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

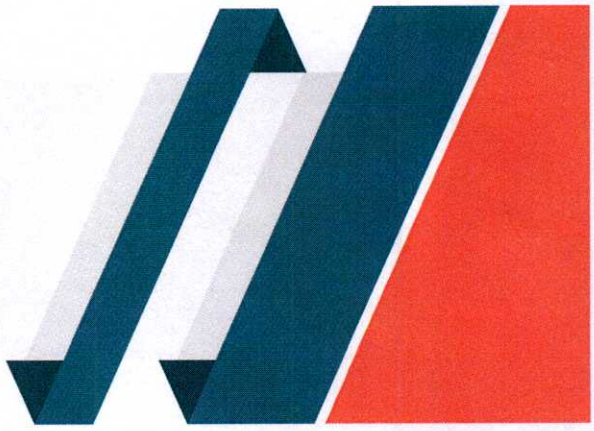

Tabla de Contenido

1. Descripción 2
2. Base Legal 2
3. Propósito 3
4. Alcance 4
5. Abreviaciones, acrónimos, definiciones y significados 4
6. Política 10
7. Responsabilidades 19
8. Sanciones 27
9. Solicitud de exenciones 27
10. Cláusula Derogatoria 27
11. Vigencia 27
12. Referencias 27
13. Description 29
14. Legal Basis 29
15. Purpose 30
16. Scope 31
17. Abbreviations, Acronyms, Definitions, and Meanings 31
18. Policy 36
19 Responsibilities 46
20. Penalties 53
21. Exemption Request 53
22. Derogatory Clause 53
23. Effective Date 54
24. References 54

Firmas de aprobación / *Approval Signatures* 55

Historial de Revisiones / *Revision History* 56

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: - Número de Seguro Social - Número de licencia de conducir, tarjeta electoral u otra identificación oficial - Números de cuentas bancarias o financieras de cualquier tipo, con o sin claves de acceso que puedan habérsele asignado - Nombres de usuario y claves de acceso a sistemas informáticos públicos o privados - Información médica protegida por la Ley HIPAA - Información contributiva - Evaluaciones laborales
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 (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. 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	**Respuesta**
Impacto severo en operaciones críticas, datos sensibles comprometidos, o amenaza inminente a la seguridad de la agencia o datos gubernamentales.	Activación inmediata del CSIRT-PRITS.
Ejemplos - *Violación de datos masiva* 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. - *Ransomware paralizante* Infección por *ransomware* que bloquea el acceso a sistemas y datos críticos, interrumpiendo severamente las operaciones esenciales de la agencia. - *Ataque DDoS catastrófico* 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 Impacto significativo en operaciones, posible compromiso de datos sensibles, o amenaza seria a la seguridad.	**Respuesta** 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 Impacto moderado en operaciones, datos no críticos afectados, o amenaza potencial a la seguridad.	**Respuesta** 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.

CLASIFICACIÓN MEDIA
Ejemplos - *Fuga de datos de clientes/ciudadanos limitada* Se produce una filtración de datos personales de un pequeño grupo de clientes/ciudadanos debido a una configuración incorrecta del servidor. - *Denegación de servicio a un servicio no crítico* Un ataque DDoS causa la caída temporal de un servidor web secundario, afectando a una parte limitada de los usuarios.

CLASIFICACIÓN BAJA	
Impacto Impacto mínimo en operaciones, sin compromiso de datos sensibles, amenaza limitada a la seguridad.	**Respuesta** El CSIRT-PRITS no se activa. El personal de las agencias y/o proveedores de servicios contratados asociados responderán al incidente. Deberán notificar al CSIRT-PRITS sobre las medidas tomadas.
Ejemplos - *Intento fallido de inicio de sesión* Un usuario introduce incorrectamente su contraseña varias veces, lo que activa una alerta de seguridad, pero no compromete el sistema. - *Descubrimiento de una vulnerabilidad menor* Un escaneo de seguridad detecta una vulnerabilidad de bajo riesgo en un *software* obsoleto que no está expuesto a Internet.	

7. Responsabilidades

7.1 Principal Oficial de Seguridad Cibernética del Gobierno de Puerto Rico (CISO)

El CISO desempeñará un rol fundamental en la supervisión y gestión del PRIC. Sus responsabilidades abarcan el desarrollo, mantenimiento, medición, prueba y mejora continua de este programa crítico. A continuación, se detallan sus principales responsabilidades:

7.1.1 Gestión y revisión del Programa

7.1.1.1 Revisará el funcionamiento del PRIC y del CSIRT-PRITS al menos una vez al año.
7.1.1.2 Examinar los informes operativos y las métricas asociadas al PRIC anualmente.
7.1.1.3 Organizará o participará en un simulacro de respuesta a incidentes y analizar sus resultados, como mínimo una vez al año.
7.1.1.4 Revisará y actualizará la política de respuesta a incidentes anualmente.
7.1.1.5 Asegurará la comunicación efectiva de esta política a todas las partes interesadas, al menos una vez al año.

7.1.2 Desarrollo y mantenimiento del plan de respuesta a incidentes

El CISO y las personas designadas por éste serán responsables de desarrollar, mantener, actualizar e implementar un plan de respuesta a incidentes que incluya:

7.1.2.1 Identificación y asignación de roles
7.1.2.1.1 Identificará a los miembros del CSIRT-PRITS.
7.1.2.1.2 Asignará funciones y responsabilidades específicas a cada miembro.

