30è aniversari de l'Aseitec

SOM INDÚSTRIA DIGITAL

aseit 30 anys
Associació TIC catalana

Està la teva empresa preparada per suportar un ciberatac?

Carles Flamerich – CEO Apolo Analytics i Light Eyes

APOLO ANALYTICS

LightEyes

Qui som?

APOLO ANALYTICS

Apolo: eina de ciberseguretat per garantir la continuïtat de les empreses.

Unificació de dades: Integra i unifica en una plataforma centralitzada (FW, EDR, Endpoints).

Tecnologies avançades: Cloud, IA, Machine Learning adaptats a IT/OT

Servei personalitzat: Informes i alertes clares, adaptació a l'empresa.

Compliment normatiu: controls obligatoris ENS, NIS2, ISO27001.

LightEyes

Protecció de dades i continuïtat de negoci: Consultora en Transformació Digital i Ciberseguretat.

Professionals certificats: màximes certificacions en ciberseguretat.

Serveis: Auditories, consultoria (CISOaaS), formació i conscienciació.

Resposta a incidents: CSIRT (LE CERT) i Red Nacional de SOCs.

Problemàtiques dels ciberatacs en relació a les PIMES

99,8 %

creuen que no són objectiu d'atac.

61%

van ser objectiu d'atac durant el 2021.

Les **pèrdues** oscil·len entre **2000 i 200.000 € per atac.**

Mitjana de 11.400€ per atac.

57%

de les empreses que pateixen un ransomware, acaben pagant el rescat.

60%

tanquen als 6 mesos posteriors d'un ciberatac.

91%

dels atacs son causats per **errors humans**

17%

tenen **ciberassegurances**

58%

no monitoritzen els seus actius

Espanya és el 3r país més atacat del món

però és un dels països que menys inverteix en ciberseguretat.

+4M

de dispositius vulnerables a España, la majoria a Barcelona, Madrid i València

Tendències del cibercrim al 2024

Atacs a la cadena de subministrament

Crisi geopolítica i climàtica

Hacktivisme

Inversió diferencial en ciberseguretat entre PIMES i Grans Corporacions

Democratització de la tecnologia

Intel·ligència artificial

Tendència de ciberincidents a Espanya

Ha doblat el cibercrim... ha doblat el pressupost?

2018	7,5%
2019	9,9%
2020	16,3%
2021	15,6%
2022	16,1%

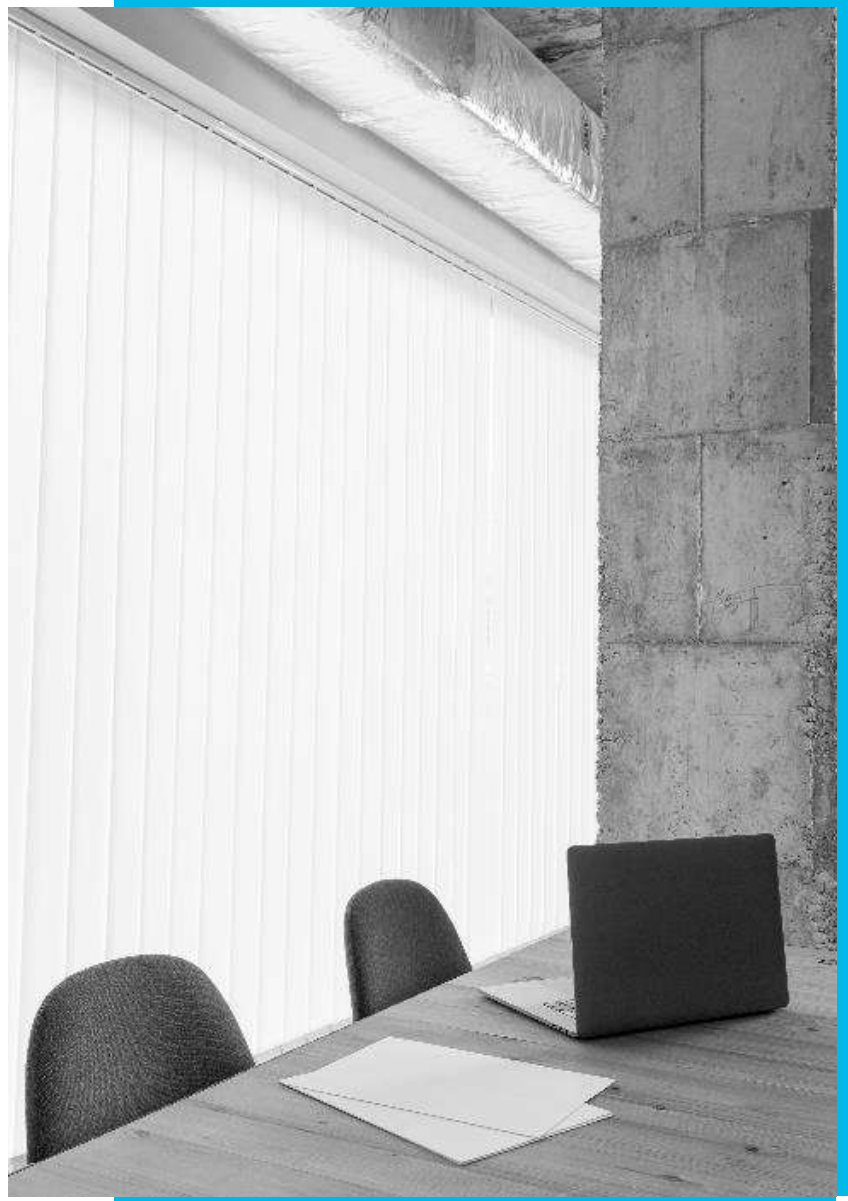
Tabla nº 2. % que representa la Cibercriminalidad sobre el total de infracciones penales. Fuente: Sistema Estadístico de Criminalidad (SEC)

