Maig del 2024. Informe tecnològic.

La ciberseguretat a Catalunya

Generalitat de Catalunya

La ciberseguretat a Catalunya. Informe tecnològic.

ACCIÓ
Generalitat de Catalunya

Realització
Unitat d'Estratègia i Intel·ligència Competitiva d'ACCIÓ
Agència de Ciberseguretat de Catalunya

Barcelona, maig del 2024

Generalitat de Catalunya

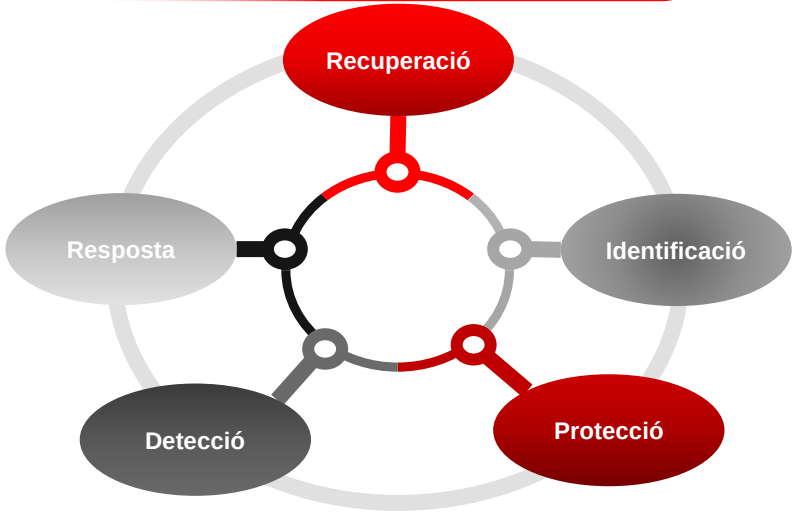
Índex de continguts

Resum executiu

Resum executiu: la ciberseguretat a Catalunya (I)

La ciberseguretat és el conjunt de mesures físiques, lògiques i de governança que protegeixen les propietats de les dades i els sistemes d'informació.

Gestió holística i integral de les amenaces



Sectors de demanda essencials

- Energia
- Transport
- Banca
- Infraestructures del mercat financer
- Salut
- Aigua potable
- Aigües residuals
- Infraestructura digital
- Gestió de serveis TIC (B2B)
- Administració pública
- Espai

Mercat mundial

La facturació mundial en ciberseguretat creixerà un **10% anual** entre el 2023 i el 2028, fins als **275.000 M$**

La regió d'**Àsia** (12,3%) serà la que més creixerà, seguida d'**Europa** (10,3%) i **Amèrica** (9,8%)

Tendències principals

- Potenciar la ciberseguretat a les **eleccions**
- Les **tensions geopolítiques** impulsen l'augment del ciberespionatge i els atacs DDoS
- Preocupa l'**ús de la IA** per cometre fraus
- El **sector sanitari** continua sent un objectiu preferent dels ciberatacs

Generalitat de Catalunya

Resum executiu: la ciberseguretat a Catalunya (II)

Catalunya compta amb 516 empreses de ciberseguretat que facturen 1.244 M€ i donen feina a 9.458 treballadors.

516 empreses

Les empreses augmenten un **4,2%** respecte del 2023, i un **46,6%** en els darrers sis anys.

Facturen **1.244 M€** (+16,1% respecte del 2023 i +54,3% en els darrers sis anys) i ocupen **9.458** treballadors (+0,5% i +60,4%, respectivament).

El **26,9%** tenen menys de 10 anys i el **16,7%** són startups.

El **89,9%** de les empreses es dediquen a la protecció i el **58,7%**, a la identificació.

Catalunya, territori atractiu per la ciberseguretat

El 2023, Catalunya ha estat la **3a regió de la UE en nombre de projectes** en ciberseguretat.

El **36%** dels 140 *hubs* tecnològics d'empreses estrangeres establerts a Catalunya estan enfocats a la ciberseguretat.

Barcelona és la **10a ciutat de la UE** en valor de rondes tancades per a startups de ciberseguretat, amb 85,2 milions de dòlars (2019-2023).

Iniciatives per potenciar la ciberseguretat a Catalunya

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

BARCELONA CYBERSECURITY CONGRESS

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA — CENTRE DE COMPETÈNCIES I D'INNOVACIÓ EN CIBERSEGURETAT

DCA Digital Catalonia Alliance

CYBER SECURITY CAT

DIH4CAT Digital Innovation Hub de Catalunya

La manca de talent, el repte mundial al qual també s'enfronta Catalunya

La **necessitat de professionals** de la ciberseguretat a Catalunya **no coberta** se situa en unes **12.000 persones**.

