Medidas de proteccion

MEDIDAS PASIVAS

¿De qué se trata?

Son aquellas que se implementan en el sistema informático, generalmente desde su instalación, con el objetivo de minimizar los efectos de accidentes, averías o fallos. Un ejemplo de estas medidas es la instalación de una alarma contra incendios.

¿Cuáles son algunos ejemplos?

Escanear y desinfectar de malwares todos los equipos informáticos que se hayan visto afectados por esta intromisión en la seguridad.

Recuperar las copias de seguridad o backups más recientes con toda nuestra información guardada y en buen estado.

Realizar particiones de discos duros para almacenar las copias y evitar que el malware se extienda a más equipos.

MEDIDAS ACTIVAS

¿De qué se trata?

Estas se utilizan en el día a día para combatir daños en el sistema provocados principalmente por el factor humano, e implican la supervisión constante de un administrador. Un ejemplo es la instalación, configuración y supervisión de un firewall.

¿Cuáles son algunos ejemplos?

Usar contraseñas seguras y cambiarlas cada cierto tiempo: es imprescindible para la seguridad digital. Nada de poner el nombre del perro o la fecha de nacimiento; lo ideal es mezclar números, letras, diferentes caracteres y mayúsculas y minúsculas.

Instalar softwares de protección, firewalls y antivirus: son una barrera importantísima para frenar cualquier tipo de ataque.

Encriptar los datos importantes: de esta manera no serán tan accesibles para los posibles hackers y estarán ocultos de las intrusiones informáticas.

Referencias: ¡Sé una persona de bien y cita tus fuentes!

Medidas de proteccion

MEDIDAS PREVENTIVAS

¿De qué se trata?

Se adoptan para evitar que ocurra el problema. También se conocen como medidas proactivas.

¿Cuáles son algunos ejemplos?

La autenticación de dos factores o 2FA es otro método de seguridad adicional, en el que la persona usuaria tiene que proporcionar dos formas diferentes de identificación para poder acceder a una cuenta.

Contar con un duplicado o backup en la nube es fundamental para poder recuperar la información de manera fácil y rápida. Nuestra información quedará guardada y podremos recurrir a ella siempre que necesitemos.

Correos electrónicos, spam, documentos adjuntos, mensajes de texto, popups, enlaces, sitios web... Si provienen de una persona desconocida, hay que tener máxima precaución antes de hacer clic en ellos, ya que pueden tratarse de virus informáticos.

MEDIDAS PALIATIVAS

¿De qué se trata?

Se aplican para mitigar los efectos de un problema una vez que ya ha ocurrido.

¿Cuáles son algunos ejemplos?

Si un servidor deja de responder debido a una sobrecarga o a un fallo temporal, reiniciarlo puede restaurar su funcionamiento.

Cuando se detecta una vulnerabilidad de seguridad o un bug en un sistema, a veces se aplica un parche temporal para mitigar el problema hasta que se pueda desarrollar una actualización o solución definitiva.

Si una funcionalidad específica de una aplicación o sistema está causando problemas (por ejemplo, bloqueos o mal rendimiento), se puede optar por desactivarla temporalmente mientras se investiga la causa y se desarrolla una solución más adecuada.

Referencias: ¡Sé una persona de bien y cita tus fuentes!