

# «Bàsics» de la Ciberseguretat



René Serral <[rene.serral@upc.edu](mailto:rene.serral@upc.edu)>

# Qui sóc?

**René Serral Gracià**

**Director de l'esCERT-UPC**

**Director Acadèmic de l'àrea de  
Ciberseguretat a l'inLab FIB**

**20+ d'experiència docent a la FIB**

Operating Systems Administration

Cybersecurity

Cloud Computing



rene.serral@upc.edu



@serralRene



rené-serral-gracià

# Agenda

Introducció

Malware

Enginyeria Social

Fake news i com les podem combatre

Què és un pla de ciberseguretat?

Novetats i tendències en  
Ciberseguretat



# Seguretat?

Ús massiu d'Internet

**Eina extremadament poderosa**

Però un gran poder... requereix una gran responsabilitat

**Desconeixement dels usuaris**

**Ús lucratiu de la xarxa**

**Aparició de (ciber)delincuents**

On hi ha calers...





# Què busquem?



**Confidencialitat:** garantir que les dades només siguin accessibles per a les persones autoritzades

**Integritat:** Protegir la fiabilitat de les dades evitant modificacions/destrucció no autoritzades

**Disponibilitat:** garantir que les dades i els sistemes siguin accessibles i utilitzables quan sigui necessari pels usuaris legítims



# Què busquem?



**Autenticació:** verificació de la identitat d'usuaris, sistemes o dispositius

**Autorització:** Atorgar o denegar drets d'accés a entitats autenticades

**Accountability:** Seguiment i registre de les activitats de les entitats autenticades (o no) per auditoria



# Com ho podem aconseguir?

## Patint molt...

### Generalment xifrar ens proporciona la primera línia de defensa

Proporciona confidencialitat i integritat

Senta la base per la posterior Autenticació

### **PERO** no negligir altres aspectes

Robustesa de les contrasenyes

M2F

## Sentit comú



# Malware

## Què és?

Aplicacions malicioses

## Què fan?

Robar informació – dades personals

Robar recursos → CPU

Robar diners

Segrestar dades i sistemes

## Com?

Virus, Worms, Troians, ...

Aprofitant vulnerabilitats del programari

Amb Enginyeria Social







# Qui són els atacants?

## Advanced

Tenen grans coneixements tècnics

Molts calers

## Persistent

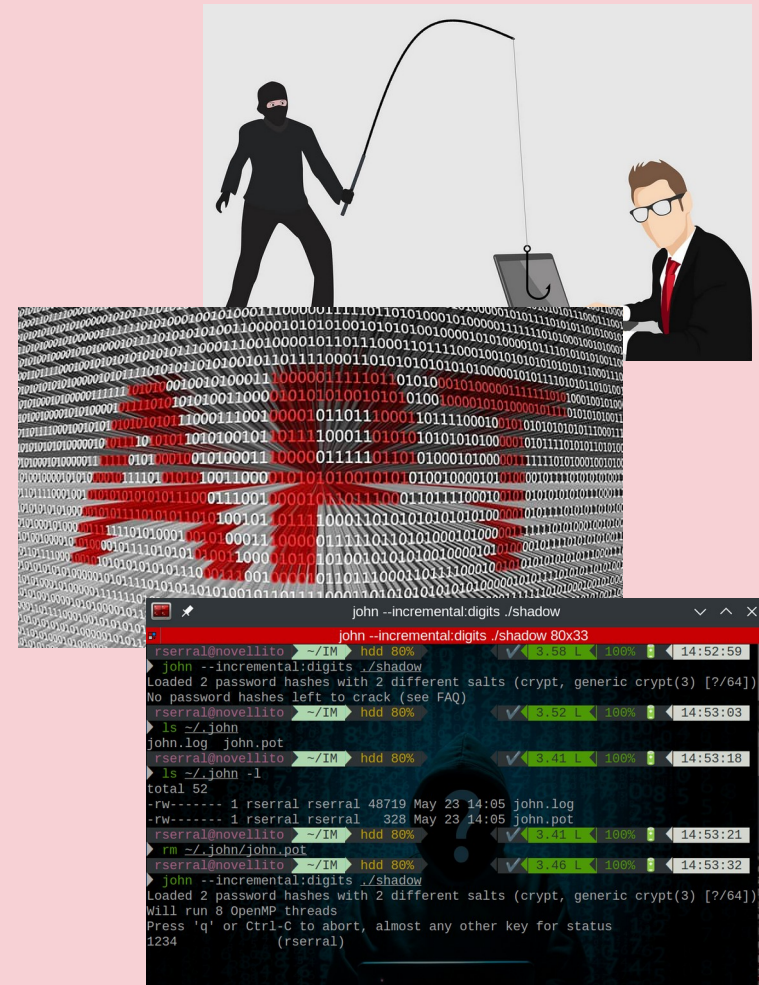
Els atacs poden durar mesos → Exfiltració

