC), adscrito a la Oficina para la Evaluación de Incidentes Cibernéticos (OEIC). Este programa se alineará con las responsabilidades legales de la OEIC y tendrá como objetivos principales:

- Gestionar los riesgos de seguridad de la información asociados a incidentes.
- Detectar, responder y mitigar las consecuencias de ciberataques y otras amenazas contra los sistemas de información y los datos gubernamentales.
- Establecer directrices para el intercambio y la comunicación de información relacionada con incidentes.
- Conservar todos los artefactos necesarios resultantes de incidentes y procedimientos de respuesta para análisis posteriores y mejora continua.
- Informar y capacitar a las partes interesadas sobre sus roles y responsabilidades en el proceso de respuesta a incidentes.
- Comunicar, gobernar, operar y mejorar las actividades relacionadas con la respuesta a incidentes.

### 6.1.1 Métricas de desempeño

Para evaluar la eficacia del PRIC y garantizar la mejora continua, se establecerá un sistema de medición basado en indicadores clave de desempeño (KPIs). Estos KPIs permitirán monitorear el desempeño del programa, identificar áreas de mejora y tomar decisiones basadas en datos.

#### 6.1.1.1 Recopilación y almacenamiento de datos

Se recopilarán y almacenarán datos de manera centralizada y accesible, lo que permitirá realizar análisis detallados y generar informes personalizados. La información recopilada incluirá, como mínimo:

6.1.1.1.1 Número y tipo de incidentes
Se contabilizarán todos los incidentes reportados, clasificándolos por tipo (por ejemplo, *phishing*, *malware*, denegación de servicio) para identificar tendencias y patrones.

6.1.1.1.2 Tiempo de detección y resolución
Se medirá el tiempo transcurrido desde la detección inicial del incidente hasta su resolución completa, incluyendo todas las fases del ciclo de vida del mismo.

6.1.1.1.3 Impacto del incidente
Se evaluará el impacto del incidente en términos de pérdida de datos, interrupción de servicios, costos financieros y reputación.

6.1.1.1.4 Causa raíz
Se identificará la causa raíz de cada incidente para implementar medidas correctivas y preventivas.

6.1.1.1.5 Acciones correctivas
Se documentarán las acciones tomadas para resolver el incidente y prevenir su recurrencia.

6.1.1.1.6 Lecciones aprendidas
Se capturarán las lecciones aprendidas de cada incidente para mejorar los procesos y procedimientos de seguridad.

Para cada uno de los requisitos mencionados, se presentarán métricas específicas que permitirán evaluar el cumplimiento y

la efectividad del programa. A continuación, se detallan las métricas propuestas.

| Elemento | Indicador Clave de Desempeño (KPI) | Métrica |
|---|---|---|
| Número de incidentes | Tasa de incidentes por tipo | Número de incidentes por tipo de amenaza dividido por el número total de incidentes. |
| Tiempo para resolver el incidente | Tiempo medio de resolución | Promedio de tiempo en resolver un incidente, desglosado por tipo de incidente. |
| | Tiempo de detección | Tiempo promedio entre la ocurrencia del incidente y su detección. |
| Evaluaciones objetivas de incidentes | Porcentaje de incidentes evaluados | Porcentaje de incidentes que han sido evaluados y clasificados según su gravedad e impacto. |
| | Tasa de cumplimiento de las medidas correctivas | Porcentaje de acciones correctivas implementadas después de cada incidente. |
| Informes de incidentes | Cumplimiento de los informes de incidentes | Porcentaje de incidentes con informes completos que incluyen toda la información relevante. |
| | Tiempo para generar informes | Tiempo promedio para generar un informe de incidente después de su resolución. |
| Lecciones aprendidas | Número de lecciones aprendidas implementadas | Número de mejoras implementadas como resultado de las lecciones aprendidas. |

| Elemento | Indicador Clave de Desempeño (KPI) | Métrica |
|---|---|---|
| | Tasa de recurrencia de incidentes | Porcentaje de incidentes que se repiten después de haber sido mitigados |

6.1.1.2 Análisis y mejora continua
Los datos recopilados se analizarán de forma regular para identificar tendencias, patrones y áreas de mejora. Los resultados de estos análisis se utilizarán para ajustar el PRIC, mejorar los procesos de seguridad y tomar decisiones informadas.

6.1.1.3 Comunicación y transparencia
Se establecerán mecanismos de comunicación claros y transparentes para informar a las partes interesadas sobre el desempeño del programa, los incidentes ocurridos y las acciones tomadas.

