

# Projecte ASIX 2k22

Escola Del Treball

2HISX 2021-2022

Aaron Andal & Cristian Condolo

## CryptoSEC: “*Careful where you step in*”



## Index

- Objectius
  - Proposta final (LAN CryptoSEC)
- DNS
  - DNSSEC
- DHCP
- FIREWALL (IPTABLES)
- APACHE2
- OPENVAS
- HACKING & PENTESTING
  - BRUTE FORCE ATTACK - PASSWORD CRACKING (JOHN)
  - MITM - ARP POISONING / SPOOFING

- MITM - DNS POISONING / SPOOFING
- MITM - ARP SPOOFING + SNIFFING
- EMAIL PHISHING
- KALI LINUX
  - ETTERCAP
  - SETOOLKIT
  - BETTERCAP
  - WIRESHARK
- PREVENCIÓ I PROTECCIÓ
- CONCLUSIÓ

## La ciberseguretat

En la societat d'avui en dia, l'ús de les tecnologies de la informació, ens faciliten intercanviar informació des de qualsevol part del món.



> **Img Source:** <https://www.infodefensa.com/images/showid2/5311974?w=900&mh=700>

Milions de dades, viatgen per la “xarxa” anomenada “Internet”, que bàsicament són un conjunt de dispositius interconnectats entre si.

Internet, abasta una rutina quotidiana d'ús de *xarxes socials*, *entreteniment*, *educació*, *formació*, *medis de comunicació*, *televisió*, etc.

Tota aquesta informació viatja en una xarxa on hi ha “**de tot**”.



> **Img Source:** <https://www.lasrozas.es/sites/default/files/inline-images/Ciber.jpg>

## Que és la ciberseguretat?

La ciberseguretat és la pràctica d'establir “*zones de defensa*” a diferents dispositius com ordinadors, servidors, dispositius mòbils, xarxes, etc., d'atacs maliciosos (Com virus o exploits) o de denegació de servei (DoS).

També es coneix com a **seguretat de tecnologia de la informació** o **seguretat de la informació electrònica**.

El terme s'aplica en diferents contextos, des dels negocis fins a la **informàtica mòbil**, i es pot dividir en algunes categories comunes.

El seu funcionament es basa a implantar tècniques i eines de **maquinari / programari** perquè elaborin **barreres** que impedeixin l'accés desconegut a la informació delicada. La protegeix i treu a l'enemic si es tracta d'una **vulneració**.

Un ciberatac no només consisteix en la **pèrdua i destrucció de dades** confidencials, sinó que també **afecta** el nivell de **productivitat i rendibilitat**, portant com a conseqüència la pèrdua del capital, de la confiança per part dels clients i de la competitivitat davant del mercat legal.



> **Img Source:** [https://static.vecteezy.com/system/resources/previews/001/406/100/non\\_2x/types-of-cyber-security-to-keep-in-mind-free-vector.jpg](https://static.vecteezy.com/system/resources/previews/001/406/100/non_2x/types-of-cyber-security-to-keep-in-mind-free-vector.jpg)

La **ciberseguretat** s'ha tornat un assumpte de vital importància per a tota mena d'empreses, sense importar la mida.

Gràcies a les diferents eines que disposa aquesta matèria, el teu sistema pot estar protegit de **atacs**, d'**hackers** o qualsevol classe de **delicte informàtic**.

La ciberseguretat es dedica a complir tres objectius la prevenció, la detecció i la recuperació.

Entre els principals **tipus de ciberseguretat** es troben els següents:

- **Seguretat informàtica en àmbit de xarxa:** és la pràctica de protegir una xarxa informàtica dels intrusos, siguin atacants dirigits o codi maliciós oportunista.
- **Seguretat informàtica en àmbit de software:** s'enfoca a mantenir el programari i els dispositius d'amenaques lliures. Una aplicació afectada podria oferir accés a les dades que està destinada a protegir.
- **Assegurar la informació:** La seguretat de la informació protegeix la integritat i la privadesa de les dades, tant en l'emmagatzematge com en el trànsit.
- **Seguretat operativa:** inclou els processos i decisions per manejar i protegir els recursos de dades.
- La **recuperació davant de desastres** i la **continuïtat del negoci** defineixen la manera com una organització respon a un incident de ciberseguretat de qualsevol altre esdeveniment que causi que s'aturin les seves operacions o es perdin dades.

La capacitació de l'usuari final és fonamental en el factor de més imprevisible: **les persones**.

Si s'incompleixen les bones pràctiques de seguretat, qualsevol persona pot introduir accidentalment un virus en un sistema que altament seria segur.

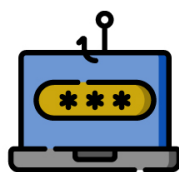
Ensenyar-los als usuaris a eliminar els **fitxers adjunts** de correus **electrònics sospitosos**, a no connectar unitats **USB no identificades** i altres lliçons importants és crucial per a la seguretat de qualsevol **organització**.

Tipus d'amenaces davant la “Ciberseguretat”

## Tipos de amenazas de Ciberseguridad



Malware



Phishing



Spear Phishing



Ataque de Denegación de Servicio



Amenaza Avanzada Persistente (APT)



Inyección SQL



Ransomware



Ataque DNS

Fuente: StealthLabs

> Img Source: <https://pbs.twimg.com/media/E3nXigSXwAANyGi.jpg:large>

## Bibliografia

### Ciberseguretat

- <https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security>
- <https://www.santaluciaimpulsa.es/ciberseguridad-en-la-actualidad/>

- <https://madridpress.com/art/297262/la-ciberseguridad-en-la-actualidad>
- [https://www.cisco.com/c/es\\_mx/products/security/what-is-cybersecurity.html](https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html)
- <https://www.infosecuritymexico.com/es/ciberseguridad.html>
- <https://www.hiberus.com/crecemos-contigo/que-es-la-ciberseguridad/>