7.1.2.2 Activación y utilización del plan
7.1.2.2.1 Especificará las condiciones para poner en marcha el plan.
7.1.2.2.2 Definirá los procesos para activar el CSIRT-PRITS.

7.1.2.3 Procesos de gestión de incidentes
7.1.2.3.1 Detallará métodos y procedimientos para la notificación, declaración, categorización, priorización y escalado de incidentes.

7.1.2.3.2 Documentará procesos de detección, análisis y verificación de incidentes.
7.1.2.3.3 Establecerá procedimientos para la recolección y preservación de evidencias.
7.1.2.3.4 Desarrollará estrategias de contención, erradicación y recuperación.

7.1.2.4 Movilización de recursos externos
7.1.2.4.1 Identificará la autoridad para aprobar la movilización de recursos externos y establecerá los criterios y procedimientos para su activación

7.1.2.5 Notificaciones y comunicaciones
7.1.2.5.1 Documentará procesos y plazos para notificar a individuos afectados, entidades asociadas y agencias reguladoras.
7.1.2.5.2 Mantendrá una lista actualizada de contactos de respuesta a incidentes que incluya miembros del CSIRT-PRITS, partes interesadas internas, agencias gubernamentales relevantes y recursos de terceros.

7.1.2.6 Actividades post-incidente
7.1.2.6.1 Establecerá procedimientos para la evaluación de la respuesta al incidente y lecciones aprendidas.
7.1.2.6.2 Definirá procesos para la comunicación de resultados y seguimiento de incidentes.
7.1.2.6.3 Establecerá procesos para la adopción de medidas de prevención técnicas necesarias.
7.1.2.6.4 Revisará la eficacia de los procedimientos y el equipo.
7.1.2.6.5 Elaborará recomendaciones y definirá los próximos pasos.

7.1.3 Pruebas y formación

7.1.3.1 Establecerá planes para realizar pruebas anuales (o más frecuentes) del plan de respuesta a incidentes.

7.1.3.2 Documentará y coordinará ejercicios de formación sobre manejo de incidentes.

7.1.3.3 Asegurará que todas las partes interesadas comprendan adecuadamente sus responsabilidades a través de programas de capacitación efectivos.

7.1.4 Mejora continua

7.1.4.1 Utilizará los resultados de las revisiones, simulacros y incidentes reales para mejorar continuamente el PRIC.

7.1.4.2 Adaptará el programa a las nuevas amenazas y cambios en el panorama de la ciberseguridad.

7.1.4.3 Fomentará una cultura de aprendizaje y mejora continua en toda la organización.

7.2 Oficial Principal de Informática (OPI) de la Agencia

El OPI desempeña un rol importante en la gestión de la ciberseguridad de la agencia. Como punto principal de contacto entre la agencia y PRITS durante incidentes de ciberseguridad, el OPI tiene responsabilidades extensas y variadas que abarcan desde la prevención hasta facilitar la respuesta a incidentes. Las principales responsabilidades del OPI incluyen:

7.2.1 Manejo de Programa de Ciberseguridad

7.2.1.1 En colaboración con PRITS, desarrollará, implementará y mantendrá un programa integral de ciberseguridad que cumpla con la Ley 40-2024.

7.2.1.2 Asegurará que la agencia tenga implementadas las políticas, estándares, procedimientos, controles, sistemas y medidas de seguridad necesarias para cumplir con los requisitos de identificación, detección, protección, respuesta y recuperación establecidos en la normativa vigente.

7.2.2 Notificación y gestión de incidentes

7.2.2.1 Informará a PRITS inmediatamente, y no más de una hora después, cuando se detecte o sospeche un incidente de ciberseguridad.

7.2.2.2 Coordinará con PRITS el proceso de gestión del incidente, incluyendo el aislamiento, mitigación, resolución y documentación del mismo.

7.2.2.3 Identificará y documentará las lecciones aprendidas tras cada incidente para mejorar continuamente las prácticas de seguridad.

7.2.3 Coordinación interna y externa

7.2.3.1 Asegurará que el personal técnico y los proveedores de servicios contratados de la agencia estén disponibles y coordinados para asistir en la respuesta a incidentes.

7.2.3.2 Participará en la coordinación con agencias locales y federales que tengan injerencia sobre los incidentes.

7.2.4 Comunicación y enlace

7.2.4.1 Mantendrá una comunicación constante con PRITS durante los incidentes de ciberseguridad.

7.2.4.2 Asegurará que la agencia esté informada y alineada con las directrices y acciones recomendadas por PRITS.

7.2.4.3 Actuará como enlace entre la agencia y otras entidades relevantes en materia de ciberseguridad.

7.2.5 Supervisión y cumplimiento

7.2.5.1 Supervisará las acciones de respuesta por parte del personal y de los proveedores de servicios contratados de la agencia, garantizando el cumplimiento de las instrucciones y requisitos establecidos por la OEIC, implementando todas las recomendaciones y directrices notificadas.

7.2.5.2 Entregará esta política a todos los proveedores de servicios contratados, asegurando que estén plenamente informados de

sus obligaciones y responsabilidades en relación con la gestión y el reporte de incidentes.

7.2.5.3 Velará por que la agencia y sus proveedores de servicios contratados cumplan con los estándares y principios mínimos de ciberseguridad establecidos en la Ley 40-2024, así como con cualquier política, carta circular, estándar o guía adicional que se emita en cumplimiento de dicha ley.

7.2.6 Mejora continua y adaptación

7.2.6.1 Se mantendrá actualizado sobre las últimas tendencias y amenazas en ciberseguridad.

7.2.6.2 Propondrá y liderará iniciativas para mejorar constantemente la postura de ciberseguridad de la agencia, alineadas con las políticas y normativas establecidas por PRITS.

