Principios de Seguridad Informática y Tipos de Malware

Autor: Robert Alberto Pertuz

Universidad

Curso: Seguridad Informática

Fecha: 23 de April de 2025

Confidencialidad, Integridad y Disponibilidad (CID)

Confidencialidad: Protege la información sensible asegurando que solo personas autorizadas accedan a ella. Se aplica mediante cifrado, controles de acceso y autenticación (Stallings, 2018). Una fuga de información puede tener consecuencias legales y éticas.

Integridad: Garantiza que los datos no sean modificados de forma no autorizada. Se asegura con hashes y control de versiones. Si se compromete, los datos pueden perder fiabilidad (Whitman & Mattord, 2022).

Disponibilidad: Asegura que los sistemas estén accesibles cuando se necesiten. Se logra con respaldo, redundancia y planes de recuperación. La falta de disponibilidad puede perjudicar seriamente la continuidad de las operaciones.

Ejemplos Prácticos de Aplicación

Confidencialidad: En una clínica, el acceso a los historiales médicos se protege con MFA y cifrado. Esto garantiza la protección de los datos del paciente.

Integridad: Una empresa de software usa hashes para validar actualizaciones. Si el hash no coincide, se impide la instalación, evitando la manipulación.

Disponibilidad: Un banco implementa servidores redundantes. En caso de fallo, el servicio se mantiene, previniendo pérdidas económicas.

Reflexión Comparativa entre CID

Los tres principios se relacionan y se complementan. Una pérdida de confidencialidad puede llevar a manipulaciones (falla de integridad). Si el sistema no está disponible, no se puede verificar la integridad ni

mantener confidencialidad (Stallings, 2018).

Preguntas de reflexión:

- En salud, la confidencialidad es prioritaria por la sensibilidad de los datos.

- En comercio electrónico, la disponibilidad es clave para mantener la operación continua.

- En organizaciones con recursos limitados, es recomendable empezar por asegurar la disponibilidad, luego la integridad y por último la confidencialidad.

Tipos de Malware y sus Impactos

Virus: Se adjunta a programas. Ej.: virus en correo electrónico. Impacto: daño a archivos, propagación en red.

Gusano: Se propaga automáticamente en red. Ej.: saturación de red empresarial. Impacto: lentitud, caída del sistema.

Troyano: Finge ser legítimo. Ej.: software descargado desde fuente dudosa. Impacto: acceso remoto, robo de datos.

Ransomware: Cifra archivos y exige rescate. Ej.: correo con enlace malicioso. Impacto: pérdida de acceso, posibles pagos económicos.

Spyware: Espía sin consentimiento. Ej.: software gratuito malicioso. Impacto: robo de información personal o financiera.

Referencias

Stallings, W. (2018). *Cryptography and Network Security: Principles and Practice* (7a ed.). Pearson.

Whitman, M. E., & Mattord, H. J. (2022). *Principles of Information Security* (7a ed.). Cengage Learning.