Protecció i Seguretat de les dades

1. Diferència entre protecció de dades i seguretat de dades

- **Protecció de dades:** Fa referència a les mesures legals, tècniques i organitzatives per garantir que les dades personals es tracten de manera lícita, transparent i segura, protegint els drets de les persones (com la privadesa). Es basa en normatives com el RGPD o la LOPD-GDD.
- **Seguretat de dades:** És un concepte més tècnic que se centra a protegir les dades (personals o no) contra accessos no autoritzats, pèrdues o alteracions, mitjançant eines com xifratge, tallafocs o controls d'accés. Forma part de la protecció de dades, però és més àmplia perquè inclou qualsevol tipus de dada.

2. Què és la LOPD-GDD i quan va entrar en vigor

- **LOPD-GDD:** És la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals, una llei espanyola que adapta el Reglament General de Protecció de Dades (RGPD) de la UE al context espanyol i introdueix mesures addicionals, com els drets digitals.
- **Entrada en vigor:** Va entrar en vigor el **6 de desembre de 2018**, l'endemà de la seva publicació al BOE.

3. Què són els drets ARCO-POL

Els drets **ARCO-POL** són els drets que tenen les persones sobre les seves dades personals segons la normativa de protecció de dades (RGPD i LOPD-GDD). Són:

- **A**ccés: Dret a saber si una organització tracta les teves dades i a obtenir-ne una còpia.
- **R**ectificació: Dret a corregir dades personals inexactes o incompletes.
- **C**ancel·lació (o supressió): Dret a sol·licitar l'eliminació de les teves dades (també conegut com a "dret a l'oblit").
- **O**posició: Dret a oposar-te al tractament de les teves dades per motius legítims (per exemple, per a publicitat).
- **P**ortabilitat: Dret a rebre les teves dades en un format estructurat i transferir-les a una altra entitat.
- **O**posició a decisions automatitzades: Dret a no ser objecte de decisions basades només en tractaments automatitzats (com perfils).
- **L**imitació: Dret a limitar el tractament de les teves dades en certs casos (per exemple, mentre es verifica la seva exactitud).

4. Defineix breument els principis de seguretat informàtica: confidencialitat, integritat, disponibilitat i autenticitat

- **Confidencialitat:** Garantir que només les persones autoritzades puguin accedir a la informació (per exemple, amb xifratge o contrasenyes).
- **Integritat:** Assegurar que les dades no siguin alterades o modificades sense autorització, mantenint-ne l'exactitud i completitud (per exemple, amb controls de verificació).
- **Disponibilitat:** Garantir que la informació i els sistemes estiguin accessibles quan es necessitin, evitant interrupcions (per exemple, amb còpies de seguretat).
- **Autenticitat:** Verificar que els usuaris o sistemes són qui diuen ser, i que la informació prové d'una font fiable (per exemple, amb autenticació de dos factors).

5. Què és una amenaça de ciberseguretat

Una **amenaça de ciberseguretat** és qualsevol acció, esdeveniment o circumstància que pot comprometre la seguretat de la informació d'una organització, posant en risc la confidencialitat, integritat o disponibilitat de les dades. Pot ser intencionada (com un atac de hackers) o no intencionada (com un error humà).

6. Defineix les següents formes en què es manifesten les amenaces de seguretat

- **Bretxa de dades:** Accés no autoritzat, divulgació o pèrdua de dades sensibles, com quan un hacker accedeix a informació personal d'una empresa.
- **Virus:** Programa maliciós que s'adjunta a fitxers o programes i es replica, infectant sistemes i causant danys com la pèrdua de dades o el mal funcionament.
- **Malware:** Terme genèric per a qualsevol programari maliciós (com virus, cucs, troians o ransomware) dissenyat per infiltrar-se, danyar o robar informació d'un sistema.
- **Atacs de denegació de servei (DoS):** Atac que busca saturar un sistema, xarxa o servidor amb tràfic excessiu per impedir que els usuaris legítims hi accedeixin, afectant la disponibilitat.