7.2.6.3 Adaptará el programa de ciberseguridad de la agencia según las necesidades cambiantes y los nuevos desafíos que surjan.

7.3 Equipo de Respuesta a Incidentes (CSIRT-PRITS)

El CSIRT-PRITS desempeña un rol esencial en la protección de los activos de información y la gestión eficaz de los incidentes de ciberseguridad. Sus responsabilidades abarcan desde la prevención hasta la recuperación post-incidente, incluyendo:

7.3.1 Monitoreo y detección

7.3.1.1 Implementará y mantendrá sistemas de monitoreo continuo para detectar anomalías y posibles incidentes de seguridad.

7.3.1.2 Identificará y clasificará rápidamente los eventos que podrían comprometer la seguridad de los activos de información.

7.3.2 Análisis y evaluación

7.3.2.1 Realizará evaluaciones exhaustivas de los incidentes detectados para determinar su alcance, impacto y origen.

7.3.2.2 Utilizará herramientas forenses y técnicas avanzadas de análisis para comprender la naturaleza y gravedad de los incidentes.

7.3.2.3 Evaluará los riesgos asociados con cada incidente y priorizará las acciones de respuesta.

7.3.3 Contención y mitigación

7.3.3.1 Implementará medidas inmediatas para contener la propagación del incidente y minimizar su impacto en los sistemas y datos.

7.3.3.2 Coordinará con los equipos técnicos relevantes para aislar los sistemas afectados y prevenir daños adicionales.

7.3.4 Erradicación

7.3.4.1 Identificará y eliminará las causas raíz de los incidentes para prevenir su recurrencia.

7.3.4.2 Desarrollará y ejecutará planes de acción para remediar vulnerabilidades y fortalecer las defensas del sistema.

7.3.5 Recuperación

7.3.5.1 Diseñará e implementará estrategias para restaurar los sistemas afectados y garantizar la continuidad de las operaciones.

7.3.5.2 Verificará la integridad de los sistemas y datos restaurados antes de reintegrarlos a la red operativa.

7.3.6 Comunicación y coordinación

7.3.6.1 Mantendrá una comunicación efectiva y oportuna con todas las partes involucradas, incluyendo la alta gerencia, usuarios afectados y autoridades concernientes.

7.3.6.2 Colaborará estrechamente con el OPI para asegurar una respuesta coordinada y alineada con las directrices de la OEIC y PRITS.

7.3.6.3 Facilitará la comunicación entre diferentes agencias durante la respuesta a incidentes.

7.3.7 Aprendizaje y mejora continua

7.3.7.1 Realizará análisis post-incidente para identificar lecciones aprendidas y áreas de mejora.

7.3.7.2 Actualizará y refinará los procesos de respuesta a incidentes basándose en la experiencia adquirida

7.3.8 Colaboración interagencial y apoyo

7.3.8.1 Trabajará en estrecha colaboración con otras agencias para compartir información sobre amenazas y mejores prácticas de seguridad.

7.3.8.2 Brindará asistencia técnica y orientación a las agencias en la investigación, mitigación y resolución de incidentes de seguridad.

7.3.8.3 Colaborará con agencias locales y federales que tengan injerencia sobre los incidentes, facilitando la coordinación y el intercambio de información relevante.

7.3.9 Documentación e informes

7.3.9.1 Mantendrá registros detallados de todos los incidentes, acciones tomadas y resultados obtenidos.

19.4 Proveedores de servicios contratados

19.4.1 Deberán cumplir estrictamente con los estándares y principios mínimos de ciberseguridad establecidos en la Ley 40-2024. Esto implica implementar medidas de seguridad robustas para proteger los datos y sistemas de la agencia, así como informar de manera oportuna cualquier incidente de seguridad.

19.4.2 Deberán cumplir con las instrucciones y requisitos establecidos por la OEIC, implementando las recomendaciones y directrices emitidas. Deberá informar a la OEIC y al OPI de la agencia sobre el avance y resultados de las acciones implementadas.

8. Sanciones

PRITS podrá imponer multas a las agencias que incumplan con lo estipulado en la Ley 40-2024. Toda divulgación de datos no autorizado, modificación no autorizada o pérdida de datos, cuando medie obstrucción, negligencia, mala fe, temeridad o negativa caprichosa en el manejo o informe de un ciberataque, conllevará sanciones, multas, y en ocasiones despidos, recisión de contrato, e inhabilitación para contratar restitución de dinero entre otras sanciones aplicables bajo la Ley 40-2024.

9. Solicitud de exenciones

Cuando el cumplimiento de esta política no sea factible, técnicamente posible o se requiera una desviación, la agencia deberá enviar una solicitud formal por escrito al CISO y al PEII. Esta solicitud se enviará por correo electrónico a cumplimientocyber@prits.pr.gov y deberá ser presentada por el OPI o la persona designada por la autoridad nominadora.

10. Cláusula Derogatoria

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

11. Vigencia

Esta política tendrá vigencia inmediata.

12. Referencias

Número de identificación	Título	Versión
NIST CSWP 29 • RS.RP-1 • RS.CO-1:5	The NIST Cybersecurity Framework (CSF)	2.0
NIST SP 800-61r2	Computer Security Incident Handling Guide	Rev. 2
PRITS-SOP-0007- OPE	Procedimiento para informar incidentes de seguridad de la información	1.0
NIST SP 800-53r5 • RA-3 (a, b, c, d) • RA-5 (a, b, 1, 2, 5, 6) • PS-7	Security and Privacy Controls for Information Systems and Organizations	Rev. 5
Ley Núm. 40-2024	Ley de Ciberseguridad del Estado Libre Asociado de Puerto Rico	N/A

Este espacio se ha dejado intencionalmente en blanco.