Cerquen mecanismes per garantir la persistència

## Threat

Desestabilització econòmica i política

Afectació a la reputació de l'”enemic”



# Ransomware

**Perpetrat generalment per APT**

**Molts cops amb víctimes seleccionades  
curosament**

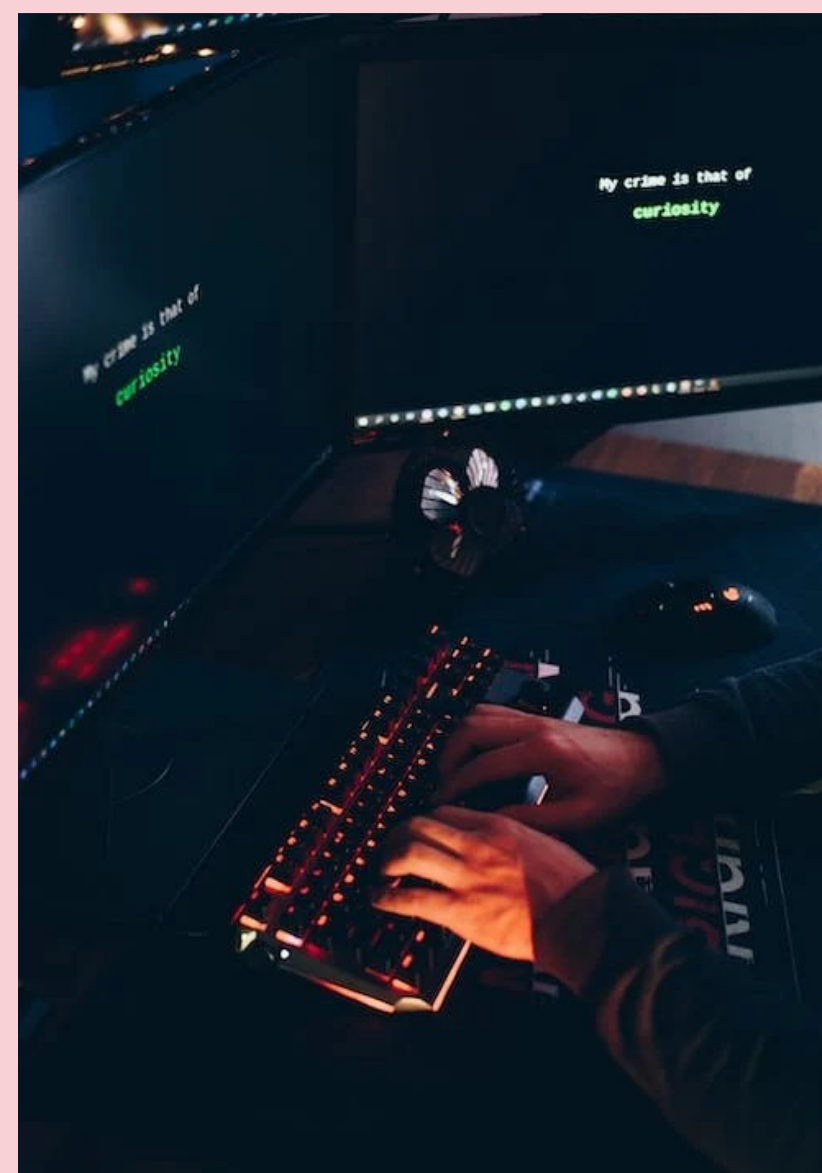
**Característiques dels atacs**

Aprofiten de o-day i vulnerabilitats

Utilitzen enginyeria social

**Objectius**

Obtenir un rèdit econòmic



# Ransomware: Passos

**Accedir al sistema**

**Expandir-se per tot el sistema sigilosament**

**Exfiltrar informació**

**Coordinar un atac a tota la infraestructura**

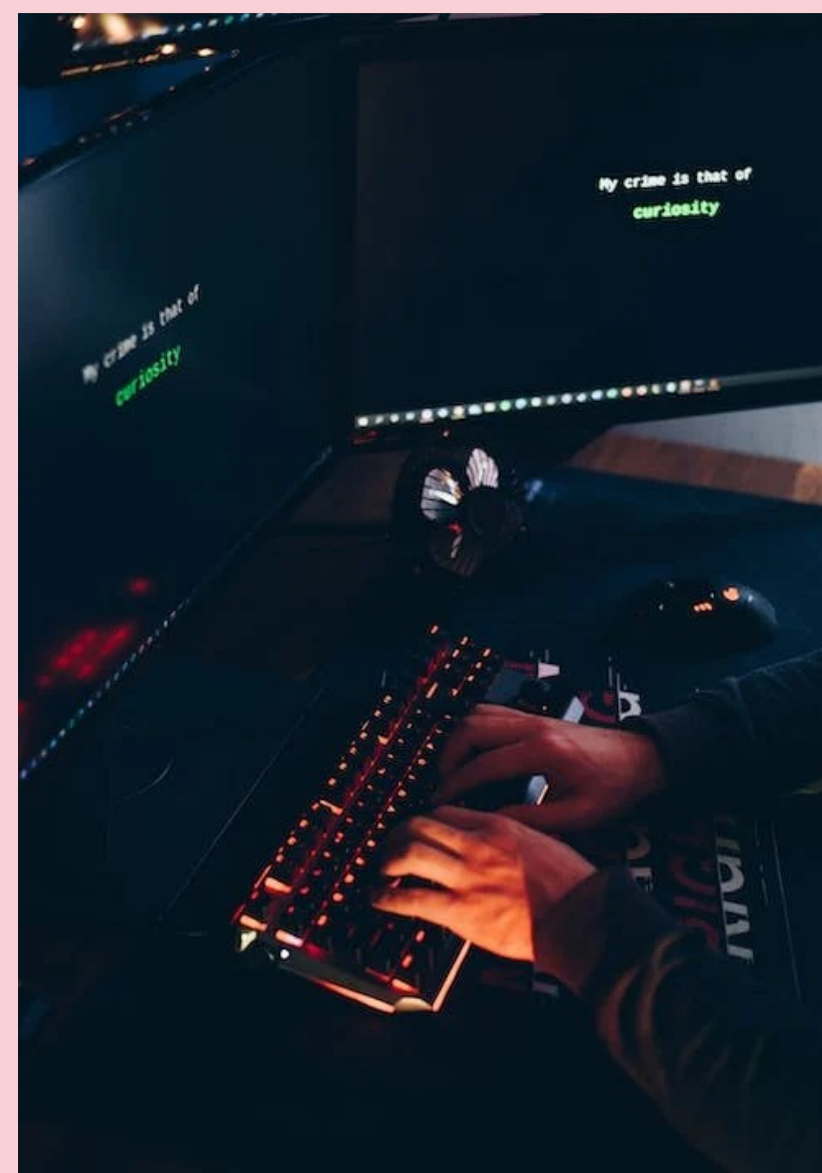
Xifrant les dades

Invalidant els sistemes

