Enginyers Industrials de Catalunya

Comissió de Societat Digital
Grup de Treball de Ciberseguretat

Ciberseguretat Industrial

Una visió pràctica per a les Pimes

Sergi Gil – Jordi Ubach

15 d'abril de 2021

Sobre nosaltres

Sergi Gil López

Enginyer Industrial | E.T.I. de Sistemes
Màster en Indústria 4.0 i Ciberseguretat

sgil@engimatica.cat

https://www.linkedin.com/in/sergigil/

Engimàtica
CIBERSEGURETAT INDUSTRIAL

Jordi Ubach

Consultor-formador Ciberseguretat | Forense informàtic
Lead auditor ISO 27001-ENS | ICS Security Consultant

jordi.ubach@tecnoideas20.com

https://www.linkedin.com/in/jordi-ubach-9971a1a5/

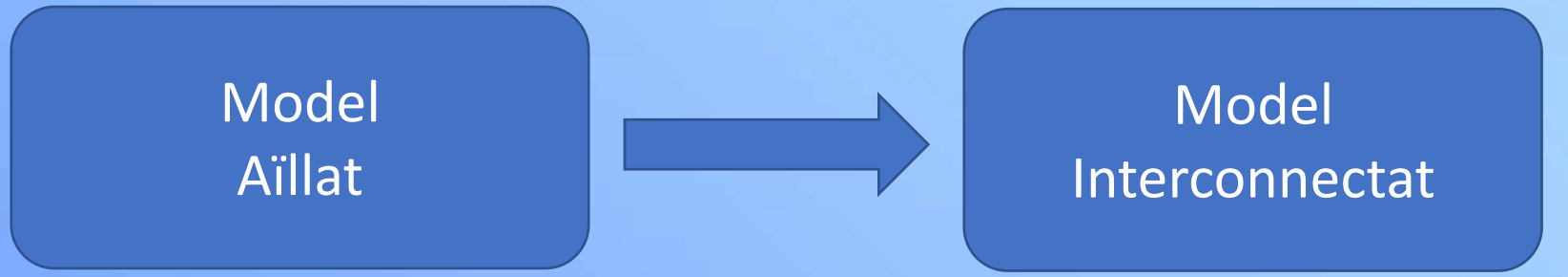
TECNO ideas2.0 ciberseguridad

Contingut de la sessió

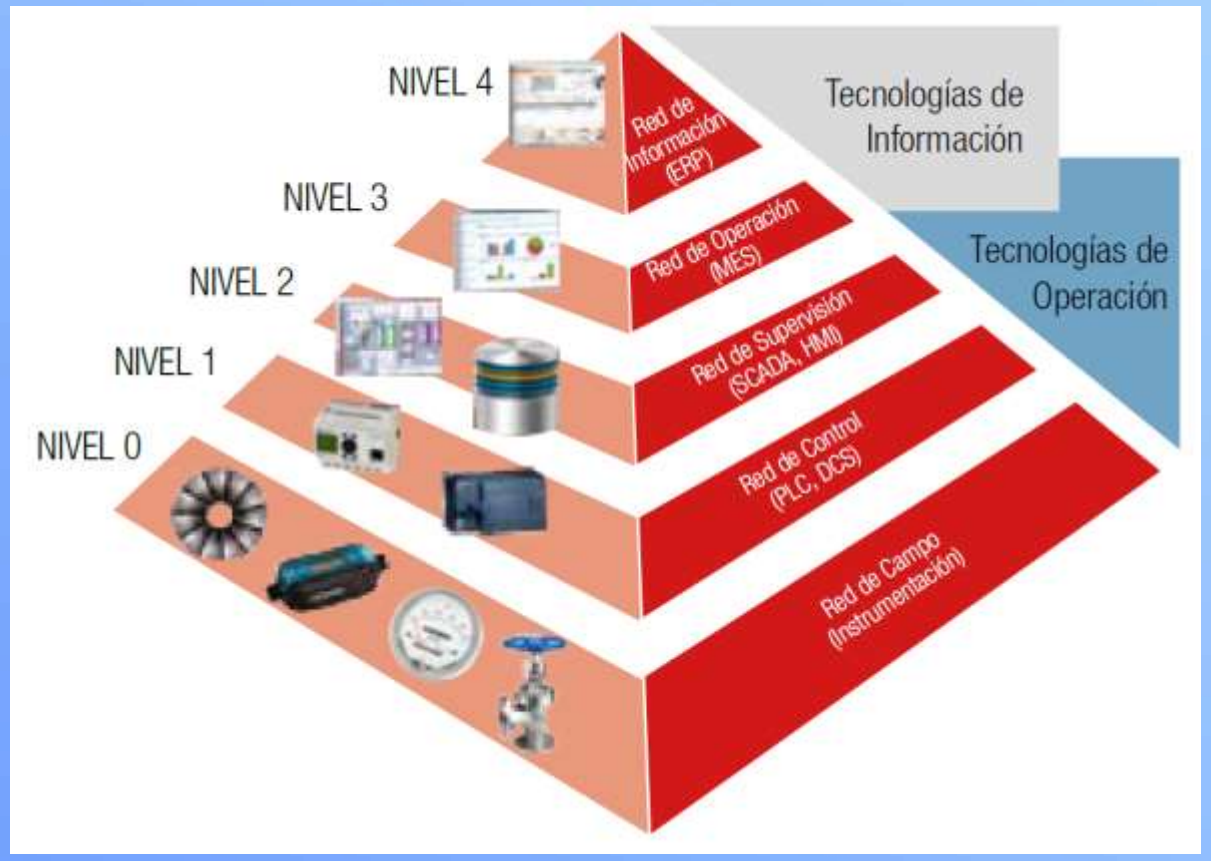
- **Sistemes de Control Industrial**
  - Digitalització i Indústria 4.0
  - Diferències entre IT/OT
  - Impacte d'un ciberatac
  - Evolució de la seguretat industrial
- **Ciberdelinqüència**
  - Qui ens pot voler atacar?
  - Tipus d'atacs
  - Etapes d'un atac
  - Què podem fer per protegir-nos?
- **Ciberamenaces**
- **Ciberseguretat Industrial**
  - Situació de les Pimes Industrials
  - Com abordar la Ciberseguretat
  - Norma ISA/IEC 62443
  - Assegurança de Ciberriscos
  - Reptes de la Ciberseguretat Industrial
  - Recomanacions de seguretat
- **Part pràctica**
  - Exemples de sistemes vulnerables
- **Torn de preguntes**

Digitalització i Indústria 4.0

La transformació digital y la irrupció de la Indústria 4.0 està transformant la concepció dels Sistemes de Control Industrial (ICS).



