Generalitat de Catalunya
Centre de Seguretat de la Informació de Catalunya

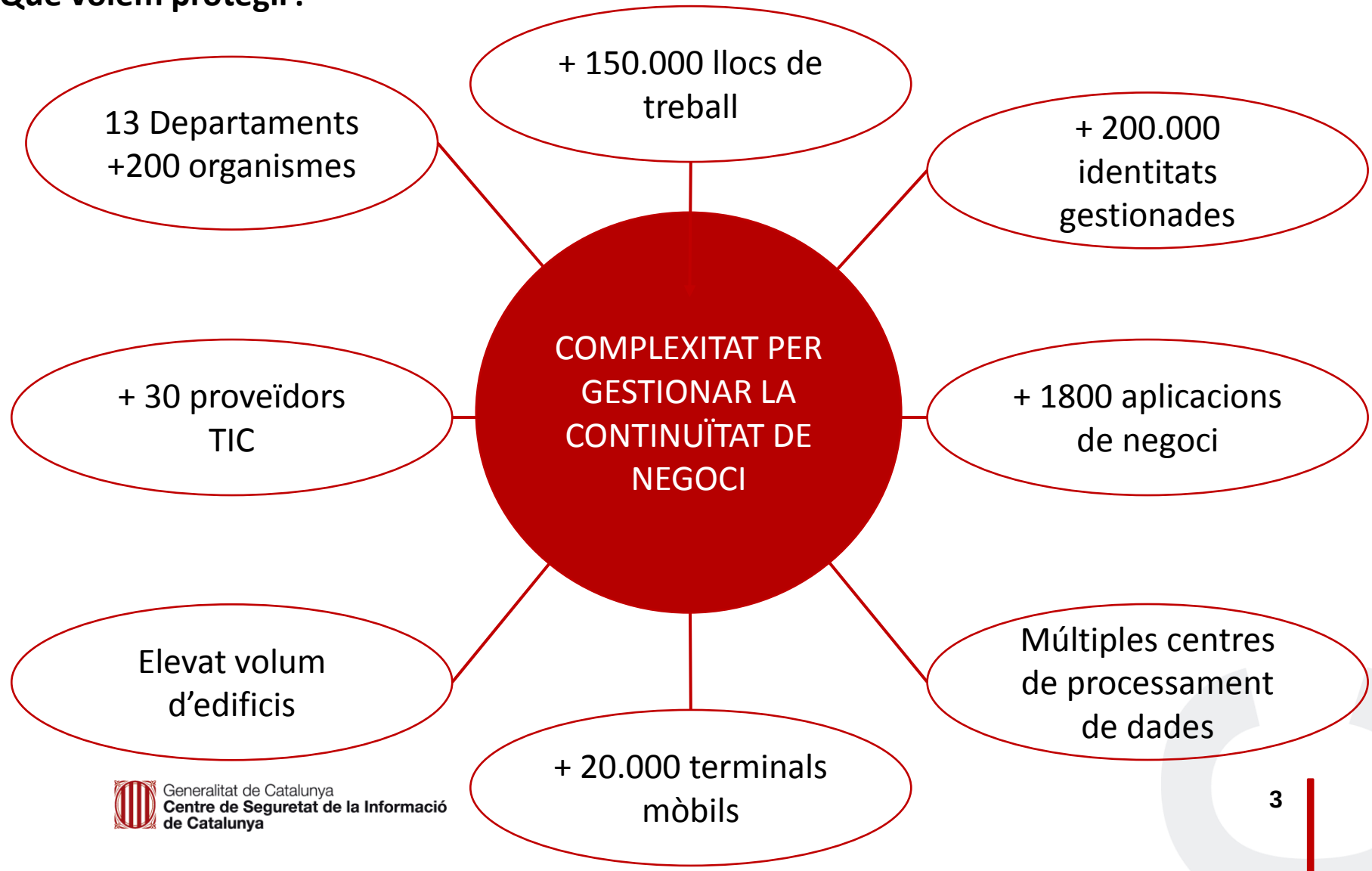
Continuïtat de negoci - Els nous escenaris de risc

