**Integridad de Archivos: Un Pilar de la Ciberseguridad**

**Descripción:**

La **integridad de archivos** se refiere a la protección de los archivos contra alteraciones no autorizadas. Asegurar que los archivos no hayan sido modificados de manera inapropiada es crucial para mantener la confianza en la precisión y la fiabilidad de los datos. Mediante técnicas como el uso de sumas de verificación (hashes) y firmas digitales, se puede verificar la autenticidad de los archivos y detectar posibles manipulaciones, protegiendo así la integridad de la información crítica en sistemas informáticos.

**Métodos para Asegurar la Integridad de Archivos**

Para garantizar la integridad de los archivos, se utilizan diversos métodos y técnicas, tales como:

1. **Sumas de Verificación (Hashing):** Se generan valores únicos (hashes) para cada archivo mediante algoritmos como MD5, SHA-1 o SHA-256. Cualquier cambio en el archivo resulta en un hash diferente, permitiendo la detección de modificaciones.
2. **Firmas Digitales:** Se aplican criptográficamente para verificar la autenticidad del origen y la integridad del archivo. Una firma digital asegura que el archivo proviene de una fuente confiable y que no ha sido alterado desde su creación.
3. **Control de Acceso:** Implementar políticas estrictas sobre quién puede acceder y modificar los archivos. Esto incluye el uso de permisos adecuados y autenticación fuerte para proteger archivos críticos de cambios no autorizados.
4. **Monitoreo y Auditoría:** Realizar un seguimiento constante de los archivos para detectar y registrar cualquier cambio. Esto incluye el uso de herramientas de monitoreo que alertan sobre modificaciones inesperadas.

Estos métodos ayudan a prevenir y detectar posibles brechas de seguridad y a mantener la integridad y confiabilidad de los datos almacenados.