Pautes i pràctiques de tractament segur de la informació
Part I

T1 CID, Vulnerabilitats, Enginyeria Social

Objectius d’un sistema ~~segur??~~

“L'únic sistema segur és aquell que està apagat i desconnectat, enterrat en un refugi de formigó, envoltat per gas verinós i custodiat per guardians ben pagats i molt ben armats. Encara així, jo no apostaria la meua vida per ell” (Eugene Spafford).

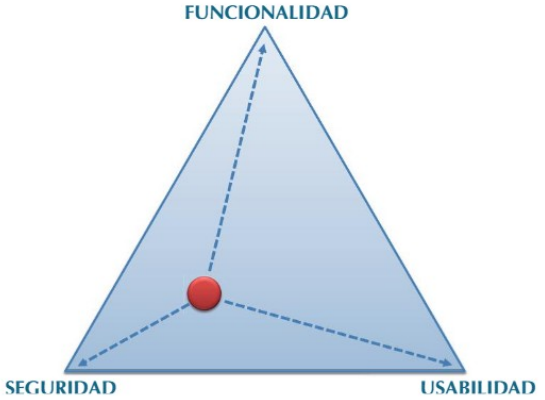
Parlar de seguretat informàtica en termes absoluts és impossible i per eixe motiu es parla més aviat de **Fiabilitat** del sistema.

Seguretat ?? informàtica

Cheswick, W

"*Firewalls and Internet Security. Repelling the Wily Hacker*,"

“No existeix la seguretat absoluta”.
“La seguretat és sempre una qüestió econòmica”.
“La seguretat comporta un compromís amb la comoditat”.
“Una cadena és tan forta com el seu enllaç més feble”.
“Un atacant no travessa la seguretat, l'envolta”.
“És mala idea confiar en la «seguretat per foscor»”.
“No dones a una persona o programa més privilegis que aquells estrictament necessaris”.



Paradoxa de la seguretat

Objectius d’un sistema ~~segur~~ fiable

Detectar els possibles problemes i amenaces.

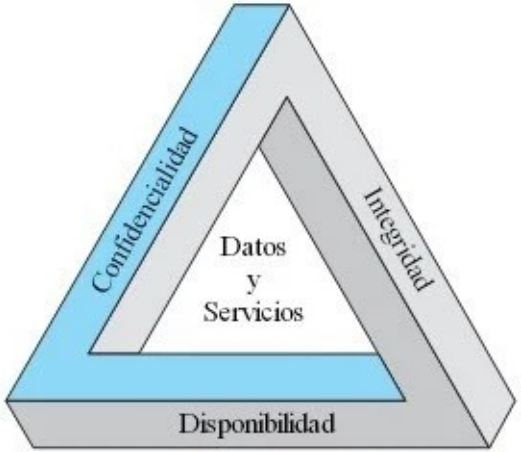
Garantir la adequada utilització dels recursos i de les aplicacions dels sistemes.

Objectius d’un sistema fiable

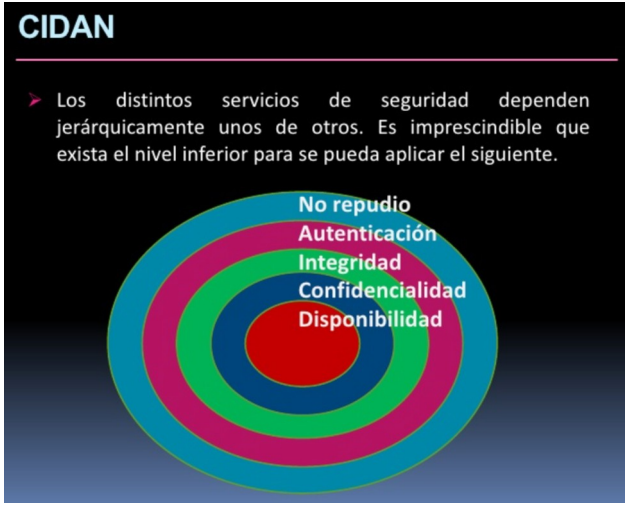
Limitar les pèrdues i aconseguir una adequada recuperació en cas d’un incident.