Les universitats catalanes ofereixen **1 grau universitari** (nou) i **13 màsters i postgraus** en ciberseguretat, mentre que **37 centres** d'estudi catalans ofereixen **47 cursos de formació professional**.

Generalitat de Catalunya

1. Definició de ciberseguretat i importància per a la indústria

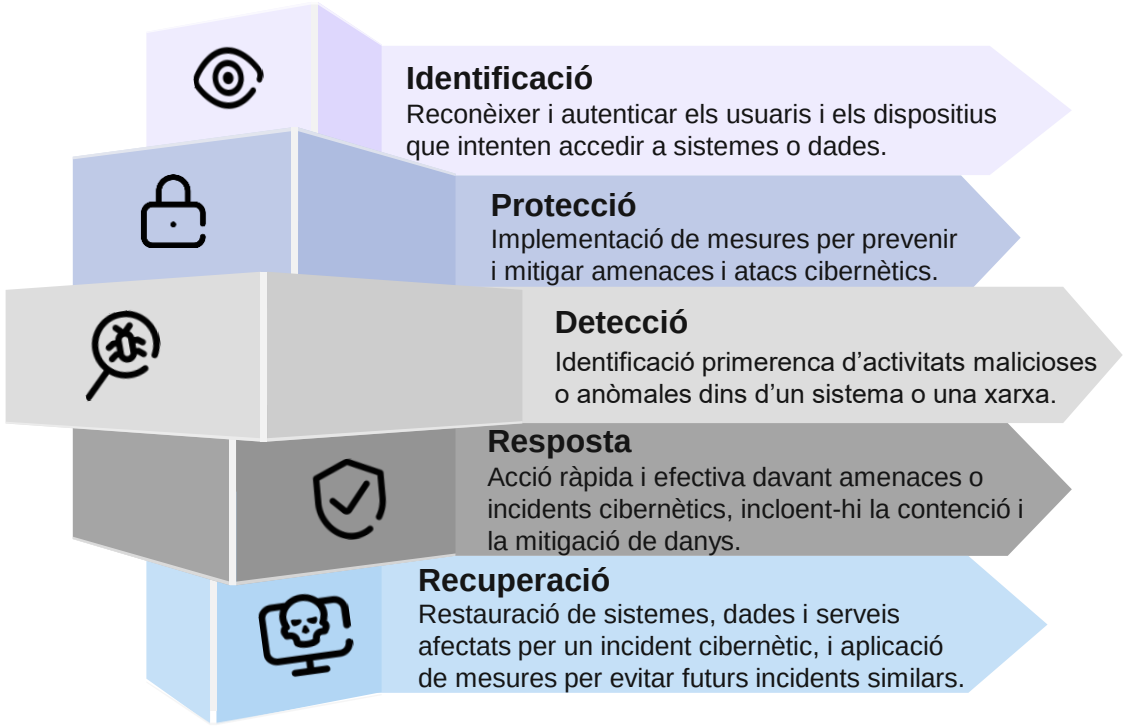
Definició de ciberseguretat

La **ciberseguretat** és el conjunt de mesures físiques, lògiques i de governança que protegeixen les propietats de les dades i els sistemes d'informació.

Les propietats de les dades i els sistemes d'informació són:

- **Confidencialitat:** garanteix que només puguin accedir a aquestes dades les persones autoritzades.
- **Integritat:** garanteix que no patiran cap alteració ni cap destrucció voluntària o accidental.
- **Disponibilitat:** garanteix plenament les funcions en el moment de fer una sol·licitud.
- **Autenticitat:** garanteix que una entitat és qui diu que és o bé confirma la font de la qual procedeixen les dades.
- **Traçabilitat:** garanteix la possibilitat de conèixer-ne l'origen, l'ús, el recorregut i la localització.

Consisteix en: una gestió holística i integral de les amenaces, des de la identificació, fins a les accions de protecció, la detecció de ciberatacs, la resposta a incidents cibernètics i la recuperació.