6.2 Equipo de Respuesta a Incidentes de Seguridad Informática

El Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT-PRITS) será un componente fundamental para garantizar una respuesta eficaz y coordinada ante incidentes. Bajo el marco del PRIC, el CSIRT-PRITS se conformará por una estructura multidisciplinaria que combinará la experiencia interna y externa para abordar las diversas facetas de un incidente.

6.2.1 Composición

El CSIRT-PRITS estará estratégicamente compuesto por:

6.2.1.1 Oficina para la Evaluación de Incidentes Cibernéticos (OEIC)
Liderará y coordinará los esfuerzos de respuesta a incidentes, proporcionando directrices, recursos y experiencia técnica durante todo el proceso. Actuará como punto central de comando en situaciones de crisis cibernética.

6.2.1.2 Personal técnico de la agencia afectada
Se incorporará al CSIRT-PRITS cuando ocurra un incidente en su agencia. Aportará conocimiento de los recursos y sistemas específicos de la agencia, facilitará el acceso a sistemas afectados y proporcionará apoyo técnico y la información contextual necesaria.

6.2.1.3 Proveedores de servicios contratados de la agencia
Si la agencia cuenta con proveedores de servicios contratados que gestionan o tienen conocimientos especializados sobre sus sistemas, también podrán ser integrados al CSIRT-PRITS. Al igual que el personal técnico de la agencia, su rol es asistir y facilitar la respuesta.

6.2.1.4 Miembros adicionales
El Principal Oficial de Seguridad Cibernética (CISO) tendrá la autoridad para nombrar a miembros adicionales al CSIRT-PRITS según considere necesario para garantizar una respuesta efectiva. Estos miembros podrán ser expertos en áreas específicas como análisis forense digital, inteligencia de amenazas o comunicaciones de crisis.

6.2.2 Autoridad

El CSIRT-PRITS contará con la autoridad para:

6.2.2.1 Monitorear y dirigir todas las acciones realizadas durante un incidente.
6.2.2.2 Implementar los procedimientos y estrategias establecidos en el plan de respuesta a incidentes.
6.2.2.3 Autorizar modificaciones a los sistemas de información cuando sea necesario para contener o mitigar un incidente.
6.2.2.4 Tomar medidas como la confiscación o desconexión de equipos con el fin de preservar la evidencia y evitar la propagación del incidente.

6.2.2.5 Acceder a los recursos pertinentes y recopilar información relevante durante las investigaciones, incluyendo comunicaciones y registros de usuarios.

6.2.2.6 Compartir información sobre amenazas e incidentes con otras organizaciones, como, por ejemplo, agencias federales para fortalecer la colaboración y la prevención.

6.3 Gestión y respuesta a incidentes cibernéticos

6.3.1 Obligación de informar

6.3.1.1 Todos los empleados de las agencias gubernamentales, sin importar su puesto o nivel jerárquico, tienen la responsabilidad ineludible de reportar inmediatamente cualquier sospecha de incidente de seguridad a la Oficina de Informática, o su equivalente, dentro de su agencia. Esta oficina, a su vez, deberá notificar al CSIRT-PRITS.

6.3.1.2 Los proveedores de servicios contratados que brindan servicios de tecnología de la información y comunicaciones tienen un conjunto de obligaciones específicas en cuanto al informe de incidentes. Estos proveedores deben compartir información y notificar tanto a PRITS, enviando un correo electrónico a soc@prits.pr.gov, como a la agencia contratante dentro de un plazo no mayor a cuarenta y ocho (48) horas desde que detecten un incidente de seguridad o una posible amenaza que pueda comprometer datos, productos de *software*, *firmware*, o servicios confidenciales del gobierno, así como la información de cualquier persona natural o jurídica.
Adicionalmente, esta obligación de reporte también se extiende a aquellos 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.
- Manejen sistemas de información privados que contengan datos gubernamentales.

6.3.1.3 Todo proveedor de servicios de ciberseguridad contratado deberá presentar al PRITS un informe mensual detallado sobre el estado de seguridad de los sistemas y activos que administra en nombre de la agencia. Estos informes deberán incluir, como mínimo:

6.3.1.3.1 Las amenazas detectadas, los actores de amenazas y las vulnerabilidades.

6.3.1.3.2 Las acciones de respuesta y remediación inmediata.

6.3.1.3.3 El número total de incidentes de seguridad de la información que se informaron al PRITS a través de los canales establecidos.

