PROTECCIÓN DE DISPOSITIVOS

JAVIER PÉREZ MOLINERO

Introducción

- A- Importancia de la seguridad informatica.
  - 1-Protección de datos personales y sensibles.
  - 2-Prevención del robo de identidad y fraudes
  - 3-Protección contra ciberataques
  - 4-Preservación de la privacidad
  - 5-Cumplimiento legal y regulaciones
- B- Objetivo de la presentación.
  - Sensivilización de la importancia de proteger nuestros dispositivos.

A- Importancia de la seguridad informatica

1-PROTECCIÓN DE DATOS PERSONALES Y SENSIBLES

En un mundo cada vez más conectado, almacenamos una cantidad considerable de información personal y sensible en nuestros dispositivos electrónicos. Esto incluye detalles como nombres, direcciones, números de teléfono, información financiera y de tarjetas de crédito. La seguridad informática garantiza que esta información esté protegida contra accesos no autorizados, robos de identidad y fraudes financieros.

A- Importancia de la seguridad informatica

2-PREVENCIÓN DE ROBO DE IDENTIDAD Y FRAUDES

El robo de identidad es un delito en el que un individuo utiliza la información personal de otra persona sin su consentimiento para cometer fraudes o delitos financieros. La seguridad informática ayuda a prevenir el robo de identidad al proteger la información personal y asegurar que solo las personas autorizadas tengan acceso a ella.

A- Importancia de la seguridad informatica

3-PROTECCIÓN CONTRA CIBERATAQUES

Los ciberataques son cada vez más comunes y sofisticados, y pueden tener consecuencias devastadoras para individuos, empresas, escuelas e incluso para la infraestructura crítica de un país. Estos ataques pueden incluir malware, ransomware, phishing, ataques de denegación de servicio (DDoS), entre otros. La seguridad informática ayuda a proteger los dispositivos y redes contra estos ataques, minimizando el riesgo de interrupciones, pérdida de datos y daños financieros.

A- Importancia de la seguridad informatica

4-PRESERVACIÓN DE LA PRIVACIDAD

La seguridad informática también es esencial para preservar la privacidad de los usuarios en línea. Esto implica proteger la comunicación electrónica, las actividades en línea y la información personal de la vigilancia no autorizada, tanto por parte de gobiernos como de empresas privadas.
La implementación de medidas de seguridad, como la encriptación de datos y el uso de redes privadas virtuales (VPN), ayuda a proteger la privacidad en línea..

A- Importancia de la seguridad informatica

5-CUMPLIMENTO LEGAL Y REGULACIONES

Existen leyes y regulaciones que requieren que las organizaciones y los individuos protejan la información confidencial y cumplan con ciertos estándares de seguridad cibernética. Esto es especialmente importante en sectores como la salud, las finanzas, empresas e instituciones publicas, donde la privacidad y la seguridad de los datos son críticas.
La seguridad informática ayuda a garantizar el cumplimiento de estas leyes y regulaciones, evitando posibles sanciones y multas.

B- OBJETIVO DE LA PRESENTACIÓN

La sensibilización sobre la importancia de proteger nuestros dispositivos informáticos es fundamental en la sociedad digital actual. Esta conciencia ayuda a prevenir el robo de datos personales, la exposición a ciberataques y el riesgo de pérdida de privacidad.

Proteger nuestros dispositivos no solo salvaguarda nuestra información personal y financiera, sino que también contribuye a mantener la integridad de la infraestructura digital y la confianza en el uso de la tecnología.

Promover la seguridad informática entre los usuarios es clave para mitigar riesgos y garantizar una experiencia en línea segura y protegida. Donde la privacidad y la seguridad de los datos son críticas. La seguridad informática ayuda a garantizar el cumplimiento de estas leyes y regulaciones, evitando posibles sanciones y multas.

Como podemos mitigar estos riesgos:

- Actualización de sofware
- Instalación de antivirus y firewall
- Crear contraseñas seguras.
- Copias de seguridad
-

Actualización del software

La actualización del software es crucial en la protección de nuestros dispositivos informáticos. Estas actualizaciones contienen parches de seguridad que corrigen vulnerabilidades descubiertas por los desarrolladores o reportadas por la comunidad.

Mantener el software actualizado asegura que nuestras aplicaciones y sistemas operativos estén equipados con las últimas defensas contra malware, virus y otras amenazas cibernéticas.

Además, las actualizaciones suelen incluir mejoras en el rendimiento y nuevas funcionalidades, lo que garantiza una experiencia más fluida y segura para el usuario.

Actualización del software

Ignorar las actualizaciones puede dejar nuestros dispositivos vulnerables a exploits conocidos, aumentando el riesgo de compromiso de datos y pérdida de privacidad.
La actualización regular del software es una práctica fundamental para mantener la seguridad y el rendimiento óptimo de nuestros dispositivos informáticos.

Instalación de antivirus y firewall

La instalación de un antivirus y un firewall es esencial para proteger nuestros dispositivos informáticos contra una amplia gama de amenazas cibernéticas.

Los antivirus detectan y eliminan malware, como virus, troyanos y spyware, que pueden comprometer la seguridad de nuestros sistemas y robar información personal.