13. Description

The Information Security Incident Response Policy establishes a comprehensive framework for the Puerto Rico Innovation and Technology Service's (PRITS) Cyber Incident Response Program. This policy defines the essential guidelines, procedures, and responsibilities for the effective detection, timely response, and efficient recovery from incidents that may compromise the integrity, confidentiality, or availability of PRITS' information assets and those of the government entities it serves.

Grounded in best practices, including the National Institute of Standards and Technology (NIST) Cybersecurity Framework, this policy emphasizes the importance of proactive preparedness, clear role and responsibility assignments, and continuous improvement of incident response capabilities as fundamental pillars for maintaining a secure and resilient digital environment.

14. Legal Basis

This policy is issued under Law No. 75-2019, known as the "Puerto Rico Innovation and Technology Service Act (PRITS)", and Law No. 40-2024, known as the "Commonwealth of Puerto Rico Cybersecurity Act.
Law No. 75-2019, *supra*, created PRITS to establish and promote public policy on the evaluation, management, development, coordination, and effective interagency integration of the Government of Puerto Rico's technology and computer infrastructure of the Government of Pico. Furthermore, Article 6 of Law 75-2019, *id.*, gives PRITS the responsibility to create and implement strategic plans, policies, standards, and an integrated architecture for the Government's information and telecommunications technologies. It also establishes PRITS as the promoter of the discipline in the best practices in technology project management and the publication of guidelines and directives to that end.

Law No. 40-2024, *supra*, establishes a legal framework to strengthen cybersecurity in the Government of Puerto Rico, focusing on protecting government data and critical infrastructure against digital threats. The law establishes public policy, jurisdiction, and standards centered on maintaining the confidentiality, integrity, and availability of government information, improving the security of networks and critical infrastructure, as

well as strengthening capabilities to prevent and respond to cyber threats. In addition, it promotes the protection of citizens' privacy and compliance with basic cybersecurity regulations of the United States Government. Finally, it includes provisions for imposing sanctions on the Executive Branch of Government, municipalities, and their respective contracted service providers that fail to comply with the corresponding regulations.

With this policy, we reaffirm compliance with other statutory provisions, including Law No. 151-2004, as amended, known as the "Electronic Government Law". This policy is grounded in Laws 75-2019 and 40-2024. Any references to other laws are for informational purposes only and shall not be considered a basis for this policy's applicability or jurisdiction.

15. Purpose

This policy aims to strengthen the cybersecurity posture of PRITS and the Government of Puerto Rico, establishing a structured and effective approach to incident management. The specific objectives of this policy are:

- To set clear and measurable expectations for creating, maintaining, overseeing, and continuously improving incident response capabilities.

- To define and assign specific roles, responsibilities, and authority levels for incident management, ensuring a coordinated and effective response to any cybersecurity incident.

- To provide a framework aligned with recognized international standards, such as NIST CSF 2.0 and NIST SP.800-61r2, to guide incident response practices, and facilitate interoperability with other government and security entities.

- To foster a cybersecurity awareness and preparedness culture, promoting early detection, rapid notification, and effective response to potential threats.

16. Scope

The provisions of this policy apply to the Executive Branch of the Government of Puerto Rico, including any department, board, dependency, commission, bureau, office, agency, administration or organism, political subdivision, public corporations, and municipalities[2]. 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, with respect to the data generated as a result of such activities.

17. Abbreviations, Acronyms, Definitions, and Meanings

Abbreviation / Acronym	**Meaning**
CIIO	Chief Information and Innovation Officer of the Government of Puerto Rico
CIO	Chief Information Officer
CISO	Chief Information Security Officer of the Government
CSIRT	Computer Security Incident Response Team
DDoS	Distributed denial of service
IDS	Intrusion detection system
IoT	Internet of Things
IT	Information technology
KPI	Key performance indicator
NIST	National Institute of Standards and Technology
OEIC	Office for the Evaluation of Cyber Incidents *(Oficina para la Evaluación de Incidentes Cibernéticos)*
PII	Personally Identifiable Information

[2] See, Article 2 of Law 40-2024.

Abbreviation / Acronym	Meaning
PRIC	Cyber Incident Response Program *(Programa de Respuesta a Incidentes Cibernéticos)*
PRITS	Puerto Rico Innovation and Technology Service

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 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.
Chief Information Officer (CIO)	Individual responsible for managing and overseeing a government agency's technology infrastructure and operations.
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.
Confidentiality	Preserve restrictions on access and disclosure, including means to protect privacy and confidential information.

Term	Definition
Contracted service provider	Entity, whether a natural or legal person, public or private, that provides services such as networks, applications, programs, 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.
Distributed denial of service	A denial-of-service technique that uses numerous hosts to perform the attack.
Government	Is the Commonwealth of Puerto Rico.
HIPAA	Health Insurance Portability and Accountability Act of 1996; a federal law that required the federal Department of Health and Human Services to establish regulatory standards to protect the privacy and security of individually identifiable health information.
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.

Term	Definition
Incident management	All administrative, physical, and technical procedures applied for the investigation and mitigation of 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.
Information resource	Information and related resources, such as personnel, equipment, software, information technology, and more.
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 Policy, the terms 'incident', 'cyber incident', 'information security incident', and 'computer security incident' shall be used interchangeably.
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.