David Forner

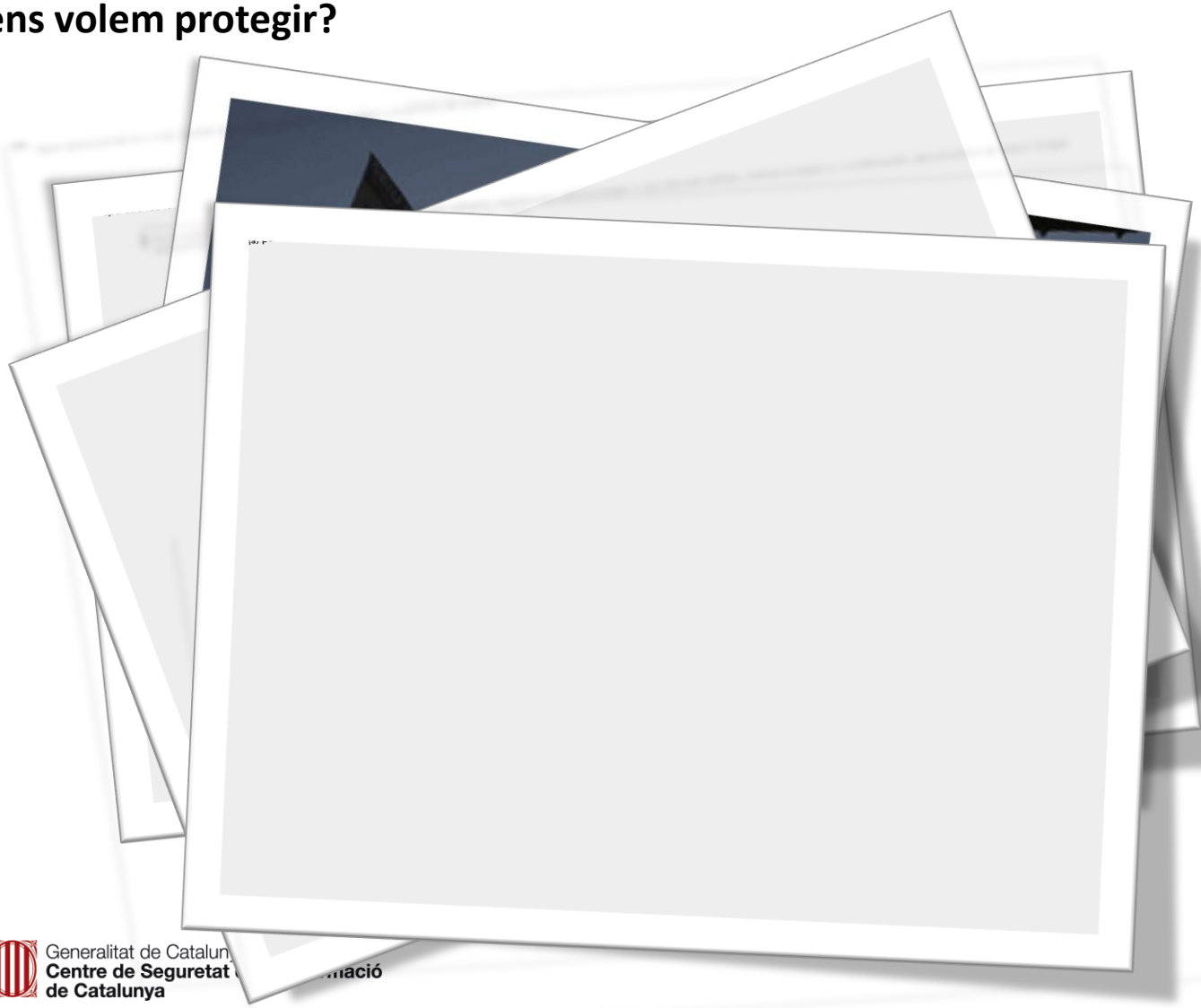
Centre de Seguretat de la Informació de Catalunya

ÍNDEX

Què volem protegir?



De què ens volem protegir?



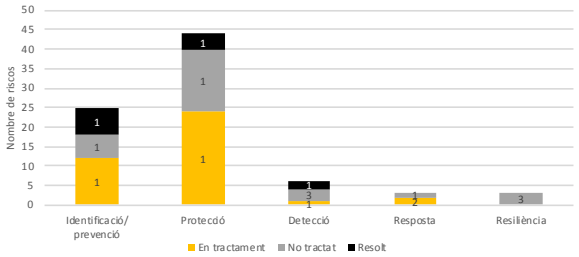
Com ens volem protegir?

Com ens volem protegir?

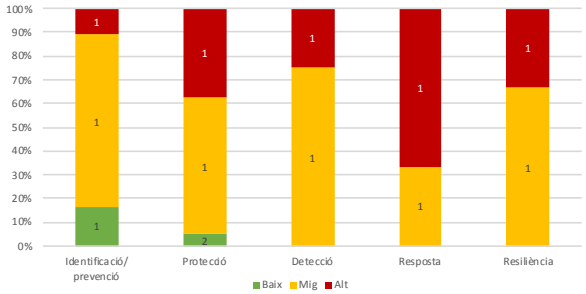
- Prevenció
- Protecció
- Detecció
- Resposta
- Resiliència

L'estat actual dels riscos és:

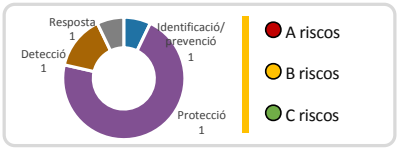
- N riscos mitigats
- J riscos en tractament
- P riscos no tractats



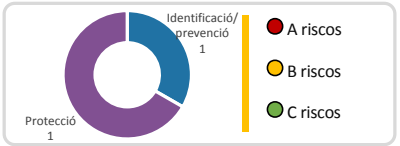
Dels riscos no mitigats, els seus nivells de risc i la seva classificació per funció és la següent:



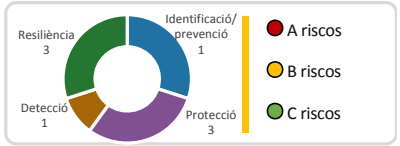
Lloc de Treball i Correu



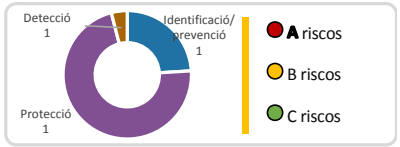
Aplicacions



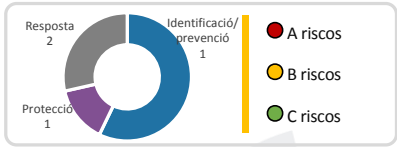
CPDs



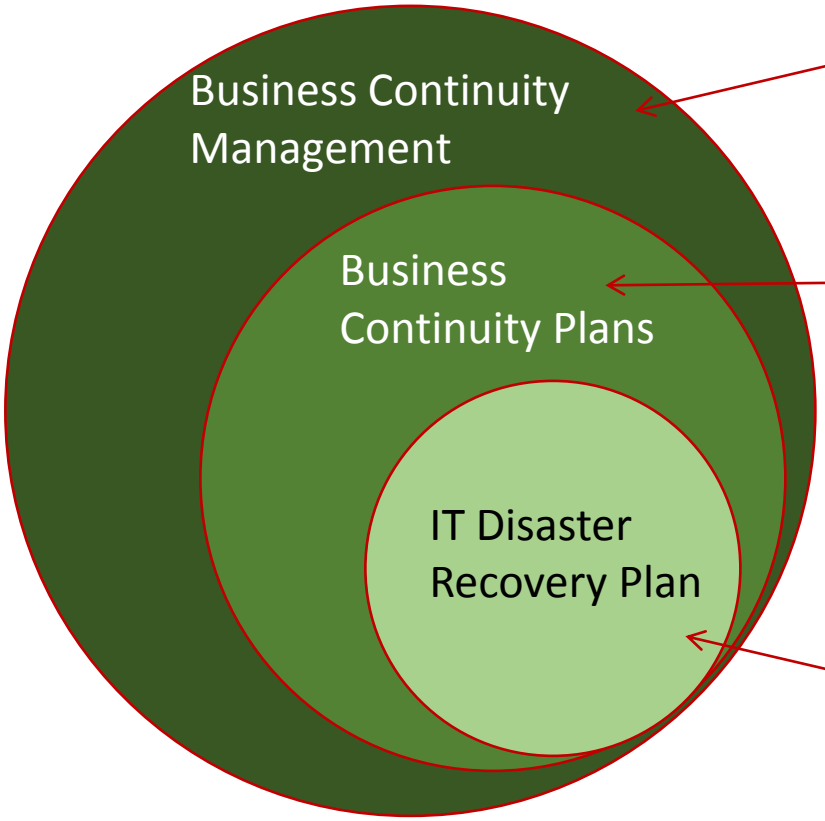
Comunic.