**Demandar un rescat per les dades**

Generalment implica extorsió i amenaces

**Sortir del sistema (o no...)**





# Cryptojacking

**Aconseguir recursos d'un dispositiu aliè**

CPU

RAM

Disc

**Usar els dispositius per aconseguir criptomonedes**

**Cada cop menys comú**

Minar criptomonedes ja no surt a compte



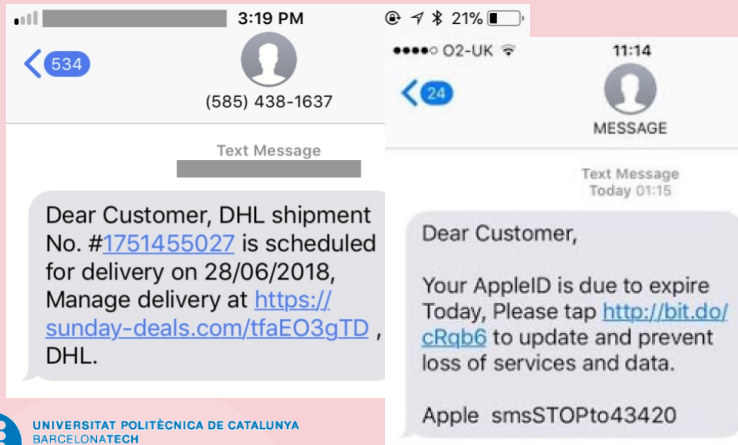
# Enginyeria Social

Procés iteratiu per a aconseguir penetrar un sistema

Usant relacions personals

Basat en l'astúcia

Basat en la teoria de grans números



# Enginyeria Social

**Fa temps es basava en atacs pràcticament aleatoris**

**Actualment es realitzen atacs dirigits**

A través de OSINT (Open Source Intelligence)