Term	Definition
Municipality(-ies)	Any of the 78 municipalities of Puerto Rico. For purposes of this policy, the terms Municipality(-ies) and Agency(-ies) will be used interchangeably.
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.
Personally identifiable information (PII)	Any representation of information that is readable without the need for a special cryptographic key to access it or that facilitates the tracing of an individual's identity, including the name or first initial and last name of an individual combined with other information that is linked or likely to be linked to a specific individual, such as: - Social Security number - Driver's license number, voter registration card, or other government-issued ID - Bank or financial account numbers of any kind, with or without access codes, that may have been assigned to you - Usernames and passwords for access to public or private computer systems - HIPAA-protected health information - Tax information - Job evaluations
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.

This space has been intentionally left blank.

Term	Definition
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.
Risk	Any reasonably identifiable circumstance or event that has a possible adverse effect on the security of networks and information resources.
Software	Computer programs and associated data that can be written or modified dynamically during execution.

18. Policy

18.1 Cyber Incident Response Program (PRIC)

PRITS will develop, implement, and maintain a Cyber Incident Response Program (PRIC), attached to the Office for Cyber Incident Assessment (OEIC). This program will be aligned with the legal responsibilities of the OEIC and will have the following main objectives:

- Manage information security risks associated with incidents.
- Detect, respond to, and mitigate the consequences of cyberattacks and other threats against government information systems and data.

- Establish guidelines for the exchange and communication of incident-related information.
- Retain all necessary artifacts resulting from incidents and response procedures for further analysis and continuous improvement.
- Inform and train stakeholders on their roles and responsibilities in the incident response process.
- Communicate, govern, operate, and improve incident response activities.

18.1.2 Performance Metrics

To assess the effectiveness of the PRIC and ensure continuous improvement, a measurement system based on key performance indicators (KPIs) will be established. These KPIs will allow you to monitor program performance, identify areas for improvement, and make data-driven decisions.

18.1.2.1 Data Collection and Storage

Data will be collected and stored in a centralized and accessible manner, allowing for detailed analysis and customized reporting. The information collected will include, at a minimum:

18.1.2.1.1 Number and type of incidents
All reported incidents will be accounted for and categorized by type (e.g., phishing, malware, denial of service) to identify trends and patterns.

18.1.2.1.2 Detection and Resolution Time
The time elapsed from the initial detection of the incident to its complete resolution will be measured, including all phases of the incident's life cycle.

18.1.2.1.3 Incident Impact

The incident's impact will be assessed in terms of data loss, service disruption, financial costs, and reputation.

18.1.2.1.4 Root Cause
Each incident's root cause will be identified so that corrective and preventive measures can be implemented.

18.1.2.1.5 Corrective Actions
Actions taken to resolve the incident and prevent recurrence shall be documented.

18.1.2.1.6 Lessons Learned
Lessons learned from each incident will be captured to improve safety processes and procedures.

Specific metrics will be presented to evaluate compliance and the program's effectiveness for each of the requirements mentioned above. The proposed metrics are detailed below.

Element	Key Performance Indicator (KPI)	Metric
Number of incidents	Incident rate by type	Number of incidents by threat type divided by the total number of incidents.
Time to resolve the incident	Mean time to resolution	Average time to resolve an incident, broken down by incident type.
	Detection time	Average time between the occurrence of the incident and its detection.
	Percentage of incidents assessed	Percentage of incidents evaluated and classified

Element	Key Performance Indicator (KPI)	Metric
Objective incident assessments		according to their severity and impact.
	Corrective action compliance rate	Percentage of corrective actions implemented after each incident.
Incident reports	Incident reporting compliance	Percentage of incidents with complete reports that include all relevant information.
	Time to generate reports	Average time to create an incident report after resolution.
Lessons learned	Number of lessons learned implemented	Number of improvements implemented as a result of lessons learned.
	Incident recurrence rate	Percentage of incidents that recur after they have been mitigated.

18.1.2.2 Analysis and Continuous Improvement
The data collected will be analyzed regularly to identify trends, patterns and areas for improvement. The results of these analyses will be used to fine-tune the incident management program, improve safety processes, and make informed decisions.

18.1.2.3 Communication and Transparency
Clear and transparent communication mechanisms Will be established to inform stakeholders about the program's performance, incidents that have occurred and actions taken.

18.2 Computer Security Incident Response Team

The Computer Security Incident Response Team (CSIRT-PRITS) will be critical to ensuring effective and coordinated incident response. Under the framework of PRIC, the CSIRT-PRITS will be a multidisciplinary structure that combines internal and external expertise to address the various facets of an incident.

18.2.1 Composition

The CSIRT-PRITS will be strategically composed of:

18.2.1.1 Office for the Evaluation of Cyber Incidents (OEIC)
Will lead and coordinate incident response efforts, providing guidance, resources, and technical expertise throughout the process. It will act as a central point of command in cyber crises.

18.2.1.2 Affected Agency Technical Staff
They will join the CSIRT-PRITS when an incident occurs in their agency. They will contribute knowledge of the agency's specific resources and systems, facilitate access to affected systems, and provide technical support and necessary contextual information.

18.2.1.3 Agency's Contracted Service Providers
If the agency has contracted service providers who manage or have specialized knowledge about its systems, they may also be integrated into the CSIRT-PRITS. Like the agency's technical staff, their role is to assist and facilitate the response.