Complir amb el marc legal i amb les requisits impostos a nivell organitzatiu.

Objectius d'un sistema fiable



+



Objectius d’un sistema fiable

Confidencialitat

L’accés a la informació es produeix sols de forma autoritzada

Objectius d’un sistema fiable

Integritat

La informació no ha sigut modificada sense autorització

Objectius d’un sistema fiable

Disponibilitat

El sistema i les dades estaran disponibles per als usuaris

Objectius d’un sistema fiable

Autenticitat

Es referix a garantir que el missatge ha sigut enviat por qui diu ser.

Objectius d’un sistema fiable

Confidencialitat, Integritat, Disponibilitat

No repudi

Impedix que l’emissor negue haver estat involucrat en una comunicació

Mecanismes de protecció

Autenticació

Autorització

Política contrasenyes

Verificador d'integritat

Xifrat

Còpies de seguretat

SAI / UPS

Control d'accés (físic)

Software anti-malware

Firewall

IDS / IPS

Certificats

Auditoria

Pegats

Snapshots

Confidencialitat, Integritat, Disponibilitat

La seguretat informàtica és diferent a ...

... la Seguretat de la informació

La seguretat informàtica és...

El conjunt de serveis i mecanismes que asseguren la **integritat** i **privacitat** de la **informació**

La seguretat informàtica és...

El conjunt de serveis, mecanismes i polítiques que asseguren que el **mode d'operació** d'un sistema siga **segur**. El que se especificà en la fase de disseny o el que es configurà en temps d'administració.

La seguretat informàtica és...

El conjunt de protocols i mecanismes que asseguren que la **comunicació** entre els sistemes estiga **lliure d'intrusos**.

Confidencialitat, Integritat, Disponibilitat

La seguretat informàtica és...

Assegurar que els recursos del **sistema d'informació** siguen utilitzats de la manera que es va decidir i que l'accés i modificació a la informació, sols siga possible a las persones que es troben acreditades i dins dels límits de la seua autorització

La seguretat de la informació...

Conjunt de mesures preventives i reactives de les **organitzacions** i de els **sistemes tecnològics** que permeten resguardar i **protegir la informació**.

La seguretat de la informació...

Manté la *confidencialitat*, la *disponibilitat* i *integritat* de dades i de la informació.

La seguretat de la informació...

Tracta els riscos, les amenaces, els anàlisis de escenaris, les bones pràctiques, les polítiques empresarials

MESURES DE SEGURETAT

La seguretat de la informació

Les **polítiques de seguretat** defineixen les responsabilitats i regles a seguir per a evitar les amenaces o minimitzar els seus efectes.

La seguretat informàtica

Els **mecanismes de seguretat** són les eines per a garantir la protecció dels sistemes o de la pròpia xarxa

TIPUS MESURES DE SEGURETAT

Segons el recurs a protegir:

- **Seguretat física** : tracta de protegir el maquinari (robatoris, inundacions, incendis …)
  - Mesures: ubicació correcta, control d'accés físic

- **Seguretat lògica**: Tracta de protegir el programari , tant a nivell de sistemes operatius com aplicació
  - Mesures:contrasenyes, permisos d'usuari, xifrat de dades, programari antimalware, filtrat de connexions ...

TIPUS MESURES DE SEGURETAT

Segons el moment en què es posen en marxa les mesures.

- **Seguretat activa**: La seguretat activa en informàtica és la que s'aconsegueix usant elements que **tracten de previndre qualsevol tipus d'atac en un sistema**. Tracten d'evitar un incident de seguretat.

- **Seguretat passiva**: S'entenen aquelles mesures posades a la disposició del sistema per a la **reducció els efectes produïts per un incident**. Se sol associar a la seguretat física i les còpies de seguretat que permeten minimitzar l'efecte d'un incident.