Transversal



On ens trobem ara?



Gestión global (Sistema de Gestión)

ISO 22301

112 emergències

DOGC
Diari Oficial de la Generalitat de Catalunya

- Identificació de procesos i actius crítics: BIAs per tots els departaments
- Anàlisi de riscos
- Proves de recuperació amb el negoci
- Etc.

Recuperación Tecnológica
- PRD
- Recuperació còpies

MARC METODOLÒGIC

On ens trobem ara?

- Regulacions
  - Llei de protecció d'infraestructures crítiques
  - Esquema Nacional de Seguretat (ENS)
  - Requeriments de la UE per rebre els fonts FEDER/FEADER
- Normativa
  - ISO 22301.
  - ISO 27001/ 27002.
  - ISO 27018 (Cloud).
- Altres referències
  - CCM (Cloud Control Matrix) de la CSA.

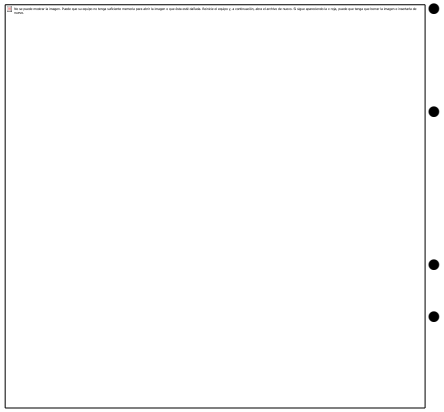
ÍNDEX

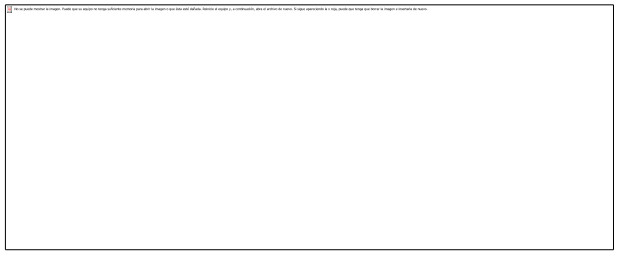
COM L'EVOLUCIÓ DE LES AMENACES HA INFLUÏT EN LA CONTINUÏTAT DE NEGOCI

SECTOR INDUSTRIAL

1997 → 2018

- ICS aïllats de xarxes externes
- Prioritat en el funcionalment de la instal·lació (fiabilitat i predictibilitat) – Control de processos
- Safety
- La seguretat lògica no prioritària
- Abast limitat d'amenaces en relació a relació a l'escenari actual
- Accessos locals controlats i limitats



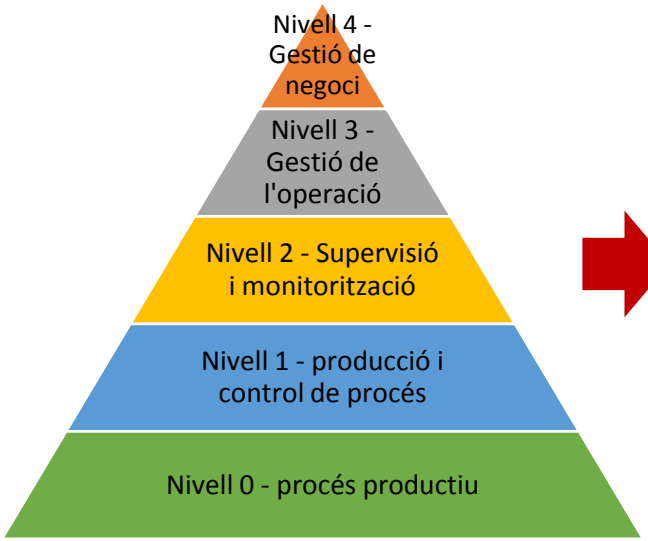


- ICS interconnectats amb altres xarxes (corporativa, internet) – NO AILLATS
- Accessos remots des de qualsevol ubicació.
- Integració del món OT amb el món IT (convergència ICS, sistemes de negoci i Internet)
- Safety
- La seguretat lògica passa a ser un nou requeriment
- Control dels sistemes industrials des de la xarxa corporativa
- Múltiples dispositius connectats a aquests equips (mòbils, tauletes, sistemes d'informació, aplicacions al núvol, ...)