18.2.1.4 Additional Members
The Chief Information Security Officer (CISO) will have the authority to appoint additional members to the CSIRT-PRITS as necessary to ensure an effective response. These members may be experts in specific areas such as digital forensics, threat intelligence, or crisis communications.

18.2.2 Authority

The CSIRT-PRITS will have the authority to:

18.2.2.1 Monitor and oversee all actions taken during an inicent.
18.2.2.2 Implement the procedures and strategies established in the incident response plan.
18.2.2.3 Authorize modifications to information systems when necessary to contain or mitigate an incident.
18.2.2.4 Take measures, such as confiscation or disconnection of equipment to preserve evidence and prevent the spread of the incident.
18.2.2.5 Access pertinent resources and collect relevant information during investigations, including communications and user logs.
18.2.2.6 Share threat and incident information with other organizations, such as federal agencies, to strengthen collaboration and prevention.

18.3 Cyber Incident Management and Response

18.3.1 Reporting Obligation

18.3.1.1 All government agency employees, regardless of position or rank, have an unequivocal responsibility to immediately report any suspected security incident to the Office of Information Technology or its equivalent within their agency. This office, in turn, must notify the CSIRT-PRITS.
18.3.1.2 Contracted service providers delivering information technology and communications services have specific obligations regarding incident reporting. These providers must share information and notify both PRITS, by emailing soc@prits.pr.gov, and the contracting agency within forty-eight (48) hours of detecting a security incident or a potential threat that could compromise government data, software products, firmware, or confidential services, as well as the information of any natural or legal person.
Additionally, this reporting obligation also extends to those providers who:

- Use or access any information technology resource owned by a government agency.
- Manage information technology systems, whether automated or manual, under the administration of an agency.
- Operate these systems on behalf of the agency.
- Manage private information systems that hold government data.

18.3.1.3 All contracted service providers shall submit a detailed monthly report to PRITS on the security status of the systems and assets they manage on behalf of the agency. These reports must include at least the following:

18.3.1.3.1 The detected threat, threat actors, and vulnerabilities.

18.3.1.3.2 Immediate response and remediation actions.

18.3.1.3.3 The total number of information security incidents reported to PRITS through the established channels.

18.3.1.3.4 The assessment made on the state of cybersecurity.

18.3.2 Incident Scope

Incidents that must be reported include, but are not limited to:

- Unauthorized access or attempts to access systems or data.
- Loss or theft of devices containing sensitive information.
- Unauthorized modification of data or systems.
- Denial-of-service (DoS) attacks or attempts thereof.
- Malware or ransomware infection.
- Leak of sensitive or confidential data.
- Misuse of agency IT resources.
- Information security policy violations.

18.3.3 Reporting Process

18.3.3.1 Any employee or contracted Service provider who detects or suspects a security incident report it to the CSIRT-PRITS through the established channels (Procedure for Reporting Information Security Incidents; PRITS-SOP-0007).

18.3.3.2 The report must include all relevant information available, such as the nature of the incident, systems affected, and any immediate action taken.

18.3.3.3 The CSIRT-PRITS shall acknowledge receipt of the report and may request additional information if necessary.

18.3.4 Incident Classification

Once a cybersecurity incident has been reported, the Government of Puerto Rico's Chief Cyber Security Officer (CISO) will thoroughly assess its nature, scope, and severity. This process will include a technical analysis of the affected systems, digital evidence collection, and the associated risk assessment. Once the incident has been confirmed, the CISO will classify it into one of the following categories: critical, high, medium, or low, depending on the impact on operations, data sensitivity, and system availability. Importantly, this classification can be revised as the incident response progresses and more information is obtained.

CRITICAL CLASSIFICATION	
Impact	**Response**
Severe impact on critical operations, compromised sensitive data, or imminent threat to agency or government data security.	Immediate activation. CSIRT-PRITS

This space has been intentionally left blank.

CRITICAL CLASSIFICATION

Examples

- *Massive data breach*
  Large-scale compromise of highly sensitive information, including, but not limited to, credit card numbers, passwords, or personal data of customers or users.
- *Paralyzing ransomware*
  Ransomware infection blocks access to critical systems and data, severely disrupting the agency's essential operations.
- *Catastrophic DDoS attack*
  Distributed denial of service (DDoS) attack causes a total or near-total disruption of the agency's online services, severely compromising their availability.

HIGH CLASSIFICATION

Impact	**Response**
Significant impact on operations, potential compromise of sensitive data, or serious security threat.	Immediate activation. CSIRT-PRITS

Examples

- *Critical data loss or corruption*
  It affects systems essential to operations and can result in significant financial loss or reputational damage.
- *Sensitive data exposure*
  Includes the unauthorized disclosure of personally identifiable information (PII), which can lead to fraud or privacy breaches.
- *Spread risk*
  The incident can potentially spread to other systems or networks, causing broader damage.
- *Threats to physical security*
  Endangers the safety of people or property, such as through attacks on critical infrastructure systems.

MEDIUM CLASSIFICATION	
Impact	**Response**
Moderate impact on operations, non-critical data affected, or potential security threat.	Immediate activation. CSIRT-PRITS

Examples

- *Compromised accounts*
  An attacker gains access to multiple employee email accounts in a department, which could enable the sending of fraudulent emails.
- *Ransomware on backup systems*
  A ransomware attack encrypts an agency's backup data, making disaster recovery more difficult.
- *Intrusion into an isolated network*
  An external attacker manages to gain access to a research network, potentially stealing data from ongoing projects.
- *Limited customer/citizen data breach*
  A personal data breach of a small group of customers/citizens occurs due to server misconfiguration.
- *Denial-of-service attack on a non-critical service*
  A DDoS attack causes a temporary outage of a secondary web server, impacting a limited subset of users.