Google/Twitter/LinkedIn

A través d'atacs a la cadena de suministrament

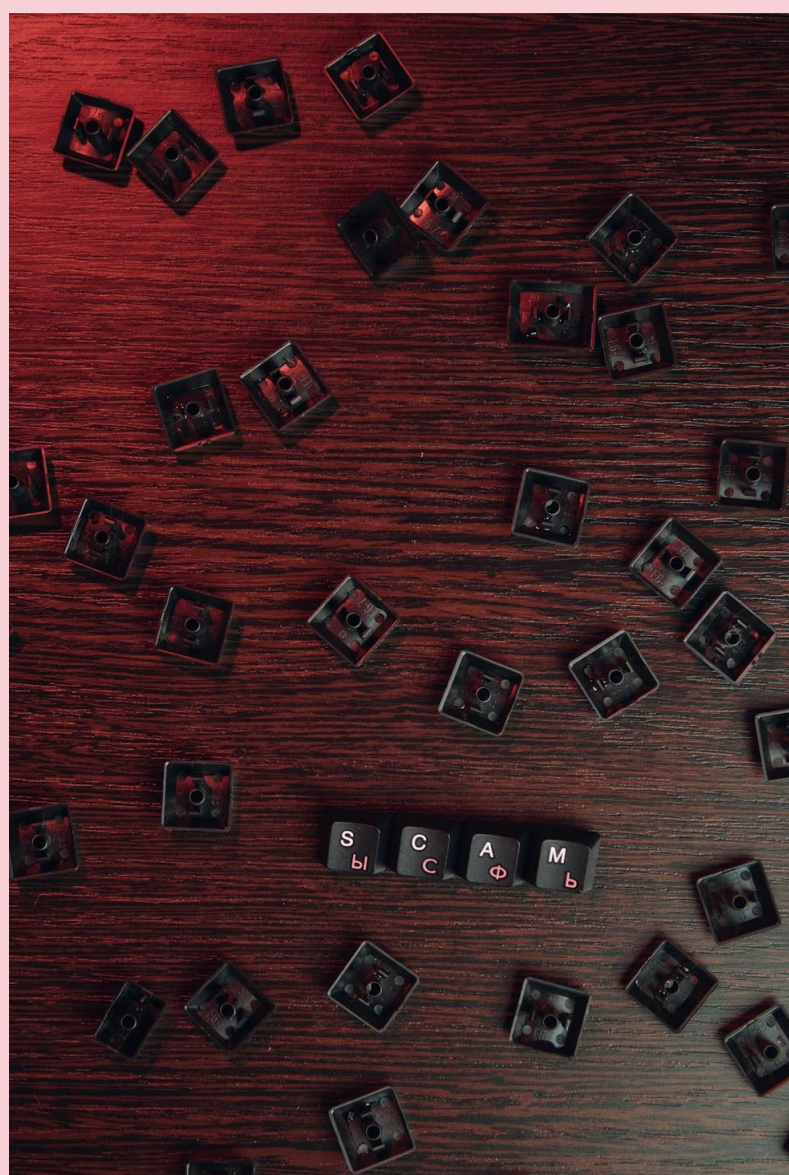
**Històricament fàcils de detectar**

Faltes i mal escrit

Llenguatge general

**Actualment evolucionat**

Utilitzant IA





# Mecanismes

## Phishing

Correus electrònics amb enllaços maliciosos

Amb promeses falses

Imitant una companya coneguda

## Vishing

Similar al phishing però a través de trucades telefòniques

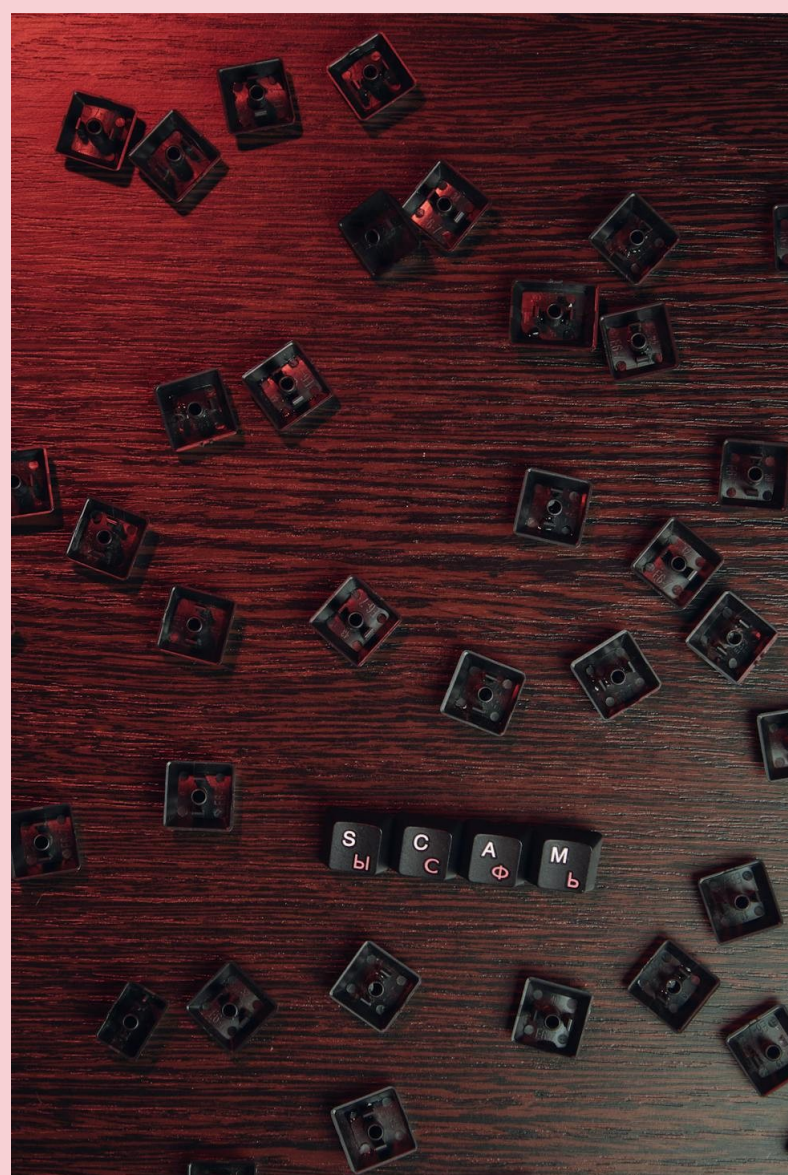
Alerta de virus

Peticions urgents de calers

## Smishing

Similar però a través d'SMS

O WhatsApp





# Physhing

AT&T 4G 3:50 PM

Messages (1) +1 (202) 609-0301 Details

Text Message  
Today 3:40 PM

WARNING:(Criminal Investigation Division) I.R.S is filing lawsuit against you, for more information call on +1 7038798780 on urgent basis, Otherwise your arrest warrant will be forwarded to your local police department and your property and bank accounts and social benefits will be frozen by government.

CORREOS

Su paquete ha llegado a **20 de marzo**. Courier no pudo entregar una carta certificada a usted. Imprima la información de envío y mostrarla en la oficina de correos para recibir la carta certificada.



CD 438685108339

[Descargar información sobre su envío](#)

