Universidad de Puerto Rico
Oficina de Sistemas de Información
UPR Administración Central

Procedimiento general para el manejo de incidentes de la Tecnología de Información en la Universidad de Puerto Rico

Revisión Febrero 2023

Documento revisado y aprobado por el Comité Institucional de Seguridad en los Sistemas de Información

Artículo 1 Titulo

Procedimiento General para el manejo de incidentes de la Tecnología de Información en la Universidad de Puerto Rico.

Artículo 2 Base Legal

Este procedimiento se adopta conforme a las disposiciones contenidas en la Ley Núm. 1 del 20 de enero de 1966, según enmendada, el Reglamento General de la Universidad de Puerto Rico y la Certificación 85 (2022-2023), Política Institucional sobre el Uso y Acceso a los Recursos de la Tecnología de Información en la Universidad de Puerto Rico. Además, las Guías para la Protección de la Información en las Computadoras u Otros Medios Removibles de Almacenamiento en Caso de Sospecha sobre el Mal Uso de la Misma (Carta Circular 14-02 de Auditores Internos.)

Artículo 3 Introducción

La Política Institucional sobre el uso aceptable de los Recursos de la Tecnología de Información en la Universidad de Puerto Rico, dispone:

A. "La Universidad puede intervenir con los recursos de TI durante el curso de alguna auditoría o querella sobre el alegado uso inapropiado de la TI y durante cualquier tipo de intervención forense que se determine realizar a causa de un incidente detectado o reportado." (Artículo VII, D.)

B. "La Universidad podrá denegar acceso a los recursos de la TI temporalmente si durante el curso de una investigación, auditoría o querella resulta necesario proteger la integridad, seguridad, o la operación continua de la TI, o para protegerse a sí misma de algún riesgo o responsabilidad." (Artículo VII, F.)

C. "Las alegadas violaciones a la seguridad y privacidad se referirán a las entidades concernientes para su revisión, auditoría o investigación. La Universidad también podrá referir las presuntas violaciones de ley a las agencias de ley y

orden correspondientes o los cuerpos disciplinarios institucionales correspondientes." (Artículo VII, G.)

E. "Cooperar y colaborar con el personal o autoridad designada cuando se esté investigando o auditando violaciones a la Política." (Artículo VIII, B-6.)

Artículo 4 Propósito y Aplicación

Este procedimiento tiene el propósito de establecer el procedimiento a seguir en situaciones de incidentes en el uso indebido o de incidentes de seguridad en los sistemas de información.

Será de aplicación a todos los usuarios que utilizan la tecnología de información de la Universidad de Puerto Rico.

Artículo 5 Definiciones

A. **Universidad** – Universidad de Puerto Rico

B. **Usuario** – Personal docente, personal no docente, estudiantes, investigadores, y terceros que usan los sistemas de información incluyendo contratistas, consultores y suplidores de la Universidad, o cualquier otro individuo que utilice TI de la Universidad.

C. **Malware** – Programa malicioso cuyo propósito es hacer daño a la TI. El término cobija variantes como viruses, "worms", "trojan horses", "ransomware", "spyware", "adware", "scareware", etc.

D. **Autorización** – Es el proceso mediante el cual se adjudican privilegios a un usuario para el uso de la TI.

E. **TI** – Tecnología de Información: dispositivos electrónicos, redes cableadas e inalámbricas, programados, información digital, comunicaciones electrónicas, cuentas de usuarios y todos los sistemas de información electrónicos.

F. **Sistema de Productividad y Colaboración Institucional -** Plataforma adoptada por la institución para mensajería electrónica, almacenamiento de archivos, videoconferencias, calendario y otros (ej. Google Workspace y Microsoft 365).

G. **Investigadores Forenses** - Oficina Auditoría Interna, consultores contratados y/o agencias externas de ley y orden.

H. **Incidente de Seguridad** – Evento que viola pilares de la seguridad cibernética (confidencialidad, integridad y disponibilidad).

Artículo 6 Procedimiento para someter una querella por el uso indebido de la TI

A. Cuando un usuario o la administración tenga motivos fundados para determinar que la TI están siendo utilizada en violación de las leyes, reglamentos o políticas institucionales de la Universidad por un usuario, se radicará una querella por escrito por parte del personal o administrador que sospecha del mal uso, o del supervisor que recibe la querella para poder proceder con la acción correspondiente. La querella será sometida a un supervisor de mayor rango que se entienda no está envuelto en el uso indebido de los sistemas de información. En tal situación, el personal de supervisión que recibe la querella procederá a orientarse con el personal técnico y legal para determinar la acción a seguir.

