| Nom i cognoms: Òscar Rodríguez |  |
| --- | --- |
| Data: 4/11/2022 |  |
| Nom de l’activitat/pràctica: ACT150 |  |

**DESENVOLUPAMENT:**

**1-. Busca, pregunta i entén en què consisteix un sistema d'autenticació biomètrica.**

* Que és un sistema d’autenticació biomètrica ? Exemples

Els sistemes d’autenticació biomètrica són mètodes que es van imposar en la majoria de situacions en què es faci necessari autenticar un usuari, depenent de qui l’utilitzi no necessitarà recordar claus o nùmeros d’identificació complexos, són difícils de falsificar.

En l’àmbit empresarial podem tenir els següents accessos biomètrics:

* Lector d’empremtes dactilars
* Control d’accés mitjançant el palmell de la mà
* Control biomètric ocular
* Sistemes de reconeixement facial
* Mecanismes de reconeixement de veu

**2-. Explica en què consisteix aquest tipus d'autenticació i descriu el seu funcionament.**

L’autentificació biomètrica és un sistema de seguretat de dades amb el qual es regula l’accés a tot tipus d’informació, aplicacions, etc. El seu funcionament és senzill, primer es verifica l’identitat i després s’autoritza o no l’accés.

**3-. Quins tipus d'autenticació biomètrica hi ha?**

* Lector d’empremtes dactilars: registren una empremta dactilar, es guarda i després si la reconeixen permeten l’accés.
* Control d’accés mitjançant el palmell de la mà: escanejen el palmell de la mà per identificar els usuaris.
* Control biomètric ocular: escanejen l’ull per identificar els usuaris.
* Sistemes de reconeixement facial: registren una cara, es guarda i després si la reconeixen permeten l'accés.
* Mecanismes de reconeixement de veu: Analitza el so de la veu de l’usuari i determina l’accés.

**4-. Classifica raonadament aquest tipus de seguretat: activa/passiva/física/lògica.**

L’autentificació biomètrica és un sistema de seguretat activa ja que el seu objectiu és preveure que personal no autoritzat accedeix. En quant a la part física o lògica crec que poden arribar a ser les dues opcions depenent del moment.

**Contrasenyes**

**5-. Enumera els aspectes que has de tenir en compte per crear una contrasenya segura.**

1. Utilitzar només combinacións de lletres, nùmeros i símbols dins del estàndard ASCII, és a dir, no posar accents.
2. Utilitzar contrasenyes noves, no utilitzar sempre les mateixes.
3. Utilitzar contrasenyes més segures i poc habituals (no utilitzar “contrasenya1234”)
4. Mai començar o terminar amb espais en blanc.

**6-. Quins són els mètodes més comuns de sustracció de contrasenya? (Com a mínim has de parlar de la enginyeria social, l'atac de força bruta, el keylogger i l'sniffer) Com funcionen? Com ens podem protegir?**

* Enginyeria social: Atac dirigit a enganyar a un usuari per poder veure informació, obtenir accés, cometre frau, etc.
* Atac de força bruta: Utilització de un software automatitzat que comprova les credencials i en cas de no tenir contrasenyes segures, les descifren.
* Keylogger: Registren les pulsacions de les tecles.
* Sniffer: Atac destinat als paquets, quan passen per una red monitoritzada els capturen i analitzen.
* Phishing: Els atacants en fan passar per entitats oficials, amics o familiars per aconseguir dades importants.