Si la carta certificada no se recibe dentro de los 30 días laborables Correos tendrá derecho a reclamar una indemnización a usted para el día manteniendo en la cantidad de 7,55 euros por cada día de cumplir. Usted puede encontrar la información sobre el procedimiento y las condiciones de la carta de mantener en la oficina más cercana. Este es un mensaje generado automáticamente.

Condiciones y Términos del Servicio de localización de envíos

La consulta del estado detallado para envíos individuales y del estado final para envíos masivos es un servicio gratuito que Correos le ofrece para sus envíos remitidos con carácter registrado. Este servicio es de carácter informativo sin que en ningún caso sustituya la información que ud. puede obtener mediante acuse de recibo o certificación de servicios postales. Correos no se responsabiliza de los errores u omisión de información, por lo que advierte que no se adopten decisiones o acciones derivadas de la información obtenida por este servicio.

[Haga clic aquí para darse de baja.](#)

@ Copyright 2014 Sociedad Estatal Correos y Telégrafos, S.A.

PayPal.com @security@halifax.co.uk para usuario [mostrar detalles](#) 10:17 (Hace 2 minutos) Responder

Este mensaje no se envió a "Spam" debido a un filtro que creaste. [Editar filtros](#)

PayPal

PayPal suspendido temporalmente su cuenta. Motivo: Incumplimiento de Facturación. Necesitamos completar una actualización de cuenta para desbloquear su cuenta. Una vez que haya completado el proceso, te enviaremos una notificación de correo electrónico que su cuenta esta disponible de nuevo.

