

Projecte ASIX 2k22

Escola Del Treball

2HISX 2021-2022

Aaron Andal & Cristian Condolo

Ciberseguretat: "*Careful where you step*"



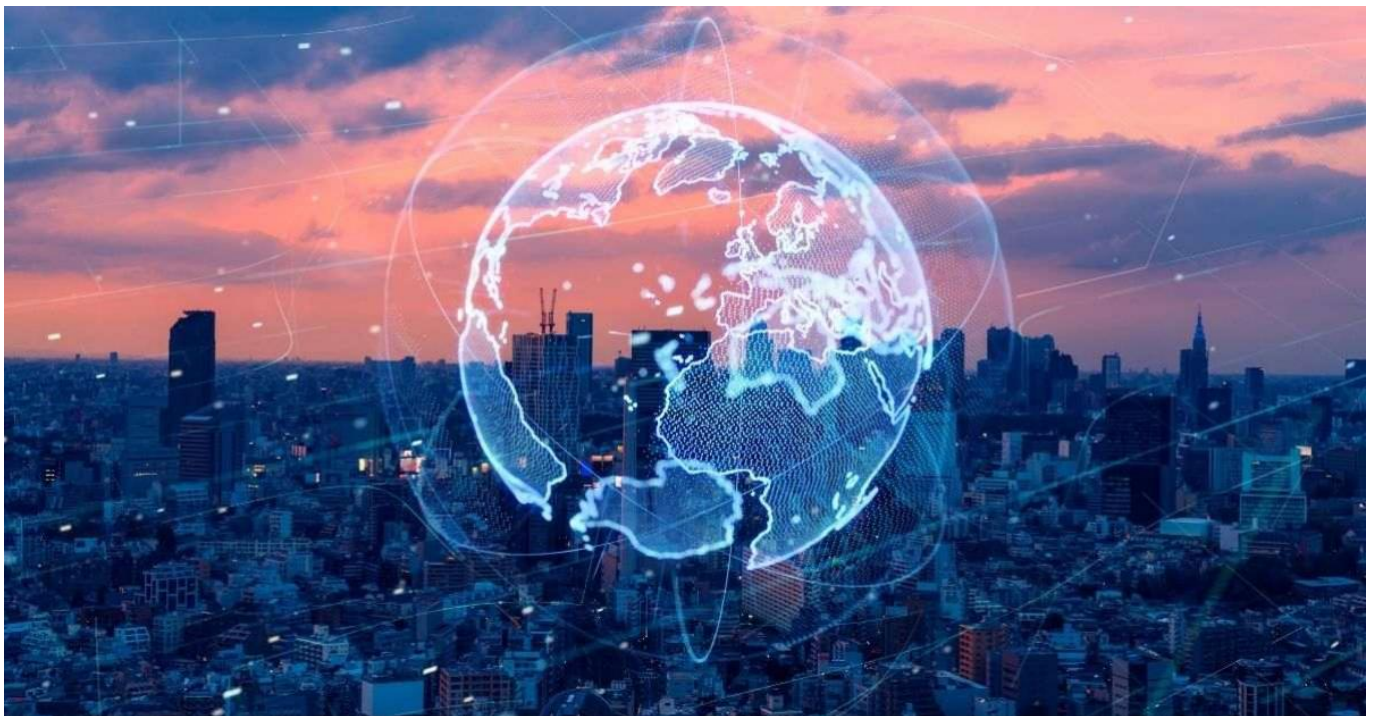
Índex

- **Objectius:** --> [readME](#) <--
- **Proposta final:** --> [readME](#) <--
- **DNS:** --> [readME](#) <--
 - **DNSSEC:** --> [readME](#) <--
- **DHCP:** --> [readME](#) <--
- **FIREWALL (IPTABLES):** --> [readME](#) <--

- **HACKING & DOS:** --> [readME](#) <--
 - **DNS SPOOF:** --> [readME](#) <--
 - **ARP SPOOF:** --> [readME](#) <--
 - **BRUTE FORCE - PASSWORD CRACKING:** --> [readME](#) <--
 - **SSLSTRIP:** --> [readME](#) <--
- **KALI LINUX:** --> [readME](#) <--
 - **ETTERCAP:** --> [readME](#) <--
 - **SETTOOLKIT:** --> [readME](#) <--
 - **PROVA:** --> [readME](#) <--
- **WAZUH:** --> [readME](#) <--

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.