Sistemes de Control Industrial (ICS)



Font: Centro de Ciberseguridad Industrial, www.cci-es.org

- Cicle de vida de més de 20 ó 30 anys
- Concebuts sense seguretat
- Protocols de comunicacions insegurs
- Habitual trobar equips obsolets i vulnerables
- Difícils o impossibles d'actualitzar
- Coexistència equips antics amb nous

Diferències entre IT/OT

Característiques	Tecnologies Informació (IT)	Tecnologies Operacions (OT)
Prioritat	Confidencialitat Integritat Disponibilitat	Disponibilitat Integritat Confidencialitat
Disponibilitat	99% (87,6 h/any)	99,99% (0,875 h/any)
Objectiu principal	Protegir la informació	Protegir a les persones i el procés
Risc principal	Revelació d'informació	Seguretat, medi ambient, econòmic
Actualitzacions	Fàcil	Difícil
Entorn	Oficina	Industrial
Ciberseguretat	Adoptada	Recent

Impacte d'un ciberatac a un ICS

- Posa en perill la seguretat i la salut dels treballadors
- Dany al medi ambient
- Dany a maquinaria i equips de producció
- Pèrdua d'integritat del producte
- Pèrdua de la confiança i la reputació de l'empresa
- Infringir requisits legals o reglamentaris
- Pèrdua d'informació confidencial
- Greus pèrdues econòmiques i sancions
- Pot suposar el tancament de l'empresa

Evolució de la Seguretat Industrial

- **Seguretat Física**: *Accessos, tancaments, càmeres, vigilants, ...*
- **Seguretat Persones**: *Prevenció de Riscos Laborals, EPIs, directives europees, marcatge CE, ...*
- **Seguretat Ambiental**: *Residus, emissions (gas, líquid, sòlid), productes tòxics per a les persones, fauna i flora, ...*

- **Ciberseguretat Informàtica IT**
- **Ciberseguretat Industrial OT**

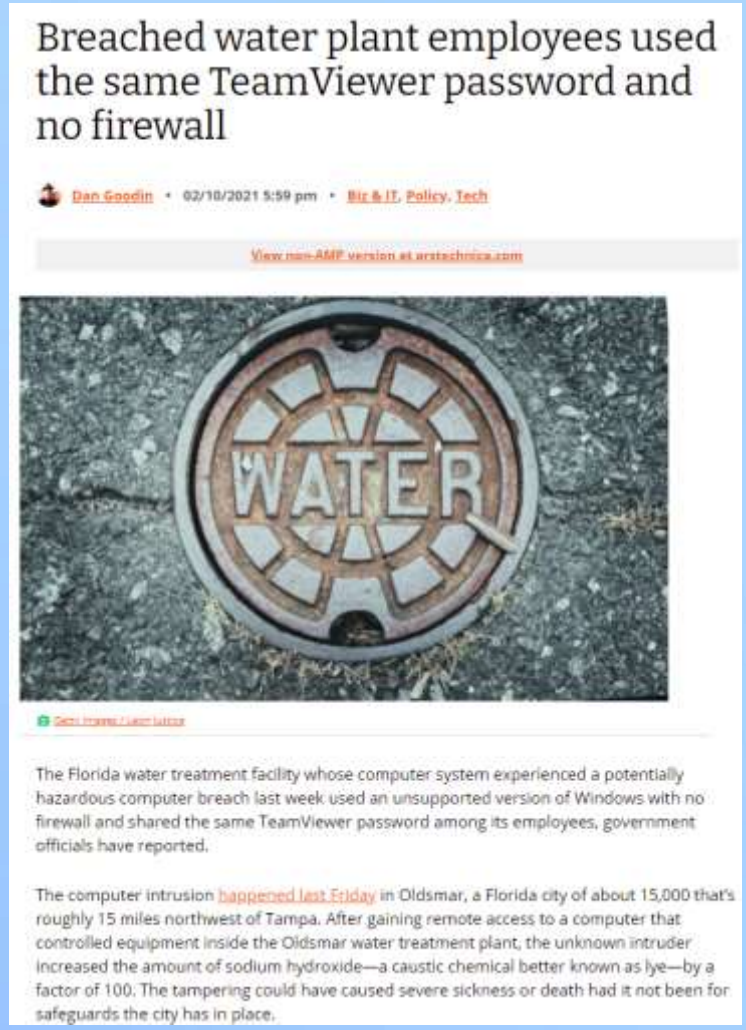
Ciberdelinqüència

- Va a més
  Atacs anuals (2020): 776 infraestructures crítiques, 1690 empreses zona OT
- Activitat molt lucrativa
  Per damunt del tràfic de drogues i de persones.
- Li pot afectar a qualsevol
  Els ciberatacs han augmentat un 125% l'últim any, fins als 40.000 diaris
  Sectors: sanitari, distribució, metal·lúrgic, ...
- Greus pèrdues econòmiques
  Producció, vendes, rescat, recuperació, sancions, clients, ...
- Pot suposar el tancament de l'empresa
  El 60% de les Pimes que pateixen un atac greu, com un Ransomware, acaben tancant en 6 mesos.

Ciberatacs per sectors

Logística

Automoció



Aigua

Ciberseguretat Industrial als mitjans

El 85% de las organizaciones industriales no están preparadas para un ataque de OT

Infraestructuras críticas 28 OCT 2020

Con solo el 12% de los encuestados indicando que el riesgo de ciberseguridad de la Tecnología operativa (OT) para su organización es bajo, es sorprendente ver que solo el 15% está altamente preparado para un ciberataque. Además, el 16% ha experimentado un incidente de OT.