Después eso, se puede acceder su cuenta en cualquier momento. La información proporcionada será tratada de forma confidencial y se almacena en nuestra base de datos segura. Si no proporcionan la información requerida de su cuenta era automáticamente eliminado de PayPal base de datos. Para asegurarnos de su autenticidad rogamos reactivar su cuenta desde el siguiente enlace:

[https://www.paypal.com/es/cgi-bin/webscr?cmd=\\_login-run?db](https://www.paypal.com/es/cgi-bin/webscr?cmd=_login-run?db)

[Help Centre](#) | [Security Centre](#)

Please do not reply to this email because we are not monitoring this inbox. To get in touch with us, log in to your account and click "Contact Us" at the bottom of any page.

Copyright © 2011 PayPal. All rights reserved.

PayPal (Europe) S.à.r.l.et Cie, S.C.A.  
Societe en Commandite par Actions  
Registered office: 22-24 Boulevard Royal, L-2449 Luxembourg  
RCS Luxembourg B 118 349  
PayPal Email ID PP881

+509 200 000 0000

Unblock | Add

March 6, 2022

Messages and calls are end-to-end encrypted. No one outside of this chat, not even WhatsApp, can read or listen to them. Tap to learn more.

Hola buenos días cómo estás? Espero que te encuentres bien adivina quién te escribe desde el extranjero 😊😊 07:04

No idea 08:09 ✓

March 7, 2022

Venga dime cuál de tus primas te puede estar escribiendo desde el extranjero 😊 19:51

Dime tres nombres y te diré quién soy si adivinas 19:51

Te has ganado un bloqueo. Felicidades 21:11 ✓

You blocked this contact. Tap to unblock.

17:58

SANTANDER

viernes, 19 de noviembre de 2021

ACCESO NO AUTORIZADO esta conectado a su cuenta online. Si no reconoce este acceso verifique inmediatamente: [bit.ly/2ZZ2WHAD](https://bit.ly/2ZZ2WHAD) 21:26

# Com evitar la Enginyeria Social

## Des del punt de vista de l'atacant té alguns problemes

Requereix la intervenció de l'usuari

De cops és complicat generar un missatge creïble

## Però compte!

Els humans ens despistem molt fàcilment

# Conscienciació



# Contrasenyas

## Com haurien de ser?

Mínim 12 caràcters

Lletres, números i signes de puntuació

Que no siguin paraules o dates conegudes

## On els guardem?

Navegador?

Cloud?

Arxius al disc?

## A sobre...

Renovacions periòdiques

Diferents a cada lloc





# Contrasenyas

**Millor no usar-les... però malauradament no podem**

**La recomanació és utilitzar gestors de contrasenyes**

**Habilitar el Multi-Factor d'Autenticació**

**Es pot confiar amb la federació d'identitats**

Tot i així compte amb els permisos que es donen





# Contrasenyas

Millor no usar-les... però malauradament no pot

La rec  
contra


Habil

Es pot  
d'ider


Tot i  
done

Sign in with Google

My GIS Test App wants access to your Google Account

 elisa.g.beckett@gmail.com

When you allow this access, **My GIS Test App** will be able to

-  See and download any calendar you can access using your Google Calendar. [Learn more](#)

**Make sure you trust My GIS Test App**











You may be sharing sensitive info with this site or app. You can always see or remove access in your [Google Account](#).

Learn how Google helps you [share data safely](#).

