

CIBERSEGURIDAD, SEGURIDAD INFORMÁTICA Y SEGURIDAD E LA INFORMACIÓN

J. P. Araiz López

7690-17-9477 Universidad Mariano Gálvez

Seminario de Tecnologías de Información

jaraizl@miumg.edu.gt

9 de agosto de 2024

Resumen

En este artículo hablaremos un poco sobre la ciberseguridad, la seguridad de la información y la seguridad informática ya que son conceptos interrelacionados pero con enfoques distintos, la ciberseguridad se refiere a la protección de sistemas informáticos y redes contra ataques cibernéticos, que pueden involucrar malware, phishing, o hacking, la seguridad de la información tiene un alcance más amplio e incluye la protección de todos los tipos de información, ya sea digital, física o verbal y la seguridad informática, por su parte, se enfoca específicamente en la protección de sistemas informáticos y los datos que estos procesan.

Palabras Clave

Ciberataque, Vulnerabilidad, Seguridad

Ciberseguridad

Es la acción de proteger los equipos, redes, aplicaciones o cualquier dispositivo electrónico de cualquier posible amenaza digital o ciberataque. Los ciberataques tienen el poder de interrumpir, dañar o destruir empresas por lo que se busca mitigar o eliminar los riesgos que estos presentan mediante buenas practicas.

Amenazas más comunes de ciberseguridad

- **Malware:** el denominado software malicioso, es cualquier código o programa informático realizado de manera intencionada para dañar algún sistema informático.
- **Ransomware:** es un tipo de malware específicamente para encriptar datos o dispositivos con la intención de solicitar un rescate por la recuperación de los mismos.
- **Phishing:** principalmente mensajes de correo electronico, texto o mensaje de voz que se utiliza para engañar a los usuarios.

- Inyección de código SQL: utilizado para tomar el control y robar información específicamente de una base de datos.
- Man-in-the-middle: son aquellos ataques en los que el cibercriminal intercepta la comunicación entre dos medios para robar datos.
- Ataque de denegación de servicios (DDoS): se enfocan en bloquear un servicio específico utilizando la sobrecarga de tráfico, normalmente se utiliza un botnet o una red de servicio para secuestrar el servicio.
- Amenaza interna: es un riesgo de seguridad introducido por un personal o usuario con malas intenciones dentro de la organización.

Seguridad Informática

Constituye un amplio conjunto de medidas o acciones de protección para evitar que una red informática y sus datos sufran alguna vulneración o ataque. La seguridad informática es esencial para la prevención de ataques ya que cada vez existe un riesgo mayor para todos los dispositivos que se conectan a una red.

Tipos de seguridad Informática

- Seguridad de red: se centra en el resguardo y seguridad de la red informática, impidiendo accesos no autorizados a los recursos de red, detectar posibles ataques o violaciones de red y garantizar al usuario un acceso seguro a los recursos en la red.
- Seguridad de aplicaciones: son las medidas que se toman los desarrolladores al momento de crear una aplicación para protegerse de cualquier vulnerabilidad y a su vez puedan proteger sus datos.
- Seguridad en internet: proporcionan seguridad al navegar por internet, utilizando cortafuegos que salvaguardan los datos que se procesan en el navegador al utilizar el internet.
- Seguridad en la nube: se ha convertido en un elemento básico en la seguridad informática, debido al crecimiento en la utilización de la nube, en general se utilizan software para garantizar la seguridad de aplicaciones o datos publicados en la nube.
- Seguridad de terminales: sirve para la protección de dispositivos personales como son los móviles, entre otros.

Seguridad de la información

Seguridad de la información se refiere al conjunto de procedimientos, acciones o herramientas utilizadas para proteger la integridad de los datos, contra cualquier acceso, divulgación o uso no autorizado.

0.1. Principios de la seguridad de la información

La CID, presentada en 1977 tiene como objetivo guiar a las organizaciones en la elección de tecnologías, políticas y prácticas para la protección de los sistemas de información. La CID esta compuestas por estos elementos:

- Confidencialidad: ninguna persona puede acceder a datos para lo que cuales no se tiene autorización.
- Integridad: toda información contenida en las bases de datos es completa, precisa y no ha sido manipulada.
- Disponibilidad: los usuarios pueden acceder a la información a la que se está autorizado cuando le sea necesario.

Observaciones y Comentarios

Los temas de ciberseguridad, seguridad informática y seguridad de la información aunque pareciesen lo mismo no lo son, cada uno tiene un enfoque específico y aunque puedan ser parte de un mismo entorno cada uno con lleva ciertas practicas especificas que unidas todas ayudan a evitar o mitigar cualquier ataque mal intencionado que puedan recibir nuestras aplicaciones o dispositivos.

Conclusiones

La seguridad informática, seguridad de la información y ciberseguridad, son temas que han tenido un aumento de importancia a nivel mundial, ya que el aumento de las tecnologías y que cada vez el mundo está más conectado ha implicado también un aumento en los ataques de personas mal intencionadas, por lo que se hace vital poder estar al día con estas buenas prácticas para evitar un riesgo que represente pérdidas para las empresas.

Referencias

- [1] *¿Qué es la ciberseguridad?* [En línea]. Disponible en:
<https://aws.amazon.com/es/what-is/cybersecurity/>
- [2] *¿Qué es la ciberseguridad?* [En línea]. Disponible en:
<https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security>
- [3] *¿Qué es la ciberseguridad?* [En línea]. Disponible en:
<https://www.ibm.com/es-es/topics/cybersecurity>
- [4] *¿Qué es la seguridad de TI?* [En línea]. Disponible en:
<https://www.ibm.com/mx-es/topics/it-security>

[5] *¿Qué es la seguridad de la información?* [En línea]. Disponible en:
<https://www.ibm.com/es-es/topics/information-security>

Repositorio git disponible en:
<https://github.com/JaraizL/SEMINARIO-DE-TECNOLOG-AS.git>