Font: www.itdigitalsecurity.es

Los proveedores provocan casi el 50% de los ciberataques a empresas españolas

Actualidad 23 JUL 2020

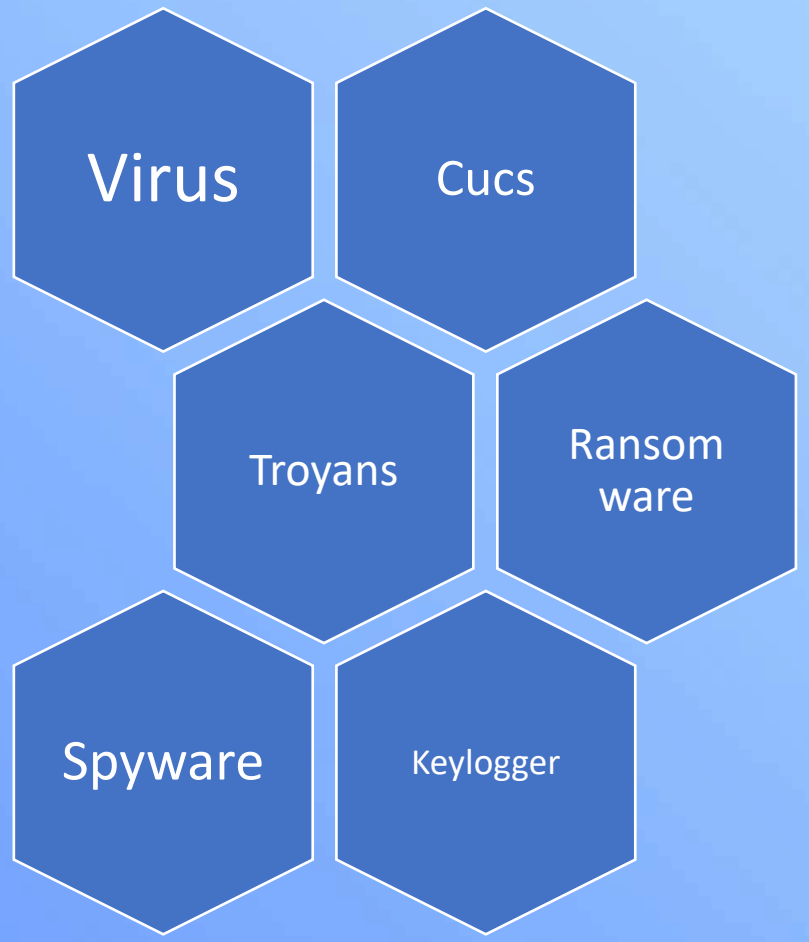
Los proveedores, la cadena de suministro, son una de las principales causas de los ciberataques que sufrieron las empresas españolas. Lo pone de manifiesto el tercer informe anual ?Empresas y Ciberseguridad? publicado por LEET Security para el que han participado más de un centenar de empresas.

Font: www.itdigitalsecurity.es

Hackers vs Ciberdelinqüents

- **Hacker (Furoner):** Persona apassionada per la informàtica, que té un gran coneixement de les xarxes i els sistemes informàtics i un viu interès per explorar-ne les capacitats i per posar a prova les seves habilitats en aquest àmbit.
- **Ciberdelinqüent:** Persona que comet un acte il·legal i sovint fraudulent per mitjà de les tecnologies de la informació i la comunicació, generalment internet.

Programari Maliciós (Malware)



RANSOMWARE

Imagen: Cisco Talos

Qui ens pot voler atacar?

Origen Intern

- Empleats
- Empreses externes

Origen Extern

- Antics empleats
- Cibercriminals
- Governs
- Terroristes
- Competència (espionatge)
- Hacktivistes
- Phishers
- Spammers

Vector

- Xarxa interna
- Internet
- Wifi
- Dispositius IIoT
- Accés físic
- Accés remot (VPN)
- Email
- Dispositiu mòbil
- USB

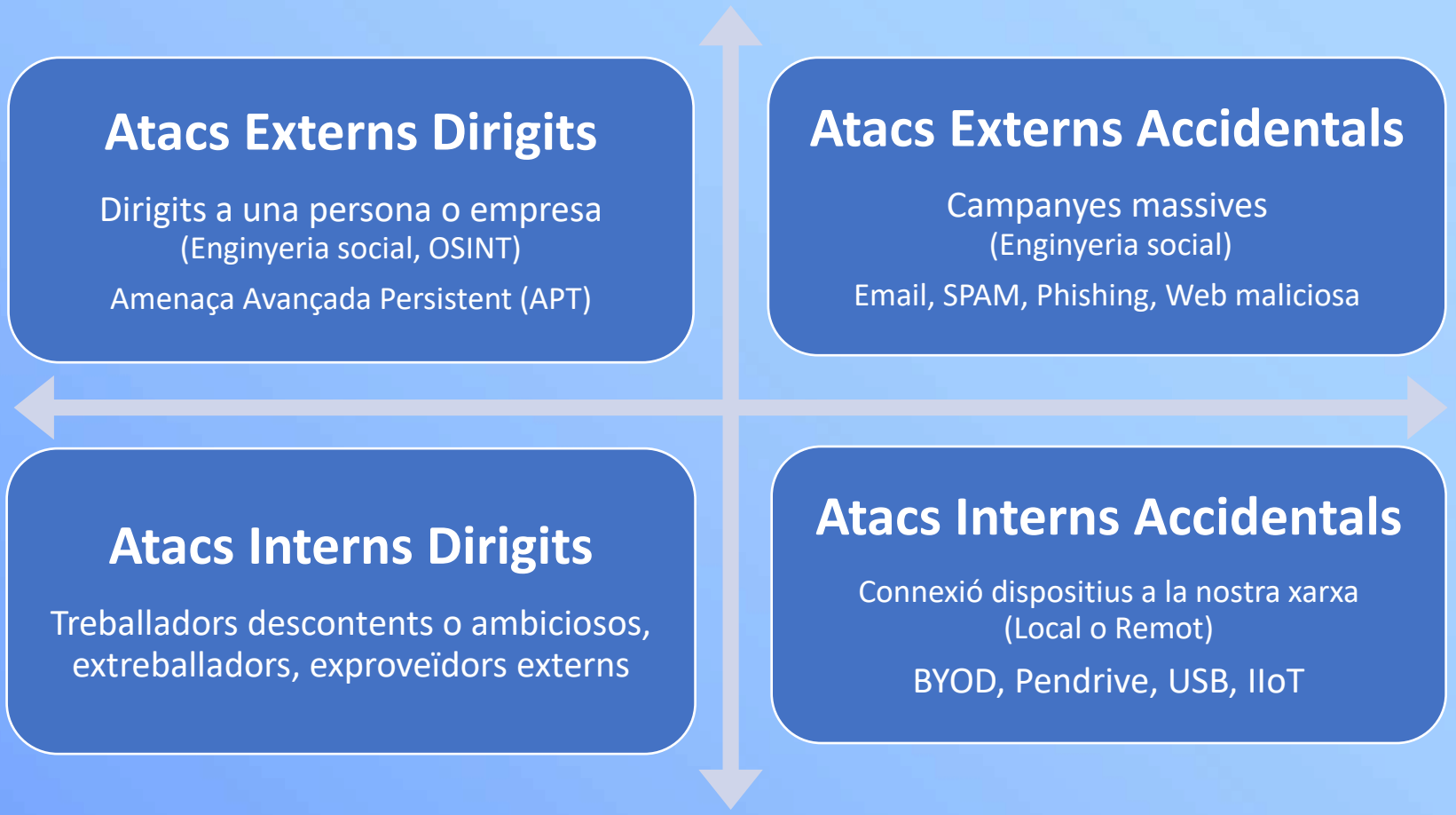
Objectiu

- Accés remot
- Denegació de servei
- Extracció d'informació
- Xifrar la informació

Conseqüències

Website defacing
Monetari (ransomware)
Robatori propietat intel·lectual
Vandalisme
Hacktivisme
Sabotatge
Pèrdua reputació

Tipus d'atacs



Formar per Prevenir

Més del 95% del atacs tenen com a origen un treballador de la mateixa empresa.