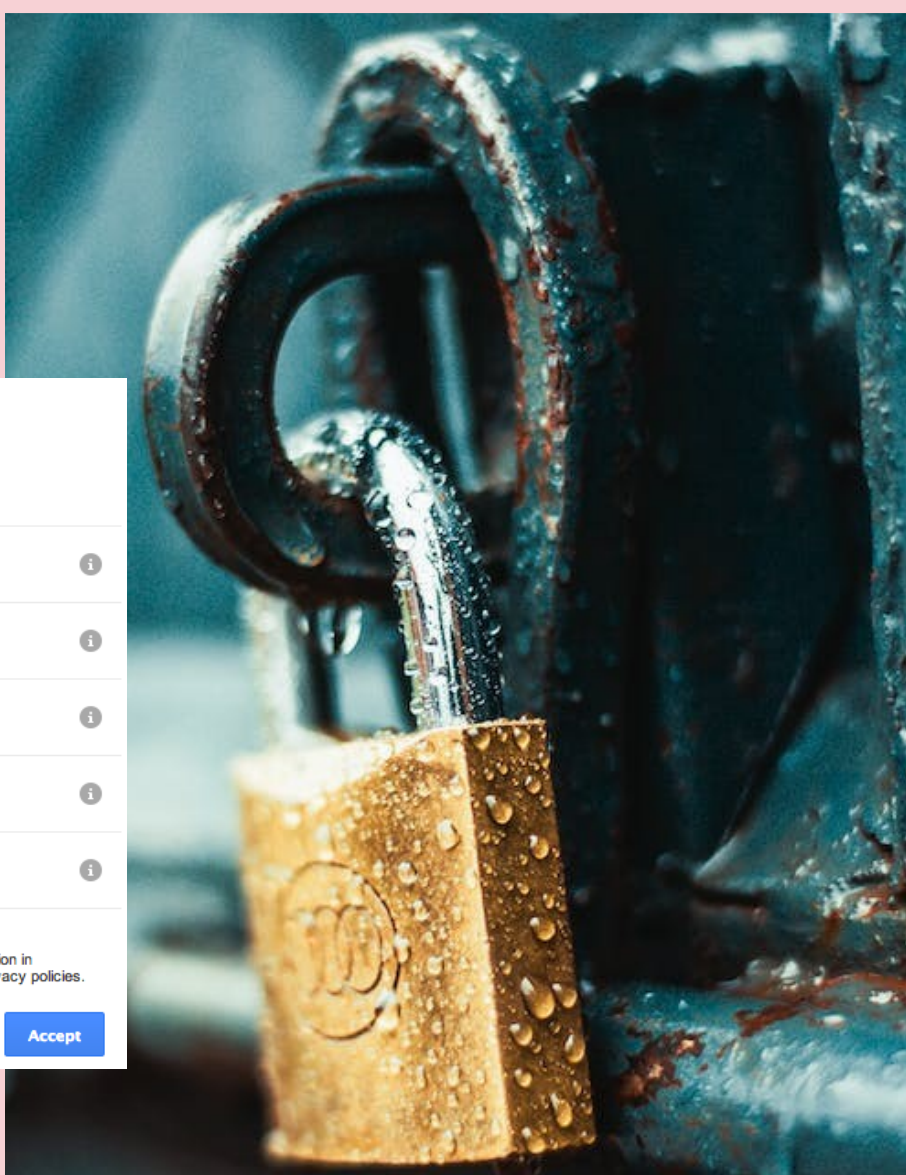
See My GIS Test App's [Privacy Policy](#) and [Terms of Service](#).

**Mitro Google Sync - Dev**

This app would like to:

-  Know who you are on Google 
-  View your email address 
-  View users on your domain 
-  View groups on your domain 
-  View group subscriptions on your domain 

Mitro Google Sync - Dev and Google will use this information in accordance with their respective terms of service and privacy policies.



# Fake news i com les podem combatre

## La falta de moderació a les xarxes socials porta a l'abús per part de certs actors

Poder de l'anonimat

Distància física...

## No es poden evitar

## Es recomana tenir presència activa en xarxes socials

Així respondre activament a qualsevol notícia

## Anàlisi de percepció social

Ajuda a perfilar els missatges i mantenir la bona reputació





# Què és un pla de ciberseguretat?

És un document per estipular les polítiques de seguretat d'una organització

Detalla les accions per millorar la seguretat

Procedimentalitzza la resposta a incidents

Ajuda en la comunicació interna de l'estat de la organització



# Què permet un pla?

**Donar una ràpida resposta a les amenaces**

**Accelera la resposta a incidents**

**En molts casos permet prevenir els problemes abans que passin**

**Posa de manifest l'estat de seguretat**





# Passos per realitzar un pla

- 1) **Avaluació dels riscos de seguretat**
- 2) **Establir objectius de seguretat**
- 3) **Avaluar la tecnologia de l'empresa**
- 4) **Seleccionar un marc de seguretat**
- 5) **Revisar les polítiques de seguretat**
- 6) **Crear un pla de gestió de riscos**
- 7) **Implementar una estratègia**
- 8) **Avaluar l'estratègia**