Com ajuda la Directiva NIS2?

- ✓ Proporciona estàndards comuns de seguretat de les xarxes i els sistemes de la informació.
- ✓ Estableix unes normes o requisits mínims de seguretat que garanteixin la protecció dels sistemes informàtics.
- ✓ D'obligat compliment per a determinats sectors.

A què obliga la Directiva NIS2?

- ✓ Disposar de software de seguretat corporativa (antivirus, EDR, tallafocs, VPN...).
- ✓ Software actualitzat a la versió més recent.
- ✓ **Monitorització i registre d'activitat i dels esdeveniments de seguretat**.
- ✓ **Formació i conscienciació en ciberseguretat.**
- ✓ **Polítiques de Seguretat Actualitzades**.
- ✓ **Realitzar proves d'intrusió ètiques**.
- ✓ **Plans de Resposta i Recuperació**.
- ✓ Control d'accessos i privilegis.
- ✓ Estratègia robusta de copies de seguretat.
- ✓ Mesures de seguretat física bàsiques.

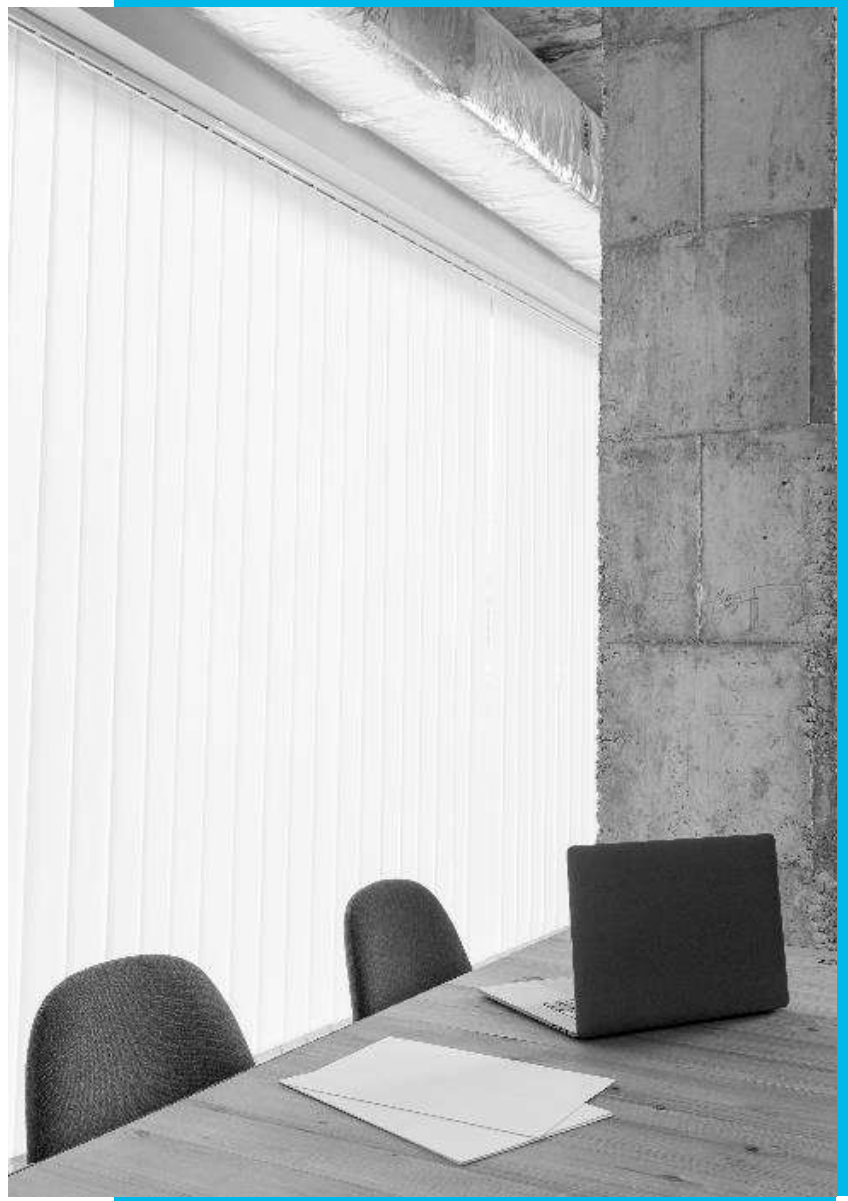


Què és l'Esquema Nacional de Seguretat?

- ✓ Proporciona marc de referència per implementar mesures de seguretat a nivell nacional.
- ✓ L'ENS defineix requisits per garantir la confidencialitat, integritat i disponibilitat dels sistemes d'informació.
- ✓ D'obligat compliment si es vol ser contractat per l'AAPP. A més dona punts per licitacions i altres projectes.

A què obliga l'ENS?

- ✓ Protecció de la Informació: confidencialitat, integritat i disponibilitat de dades.
