



CIBERSEGURIDAD



Mucho más que un antivirus.

La ciberseguridad comprende todas las medidas preventivas para detectar y evitar ataques y vulnerabilidades que ponen en juego la integridad y confidencialidad de los sistemas informáticos y sus datos. Estas acciones se encargan de proteger y asegurar al máximo la privacidad de la información.

Contar con una estrategia integral de ciberseguridad es fundamental para el mundo de hoy, donde circulan millones de datos que debemos proteger, asimismo impedir que los dispositivos de una organización sean atacados. Esto es lo que queremos garantizarte con nuestras soluciones. En **CIOMTEK** te apoyamos para desarrollar estrategias de ciberseguridad integrales y eficaces.

Un enfoque exitoso de ciberseguridad tiene múltiples capas de protección repartidas en las computadoras, redes, programas o datos que uno pretende mantener a salvo.

- **PREVISION:** Estar preparados al tener una visibilidad absoluta de los dispositivos, las amenazas, las redes, las aplicaciones, los usuarios y los procesos para evitar posibles incidentes.
- **DETECCION E IDENTIFICACION:** El monitoreo debe ser constante y diario. Tener programas especializados para la detección temprana puede hacer toda la diferencia antes de poner los activos de las organizaciones en riesgo.
- **ACCEION Y REACCION:** un ataque informático es similar a una enfermedad. Cuanto antes se reaccione, antes se podrá atender y así reducir o evitar el daño en un alto porcentaje.





Garantizar la ciberseguridad de una organización requiere la coordinación y preparación de esfuerzos en diversas capas que en conjunto puedan brindar una protección íntegra a todo el sistema de información. Estas incluyen:

- Seguridad de las aplicaciones
- Seguridad de la información
- Seguridad de la red
- Recuperación ante desastres
- Seguridad operacional
- Educación del usuario final

¿Qué puede causar que una organización sea víctima de un ataque?

Vulnerabilidades:

- Configuraciones inapropiadas.
- Software de prueba.
- Parches en software y firmware.
- Mal uso de software o protocolo de comunicación.
- Diseño pobre de arquitecturas.
- Contraseñas inseguras.



Malware

Es un tipo de software malicioso que trata de infectar una computadora o un dispositivo móvil. Los hackers utilizan el malware para extraer información personal o contraseñas, robar dinero o evitar que los propietarios accedan a su dispositivo.



Ransomware

Es un tipo de malware que impide a los usuarios acceder a su sistema. Los hackers utilizan esta técnica para bloquear los dispositivos y exigir un rescate económico para recuperar el acceso.



Phishing

Es la práctica de obtener información confidencial, por ejemplo, contraseñas o información de la tarjeta de crédito a través de un correo electrónico disfrazado, una llamada telefónica o un mensaje de texto.





¿Por qué todas las organizaciones deben contar con una estrategia de ciberseguridad?



Mayor protección

Evita y combate ataques de amenazas como ransomware, virus, malware, spyware y programas no deseados.



Rendimiento de todo tipo de dispositivos

Evita y combate ataques de amenazas como ransomware, virus, malware, spyware y programas no deseados.



Navegación segura en la web

Evita peligros en línea con sus herramientas de seguridad en la web.



Barreras de seguridad

Protege computadoras, teléfonos móviles y demás artículos tecnológicos resguardando a sus usuarios de los peligros de Internet.

¿Tu organización está preparada para los posibles ataques?

En **CIOMTEK** comprendemos la importancia de proteger tu empresa, tu información y a tus colaboradores. Por eso trabajamos con marcas de nivel mundial para darte la mejor seguridad y encontrar un plan de protección perfecto para tus necesidades.