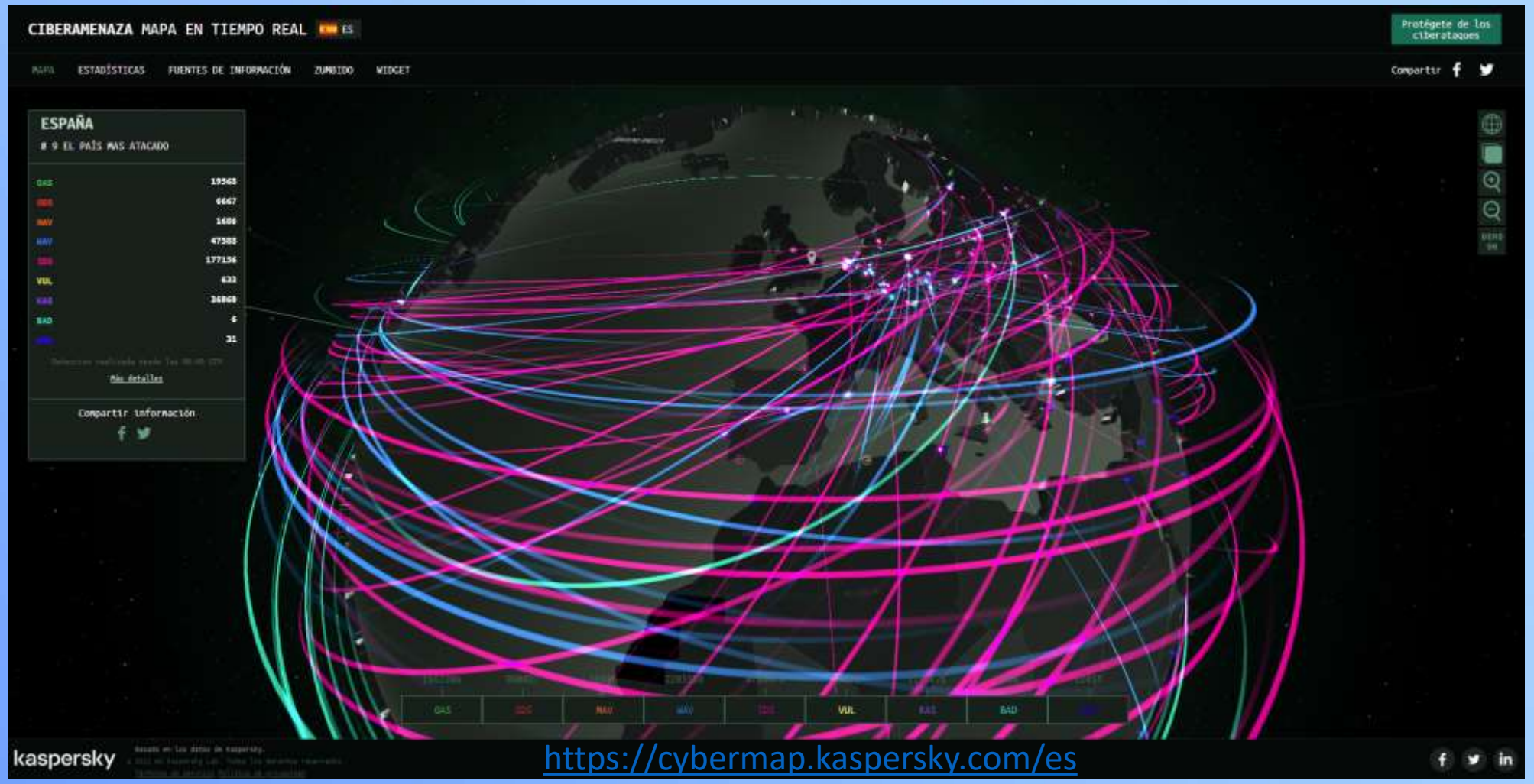
Formació i Conscienciació en Seguretat de la Informació i Ciberseguretat

Etapes d'un atac

1. **Reconeixement** (Recopilació d'informació sobre l'objectiu: OSINT, Enginyeria Social)
2. **Preparació** (Prepara l'atac de forma específica sobre l'objectiu)
3. **Distribució** (Es produeix la transmissió de l'atac)
4. **Explotació** (S'inicia l'atac, explotació vulnerabilitat coneguda o 0-day)
5. **Instal·lació** (S'instal·la el malware en la víctima)
6. **Comandament i Control** (L'atacant disposa de control sobre el sistema de la víctima)
7. **Accions sobre els objectius** (L'atacant fa el que vol i cerca altres objectius)