NOVES AMENACES

COM L'EVOLUCIÓ DE LES AMENACES HA INFLUÏT EN LA CONTINUÏTAT DE NEGOCI

ANSI ISA 95 – Capes d'automatització industrial



Amenaces

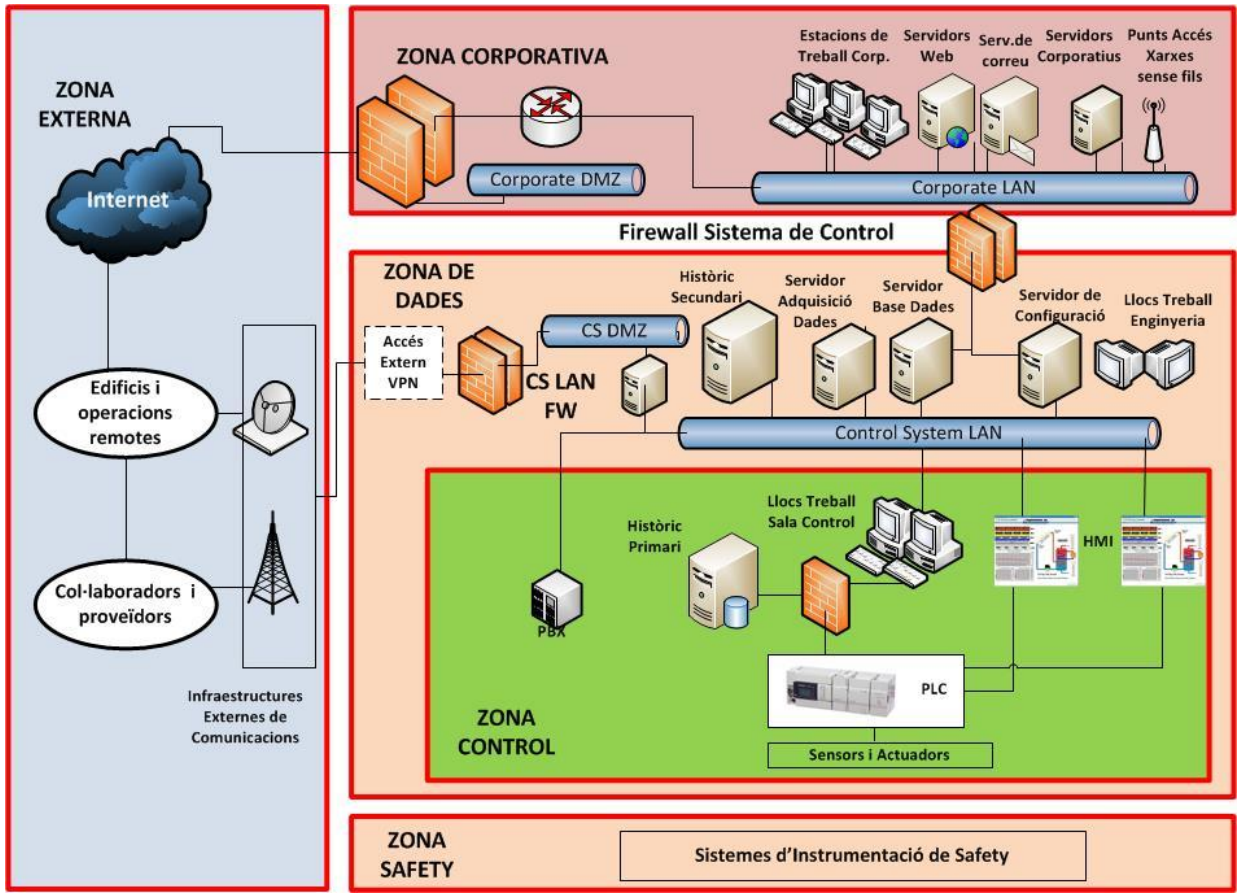
- Fuita d'Informació
- Denegació de serveis
- Accés no autoritzats als sistemes
- Etc

Amenaces que aprofiten la nostra vulnerabilitat

Vulnerabilitats

SECTOR INDUSTRIAL

Actualment els entorns industrials requereixen d'una defensa en profunditat mitjançant zones de seguretat

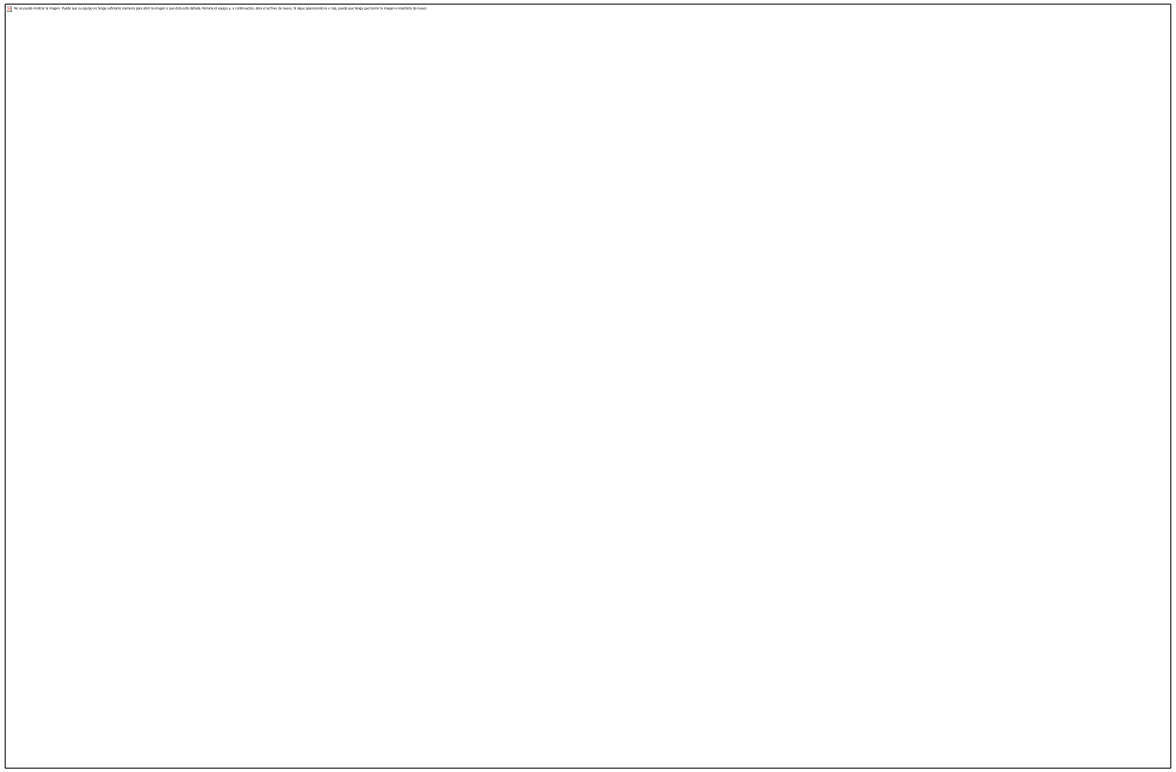


- Zona externa: és la zona de connectivitat amb Internet.
- Zona corporativa: és la zona de les comunicacions corporatives de l'operador. Habituals serveis TIC.
- Zona de dades: és la zona on es recullen i analitzen les dades generades en cada infraestructura.
- Zona de control: és la zona destinada als PLCs, HMIs, etc.
- Zona de seguretat: equips destinats a la seguretat de la infraestructura (safety).

