



ASEGURANDO SISTEMAS

CONSELLOS DE CIBERSEGURIDADE

01 REDES SEGURAS

Garantir confidencialidade, integridade e dispoñibilidade da información.

Boas prácticas:

- Segmentar redes e controlar accesos.
- Usar cifrado e VPN.
- Actualizar software e revisar configuracións.



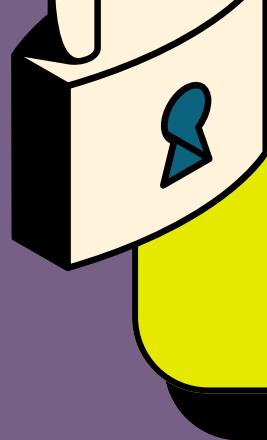
02 CRIPTOGRAFÍA

Protexe a información mediante técnicas matemáticas.

Aplicacións: sinaturas dixitais, certificados, protocolos seguros.

Recomendacións:

- Usar cifrado adecuado segundo a sensibilidade da información.
- Xestionar e almacenar claves de forma segura.



03 VULNERABILIDADES

Debilidades que poden ser explotadas por atacantes.

Como actuar:

- Identificar e avaliar vulnerabilidades.
- Corrixir ou mitigar riscos e documentar os cambios.
- Realizar probas de penetración para comprobar a seguridade.



04 INTELIXENCIA ARTIFICIAL (IA)

A IA pode ser útil, pero tamén perigosa (automatización de ataques, phishing, etc).

Boas prácticas:

- Avaliar algoritmos antes de aplicalos.
- Non depender da IA para decisiones críticas sen supervisión.
- Revisar datos e resultados para evitar errores ou sesgos.