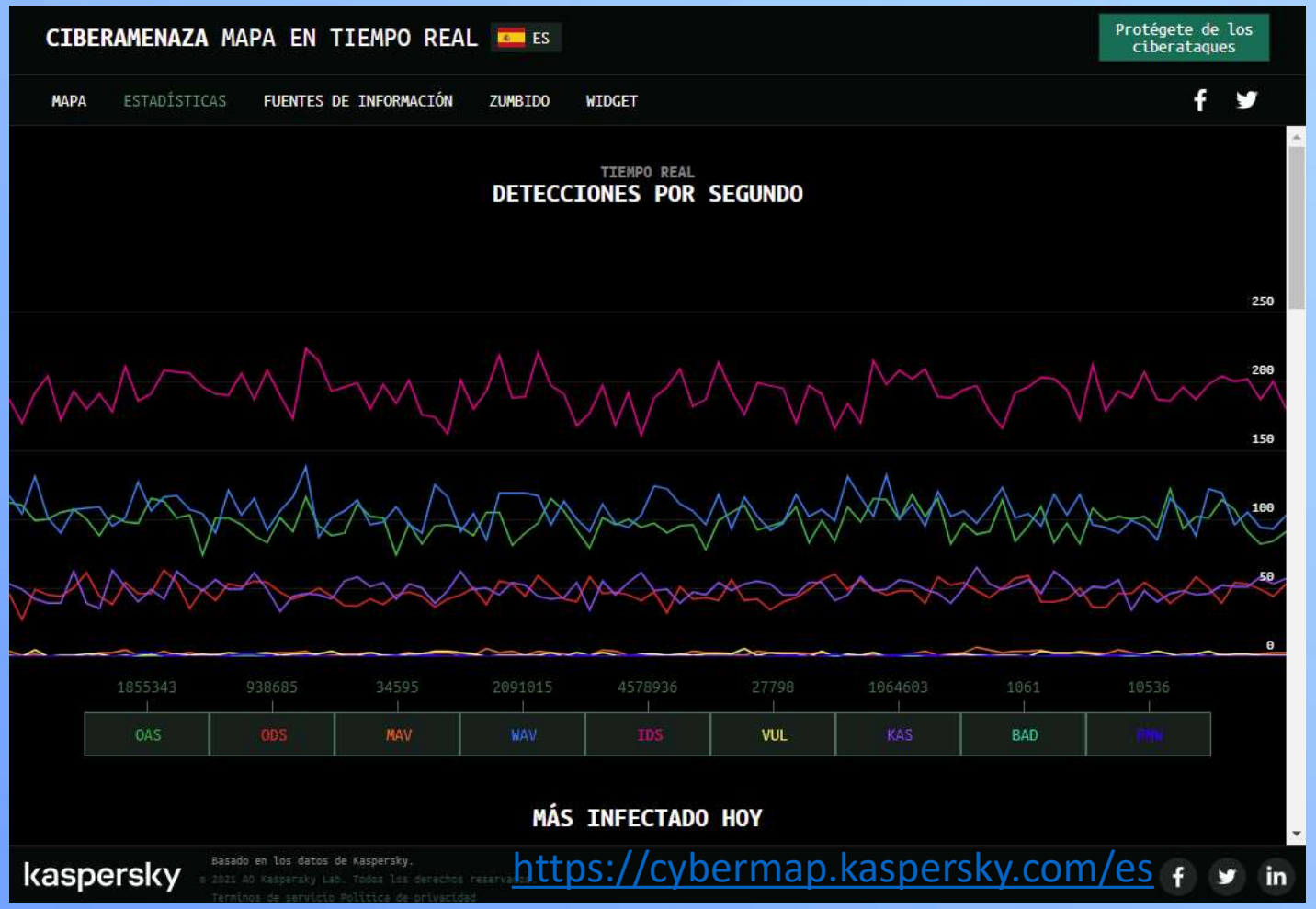
Un atac es pot prevenir en qualsevol de les etapes anterior

Mapa Ciberamenaces



https://cybermap.kaspersky.com/es

Estadístiques Ciberamenaces



https://cybermap.kaspersky.com/es

IDS – Intrusion Detection System

WAV – Web Anti-Virus
OAS – On-Access Scan

KAS – Anti-Spam
ODS – On Demand Scanner

Situació de les Pimes Industrials

- El 99% de les Pimes no es considera un objectiu atractiu per a un ciberatac.
- Mai s'han plantejat la Ciberseguretat de les instal·lacions industrials
- Els integradors de sistemes no contemplen la Ciberseguretat perquè el client no ho demana.
- Els integradors de sistemes, informàtics i programadors no són especialistes en Ciberseguretat.
- Els nous projectes encara no tenen en compte la Ciberseguretat, quan s'hauria d'integrar des de la fase de disseny.
- No existeix un Responsable de Ciberseguretat ICS/OT.
- Calen perfils híbrids: que coneguin de IT/OT/Procés.

Què ens trobem?

- Falta de coneixement del que realment està instal·lat, equips, versions, ...
- No es coneix què està passant a la xarxa i com està dissenyada.
- Falta de securització dels equips.

- Equips de control antics, sense suport per part del fabricant i amb vulnerabilitats.

  Pensar en migrar PLCs antics, en cas de fallada, difícil de trobar recanvis, sistema aturat durant setmanes.

- Accés a tots els equips des de la xarxa empresarial.
- Equips amb accés a Internet.

- Existeixen connexions remotes no documentades.

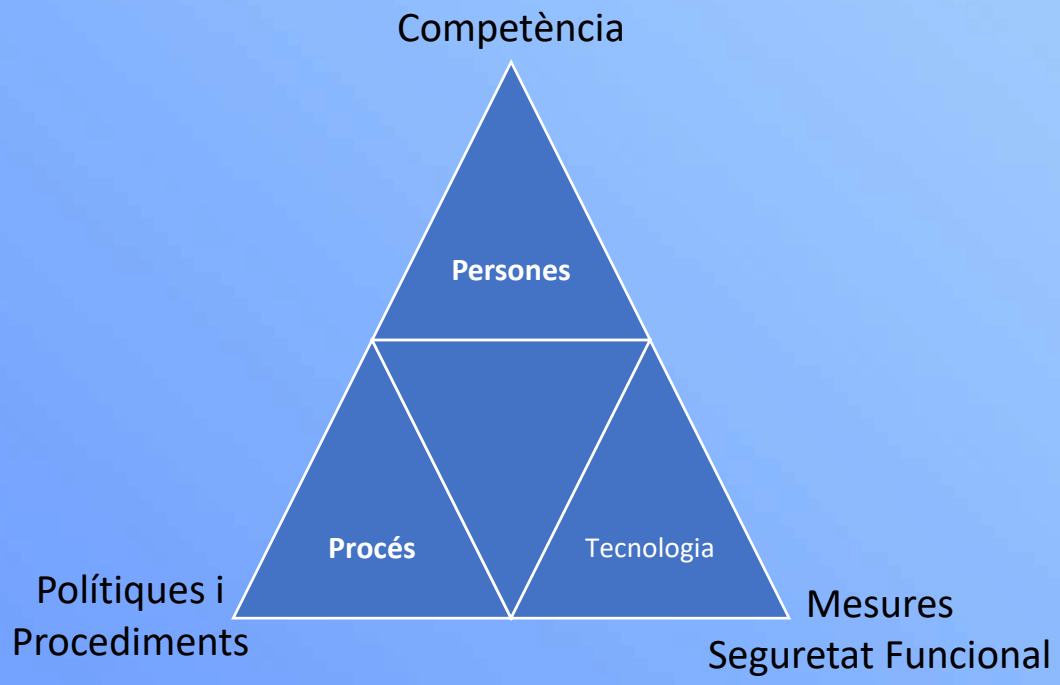
Com abordar la Ciberseguretat Industrial?

