Universidad Veracruzana

Incidentes de seguridad de la información

Ciberseguridad
UV-CSIRT

Información segura... ¡es cultura!®

Incidentes de seguridad de la información

Actualmente es más frecuente escuchar o ver noticias que nos informan sobre diversos ataques cibernéticos como phishing, malware, botnets, etc. y que se ejecutan tanto en empresas privadas como instituciones públicas, a estos ataques que sufren los sistemas conectados a Internet, y que afectan la confidencialidad, disponibilidad o la integridad de la información de cualquier empresa se les conoce como incidentes de seguridad de la información.
Recuerda que tú, como estudiante, académico o personal administrativo juegas un papel muy importante en la seguridad de la información, por lo anterior, a continuación, te compartimos los principales tipos de incidentes de seguridad a los que pudieras estar expuesto:

Identificación de un Incidente

Tipos de incidentes

A continuación, se describen algunos de los diferentes tipos de incidentes de seguridad y en qué consisten para que conozcas cómo identificarlos.

1. Infecciones por código malicioso de sistemas, equipos de trabajo o dispositivos móviles:

Este tipo de incidentes, son ocasionados por la ejecución de código malicioso como virus, scripts, gusanos, etc. iniciados en su mayoría a través de correo electrónico, páginas web comprometidas o maliciosas, SMS o redes sociales.

2. Acceso no autorizado a un sistema, robo o pérdida de datos:

- **Acceso no autorizado:** Estos incidentes se producen cuando un ciberdelincuente logra tener acceso a un sistema o recurso técnico de forma física o remota, ocasionando el borrado, modificación o extracción de información. Algunos de estos incidentes se

Incidentes de seguridad de la información

llevan a cabo mediante el uso de técnicas de ingeniería social en los que los usuarios son víctimas de engaños y proporcionan información personal o de la organización a la que pertenece.

• **Robo o pérdida de datos:** son incidentes que pueden presentarse al haber algún acceso no autorizado a equipos personales, recursos físicos o sistemas de tecnologías de la información, ocurren cuando hay una sustracción o pérdida parcial o total de la información comprometiendo la seguridad, integridad o confidencialidad de esta.

3. Fallos de disponibilidad: Estos incidentes se producen cuando existe una interrupción en algún servicio o recurso de tecnologías de la información, impidiendo el funcionamiento normal o provocando que no se pueda acceder a la información que se aloja en estos.
Algunos de estos incidentes son provocados por los conocidos ataques de denegación de servicio o por su acrónimo en inglés DOS o DDOS.

Estos pueden perjudicar a diferentes recursos tecnológicos como redes, servidores, computadoras, sistemas, etc., en los cuales los sistemas ante una saturación de peticiones no son capaces de responder ocasionando su interrupción.

4. Daño Físico: Se pueden presentar cuando existe algún daño físico derivado de alguna falla en los sistemas o en los equipos, servidores o cableado, originados de forma accidental, intencional o por eventos naturales como una inundación.

5. Fraudes: Son provocados principalmente mediante la suplantación de organizaciones o empresas legítimas como instituciones financieras o instituciones públicas. El objetivo principal de estos incidentes es engañar a los usuarios para obtener información confidencial. Los medios por los cuales regularmente se realizan estos engaños son a través de correo electrónico, sitios web falsos o llamadas telefónicas.

Incidentes de seguridad de la información

Gestión de incidentes a cargo de un equipo de respuesta a incidentes de seguridad, CSIRT

Ahora que sabemos el impacto que podría ocasionar la presencia de un incidente de seguridad en las empresas e instituciones, es fundamental que éstas cuenten con mecanismos de respuesta rápidas a incidentes de seguridad de la información para evitar que se expongan a pérdidas irreversibles de información. Para ello, existe dentro de las organizaciones áreas de seguridad conocidas como equipos de respuesta a incidentes de seguridad o también llamados CERT o CSIRT que apoyan en la gestión de estos incidentes.

La Universidad Veracruzana cuenta con un equipo de respuesta a incidentes de seguridad denominado UV-CSIRT, esta área tiene como funciones principales prevenir, identificar, analizar y dar respuesta a estos incidentes, al ser un área institucional sus servicios se enfocan solo a dar atención a incidentes que afecten a los servicios de tecnologías de la información que esta institución ofrece.

Por lo antes mencionado, si identificas alguno de estos incidentes puedes comunicarte a esta área que te podrá asesorar, el UV-CSIRT te ofrece diferentes recursos para reportar un incidente ya sea a través de su portal web en el apartado de “Reporta un incidente” en el enlace https://www.uv.mx/csirt/reporta-un-incidente-de-ciberseguridad/ o a través de correo electrónico a la cuenta de contactocsirt@uv.mx

Ciberseguridad
UV-CSIRT

a incidentes de ciberseguridad en la UV

Prevenir siempre es mejor

Por todo lo anterior, es imprescindible estar atentos para identificar cuando ocurre un incidente, y como responder ante estos, por ello es importante que sigas las recomendaciones que a continuación te compartimos para proteger tu información y crear una comunidad segura:

Incidentes de seguridad de la información

Recomendaciones para evitar ser víctima de un incidente de seguridad

- Instala y actualiza en los dispositivos de escritorio o móviles programas de protección de datos y antivirus para empresas.
- Actualiza constantemente aplicaciones y sistema operativo.
- Utiliza contraseñas seguras y diferentes para los dispositivos electrónicos y servicios.
- No abras correos electrónicos sospechosos y, en caso de hacerlo, no proporcionar datos confidenciales ni descargar archivos adjuntos.
- No compartir información confidencial fuera de los canales propios de la organización.
- No des clic a enlaces sospechosos en sitios web o de anuncios publicitarios.
- Realizar de forma frecuente copias de seguridad.
- Cifrar la información confidencial.

Recuerda visitar el sitio web de UV-CSRIT y seguir sus redes sociales donde además puedes obtener información de alertas sobre las ciberamenazas más recientes.

www.uv.mx/csirt
Facebook: /uvcsirt
Twitter: @uvcsirt

Referencias:

https://www.incibe.es/protege-tu-empresa/blog/incidentes-seguridad-conoce-tus-enemigos
https://www.incibe.es/protege-tu-empresa/tematicas/gestion-incidentes-seguridad
https://www.uv.mx/infosegura/videos/infosegura-rol-del-usuario/
https://www.uv.mx/infosegura/videos/ciberamenazas/
https://www.uv.mx/infosegura/videos/induccion-a-la-seguridad-de-la-informacion-2/