RISC

$$\text{Risc} = \frac{\text{Amenaces} * \text{Vulnerabilitats}}{\text{Mesures de seguretat}}$$

Gestió del risc

- Evitar el risc.
- Reduir el risc.
- Retindre, assumir o acceptar el risc.
- Transferir o compartir el risc

ELEMENTS VULNERABLES

La seguretat és un problema integral

Els problemes de seguretat no poden tractar-se aïlladament

Sistema de seguretat = TECNOLOGIA + ORGANITZACIÓ

La seguretat informàtica precisa d'un nivell organitzatiu que possibilite unes normes y una pauta comuna per part dels usuaris del sistema

Elements a protegir:

- **Maquinari**
- **Programari**
- **Dades** ← El més important i difícil de recuperar
- **Comunicacions**
- **Factor Humà** ← El més difícil de controlar

ELEMENTS VULNERABLES

Sistema de seguretat = TECNOLOGIA + ORGANITZACIÓ

SEGURETAT INFORMÀTICA : TECNOLOGIA

SEGURETAT DE LA INFORMACIÓ : ORGANITZACIÓ

NIVELLS DE PROFUNDITAT

- **Legals:** LOPDGDD RGPD
- **Organitzatius**: nivells d'accés , contrasenyes
- **Físiques**: ubicació d'equips, subministre elèctric
- **Comunicacions:** protocols segurs

EIXIDES PROFESSIONALS

- /las-20-mejores-carreras-en.html

AMENACES

INTERNES
EXTERNES

Amenaces provocades por persones

- El propi personal de la organització (desconeixement o no)
  - Insider (/2021/10/11/ser_malaga/)
  - Formació (caida-de-facebook, 2021)
- **Hacker** :Expert o gurú en aspectes tècnics .

  Hacker≠Ciberdelinqüent

  Chema Alonso **TEDx Talks** https://www.youtube.com/watch?v=zQ470q7z91k
  - **Newbie**: Hacker novençà
  - **Wannaber** : Els interessa el tema del hacking
  - **Lammer o Sripit-Kiddies**: pretenen fer hacking (sense coneixements d'informàtica

AMENACES FÍSIQUES LÒGIQUES

Amenaces físiques y ambientals

Las amenaces físiques i ambientals afecten a les instal·lacions i el hardware contingut en estes i suposen el primer nivell de seguretat a protegir per garantir la disponibilitat dels sistemes

- ➔ Robatoris, sabotatges, destrucció de sistemes
- ➔ Talls de subministre elèctric
- ➔ Condicions atmosfèriques : humitat, altes o baixes temperatures
- ➔ Interferències electromagnètiques