- Implicació de la direcció, cal crear una cultura de Ciberseguretat
- Empreses han de treballar conjuntament (fabricants, integradors i propietaris)
- Veure en conjunt IT/OT, centrar-nos en el procés.
- La informació ha de fluir, però de forma segura, és molt fàcil accedir de la xarxa IT a la xarxa OT, produint interrupcions a la producció
- Bona arquitectura, segmentació en zones i conductes, qui pot parlar amb qui, només comunicacions necessàries, la resta prohibida.
- Defensa en profunditat
- Reduir la superfície d'atac a la xarxa de control

Norma ISA/IEC 62443, Framework NIST

- No reinventar la roda, basar-nos en estàndards i normatives, adaptant-los a les nostres característiques

Seguretat Industrial Holística



Rols ISA/IEC 62443

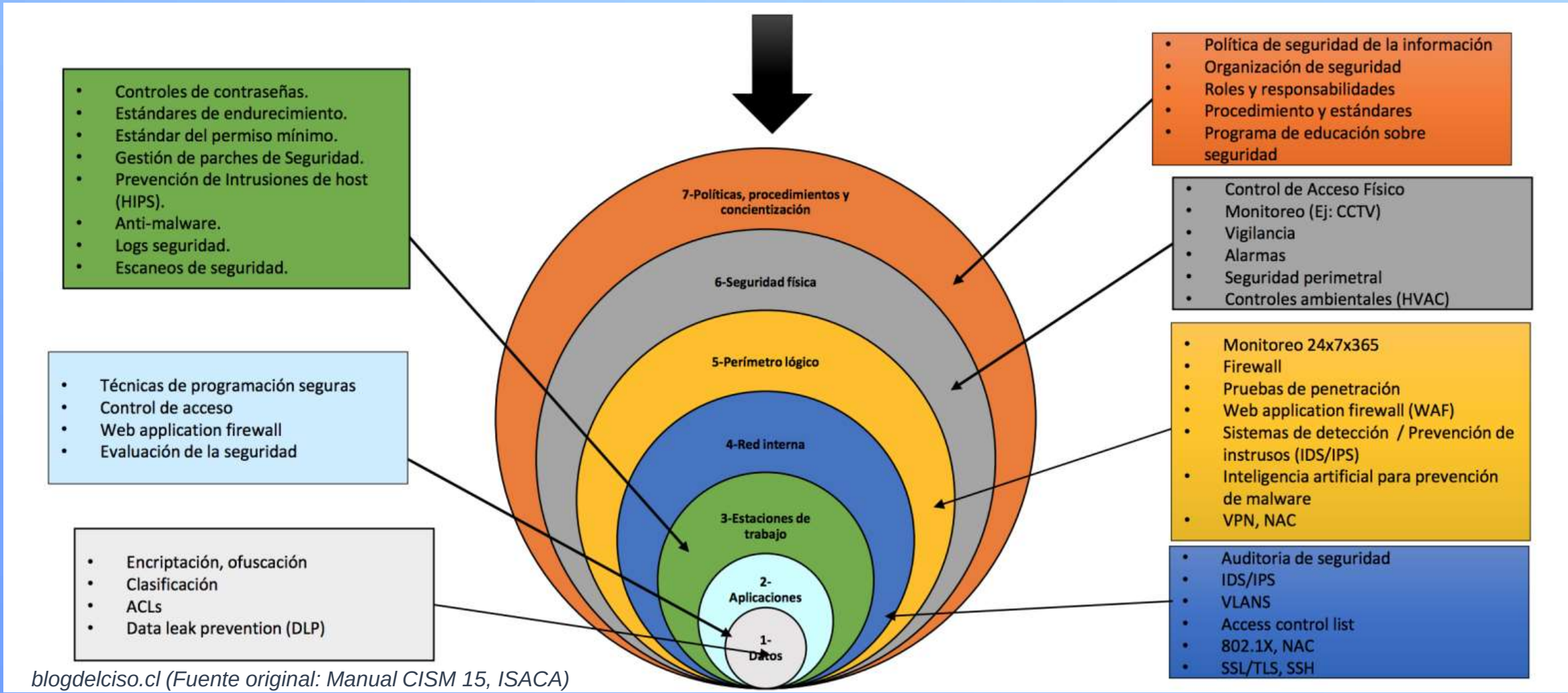
ISASecure®

- Fabricants Equips Control Industrial
- Proveïdors Serveis d'Integració
- Proveïdors Serveis de Manteniment
- Propietaris del ICS

Metodologia d'implementació norma ISA/IEC 62443

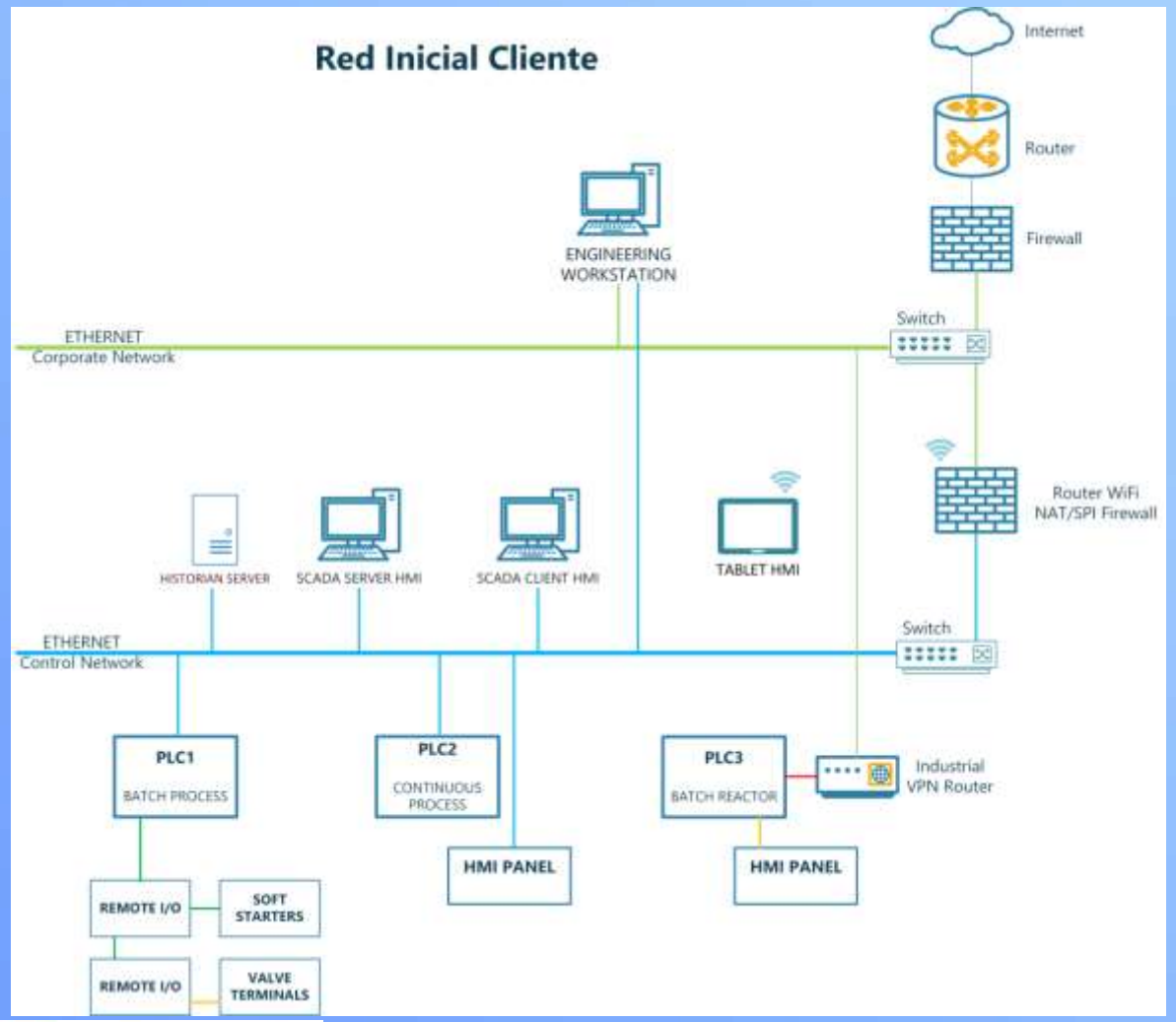
1. Reconèixer la necessitat de gestionar els riscos de Ciberseguretat
2. Implementar el Sistema de Gestió de Ciberseguretat (CSMS)
3. Definir l'abast del ICS
4. Anàlisis de riscos d'alt nivell
5. Segmentació del ICS en Zones i Conductes
6. Anàlisis de riscos detallat (de cada zona i conducte)
7. Definició i implementació de contramesures
8. Monitorització i revisió continua