LOW CLASSIFICATION	
Impact	**Response**
Minimal impact on operations, no sensitive data compromised, limited security threat.	The CSIRT-PRITS is not activated. Associated agency and/or contracted service provider personnel will respond to the incident. They must notify the CSIRT-PRITS about the measures taken.

Examples

- *Failed login attempt*
  A user enters their password incorrectly multiple times, triggering a security alert, but no system compromise occurred.

LOW CLASSIFICATION
Examples - *Discovery of a minor vulnerability* A security scan detects a low-risk vulnerability in outdated software not exposed to the Internet.

19 Responsibilities

19.1 Government of Puerto Rico Chief Information Security Officer (CISO)

The CISO will play a fundamental role in overseeing and managing the Cyber Incident Response Program (PRIC). The responsibilities encompass developing, maintaining, measuring, testing, and continuously improving this critical program. The following outlines the primary responsibilities:

19.1.1 Program Management and Review

19.1.1.1 Will review the functioning of the PRIC and the CSIRT-PRITS at least once a year.
19.1.1.2 Annually review the PRIC's operational reports and metrics.
19.1.1.3 Will organize or participate in an incident response simulation and analyze its results at least once a year.
19.1.1.4 Will review and update the incident response policy on an annual basis.
19.1.1.5 Will ensure effective communication of this Policy to all stakeholders at least once a year.

19.1.2 Development and Maintenance of the Incident Response Plan

The CISO and his/her designees will be responsible for developing, maintaining, updating, and implementing an incident response plan that includes:

19.1.2.1 Role Identification and Assignment

19.1.2.1.1 Will identify CSIRT-PRITS members.
19.1.2.1.2 Will assign specific roles and responsibilities to each member.

19.1.2.2 Plan Activation and Use
19.1.2.2.1 Will specify the conditions for activating the plan.
19.1.2.2.2 Will define the processes to activate the CSIRT-PRITS.

19.1.2.3 Incident Management Processes
19.1.2.3.1 Will detail incident reporting, classification, prioritization, and escalation methods and procedures.
19.1.2.3.2 Will document processes for incident detection, analysis, and verification.
19.1.2.3.3 Will establish procedures for evidence collection and preservation.
19.1.2.3.4 Will develop containment, eradication, and recovery strategies.

19.1.2.4 Mobilization of External Resources
19.1.2.4.1 Will identify the approving authority for external resource mobilization and will set the criteria and procedures for its implementation.

19.1.2.5 Notifications and Communications
19.1.2.5.1 Will document processes and timelines for notifying affected individuals, associated entities, and regulatory agencies.
19.1.2.5.2 Will maintain an up-to-date list of incident response contacts, including CSIRT members, internal stakeholders, relevant government agencies, and third-party resources.

19.1.2.6 Post-incident Activities

19.1.2.6.1 Will establish procedures for evaluating the incident response and lessons learned.
19.1.2.6.2 Will define processes for communicating results and tracking incidents.
19.1.2.6.3 Will establish processes for the adoption of necessary technical prevention measures.
19.1.2.6.4 Will review the effectiveness of procedures and equipment.
19.1.2.6.5 Will develop recommendations and define the next steps.

19.1.3 Tests and Training

19.1.3.1 Will develop plans to conduct annual (or more frequent) tests of the incident response plan.
19.1.3.2 Will document and coordinate incident response training exercises.
19.1.3.3 Will ensure that all stakeholders properly understand their responsibilities through effective training programs.

19.1.4 Continuous Improvement

19.1.4.1 Will use the results of reviews, simulations, and actual incidents to improve the PRIC continuously.

19.1.4.2 Will adapt the program to new threats and changes in the cybersecurity landscape.
19.1.4.3 Will foster a culture of learning and continuous improvement throughout the organization.

19.2 Chief Information Officer (CIO) of the Agency

The CIO plays an important role in managing the agency's cybersecurity. As the primary point of contact between the agency and PRITS during cybersecurity incidents, the OPI has extensive and varied responsibilities

ranging from prevention to facilitating incident response. The CIO's primary responsibilities include:

19.2.1 Cybersecurity Program Management

19.2.1.1 In collaboration with PRITS, it will develop, implement, and maintain a comprehensive cybersecurity program compliant with Law 40-2024.

19.2.1.2 Will ensure the agency has implemented the necessary policies, standards, procedures, controls, systems, and security measures to meet the identification, detection, protection, response, and recovery requirements outlined in applicable regulations.

19.2.2 Incident Notification and Management

19.2.2.1 Will inform PRITS immediately, and no more than one hour after, when a cybersecurity incident is detected or suspected.

19.2.2.2 Will coordinate with the incident management process, including isolation, mitigation, resolution, and documentation.

19.2.2.3 Will identify and document the lessons learned after each incident to continuously improve security practices.

19.2.3 Internal and External Coordination

19.2.3.1 Will ensure that the agency's technical staff and contracted service providers are available and coordinated to assist in incident response.

19.2.3.2 Will participate in coordination with local and federal agencies involved in the incidents.

19.2.4 Communication and Liaison

19.2.4.1 Will maintain constant communication with PRITS during cybersecurity incidents.

19.2.4.2 Will ensure that the agency is informed and aligned with the guidelines and actions recommended by PRITS.

19.2.4.3 Will liaise between the agency and other relevant cybersecurity entities.

19.2.5 Oversight and Compliance

19.2.5.1 Will oversee response actions by agency personnel and contracted service providers, ensuring compliance with instructions and requirements established by the OEIC and implementing all notified recommendations and guidelines.

