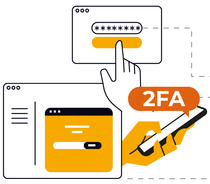
MEDIDAS de SEGURIDAD

EN EL PUESTO DE TRABAJO

Las medidas de seguridad en las empresas buscan **prevenir riesgos, proteger la información y garantizar la confidencialidad**. **Todo el personal debe estar comprometido con las políticas de seguridad**, que incluyen desde las contraseñas y el uso seguro de dispositivos hasta la prevención de ciberataques.

Presta atención a las siguientes recomendaciones para trabajar de forma segura:



1. CONTRASEÑAS

- Crea contraseñas **fuertes y robustas.**
- Implementa el **doble factor de autenticación (2FA)** si es posible.
- Utiliza **gestores de contraseñas** (KeePass, Passbolt, NordPass).

2. "MESAS LIMPIAS"

- Bloquea el ordenador cuando te ausentes (**Tecla Windows + L**).
- Apágalo cuando acabes la jornada.
- Evita dejar documentación confidencial o secreta a la vista o fuera de las cajoneras.

3. REDES

- Utiliza redes privadas virtuales (**VPN**) para las conexiones remotas a la red corporativa.
- **No te conectes** a redes **Wi-Fi públicas** sin medidas de protección, ya que pueden ser vulnerables a ataques de intermediarios como 'Man In The Middle' (MITM).

4. Correos electrónicos y MENSAJERÍA

- Aprende a identificar el **phishing**.
- No abras **archivos adjuntos** ni hagas clic en enlaces de remitentes desconocidos.
- Evita el uso del correo corporativo para **actividades personales**.
- No divulgues **información sensible corporativa** por correo.
- Consulta la **política de uso de correo de tu organización** por si estuvieras obligado a cifrar determinados correos.

5. Políticas de ACCESO y uso de DISPOSITIVOS

- **Otorga permisos** para limitar el acceso a la información. Por ejemplo, para acceder a las carpetas de la nube.
- Configura el **bloqueo automático de dispositivos** tras un tiempo de inactividad.
- Los discos duros y datos sensibles deben estar **cifrados**, especialmente en dispositivos móviles o portátiles.
- Revisa la política de uso de tu organización para garantizar la seguridad de la información.

6. ACTUALIZACIÓN y gestión de SOFTWARE

- **Actualiza el software** de tus dispositivos a la última versión.
- Instala y mantén actualizados programas **antivirus y cortafuegos**.

7. CONTROL de DISPOSITIVOS EXTERNOS

- Restringe el uso de dispositivos **USB no autorizados** o proporciona dispositivos previamente verificados por el departamento de TI.
- **Cifra los datos almacenados** en memorias USB o discos duros externos.

8. SEGURIDAD FÍSICA en el lugar de trabajo

- Las áreas con dispositivos o servidores críticos deben tener acceso restringido mediante **tarjetas, huellas o claves.**
- La **destrucción de soportes físicos** (papel, discos duros, USB...) debe ser adecuada.

9. FORMACIÓN en Ciberseguridad

- Mejorarás tu capacidad a la hora de identificar posibles fraudes (phishing, fraude del CEO, Ransomware, etc).
- Contribuyes a la creación de una cultura de seguridad robusta, reducir riesgos, asegurar el cumplimiento normativo (ENS, ISO 27001...) y proteger la información sensible.
- Consulta los **20 cursos online** que CSIRT-CV oferta en su web: **https://concienciat.gva.es/cursos/**

10. Da la voz de ALARMA

Reporta cualquier correo electrónico, mensaje de texto o llamada sospechosa a tu soporte de Ciberseguridad o de Tecnologías de la Información para que revise el caso y pueda alertar a **otros compañeros**.

Proteger la información en tu puesto de trabajo, depende de ti.

GENERALITAT VALENCIANA
Conselleria d'Hisenda, Economia i Administració Pública

CSIRT-CV
Centro Seguridad TIC de la Comunitat Valenciana

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