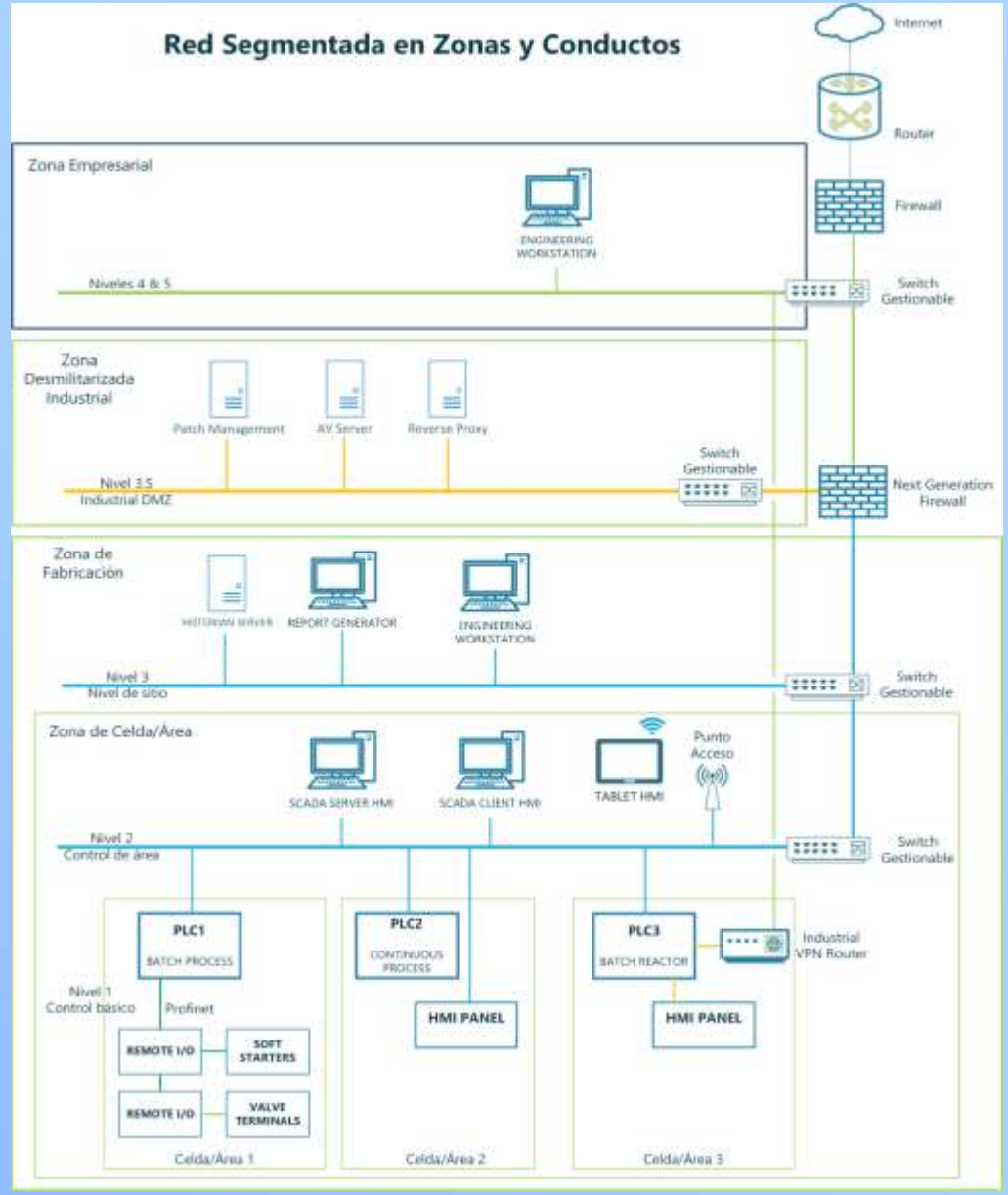
Defensa en Profunditat



blogdelciso.cl (Fuente original: Manual CISM 15, ISACA)

