

INGENIERÍA DE SISTEMAS

Ciberseguridad
Prof. Claudia Muñoz



Universidad
del Valle

Introducción a la Ciberseguridad

La ciberseguridad es el conjunto de prácticas, tecnologías y estrategias destinadas a proteger sistemas informáticos, redes, dispositivos y datos contra amenazas digitales. Su objetivo principal es evitar el acceso no autorizado, el daño, la alteración o el robo de información.



Importancia de la Ciberseguridad

- La ciberseguridad es crucial no solo para las grandes empresas o gobiernos, sino también para los usuarios individuales. Los ataques informáticos pueden tener consecuencias graves, como el robo de datos personales, el secuestro de información a través de ransomware, o la interrupción de servicios esenciales.



Tipos de amenazas de la Ciberseguridad

- **Malware:** Programas maliciosos como virus, troyanos y ransomware que infectan los sistemas para dañar o robar datos.
- **Phishing:** Técnicas de fraude en línea que intentan engañar a los usuarios para que proporcionen información personal o financiera.



Tipos de amenazas de la Ciberseguridad

- **Ataques de denegación de servicio (DDoS):** Atacar servidores o redes con tráfico masivo para interrumpir el servicio y hacerlo inaccesible.



- **Hackeo:** Acceso no autorizado a sistemas y redes con fines de robo de datos o espionaje.



Principios de la Ciberseguridad

Podemos decir que los principios de la seguridad informática son un conjunto de protocolos, medidas y operaciones destinadas a reducir los riesgos ante los problemas informáticos, a detectar y prevenir amenazas y a garantizar la recuperación del sistema.



Los principios básicos de la ciberseguridad son fundamentales para construir una base sólida que permita proteger tanto la información como los sistemas y las redes. Estos principios son cruciales para reducir las vulnerabilidades y responder de manera efectiva a posibles amenazas.





¿Qué es la tríada CIA o CID?

Las tres letras de la "tríada de la CID" significan confidencialidad, integridad y disponibilidad. La tríada de la CID es un modelo común que constituye la base para el desarrollo de sistemas de seguridad. Se utilizan para encontrar vulnerabilidades y métodos para crear soluciones.





What Does CIA Stand For?



Confidentiality



Integrity



Availability

Confidencialidad

La información no debe divulgarse a personas, grupos, organizaciones o procesos no autorizados. Los datos son confidenciales cuando solo las personas autorizadas acceden a ellos.



Disponibilidad

información debe estar disponible cuando se necesite. Si bien debemos asegurarnos de que grupos no autorizados no puedan acceder a los datos, también debemos asegurarnos de que aquellos que tengan el permiso adecuado puedan acceder a ellos en todo momento.



Integridad

La integridad se trata de garantizar que los datos no hayan sido manipulados y, por lo tanto, que se pueda confiar en ellos. El objetivo de este principio es salvaguardar la exactitud e integridad de los datos en todo momento.



Principales Fallos de seguridad de la información

1

Falta de políticas de seguridad de la información

2

Problemas de control de usuarios

3

Comprometimiento de información confidencial

4

Falta de capacitaciones e instrucciones

La **ciberseguridad** es la práctica de proteger equipos, redes, aplicaciones de software, sistemas críticos y datos de posibles amenazas digitales. Las organizaciones tienen la responsabilidad de proteger los datos para mantener la confianza del cliente y cumplir la normativa. Utilizan medidas y herramientas de ciberseguridad para proteger los datos confidenciales del acceso no autorizado, así como para evitar interrupciones en las operaciones empresariales debido a una actividad de red no deseada. Las organizaciones implementan la ciberseguridad al optimizar la defensa digital entre las personas, los procesos y las tecnologías.



Tipos de ciberseguridad

Seguridad de la red: Es una protección de ciberseguridad para los equipos y dispositivos conectados a una red.



Tipos de ciberseguridad

Seguridad en la nube: Describe las medidas que toma una organización para proteger los datos y las aplicaciones que se ejecutan en la nube. Es importante para reforzar la confianza del cliente, proteger las operaciones tolerantes a errores y cumplir con la normativa de la privacidad de datos en un entorno escalable.



Tipos de ciberseguridad

Seguridad de IoT: Dispositivos electrónicos que funcionan remotamente en Internet.



Tipos de ciberseguridad

Seguridad de los datos: La seguridad de los datos protege los datos en tránsito y en reposo con un sistema sólido de almacenamiento y una transferencia de datos segura. Los desarrolladores usan medidas protectoras, como el cifrado y las copias de seguridad aisladas, para la resistencia operativa frente a posibles brechas de seguridad.



Tipos de ciberseguridad

Seguridad de las aplicaciones: La seguridad de las aplicaciones es un trabajo coordinado para fortalecer la protección de una aplicación frente a la manipulación no autorizada durante las etapas de diseño, desarrollo y prueba. Los programadores de software escriben códigos seguros para evitar errores que puedan aumentar los riesgos de seguridad.



Tipos de ciberseguridad

Seguridad de los puntos de conexión: La seguridad de los puntos de conexión aborda los riesgos de seguridad que surgen cuando los usuarios acceden remotamente a la red de una organización.



Tipos de ciberseguridad

Planificación de la recuperación de desastres y continuidad del negocio: Describe los planes de contingencia que permiten a una organización responder de inmediato a incidentes de ciberseguridad mientras continúa funcionando con pocas o ninguna interrupción. Implementan políticas de recuperación de datos para responder positivamente a las pérdidas de datos.



¡Preguntas!