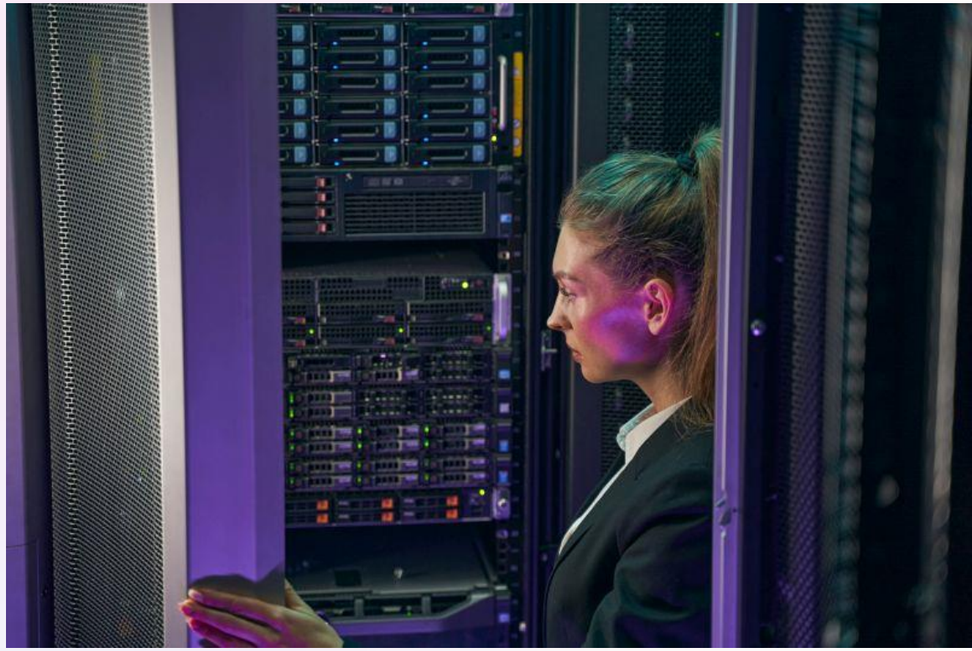
Guía de seguridad y buenas prácticas en ciberseguridad



La ciberseguridad es fundamental en el mundo digital. Descubre cómo proteger tus datos y prevenir ataques.

Introducción a la Ciberseguridad

Importancia

La seguridad es clave en la era digital. Protege tus datos y evita el robo de información personal y profesional.

1

Definición

La ciberseguridad es la práctica de proteger dispositivos, redes y software de ataques maliciosos.

2

3

Tipos de ataques cibernéticos

Desde el phishing hasta el ransomware, explora los principales riesgos que enfrentamos en línea.

Principales riesgos cibernéticos y cómo prevenirlos

Phishing

Cuida lo que compartes en línea y no hagas clic en enlaces sospechosos.

Ransomware

Si tienes datos importantes, haz copias de seguridad regulares y protege tus dispositivos con antivirus y firewalls.

Hackeo de redes Wifi

No compartas tu Wi-Fi con nadie, usa contraseñas seguras y haz una copia de seguridad regularmente.

Malware

Descarga software sólo de fuentes confiables y mantén tus sistemas operativos y antivirus actualizados.

Buenas prácticas para proteger los datos personales

Contraseñas fuertes

Usa contraseñas seguras y cámbialas regularmente, combina mayúsculas, minúsculas, números y símbolos.

Información personal

No compartas información personal, como números de seguro social, direcciones o fechas de nacimiento en línea.

Redes sociales

Vigila la privacidad y no publiques información importante sobre ti o tu familia.

Correos electrónicos

Evita compartir información privada por correo electrónico. Verifica siempre la dirección y el remitente.

Qué es la ingeniería social y cómo evitar caer en sus trampas

1

Definición

La ingeniería social es el término que se utiliza para el conjunto de técnicas de manipulación psicológica que utilizan los ciberatacantes.

2

Tipos de ingeniería social

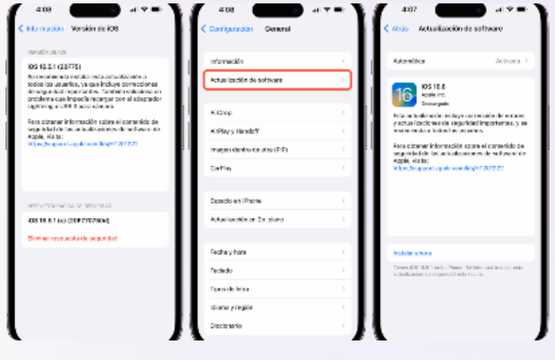
La suplantación de identidad, la creación de falsos sitios web, y la pesca de información son algunas de las técnicas más utilizadas.

3

Cómo evitarlos

Mantén tus datos privados y ten cuidado con tus interacciones en línea. Usa software de seguridad y verifica la legitimidad de los sitios web antes de compartir información.

Cómo mantener actualizado el software y los sistemas de seguridad

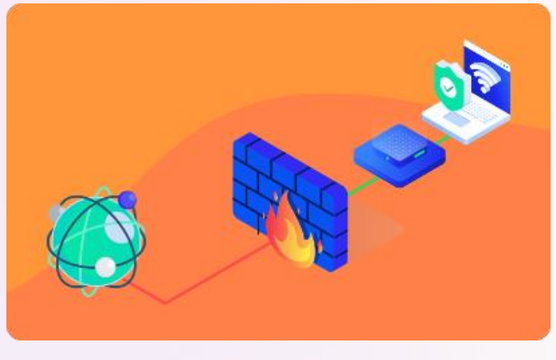


Actualiza el software

Mantén tus sistemas operativos, antivirus y software actualizados para protegerte de las últimas amenazas.

Instala antivirus

Protege tus dispositivos con software de seguridad y antivirus. Escanea periódicamente en busca de virus y malware.



Usa firewalls

Los firewalls son herramientas que protegen tus redes y datos de ciberataques. Úsalos en tus dispositivos.

Qué hacer en caso de un ataque cibernético cibernético y cómo recuperar la información información

1

Identifica el ataque

Revisa tus dispositivos para determinar la fuente y el alcance del ataque. Conoce la información que ha sido robada.

2

Notifica a las autoridades

Reporta el ataque y la pérdida de información a las autoridades competentes. Informa a tu empresa o empleador si es necesario.

3

Recupera la información

Si alguno de tus dispositivos está infectado, aísla y limpia el dispositivo. Restaura tus datos a partir de una copia de seguridad reciente.

Apoya tu proceso de remediaciones con:

ALINA

ALINA es un innovador chatbot impulsado por Inteligencia Artificial que te ayudará a resolver las remediaciones propuestas en este informe.

https://grupooruss.com/alina

¡Gracias!

www.grupooruss.com