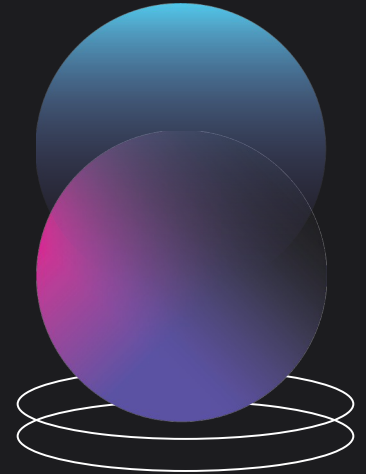
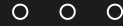


Seguridad en Redes

Frann Fons

Conceptos y Fundamentos en la Protección de Datos





Introducción

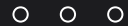
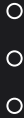
La seguridad en redes es un aspecto crucial en la era digital actual, protegiendo la integridad y confidencialidad de los datos. Este curso explorará amenazas comunes y estrategias defensivas esenciales, proporcionando conocimientos sobre conceptos y técnicas prácticas.

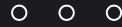




01

Qué es Seguridad en Redes





Definición de Seguridad Informática

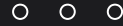
La seguridad informática refiere a la protección de sistemas informáticos y datos contra accesos no autorizados, modificaciones o destrucción. Esto incluye la implementación de políticas y herramientas para salvaguardar la información tanto en entornos personales como corporativos.



Objetivo Principal de la Seguridad

El objetivo principal de la seguridad es garantizar la disponibilidad, integridad y confidencialidad de los activos digitales. Esto implica asegurar que la información esté accesible solo a los usuarios autorizados, permanezca inalterada y esté disponible cuando se necesite.






Concepto de Seguridad en Redes

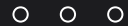
La seguridad en redes se refiere al conjunto de políticas, prácticas y herramientas diseñadas para proteger la infraestructura de red contra accesos no autorizados y ataques cibernéticos. Es esencial para la protección de datos y sistemas dentro de cualquier organización, asegurando que los recursos de red sean utilizados de manera segura y efectiva.





02

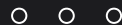
Principios Clave



Confidencialidad

La confidencialidad en la seguridad de redes garantiza que solo los usuarios autorizados puedan acceder a la información. Esto se logra mediante mecanismos de control de acceso, encriptación de datos y autenticación de usuarios, evitando que terceros no autorizados tengan acceso a información sensible.





Integridad

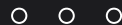
La integridad se refiere a la protección de la información contra modificaciones no autorizadas. Esto implica no solo la validación de la autenticidad de los datos, sino también mecanismos que aseguren que la información se mantenga sin cambios durante su transmisión o almacenamiento, detectando posibles alteraciones.



Disponibilidad

La disponibilidad asegura que los sistemas y datos estén accesibles en todo momento para los usuarios autorizados. Esto incluye la implementación de medidas como redundancia, copias de seguridad y actualizaciones constantes, minimizando así los tiempos de inactividad y garantizando la continuidad del servicio.





Conclusiones

La comprensión y aplicación de los principios clave de la seguridad en redes es vital para cualquier organización. Al asegurar la confidencialidad, integridad y disponibilidad de la información, se puede crear un entorno digital más seguro, protegiendo los activos digitales y previniendo posibles ataques y vulnerabilidades.