AMENACES

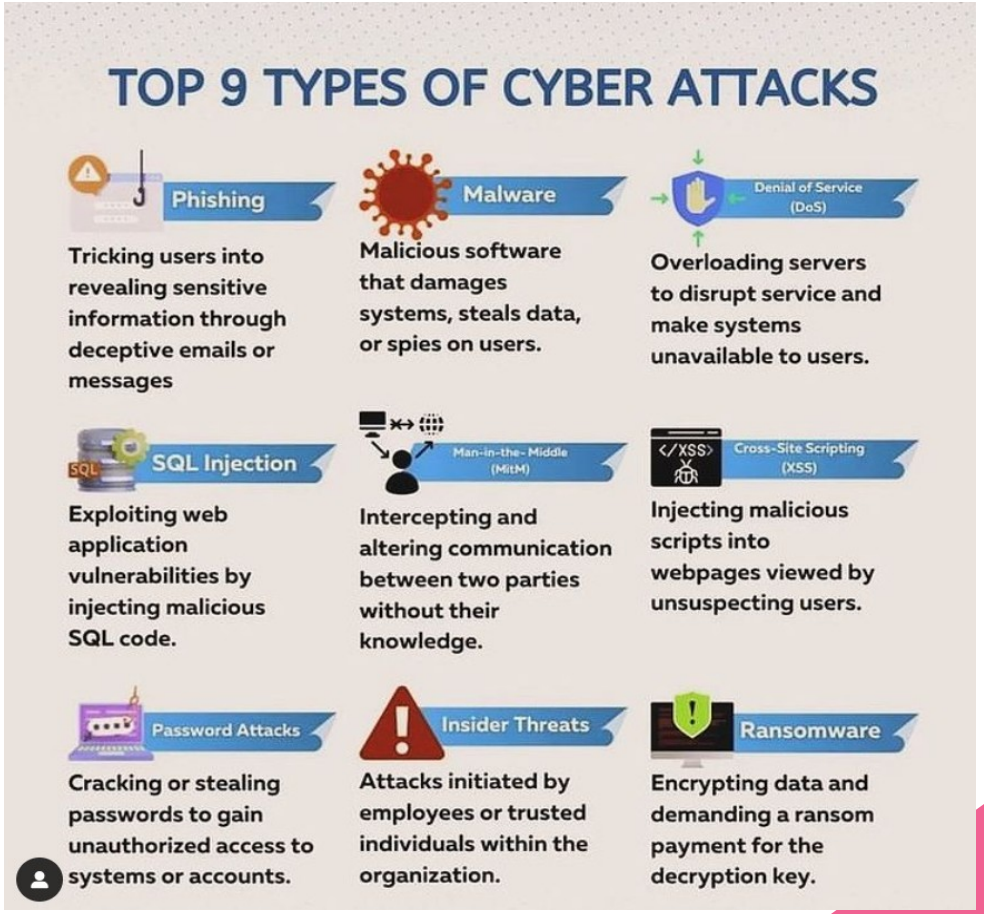
Amenaces lògiques

Es un software o codi que d'una forma o altra poden afectar o danyar al nostre sistema, creat de forma intencionada per allò , **malware**

- *Rogueware* o falsos programes de seguretat
- *Portes traseres* o backdoors
- *Virus*
- *Cucs* o worm
- *Troians*
- *Keylogger*
- *Rootkit*
- *Programes conills o bacteris*
- *Canals cuberts*

TÈCNIQUES D'ATAC

Las amenaces es poden classificar en funció de la tècnica que s'use per a realitzar l'atac



TÈCNIQUES D'ATAC

Las amenaces es poden classificar en funció de la tècnica que s'use per a realitzar l'atac
https://www.youtube.com/watch?v=gpdXALfadIM **TEDx Talks** Javier Zubieta

- *Scam*
- Malware
- *Ingenieria Social* Test de Phishing (spear phishing, whaling)
- *Estafa nigeriana*
- Spam
- Sniffing
- *Spoofing*
- *Pharming* (*El pharming consisteix a disfressar llocs web falsos com si foren autèntics per a obtindre així la informació que s'introduïsca en ells.*)
- Password cracking
- Botnet
- Denegació de servei DoS , DDoS
- SQLi

Apren Ciberseguretat

#AprendeCiberseguridad con INCIBE

VuInerabilitats

- *Pentesting*
- *Adware*
- *Defacement*
- *Cybersquatting*
- *Typosquatting*
- *Malvertising*
- *Spear phising*
- *Deepfakes*
- *Man-in-the-Middle*
- *Pretexting*
- *Jailbreaking*
- *Cyberbullying*
- *Warshipping*
- *Hacker vs Ciberdelincuente*
- *Phishing*
- *Spyware*
- *Smishing*
- *Vishing*
- *Malware*
- *Ransonware*
- *Ingenieria social*
- *Sexting*
- *Sextorsion*
- *Grooming*
- *Mediación parental*

VULNERABILITAT

- Una **vulnerabilitat** (en termes d'informàtica) és una feblesa o fallada en un sistema d'informació que posa en risc la seguretat de la informació podent permetre que un atacant puga comprometre la integritat, disponibilitat o confidencialitat d'aquesta, per la qual cosa és necessari trobar-les i eliminar-les al més prompte possible. Aquests «forats» poden tindre diferents orígens per exemple: fallades de disseny, errors de configuració o mancances de procediments.
- Una **amenaça** és tota acció que aprofita una vulnerabilitat per a atemptar contra la seguretat d'un sistema d'informació. És a dir, que podria tindre un potencial efecte negatiu sobre algun element dels nostres sistemes. Les amenaces poden procedir d'atacs (frau, robatori, virus), successos físics (incendis, inundacions) o negligència i decisions institucionals (mal maneig de contrasenyes, no usar xifratge).