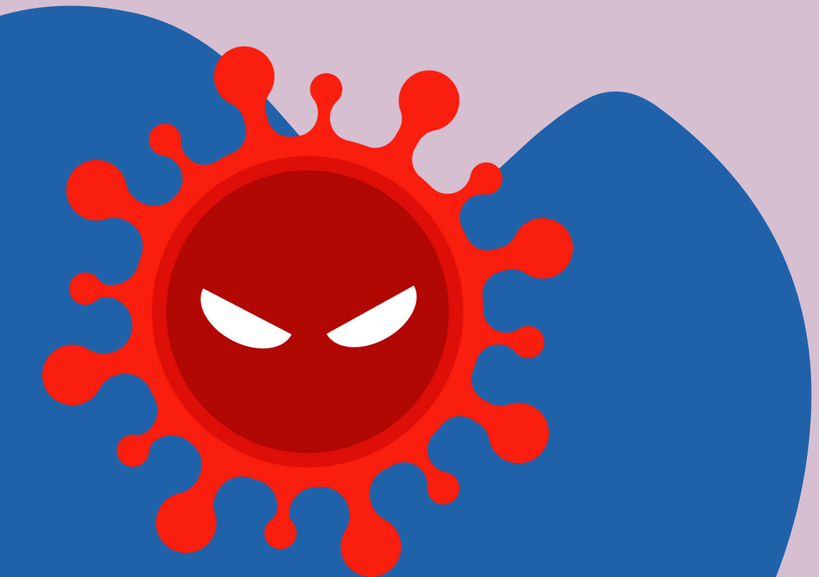
Los firewalls actúan como una barrera defensiva, monitoreando y controlando el tráfico de red entrante y saliente.

Esto ayuda a prevenir intrusiones no autorizadas y protege contra ataques de hackers y malware que intentan acceder a nuestros dispositivos a través de internet.

tivirus y un firewall proporcionan una capa adicional de seguridad ayuda a mantener nuestros datos seguros y nuestra privacidad la mientras navegamos por la web y utilizamos aplicaciones en línea.

Instalación de antivirus y firewall

Esto ayuda a prevenir intrusiones no autorizadas y protege contra ataques de hackers y malware que intentan acceder a nuestros dispositivos a través de internet.
Un antivirus y un firewall proporcionan una capa adicional de seguridad que ayuda a mantener nuestros datos seguros y nuestra privacidad protegida mientras navegamos por la web y utilizamos aplicaciones en línea.



CREAR UNA CONTRASEÑA SEGURA

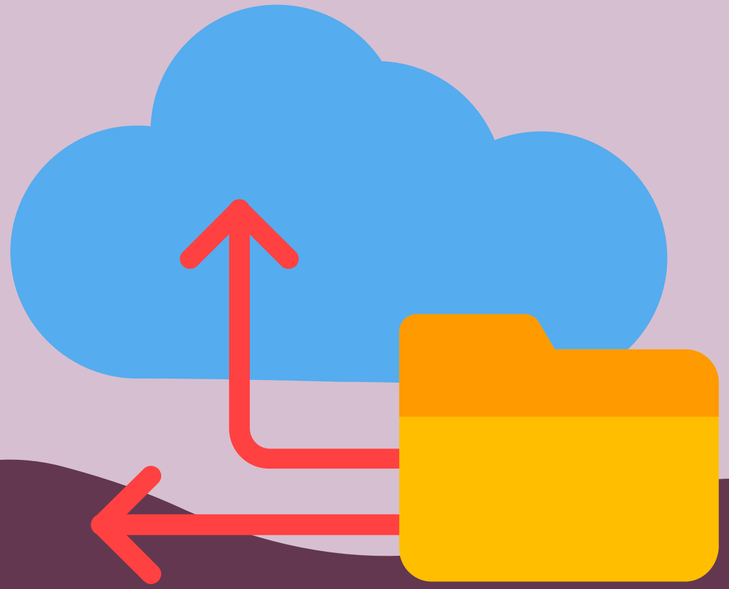
Crear contraseñas seguras es fundamental para proteger nuestras cuentas y datos en línea. Una contraseña segura debe ser lo suficientemente compleja como para ser resistente a los intentos de hacking, pero lo suficientemente fácil de recordar para que no tengamos que escribirla o almacenarla en lugares inseguros.

Pautas a seguir para crear contraseñas

- Longitud adecuada.
- Combinación de caracteres
- Evita información personal
- No uses palabras conmunes
- Contraseña unicas
- Actualiza regularmente
- Considera el uso de frases de contraseña
- Utiliza gestores de contraseñas.

COPIAS DE SEGURIDAD

Realizar copias de seguridad regulares es esencial para proteger nuestros datos contra pérdidas accidentales, ataques de malware o fallos del sistema.



Razones para realizar copias de seguridad

- Prevención de pérdidas de datos.
- Recuperación rápida
- Protección contra ransomware.
- Conservación de la información historica.
- Cumplimento normativo.
- Migración y actualización de sistemas.

Herramientas para realizar copias de seguridad

- Time Machine (macOS)
- Windows Backup (Windows)
- Onedrive
- Disco duros

Recursos didacticos

https://youtu.be/uCaoUBVYPOM?feature=shared

https://youtu.be/uCaoUBVYPOM?feature=shared

https://youtu.be/uCaoUBVYPOM?feature=shared

GRACIAS

Entre todos conseguiremos un mundo digital mas seguro