19.2.5.2 Will deliver this policy to all contracted service providers, ensuring they are fully aware of their obligations and responsibilities regarding incident management and reporting.

19.2.5.3 Will ensure that the agency and its contracted service providers comply with the minimum cybersecurity standards and principles established in Law 40-2024, as well as with any additional policies, circulars, standards, or guidelines issued in compliance with said law.

19.2.6 Continuous Improvement and Adaptation

19.2.6.1 Will stay up-to-date on the latest cybersecurity trends and threats.

19.2.6.2 Will propose and lead initiatives to constantly improve the agency's cybersecurity posture, aligned with the policies and regulations established by PRITS.

19.2.6.3 Adapt the agency's cybersecurity program to changing needs and emerging challenges.

19.3 Incident Response Team (CSIRT-PRITS)

The CSIRT-PRITS is essential in protecting information assets and effectively managing cybersecurity incidents. Its responsibilities range from prevention to post-incident recovery, including:

19.3.1 Monitoring and Detection

19.3.1.1 Will implement and maintain continuous monitoring systems to detect anomalies and potential security incidents.
19.3.1.2 Will quickly identify and classify events that could compromise the security of information assets.

19.3.2 Analysis and Evaluation

19.3.2.1 Will thoroughly assess detected incidents to determine their scope, impact, and origin.
19.3.2.2 Will use forensic tools and advanced analysis techniques to understand the nature and severity of incidents.
19.3.2.3 Will assess the risks associated with each incident and prioritize response actions.

19.3.3 Containment and Mitigation

19.3.3.1 Will implement immediate measures to contain the spread of the incident and minimize its impact on systems and data.
19.3.3.2 Will coordinate with relevant technical teams to isolate affected systems and prevent further damage.

19.3.4 Eradication

19.3.4.1 Will identify and eliminate the root causes of incidents to prevent recurrence.
19.3.4.2 Will develop and execute action plans to remediate vulnerabilities and strengthen system defenses.

19.3.5 Recovery

19.3.5.1 Will design and implement strategies to restore affected systems and ensure operational continuity.

19.3.5.2 Will verify the integrity of restored systems and data before reintegrating them into the operational network.

19.3.6 Communication and Coordination

19.3.6.1 Will maintain effective and timely communication with all relevant parties, including senior management, affected users, and relevant authorities.

19.3.6.2 Will collaborate closely with the CIO to ensure a coordinated response aligned with the OEIC and PRITS guidelines.

19.3.6.3 Will facilitate communication between different agencies during incident response.

19.3.7 Learning and Continuous Improvement

19.3.7.1 Will conduct post-incident analysis to identify lessons learned and areas for improvement.

19.3.7.2 Will update and refine incident response processes based on experience gained.

19.3.8 Interagency Collaboration and Support

19.3.8.1 Will work closely with other agencies to share threat intelligence and security best practices.

19.3.8.2 Will provide technical assistance and guidance to agencies in investigating, mitigating, and resolving security incidents.

19.3.8.3 Will collaborate with local and federal agencies involved in the incidents, facilitating coordination and the exchange of relevant information.

19.3.9 Documentation and Reports

19.3.9.1 Will maintain detailed records of all incidents, actions taken, and outcomes achieved.

19.4 Contracted Service Providers

19.4.1 Contracted service providers must strictly comply with the minimum cybersecurity standards and principles established in Law 40-2024. This entails implementing robust security measures to protect the agency's data and systems, as well as promptly reporting any security incidents.

19.4.2 Must comply with the instructions and requirements established by the OEIC, implementing the recommendations and guidelines issued. They must inform the OEIC and the agency's CIO of the progress and results of the implemented actions.

20. Penalties

PRITS may impose fines on agencies that fail to comply with the provisions of Law 40-2024. Any unauthorized disclosure, unauthorized modification, or loss of data, when there is obstruction, negligence, bad faith, recklessness, or willful refusal in the handling or reporting of a cyberattack, shall result in sanctions, fines, and in some cases, dismissal, contract termination, disqualification from contracting, restitution of funds, and other applicable sanctions under Law 40-2024.

21. Exemption Request

When compliance with this policy is not feasible or technically possible, or if a deviation is necessary, the agency shall submit a formal written request to the CISO and CIIO. This request shall be emailed to cumplimientocyber@prits.pr.gov and must be submitted by the CIO or the designated individual.

22. Derogatory Clause

This policy supersedes any prior circulars, memoranda, administrative orders, policies, regulations, written communications, or instructions that are, in whole or in part, inconsistent with this policy.

23. Effective Date

This policy will be effective immediately.

24. References

Identification Number	Title	Version
NIST CSWP 29 • RS.RP-1 • RS.CO-1:5	The NIST Cybersecurity Framework (CSF)	2.0
NIST SP 800-61r2	Computer Security Incident Handling Guide	Rev. 2
PRITS-SOP-0007-OPE	Procedure for Reporting Information Security Incidents	1.0
NIST SP 800-53r5 • RA-3 (a, b, c, d) • RA-5 (a, b, 1, 2, 5, 6) • PS-7	Security and Privacy Controls for Information Systems and Organizations	Rev. 5
Law No. 40-2024	Commonwealth of Puerto Rico Cybersecurity Act	N/A

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***