A partir d'aquesta informació serà necessari disposar de barreres lògiques i físiques d'aïllament entre aquestes zones.

SECTOR INDUSTRIAL

En els darrers anys, s'han produït diferents atacs a plantes industrials i infraestructures crítiques que han afectat els processos industrials: Stuxnet, Duqu, Shamoon, Dragonfly, SandWorm, Trojan, Laziok... entre d'altres.



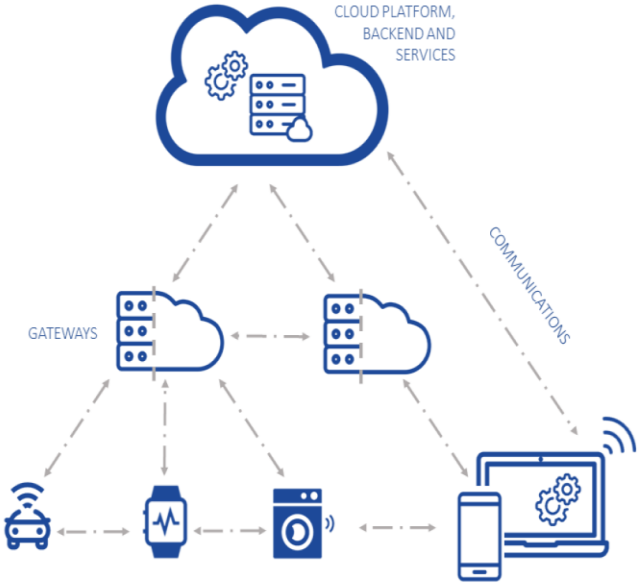
ÍNDEX

A QUINS NOUS RISCOS ESTEM EXPOSATS

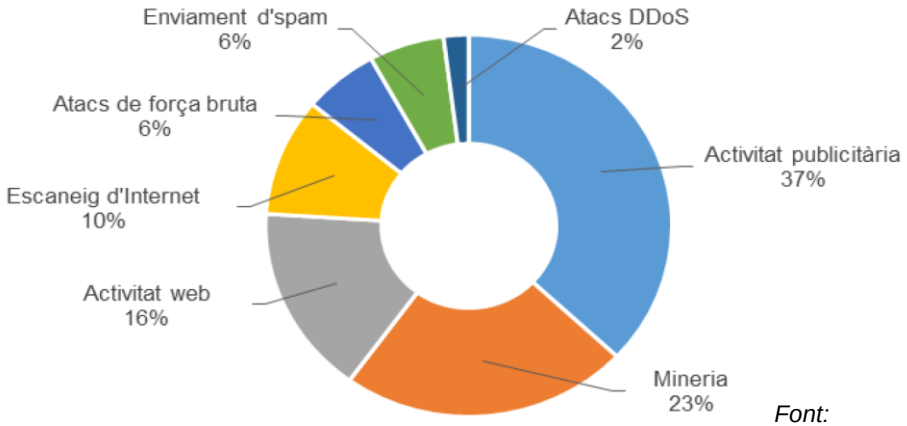
EL MÓN IOT

20.000 M d'IoT el 2020 (Gartner)

VOLUM DE VULNERABILITATS CREIXENT



Font: ENISA

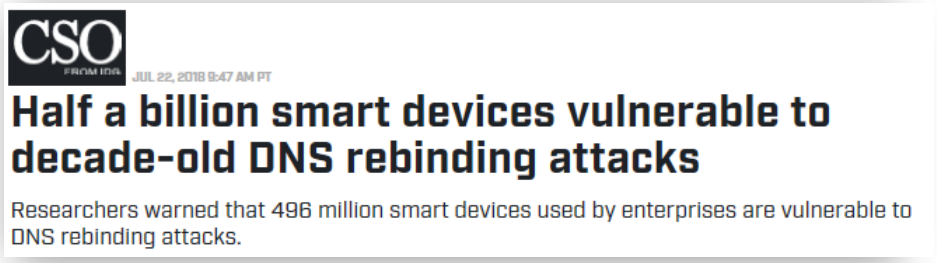


Font: Vectra

EL MÓN IOT

500 milions de dispositius *IoT* vulnerables

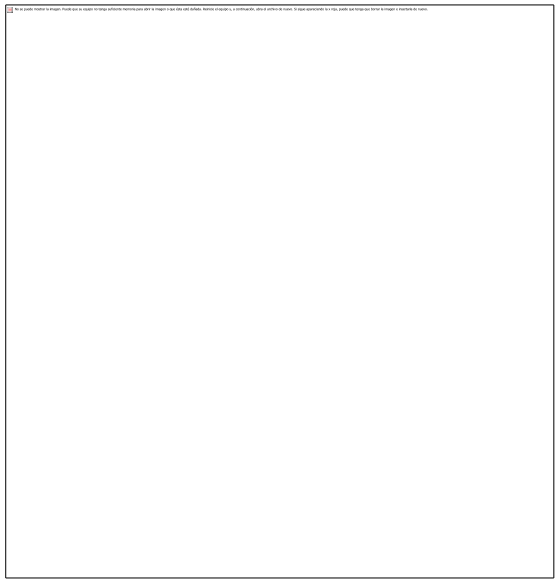
- Investigadors afirmen que hi ha mig milió de dispositius *IoT* vulnerables a atacs *DNS Rebinding* i ser utilitzats com a *proxies* per dirigir atacs o escanejar .
- Impressores, *smart TVs*, càmeres IP, altaveus, encaminadors, *switches*, reproductors i altaveus d'*streaming*. [60] [61]


