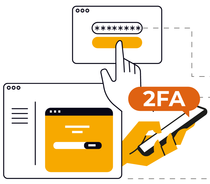
MESURES de SEGURETAT

EN EL LLOC DE TREBALL

Les mesures de seguretat en les empreses busquen **previndre riscos, protegir la informació i garantir la confidencialitat. Tot el personal ha d'estar compromés amb les polítiques de seguretat**, que inclouen des de les contrasenyes i l'ús segur de dispositius fins a la prevenció de ciberatacs.

Para atenció a les següents recomanacions
per a treballar de manera segura:



1. CONTRASENYES

- Crea contrasenyes **fortes i robustes.**
- Implementa el **doble factor d'autenticació (2FA)**, si és possible.
- Utiliza **gestors de contrasenyes** (KeePass, Passbolt, NordPass).

2. "TAULES NETES"

- Bloqueja l'ordinador quan t'absentes (**Tecla Windows + L**).
- Apaga'l quan acabés la jornada.
- Evita deixar documentació confidencial o secreta a la vista o fora de les calaixeres.

3. XARXES

- Utilitza xarxes privades virtuals (**VPN**) per a les connexions remotes a la xarxa corporativa.
- **No et connectes** a xarxes **Wifi públiques** sense mesures de protecció, ja que poden ser vulnerables a atacs d'intermediaris com 'Man In The Middle' (MITM).

4. Correus electrònics i MISSATGERIA

- Aprén a identificar la pesca (**phishing**).
- No òbrigues **arxius adjunts** ni faces clic en enllaços de remitents desconeguts.
- Evita l'ús del correu corporatiu per a **activitats personals**.
- No divulgues **informació sensible corporativa** per correu.
- Consulta la **política d'ús de correu de la teua organització** per si estigueres obligat a xifrar determinats correus

5. Polítiques d'accés i ús de DISPOSITIUS

- **Atorga permisos** per a limitar l'accés a la informació. Per exemple, per a accedir a les carpetes del núvol.
- Configura el **bloqueig automàtic de dispositius** després d'un temps d'inactivitat.
- Els discos durs i les dades sensibles han d'estar **xifrats**, especialment en dispositius mòbils o portàtils.
- Revisa la política d'ús de la teua organització per a garantir la seguretat de la informació.

6. ACTUALITZACIÓ i gestió de PROGRAMARI

- **Actualitza el programari** dels teus dispositius a l'última versió.
- Instal·la i mantín actualitzats **programes antivirus i tallafocs.**

7. CONTROL de DISPOSITIUS EXTERNS

- Restringix l'ús de dispositius **USB no autoritzats** o proporciona dispositius prèviament verificats pel departament de TI.
- **Xifra les dades emmagatzemades** en memòries USB o discos durs externs.

8. SEGURETAT FÍSICA en el lloc de treball

Les àrees amb dispositius o servidors crítics han de tindre accés restringit mitjançant **targetes, empremtes o claus.**

La **destrucció de suports físics** (paper, discos durs, USB...) ha de ser adequada.

9. FORMACIÓ en Ciberseguretat

- Millorarà la teua capacitat a l'hora d'identificar possibles fraus (phising, frau del CEO, ransomware...).
- Contribuïxes a la creació d'una cultura de seguretat robusta, reduir riscos, assegurar el compliment normatiu (ENS, ISO 27001...) i protegir la informació sensible.
- Consulta els **20 cursos en línia** que CSIRT-CV oferix en el seu web: **https://concienciat.gva.es/va/cursos/**

10. Dona la veu d'ALARMA

Reporta qualsevol correu electrònic, missatge de text o telefonada sospitosa al teu suport de ciberseguretat o de tecnologies de la informació perquè revise el cas i puga alertar **altres companys**.

Protegir la informació en el teu lloc de treball, depén de tu.

GENERALITAT VALENCIANA
Conselleria d'Hisenda, Economia i Administració Pública

CSIRT-CV
Centre Seguretat TIC de la Comunitat Valenciana

www.csirtcv.gva.es
concienciat.gva.es