Artículo 7 Procedimiento para intervención en caso de eventos de seguridad

A. Cuando se es detectado un evento que compromete la seguridad de la TI, tales como accesos no autorizados, modificación de contenido (*information defacement*), malware, denegación de servicios (DoS), filtración de datos (*data breach*), ransomware u otro, se procederá a notificar inmediatamente al Director de la Oficina de Sistemas de Información de la Unidad para tomar la acción correspondiente que se determine. Esto puede incluir, pero no limitarse a <u>aislar y contener las comunicaciones, equipo o servicios afectados. El personal técnico procederá a atender la situación hasta asegurarse que el evento ha sido debidamente aislado.</u>

B. Se documentará todo evento y la resolución de este. Dependiendo de la severidad e impacto, se notificará a los usuarios, la Oficina de Auditores Internos y/o a las agencias de ley y orden.

C. En caso de determinarse que ha sucedido una destrucción, daño o fuga de información (*data breach*) se procederá a:

   a. Documentar todos los detalles conocidos del incidente:
      i. Fecha y hora conocida del incidente y/o descubrimiento de este.
      ii. Fecha y hora en que se documenta y se informa.
      iii. Descripción de la información afectada o divulgada.
      iv. Mejor estimado de usuarios afectados.
      v. Acción tomada para mitigar el problema que causó el evento.
   b. El Director de la Oficina de Información de la Unidad notificará inmediatamente de tomar conocimiento del incidente al CIO y CISO de la Universidad quienes determinarán si el evento representa un riesgo a la seguridad, privacidad y confidencialidad de los usuarios.
      i. Si representa un alto riesgo por ser datos restrictos, se procederá a notificar a los usuarios afectados y a las agencias reguladoras de la institución dentro de un período no mayor de 72 horas.
      ii. Si no representa riesgo para los usuarios, sólo se notificará a las agencias que se requieran, y se continuará con una investigación que pueda determinar los efectos a la institución.
   c. Se utilizará recursos para investigar todos los detalles del incidente y se documentará todo el proceso y los hallazgos.

Artículo 8 Procedimiento para la intervención del sistema de productividad y colaboración institucional

A. Cuando la Universidad pierde contacto con un usuario custodio de una cuenta institucional, o cuando en una investigación en curso se requiere que se provea la información contenida en el sistema de productividad y colaboración

institucional, como correos electrónicos o documentos almacenados en la plataforma, se referirá la petición de intervención al Director de la Oficina de Sistemas de Información de la Administración Central. Este procederá según se establece en la *Guía para el Intervención de Información en el Sistema de Productividad y Colaboración Institucional*.

Artículo 9 Procedimiento de incautación de cuentas, equipo y manejo de la evidencia

Cuando se determine que una querella tiene fundamentos y se requiere incautar cuentas o equipo como evidencia para continuar la investigación, se realizará el siguiente procedimiento:

A. Se consultará con los investigadores oficiales y con el personal técnico la disponibilidad de las herramientas necesarias para ejecutar la incautación y preservación de la evidencia.
B. En sistemas centralizados, el supervisor inmediato de mayor jerarquía solicitará a la Unidad de TI encargada de los recursos a incautar la cuenta y/o monitorear el sistema (bitácoras) o la cuenta involucrada.
C. Se documentará las condiciones de los equipos a ser incautados (posición, conexiones, área donde se encuentra) y se tomará fotografías o video (pantalla, conexiones, parte delantera y trasera del equipo). Además, el área donde se encuentra la escena será verificada sistemáticamente y documentada, tomando nota principalmente de evidencia de daños preexistentes.

D. En sistemas centralizados donde no es práctico remover la evidencia física de la escena, será copiada la evidencia digital mediante procedimiento forense. Para dicho propósito se utilizará el equipo adecuado y se deberá cumplir con los siguientes:

    1. El personal involucrado debe ser removido de los predios donde se encuentra la evidencia y sus accesos deben ser suspendidos. El personal involucrado puede pedir representación de un tercero que sirva como testigo del procedimiento que se realizará.

2. Mientras sea posible, el equipo será aislado de la red.

3. Se consultará con el personal de investigación forense el manejo inicial de intervención para no afectar la investigación. Se determinará, en coordinación con la gerencia institucional, si el impacto en los procesos requiere que se mantenga los sistemas disponibles para ejecutar el procedimiento forense.

F. Imágenes forenses serán almacenadas y custodiadas de la misma forma que la evidencia original. Más de una copia puede ser requerida y almacenada en lugares diferentes.

J. El análisis del equipo y la información adquirida como evidencia debe hacerse con requerimientos que serán determinados caso por caso, en común conocimiento de todas las partes involucradas, con la debida asesoría legal y técnica. Todos los procedimientos deben ser documentados detalladamente y reproducibles por diferente personal técnico.