CSO FROM IDG

JUL 22, 2018 9:47 AM PT

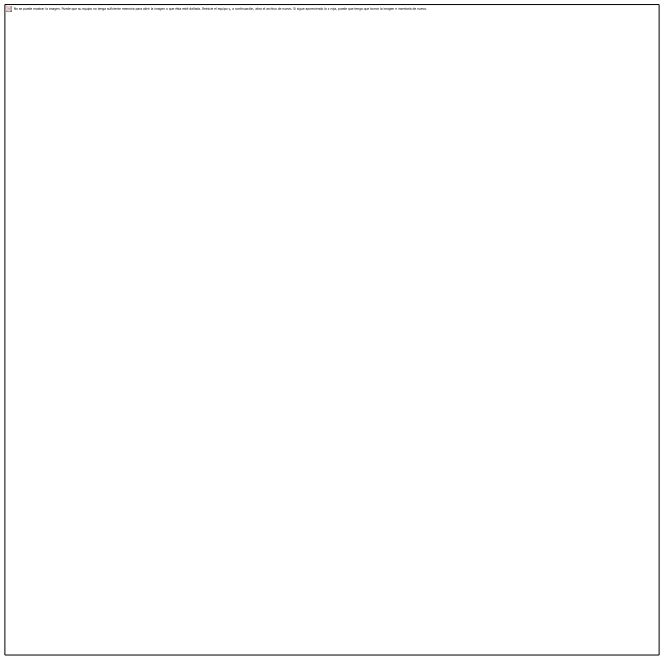
Half a billion smart devices vulnerable to decade-old DNS rebinding attacks

Researchers warned that 496 million smart devices used by enterprises are vulnerable to DNS rebinding attacks.



A UNS ENTORNS CADA COP MÉS VULNERABLES

- Multiplicitat de protocols diferents
- Obsolescència (el món TI té uns cicles de vida molt curts a diferència del món OT que fins ara eren més llargs)
- Volum de tipologies d'equips tan gran i creixent que complica l'aplicació de mesures de seguretat i protecció.



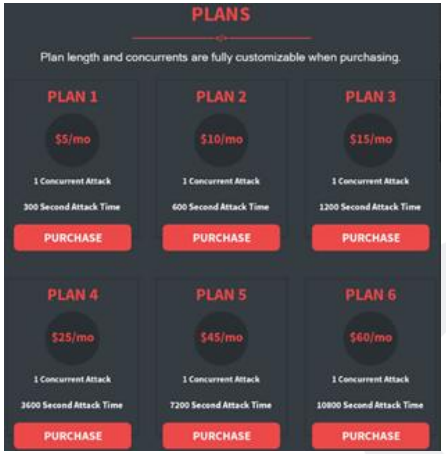
ATACS CADA COP MÉS SOFISTICATS I A COSTOS MÉS BAIXOS

Ex: atacs de denegació de servei contra qualsevol entitat que poden afectar seriosament la continuïtat dels seus serveis crítics

- Un informe d'**Armor,** publicat el març de 2018, detalla els preus de dades i serveis al mercat negre publicat. [32]

  Els preus d'un atac *DDoS* poden variar entre **10 $ (1 hora) i 1200 $ (una setmana)**

Atacs a la carta



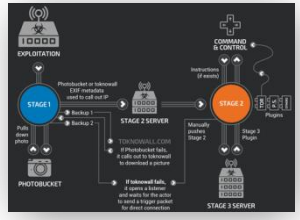
Informe complet de **Kaspersky** constata el preu al mercat dels serveis d'atacs *DDoS* i el benefici final pels cibercriminals. S'ofereixen atacs *DDoS* de 60 minuts des de 25 $ fins a 60 $, amb un preu mig de 20 $. [33]

- Un atac de **30** minuts amb una amplada de banda de **125** Gbps i serveis de seguiment i eines per resoldre incidències costaria **60** $.
- Un atac de **60** minuts amb una amplada de banda de **125** Gbps i serveis de seguiment i eines per resoldre incidències costaria **90** $.

ATACS CADA COP MÉS SOFISTICATS I A COSTOS MÉS BAIXOS

Exemples

VPN Filter



- M*alware botnet* **VPNFilter**, una infecció massiva amb una **afectació de més de 500.000 routers** a 54 països, afectant a fabricants: **Linksys**, **MikroTik**, **NETGEAR** i **TP-Link.**
- **VPNFilter** permet el robatori de credencials web i monitoritzar entorns ICS (possible relació amb BlackEnergy).
- **VPNFIlter** va afectar una planta química a Ucraïna.

Atacs de phising

Els atacs de *phishing* són una de les principals causes de fuites de dades als **centres sanitaris**. Els atacs acaben comprometent els comptes de correu dels empleats on hi ha informació sensible dels pacients.

