

PROGRAMARI MALICIÓS

Malware: software diseñado per fer mal o robar dades d'un ordinador o dispositiu.

Tipos principals:

- **Virus:** s'adjunta a fitxers i es propaga quan s'executen.
- **Gusanos (worms):** es reproduïxen sols per la xarxa.
- **Trojanos:** aparenten ser útils però obren una porta al atacant.
- **Ransomware:** xifra fitxers i demana rescat.
- **Spyware:** espia l'activitat i roba informació.
- **Adware:** mostra anuncis intrusius; pot ser molest i insegur.
- **Rootkits / botnets:** permeten control remot o amaguen l'activitat maliciosa.

Com es propaga: descàrregues infectades, enllaços phishing, USBs, correus electrònics, vulnerabilitats sense parchear.

POLÍTICA DE CONTRASENYES

La política de contrasenyes és un conjunt de normes que una empresa, escola o plataforma estableix per protegir els comptes d'usuaris. La política de contrasenyes ajuda a protegir la informació personal i evitar accessos no autoritzats.

Normalment inclou:

- **Longitud i complexitat:** Requereix que les contrasenyes tinguin una longitud mínima de 12 caràcters, ha d'incloure majúscules, minúscules, números i caràcters especials.
- **Autenticació multifactor:** Agrega una capa extra de seguretat implementant autenticació multifactor. D'aquesta manera, encara que un atacant obtingui la contrasenya, necessita un segon factor (com un codi en el mòbil) per a accedir.
- **Rotació periòdica:** Estableix una política que obligui els empleats a canviar les seves contrasenyes cada 60 o 90 dies. A més, que no es puguin reutilitzar contrasenyes antigues.
- **Prohibició de contrasenyes comunes:** l'ús de contrasenyes comunes o fàcils d'endevinar, com «123456», «contrasenya» o «*admin».
- **Ús d'un gestor de contrasenyes:** Facilita l'ús de contrasenyes complexes proporcionant o recomanant gestors de contrasenyes als empleats. Aquestes eines permeten emmagatzemar i generar contrasenyes segures sense necessitat de recordar-les manualment.

CÀLCUL DE POTENCIA CONSUMIDA

Saber **quanta energia elèctrica** utilitza un dispositiu: la fórmula **$P = V \times I$** .

(on *P* és la potència (en watts), *V* és la tensió (en volts) i *I* és la intensitat del corrent (en amperes).)

EINES BIOMÈTRIQUES

Eines biomètriques: són tecnologies que identifiquen persones mitjançant característiques físiques o de comportament, com l'empremta digital, el reconeixement facial, la veu o l'iris. S'utilitzen molt per a la seguretat i l'accés a dispositius o llocs.

VULNERABILITATS

Les vulnerabilitats són **punts febles en un sistema informàtic** que poden ser aprofitats per persones malintencionades (*hackers*) per accedir, robar o danyar informació.