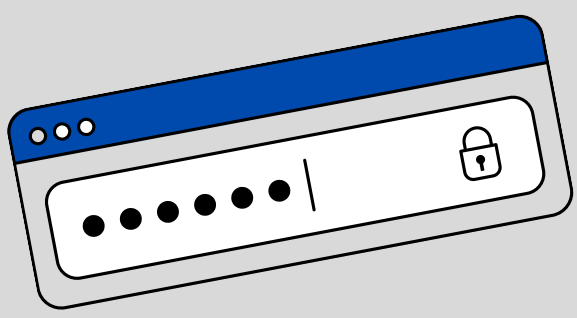
USO SEGURO DE DISPOSITIVOS

+ IA

1 SEGURIDADE BÁSICA EN DISPOSITIVOS E CONTAS



- Manter sistemas e apps actualizados.
- Usar contrasinais fortes, bloqueos de pantalla e 2FA.
- Evitar Wi-Fi públicas e dispositivos externos non coñecidos.
- Realizar copias de seguridade periódicas de documentos.

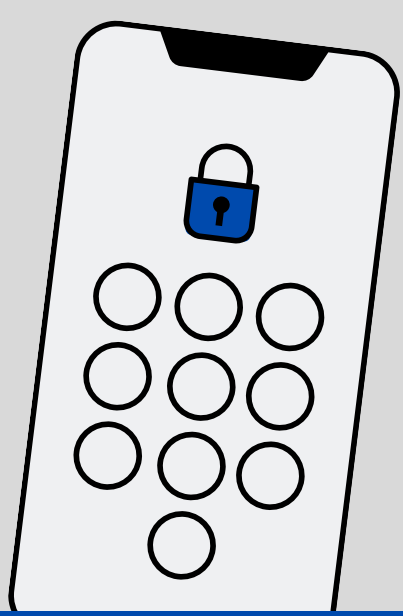
2 PROTECCIÓN DE DATOS E RESPONSABILIDADE PROFESIONAL

- Tratar só cos datos necesarios para o servizo.
- Garantir confidencialidade, integridade e seguridade na súa xestión.
- Eliminar ou anonimizar datos cando xa non sexan precisos.
- Informar de maneira transparente sobre o uso dos datos cando proceda.
- Comprender obrigas legais básicas (LOPDGDD, RGPD a nivel introdución).

3 COMUNICACIÓN DIXITAL SEGURA NO ÁMBITO LABORAL

- Verificar remitentes e evitar ligazóns ou arquivos sospeitosos.
- Non compartir contrasinais ou información sensible por medios non seguros.
- Protexer a privacidade no uso das ferramentas colaborativas (Drive, Teams, etc.).
- Manexar con prudencia as redes sociais e mensaxería cando se represente á empresa.

4 INTELIXENCIA ARTIFICIAL APLICADA AO TRABALLO



- Non introducir información sensible de clientes, datos persoais ou documentación interna en plataformas de IA abertas.
- Validar sempre as respostas; a IA pode cometer erros, ter sesgo ou contido inventado.
- Empregar a IA como apoio para mellorar a produtividade, non para sustituír o criterio profesional nin as obrigas éticas.

IES DE TEIS