Ransomware Water Utilities

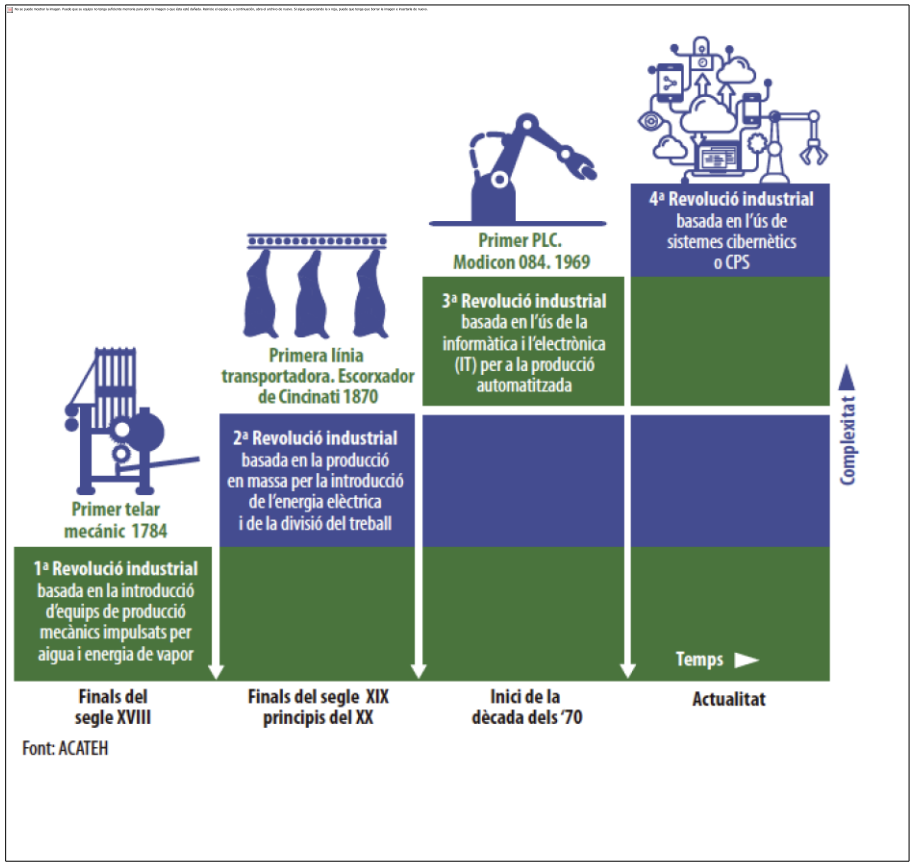
Una **infraestructura crítica de subministrament d'aigua, al nord de Califòrnia**, va ser afectada amb un atac del ransomware Ryuk, una setmana després del pas de l'huracà Florence**.**