Millons de dades, viatgen per la "xarxa" anomenada "Internet", que bàsicament son un conjunt de dispositius interconnectats entre sí.

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

Tota aquesta informació viatja en un xarxa on hi ha "**de tot**".



Molta de la informació que viatja per Internet, pot ser que sigui confidencial i delicada, n'hi ha que viatja *segur* i d'altre *insegur*, si viatja insegur... és un problema **greu**....

Un dels principals problemes de l'ús de les tecnologies de la informació, es la *incapacitat* de prevenir aquests *atacs* quant ja es produeixen. És a dir, el desconeixement de la seguretat d'avant d'aquestes tecnologies d'ús cotidià.

Com ja diu el refrà: "**Millor prevenir que lamentar**", la solució davant d'aquests problemes a usuaris inexperts, és la **ciberseguretat**.



Qu   es la ciberseguretat?

La ciberseguretat   s la pr  ctica d'establir "zones de defensa" a diferents dispositius com ordinadors, servidors, dispositius m  bils, xarxes ...etc, d'atacs maliciosos (Com virus o exploits) o de denegaci   de servei (DoS).

Tamb   es coneix com a **seguretat de tecnologia de la informaci  ** o **seguretat de la informaci   electr  nica**.

El terme s'aplica en diferents contextos, des dels negocis fins a la **inform  tica m  bil**, i es pot dividir en algunes categories comunes.

El seu funcionament es basa en implantar t  cniques i eines de **maquinari / programari** perqu   elaborin **barreres** que impedeixin l'acc  s desconegut a la informaci   delicada. La protegeix i treu a l'enemic si es tracta d'una **vulneraci  **.

Un ciberatac no nomes consisteix en la **p  rdua i destrucci   de dades** confidencials, si no que tamb   **afecta** el nivell de **productivit   i rentabilit  **, portant com a conseq  ncia la p  rdua del capital, de la confian  a per part dels clients y de la competitivitat davant del mercat legal.



La **ciberseguretat** s'ha tornat un assumpte de vital importància per a tot tipus d'empreses, sense importar el tamany.

Gràcies a les diferents eines que disposa aquesta matèria, el teu sistema pot estar protegit de **atacs**, d'**hackers** o qualsevol tipus 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, ja siguin atacants dirigits o codi maliciós oportunista.
- **Seguretat informàtica en àmbit de software:** s'enfoca a mantenir el programari i els dispositius d'amenaça 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 **continuitat del negoci** defineixen la manera com una organització respon a un incident de ciberseguretat o a qualsevol altre esdeveniment que causi que s'aturin les seves operacions o es perdin dades.

La capacitat 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.

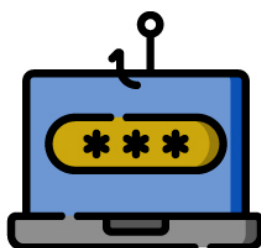
Ensenyar-los als usuaris a eliminar els **fitxers adjunts** de correus **electrònics sospitosos**, a no connectar unitats **USB no identificades** i altres lliçons importants és fonamental per a la seguretat de qualsevol **organització**.

Tipus d'amenaçes davant la "Ciberseguretat"

Tipos de amenazas de Ciberseguridad



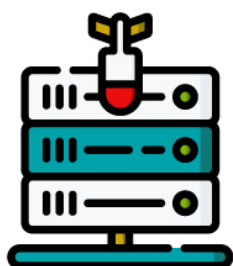
Malware



Phishing



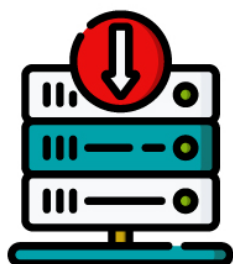
Spear Phishing



Ataque de Denegación de Servicio



Amenaza Avanzada Persistente (APT)



Inyección SQL



Ransomware



Ataque DNS

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>