

MEDIDAS DE SEGURIDAD ACTIVAS



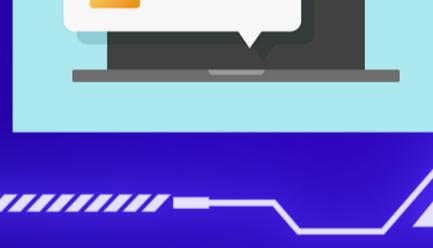
INSTALAR SOFTWARES DE ANTIVIRUS COMO MALWAREBYTES

Tener un antivirus siempre nos dará mas seguridad que no tenerlo.



USAR CONTRASEÑAS SEGURAS Y CAMBIARLAS CADA CIERTO TIEMPO

Es imprescindible para la seguridad digital. Lo ideal es mezclar números, letras, caracteres y mayúsculas y minúsculas.



ENcriptar LOS DATOS CON CRYPTOMATOR

De esta manera no serán tan accesibles para los posibles hackers y estarán ocultos de las intrusiones informáticas.



ACTUALIZAR DE FORMA CONSTANTE TODAS LAS APLICACIONES

Como pueden ser: Whatsapp, Facebook, Avast, Maps, etc. Todas deben ser actualizadas para evitar brechas por las que puedan colarse.



MEDIDAS DE SEGURIDAD PASIVAS



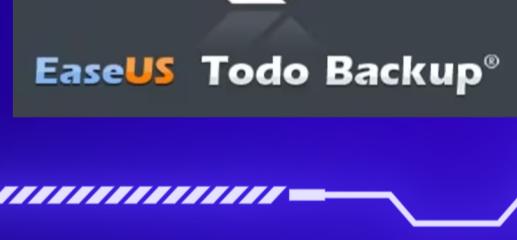
ESCANEAR Y DESINFECTAR DE MALWARES CON McAfee

Todos los equipos informáticos que se hayan visto afectados, saben que estos programas están trabajando en la seguridad de nuestros equipos.



RECUPERAR LAS COPIAS DE SEGURIDAD CON EASEUS TODO BACKUP

Con toda nuestra información guardada y en buen estado.



REALIZAR PARTICIONES DE DISCOS DUROS CON DISKPART

Para almacenar las copias y evitar que el malware se extienda a más equipos.

```
C:\>diskpart
```

USAR ALGÚN ALMACENAMIENTO EN LA NUBE COMO ICLOUD

Es sencillo, es barato y puede salvarnos la vida ante un ataque contra nuestros sistemas.

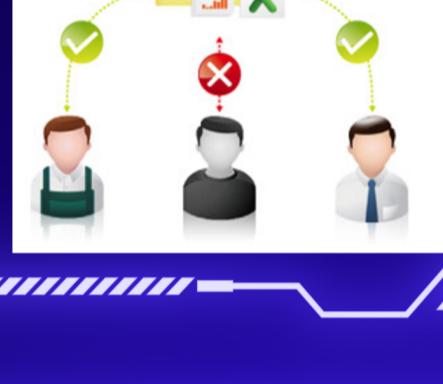


MEDIDAS DE SEGURIDAD PREVENTIVAS



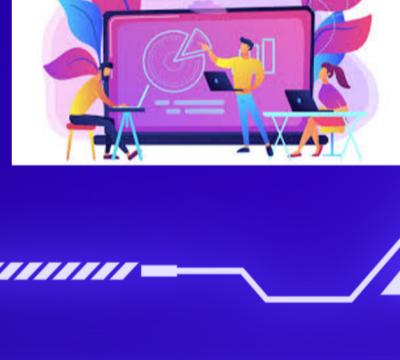
REVISIÓN PERIÓDICA DE PERMISOS Y CUENTAS

Revisar y ajustar regularmente los permisos de usuarios y sistemas, eliminando cuentas obsoletas y minimizando el acceso innecesario.



EDUCACIÓN Y CAPACITACIÓN DE LOS USUARIOS

Capacitar regularmente a los empleados sobre buenas prácticas de seguridad, como la gestión de contraseñas, la identificación de correos maliciosos y el uso adecuado de los sistemas.



PRUEBAS DE RECUPERACIÓN ANTE DESASTRES

Simular escenarios de desastre para probar la capacidad del sistema y del equipo de TI para recuperar el servicio rápidamente.



HACER AUDITORÍAS DE SEGURIDAD Y PRUEBAS DE PENETRACIÓN

Realizar auditorías y pruebas de penetración para identificar vulnerabilidades de seguridad antes de que puedan ser explotadas.



MEDIDAS DE SEGURIDAD PALIATIVAS



IMPLEMENTAR PARCHES TEMPORALES

Aplicar parches rápidos o soluciones provisionales que mitiguen los efectos del problema mientras se trabaja en una solución más definitiva.



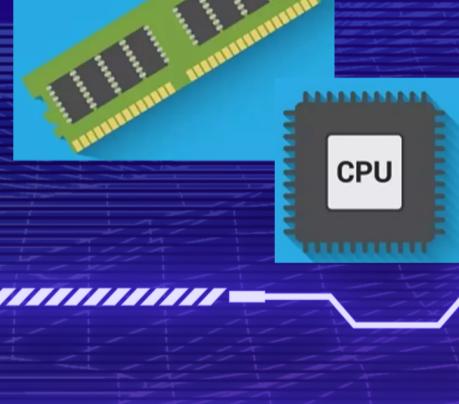
CONTENCIÓN DE ERRORES COMO CON FEC.

Implementar mecanismos que detecten errores y los aíslan para evitar que se propaguen a otras partes del sistema.



AUMENTAR TEMPORALMENTE LOS RECURSOS

Asignar recursos adicionales (como memoria RAM o CPU) temporalmente para mitigar problemas de rendimiento.



LIMITAR ACCESO AL SISTEMA

Reducir la cantidad de usuarios o servicios que pueden acceder simultáneamente al sistema.