ÍNDEX

LLIÇONS APRESES

CAL ADAPTAR-NOS I CONTEMPLAR NOUS ESCENARIS DE RISC

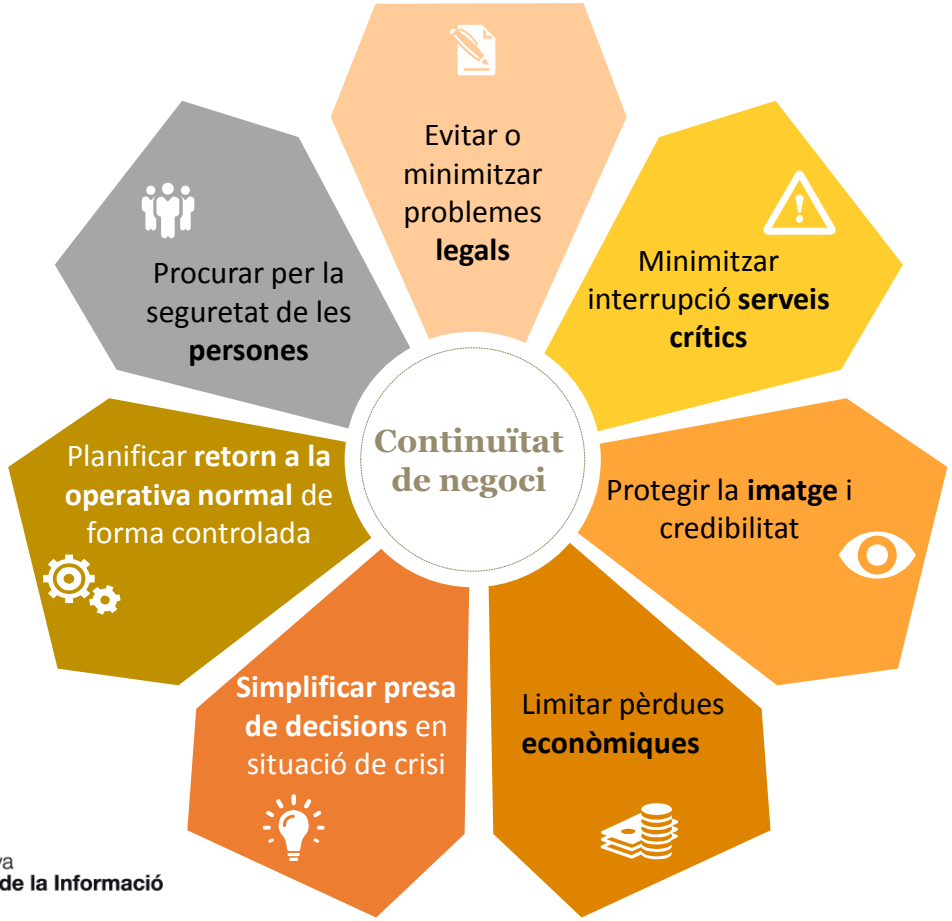
EL MÓN IT I EL MÓN OT HAN CONVERGIT



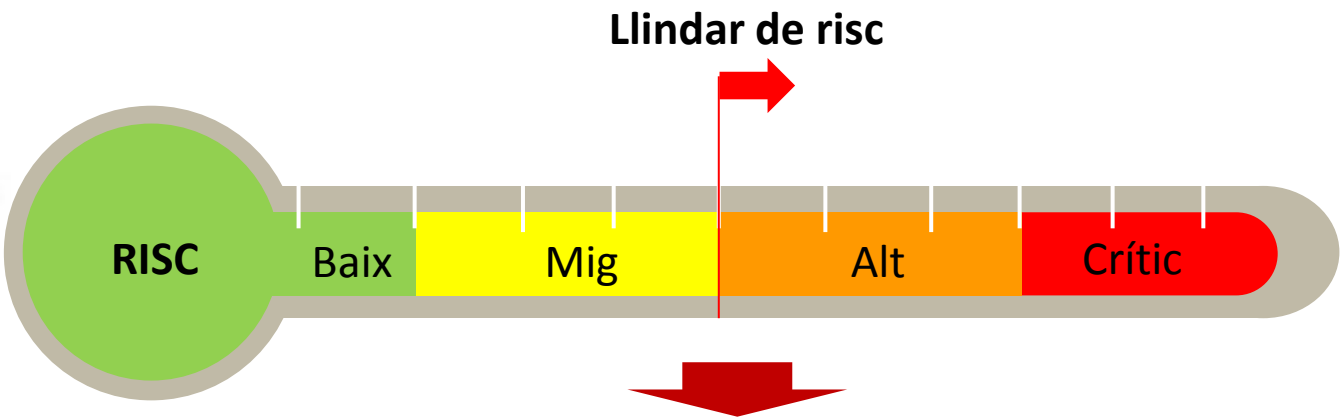
LLIÇONS APRESES

CAL VALORAR I PRIORITZAR LES NOSTRES ACTUACIONS

CAL TENIR CLARS ELS OBJECTIUS QUE PERSEGUIM (QUÈ VOLEM PROTEGIR, DE QUÈ ENS VOLEM PROTEGIR)



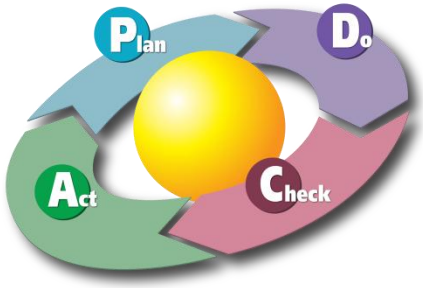
ACOTAR MOLT BÉ EL NOSTRE LLINDAR DE RISC (RISC APPETITE)



Tractament dels riscos	
 **Evitar el risc:** Eliminar l'actiu	 **Acceptar el risc:** Ser conscients del risc i monitoritzar-ho
 **Mitigar el risc:** Aplicar salvaguardes	 **Transferir el risc:** Contractar assegurances,,…

LLIÇONS APRESES

PLANIFIQUEU BÉ LES FASES I RECURSOS



Execució de proves:

- Despatx
- Comunicacions
- Lloc de treball
- Xarxa local
- Evacuació
- Etc.

Anàlisi de riscos:

Anàlisi de riscos sobre els actius que donen suport als processos crítics de negoci i revisió física de les instal·lacions dels CPDs

Auditoria Externa

Mesurar el grau d'evolució del SGCN respecte el cicle de millora passat anterior i analitzar el seu grau d'adequació amb la norma ISO22301

Revisió dels procediments

Revisió dels procediments operatius i tècnics que s'han d'executar en cas de contingència

Anàlisi d'impacte (BIA) i estratègies:

Revisió dels processos crítics, anàlisi de les estratègies de continuïtat definides en cas de contingència i anàlisi de riscos als quals estan subjectes els actius de l'Organització

Política de Continuïtat:

Revisió de la Política de Continuïtat, objectius, mètriques i indicadors de l'Organització

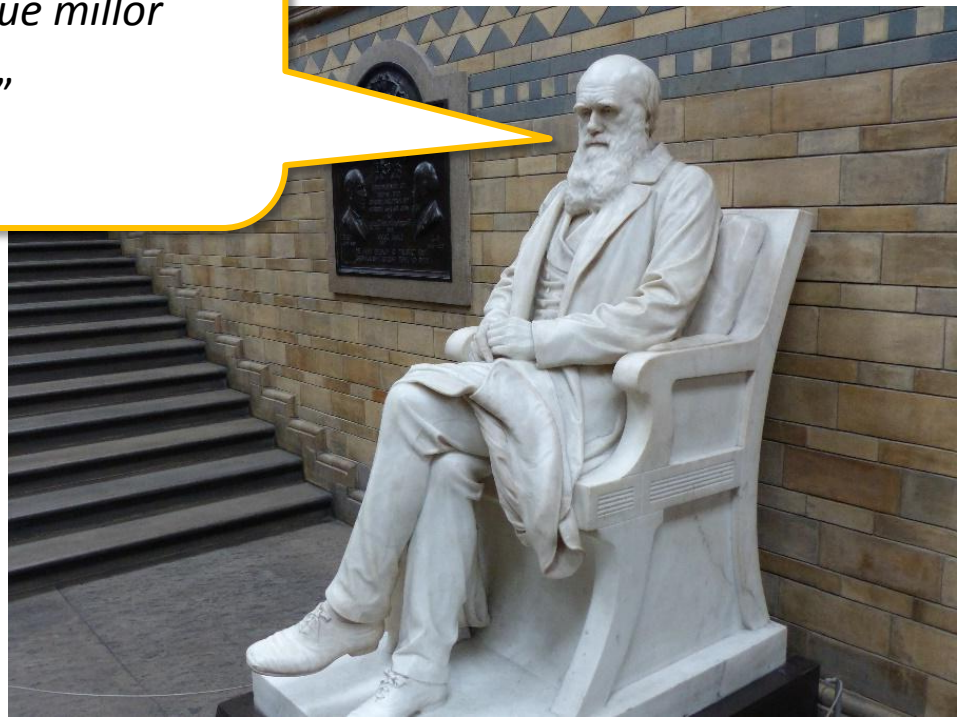
Formació i conscienciació

Garantir que el personal del l'entitat coneix el Pla de Continuïtat de l'Organització i és conscient de la importància de la seva participació

CONSTRUÏU/ DISSENYEU DE FORMA SEGURA (PREVENCIÓ, PROTECCIÓ) PER EVITAR L'ACTIVACIÓ DE PLANS DE CONTINUÏTAT

“La espècie més forta no és la que sobreviu… sinó aquella que millor s’adapta al canvi”

Charles Darwin




KEEP
CALM
:-)
YOU HAVE
A PLAN


MOLTES
GRÀCIES!!

Generalitat de Catalunya
Centre de Seguretat de la Informació de Catalunya

David Forner

Centre de Seguretat de la Informació de Catalunya