- ✓ Documentació de polítiques i procediments de seguretat de la informació
- ✓ **Monitorització i registre d'activitat i dels esdeveniments de seguretat**.
- ✓ **Formació i conscienciació en ciberseguretat.**
- ✓ **Gestió de riscos: identificar i gestionar riscos sistemàticament**
- ✓ **Auditories i avaluacions periòdiques**
- ✓ Continuïtat de negoci: copies de seguretat i resposta d'incidents
- ✓ Responsabilitats clarament definides (seguretat, servei, informació...)
- ✓ Controls tècnics i prevenció d'incidents
- ✓ Adaptabilitat i millora contínua: actualitzar mesures de seguretat



Conclusions i recomanacions

- Tenir un **Pla Director de Seguretat**
- **Monitoritzar**: no es pot protegir el que no es veu
- **Prevenció**, no reacció
- Complir amb els bàsics: **ENS, NIS2**
- No podem ser experts en tot: **contractar proveïdors**
- **PIMES son un objectiu dels ciberdelinqüents**
- **Pressupost ciberseguretat: obligatori**

Light Eyes com a proveïdor de Ciberseguretat

- **Servies essencials:**
  - CISO as a Service
  - SOC as a Service
  - Auditories i pentesting
  - Formació i conscienciació
  - Cumpliment NIS2 i ENS

- **Serveis complementaris:**
  - Gestor de contrasenyes
  - Filtre de correu
  - Còpies de seguretat
  - Bosses d'hores tècniques

Light Eyes com a proveïdor de Ciberseguretat

https://apoloanalytics.com/light-eyes/

(no és phishing)

Gràcies per la vostra atenció

aseit 30 anys

Associació TIC catalana