6.3.1.3.4 El avalúo realizado sobre el estado de la ciberseguridad.

6.3.2 Alcance de los incidentes

Los incidentes reportables incluyen, pero no se limitan a:

- Accesos no autorizados o intentos de acceso a sistemas o datos.
- Pérdida o robo de dispositivos que contienen información sensible.
- Modificación no autorizada de datos o sistemas.
- Ataques de denegación de servicio (DoS) o intentos de los mismos.
- Infección por *malware* o *ransomware*.
- Filtración de datos sensibles o confidenciales.
- Uso indebido de recursos de TI de la agencia.
- Violaciones de las políticas de seguridad de la información.

6.3.3 Proceso de informar

6.3.3.1 El empleado o proveedores de servicios contratados que detecte o sospeche un incidente de seguridad debe reportarlo al CSIRT-PRITS a través de los canales establecidos (Procedimiento para informar incidentes de seguridad de la información; PRITS-SOP-0007-OPE).

6.3.3.2 El informe debe incluir toda la información relevante disponible, como la naturaleza del incidente, sistemas afectados, y cualquier acción inmediata tomada.

6.3.3.3 El CSIRT-PRITS acusará recibo del informe y podrá solicitar información adicional si es necesario.

6.3.4 Clasificación de incidentes

Una vez reportado un incidente de ciberseguridad, el Principal Oficial de Seguridad Cibernética del Gobierno de Puerto Rico (CISO), o la persona designada por éste, llevará a cabo una evaluación exhaustiva para determinar su naturaleza, alcance y gravedad. Este proceso incluirá un análisis técnico de los sistemas afectados, la recopilación de evidencia digital y la evaluación de los riesgos asociados. Una vez se ha confirmado el incidente, el CISO, o la persona designada, lo clasificará en una de las siguientes categorías: crítica, alta, media o baja, según el impacto en las operaciones, la confidencialidad de los datos y la disponibilidad de los sistemas. Es importante destacar que esta clasificación puede ser revisada a medida que avanza la respuesta al incidente y se obtiene más información.

| **CLASIFICACIÓN CRÍTICA** | |
|---|---|
| **Impacto**<br><br>Impacto severo en operaciones críticas, datos sensibles comprometidos, o amenaza inminente a la seguridad de la agencia o datos gubernamentales. | **Respuesta**<br><br>Activación inmediata del CSIRT-PRITS. |
| **Ejemplos**<br><br>- *Violación de datos masiva*<br>Compromiso a gran escala de información altamente confidencial, incluyendo, pero no limitado a, números de tarjetas de crédito, contraseñas o datos personales de clientes o usuarios.<br><br>- *Ransomware paralizante*<br>Infección por *ransomware* que bloquea el acceso a sistemas y datos críticos, interrumpiendo severamente las operaciones esenciales de la agencia.<br><br>- *Ataque DDoS catastrófico*<br>Ataque de Denegación de Servicio Distribuido (DDoS) que causa una interrupción total o casi total de los servicios en línea de la agencia, comprometiendo gravemente su disponibilidad. | |

| **CLASIFICACIÓN ALTA** | |
|---|---|
| **Impacto**<br>Impacto significativo en operaciones, posible compromiso de datos sensibles, o amenaza seria a la seguridad. | **Respuesta**<br>Activación inmediata del CSIRT-PRITS. |

**Ejemplos**

- *Pérdida o corrupción de datos críticos*
  Afecta sistemas esenciales para las operaciones y puede resultar en pérdidas financieras significativas o daños a la reputación.
- *Exposición de información sensible*
  Incluye la divulgación no autorizada de información de identificación personal (IIP) que puede llevar a fraudes o violaciones de privacidad.
- *Riesgo de propagación*
  El incidente tiene el potencial de extenderse a otros sistemas o redes, causando un daño más amplio.
- *Amenazas a la seguridad física*
  Pone en peligro la seguridad de personas o bienes, como, por ejemplo, a través de ataques a sistemas de infraestructura crítica.

| **CLASIFICACIÓN MEDIA** | |
|---|---|
| **Impacto**<br>Impacto moderado en operaciones, datos no críticos afectados, o amenaza potencial a la seguridad. | **Respuesta**<br>Activación del CSIRT-PRITS a discreción del CISO. |

**Ejemplos**

- *Cuentas comprometidas*
  Un atacante obtiene acceso a múltiples cuentas de correo electrónico de empleados de un departamento, lo que podría permitir el envío de correos fraudulentos.
- *Ransomware en sistemas de respaldo*
  Un ataque de *ransomware* encripta los datos de respaldo de una agencia, lo que dificulta la recuperación en caso de desastre.
- *Intrusión en una red aislada*
  Un atacante externo logra acceder a una red de investigación, potencialmente robando datos de proyectos en curso.