Segmentació en Zones i Conductes segons ISA/IEC 62443





Enginyers Industrials de Catalunya

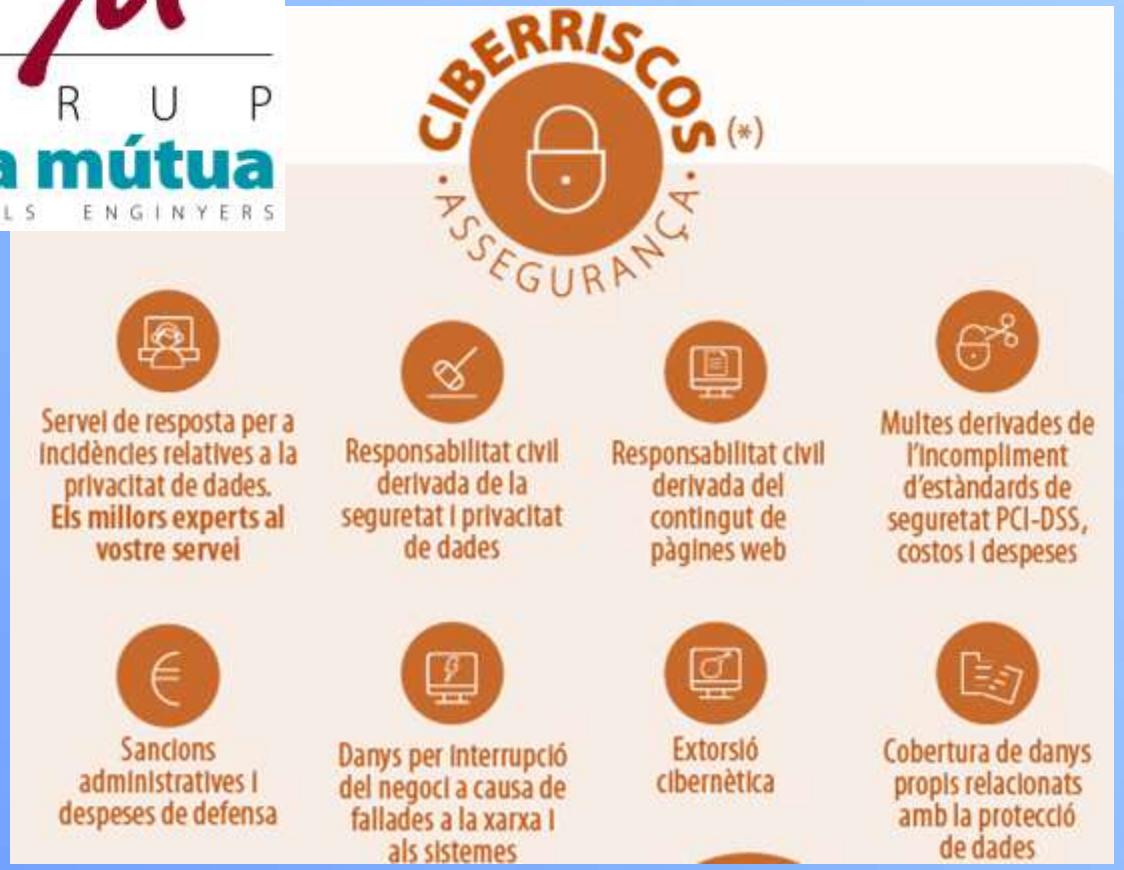
Comissió de Societat Digital - GT Ciberseguretat

Sergi Gil – Jordi Ubach

Passos a seguir per començar amb bon peu

- **Diagnòstic/Auditoria de Ciberseguretat:**
  - **Identificació i caracterització d'actius** (Sistemes passius/actius)
  - **Identificació de vulnerabilitats** (Mètodes manuals/automàtics)
  - **Avaluació de riscos**
  - **Aplicar mesures correctores** (segmentació zones i conductes, defensa en profunditat)
  - **Determinació ciber risc residual**
- **Definir Polítiques**
  - **Política de gestió d'actius**
  - **Política d'ús acceptable**
  - **Política de seguretat de xarxa**
  - **Política de còpies de seguretat**
- **Definir Plans de Continuïtat**
- **Formació i conscienciació en protecció de dades i ciberseguretat**

Assegurança de ciberriscos



Té com objectiu fer front a possibles atacs cibernètics que poden causar danys a nosaltres i als nostres clients

- Un Ciberatac és un delicte, i per tant la empresa que ho pateix ha de trucar a les autoritats per posar en coneixement i fer la corresponent denúncia.
- Des de maig de 2018, la directiva europea de protecció de dades obliga a les empreses que pateixen un atac informàtic a comunicar-ho en 72 hores a les persones afectades i a l'Agència de Protecció de dades. (que ara pot establir sancions que poden anar del 4% de facturació fins a 20 milions d'euros).

El cost mig d'un ciberatac en pimes és d'entre 30.000 i 50.000 euros, podent arribar a xifres de 300 mil €.

La seguretat 100% no existeix.

Sergi Gil – Jordi Ubach

Reptes de la Ciberseguretat Industrial

- Actualització de sistemes antics (legacy)
- Seguretat Cloud, accés a dades en temps real, digitalització, manteniment preventiu
- Dispositius IIoT, early legacy, no modificables per software i necessitaran canviar els dispositius. Molts no integren la capa de Ciberseguretat.
- Disseny de noves instal·lacions integrant la seguretat i Ciberseguretat, al llarg de tot el cicle de vida.

Recomanacions de seguretat

- Tancar tots els accessos remots, només obrir-los quan és estrictament necessaris.
- Ull connexions mòbils a màquines disponibles permanentment per manteniment.

- Control d'accessos remots granulars, mínims privilegis necessaris, no accés a tot el sistema. Zero Trust.
- Disseny segur, hardening de sistemes, segmentar en zones i conductes
- Gestió de canvis en programes, s'ha de verificar també la Ciberseguretat, que no introdueixi un forat de seguretat.
- Realitzar còpies de seguretat i comprovar que funcionen.

Manteniment remot

- Fixar requisits de seguretat, pels proveïdors
- Solució d'accés remot degudament dissenyada, autentificació multifactor, registre de logs, forensics, mínim privilegis necessaris

- Els proveïdors també han de ser cibersegurs, ho mateix que fem nosaltres ho han de fer ells. Els podem auditar.
- Contractes de confidencialitat, ja que poden tenir accés a informació sensible nostre.
- Només utilitzar plataformes aprovades pel propietari, no utilitzar altres sistemes no aprovats d'un proveïdor.
- Determinar si poden accedir quan volen o en unes franges o moments específics

Conclusions

Els mètodes de detecció, anàlisis i protecció del món IT no es poden aplicar tal qual en el món OT. Poden causar aturades intempestives.

La norma ISA/IEC-62443 proporciona un marc flexible per abordar i mitigar les vulnerabilitats de seguretat actuals i futures en els Sistemes d'Automatització i Control Industrial (IACS).

La seguretat no depèn únicament de la tecnologia, la formació del personal en Ciberseguretat és clau per prevenir incidents.

Reflexions

La seguretat completa no existeix, ningú pot assegurar que no patirem un incident de seguretat

Hi ha dos tipus d'empreses, les que han estat atacades i les que ho seran

La inversió en Ciberseguretat no ha de veure's com una despesa sinó com una inversió per minimitzar les pèrdues que pot generar una aturada de la producció durant dies o setmanes

La Ciberseguretat és una carrera de fons en la que mai s'arriba a la meta

Part pràctica

Gràcies per la seva atenció