# Bones pràctiques en el disseny d'un pla

**Entendre que és necessari**

**Forma part d'un procés iteratiu**

**La ciberseguretat és transversal**

Pel que tota l'empresa n'ha d'estar conscienciada

**Estar al dia de les normatives**

Depenent del negoci estem obligats a prendre unes mesures concretes





# Bones pràctiques en el disseny d'un pla

**No negligir-ne la seva importància**

**Ser ambiciós amb els objectius**

Però sense perdre de vista la realitat

**Revisar-lo periòdicament**

**Ser proactius en la seva realització**



# Bones pràctiques en el disseny d'un pla

## Fer un pla és un procés costós

Cal prioritzar les parts més crítiques

Anar iterant cap a les que no ho són tant

Millor no esperar a tenir un pla finalitzat per començar a aplicar-lo

## Cal començar per accions petites

Excel amb les diferents accions

Actualitzar el servidor de base de dades

Configurar el firewall

## Tenir visió a llarg plaç per garantir-ne l'escalabilitat





# Novetats i tendències en Ciberseguretat

## Intel·ligència artificial

Hype però està començant a donar fruits

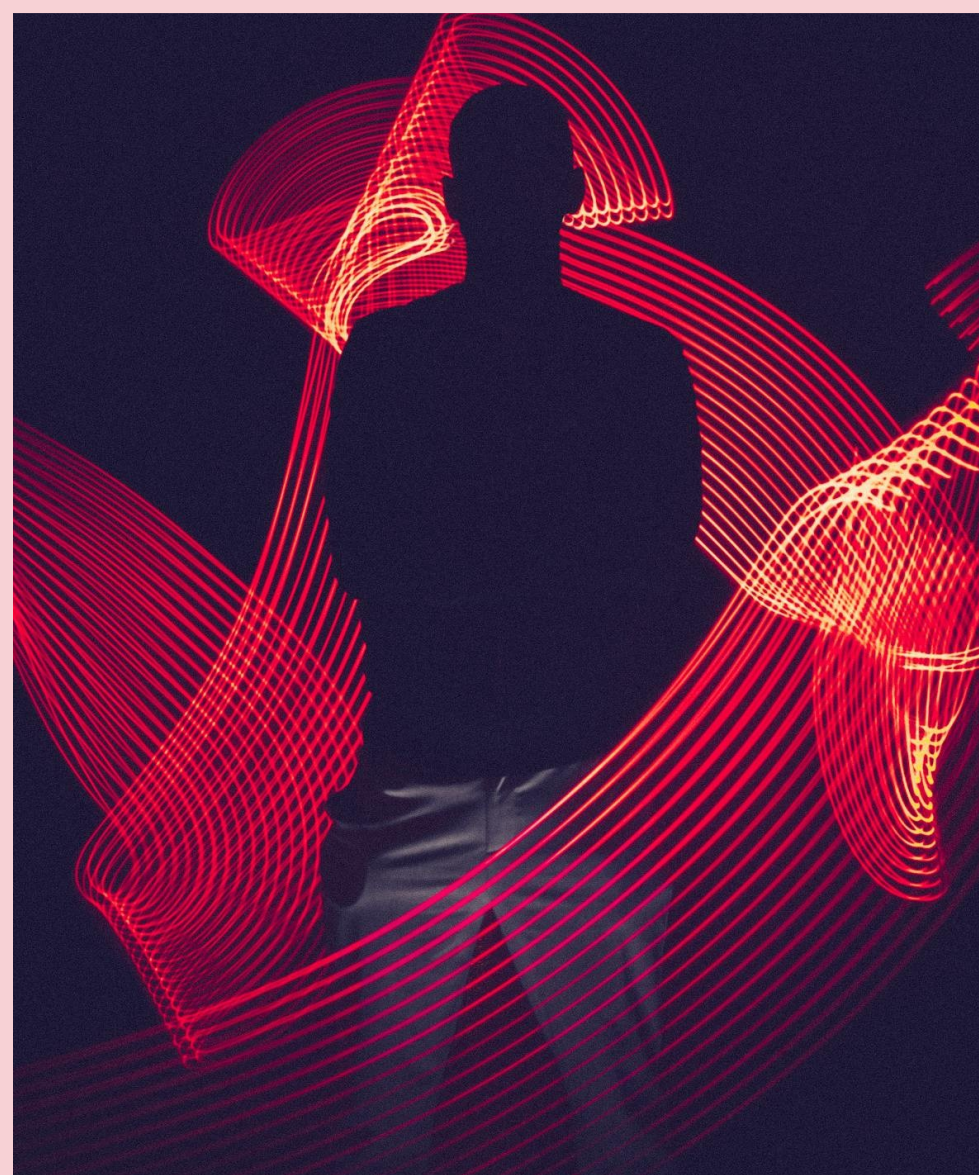
Models basats en el comportament

## Automatització en la resposta

Fins ara ha suposat més problemes que solucions

## Computació quàntica

Encara molt incipient però serà brutalment disruptiu quan arribi





A person is silhouetted against a sunset over a lake. The sun is low on the horizon, creating a bright orange glow and a reflection on the water. The person is standing on the shore, looking out at the water. The background shows rolling hills and a forest. The word "Preguntas?" is written in white, italicized font inside a semi-transparent white box in the upper center of the image.

*Preguntas?*