VULNERABILITAT

- Els **vectors d'atac** són la ruta triada per a explotar les febleses o vulnerabilitats que poden ser presents en ordinadors, aplicacions, servidors de correu electrònic, programari, pàgines web, navegadors, xarxes, etc., i dur a terme atacs informàtics
- Un **atac informàtic** fa referència a la realització d'una temptativa de posar en risc la seguretat informàtica d'un equip o conjunt d'equips, amb la finalitat de causar danys deliberats que afectin el seu funcionament

VULNERABILITAT

- Quan es descobreix una vulnerabilitat, es detalla en un “paper”
- Quan s'informa d'una vulnerabilitat, es valora i es classifica
- Existeixen bases de dades de vulnerabilitats

Calculadora de perillositat d'una vulnerabilitat https://www.first.org/cvss/

BBDD vulnerabilitats https://nvd.nist.gov/

VULNERABILITAT

0-day

Una nova vulnerabilitat per a la qual no es van crear pegats o revisions, i que s'empra per a dur a terme un atac

Vulnerabilidad zero-day

Definición zero-day

CSIRT - CERT

Computer Security Incident Response Team
Equipo de respuesta a incidentes de seguridad informáticos

Computer Emergency Response Team
Centro de respuesta ante emergencias informaticas

INCIBE *https://www.incibe-cert.es/*

Cert CV *http://www.csirtcv.gva.es/* miembro de *csirt.es*

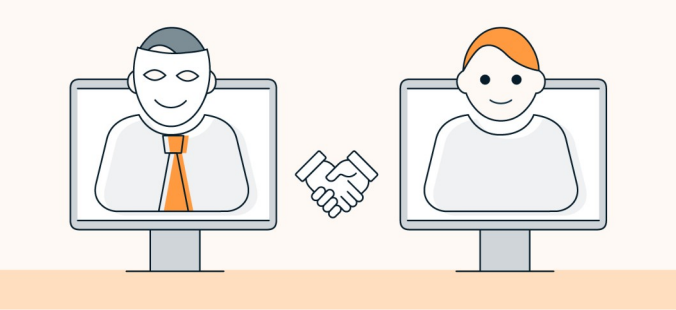
CCN-CERT *https://www.ccn-cert.cni.es/*

CSIRTs otros paises *enisa.europa.eu*

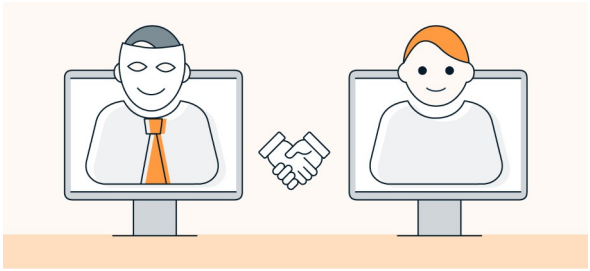
Enginyeria Social

L'enginyeria social és una tècnica utilitzada pels atacants per a manipular a les persones amb la finalitat d'obtindre accés a informació confidencial, sistemes o recursos sense necessitat de vulnerar sistemes de seguretat tradicionals.

En lloc d'aprofitar fallades en programari o maquinari, els atacants s'enfoquen a explotar la psicologia humana, com la confiança, la por o la urgència, per a induir a les víctimes a realitzar accions que comprometen la seua seguretat



Enginyeria Social



Vectors d'atac a persones

- Reciprocitat
- Urgència
- Consistència o costum
- Confiança
- Autoritat com a via per a la suplantació d'identitat
- Validació social o necessitat d'aprovació del col·lectiu

Enginyeria Social

Existeixen diverses formes en les quals els atacants empren l'enginyeria social per a aconseguir els seus objectius. Els mètodes més comuns inclouen:

- Phishing
- Vishing (telefònic)
- Baiting (S'oferix algo de valor, com un arxiu free , un pendrive en un pàrquing)
- Deep fake
- Quizzes
- Pretexting

Enllaç INCIBE

Prevenció:

Verificar les fonts
Desconfiar de sol·licituds URGENTS
No fer click en enllaços desconeguts
Donar formació al usuaris i empleats
Usar MFA sempre que siga possible