**Hashing y su importancia en ciberseguridad**

Contenido de las diapositivas

* Cabecera Introducción al Hashing

Contenido El hashing es una técnica clave en ciberseguridad que transforma datos en una cadena única de caracteres de longitud fija. Es esencial para proteger contraseñas y verificar la integridad de datos.

* Cabecera Objetivo de la Sesión

Contenido Entender la función del hashing en la ciberseguridad y aprender a usar funciones de hashing en sistemas Linux.

* Cabecera Conceptos Clave de Hashing

Contenido Propiedades del hashing: determinismo, resistencia a colisiones y preimágenes. Aplicaciones principales: gestión de contraseñas y verificación de integridad de archivos.

* Cabecera Función del Hashing en Seguridad

Contenido El hashing es usado para asegurar contraseñas en bases de datos, evitando almacenamiento de textos claros, y para verificar que archivos no han sido manipulados.

* Cabecera Demostración Práctica

Contenido Uso de comandos de hashing en Linux, como `md5sum` y `sha256sum`, para generar y verificar hashes de archivos, asegurando su integridad.

* Cabecera Discusión: Experiencias con Hashing

Contenido Intercambio de experiencias sobre la implementación de hashing en seguridad personal y profesional, analizando beneficios y limitaciones.

* Cabecera Conclusión y Preguntas

Contenido Reflexión sobre la importancia del hashing y sus aplicaciones en la protección de datos. Zona de preguntas para aclarar dudas.