Ciberseguridad

¿Qué es la ciberseguridad?

Prácticas, tecnologías y procesos diseñados para proteger sistemas informáticos, redes, programas y datos de ataques, daños, acceso no autorizado, robo de información y otras amenazas cibernéticas.

Objetivos

Confidencialidad

Protección de la información para evitar que sea revelada o accedida por personas no autorizadas

Integridad

Precisión y confiabilidad de la información.

Disponibilidad

Garantizar que la información y los recursos estén disponibles y accesibles cuando sea necesario.

Aspectos clave

Seguridad de la red

Proteger las redes de computadoras y sistemas de comunicación contra accesos no autorizados y ataques.

Seguridad de la información

Garantizar la confidencialidad, integridad y disponibilidad de la información almacenada y transmitida.

Gestión de accesos

Controlar y gestionar el acceso a sistemas y datos para garantizar que solo personas autorizadas tengan permiso.

Aspectos clave

Seguridad de aplicación

Asegurar que las aplicaciones y programas estén diseñados y desarrollados de manera segura, y que se apliquen parches y actualizaciones regularmente.

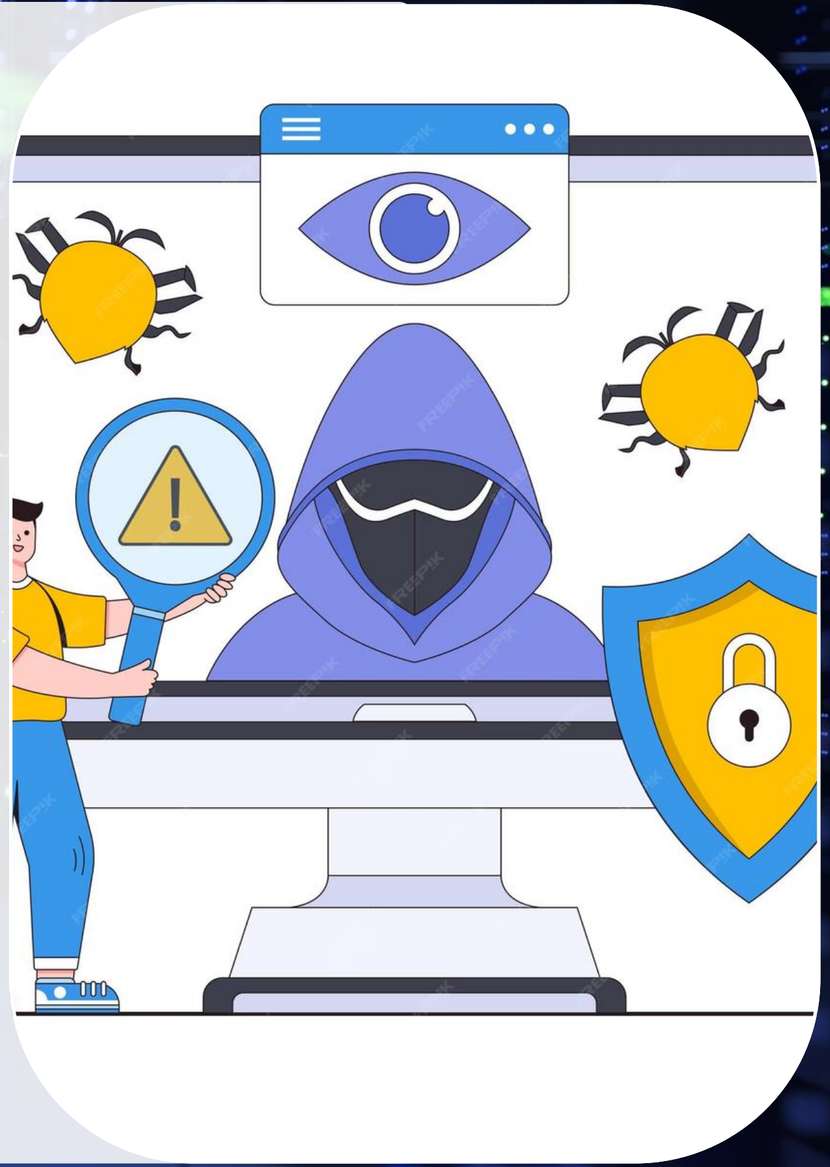
Educación y concientización

Capacitar a los usuarios y al personal de una organización sobre las mejores prácticas de seguridad y concientizar sobre posibles amenazas.

Monitoreo y detección de amenazas

Implementar sistemas de monitoreo continuo para detectar y responder a posibles amenazas en tiempo real.

Riesgos y amenazas



Riesgo y amenzas

- Daño físico
- Acciones humanas
- Fallos del equipo
- Ataques internos o externos
- Perdida de datos
- Errores en las aplicaciones

Tipos de ataque

Tipos de ataques

- Spoofing
- Sniffing
- Malware
- DoS
- Ingeniería social
- Etcétera

Mecanismos de defensa

Mecanismo de defensa

- Firewall
- Antivirus
- Capacitación
- Etcétera

Ciberseguridad en Consultiva

Actividad individual