Actua sobre:

Persones Processos Tecnologies

Generalitat de Catalunya

Riscos cibernètics

Operacional

Un incident cibernètic pot afectar la gestió operativa de les organitzacions i la presa de decisions, que depenen, cada vegada més, de l'ús de les noves tecnologies. Les interrupcions també poden afectar clients i proveïdors de la cadena de subministrament i, en el cas dels serveis essencials, l'estabilitat social i l'econòmica.

L'atac de *ransomware* a l'Hospital Clínic va paralitzar-ne l'activitat: es van cancel·lar 150 intervencions i més de 2.000 visites externes, i va caldre l'activitat manual i la derivació del transport sanitari urgent a altres hospitals.

Econòmic

Un incident cibernètic pot causar la pèrdua de dades o l'aturada de sistemes que impliquin una interrupció de la productivitat i els ingressos. A més, la recuperació posterior a l'incident també pot tenir un cost econòmic elevat: anàlisi forense, restauració de dades i sistemes, recuperació de la reputació, sancions, etc.

El 2023, els atacs de BEC (estafa de correu professional) van representar pèrdues de 6,7 mil milions d'euros. El 67% de les pèrdues per estafes cibernètiques van ser a causa d'atacs de BEC.

Legal

Un incident cibernètic pot revelar una negligència o el fet que els sistemes d'informació no estiguessin protegits degudament, i això pot derivar en sancions. En el cas de les dades personals, que són un actiu buscat pels cibercriminals, el tractament inadequat pot ser objecte de sancions econòmiques molt importants.

El 2023, a la UE es van imposar multes per un valor total aproximat de 2,1 mil milions d'euros a causa de les infraccions del Reglament general de protecció de dades (RGPD).

Reputacional

Un incident cibernètic pot afectar l'opinió que els clients o la ciutadania tenen d'una organització, d'una marca o bé d'un producte o servei, i això pot acabar impactant en el balanç econòmic. Recuperar la reputació després d'un incident pot representar un sobreesforç en termes econòmics i de temps.

El 2023, el 21% de les empreses víctimes d'atacs cibernètics van indicar que l'impacte va ser suficient per amenaçar la viabilitat del negoci.

Fonts: Hospital Clínic, Nasdaq, Statista i Hiscox

Actors darrere dels ciberatacs

	CIBERCRIM	ESTATS	CIBERTERRORISME	*HACKTIVISME*	*HACKING* ÈTIC
Motivacions	· Ànim de lucre · Prestació de serveis cibercriminals	· Aconseguir avantatge competitiu · Protecció de la seguretat nacional · Conflictes geopolítics	· Reivindicacions ideològiques	· Reivindicacions ideològiques	· Aprendre i ampliar capacitats · Ànim de lucre · Progrés i carrera professional
Vectors d'amenaça	· Enginyeria social · Explotació de vulnerabilitats · *Malware* · Atacs de DDoS	· Grups APT patrocinats per estats · Explotació de vulnerabilitats 0-day · *Malware* i *spyware* · Desinformació	· *Malware* · Explotació de vulnerabilitats	· Atacs de DDoS · Explotació de vulnerabilitats · Personal intern · Difusió d'informació en xarxes social	· Explotació de vulnerabilitats · Enginyeria social
Impactes	· Pèrdua d'informació empresarial i personal · Interrupció de l'activitat · Dany reputacional · Sancions	· Interrupció de serveis essencials · Afectació a l'estabilitat social i econòmica · Filtració d'informació estratègica	· Interrupció de serveis essencials · Afectació a l'estabilitat social i econòmica · Danys en el món físic	· Interrupció de l'operativa · Pèrdua de dades · Pèrdua reputacional	· Revelació de vulnerabilitats · Exigència d'una recompensa
Exemples rellevants	· Creuers del Port de Barcelona va ser víctima d'un atac de *ransomware* en què es va exigir un rescat per recuperar els sistemes d'informació	· La utilització de *deepfakes* per influir en processos electorals esdevé una de les principals preocupacions pels estats aquest 2024	· El grup cibercriminal pro-iranià Av3ngers va atacar tecnologies israelianes i va causar un tall del subministrament d'aigua a dues localitats irlandeses	· El grup *hacktivista* R00TK1T va robar dades en un ciberatac a la farmacèutica Sanofi i va acusar-la d'experimentar amb humans	· La Generalitat de Catalunya impulsa diferents iniciatives de *Bug Bounty* per identificar vulnerabilitats en els sistemes d'informació

Magnituds del cibercrim

Es calcula que el 2023 el cost provocat per l'activitat del **cibercrim** a nivell mundial ha estat d'uns **8 bilions d'€**.

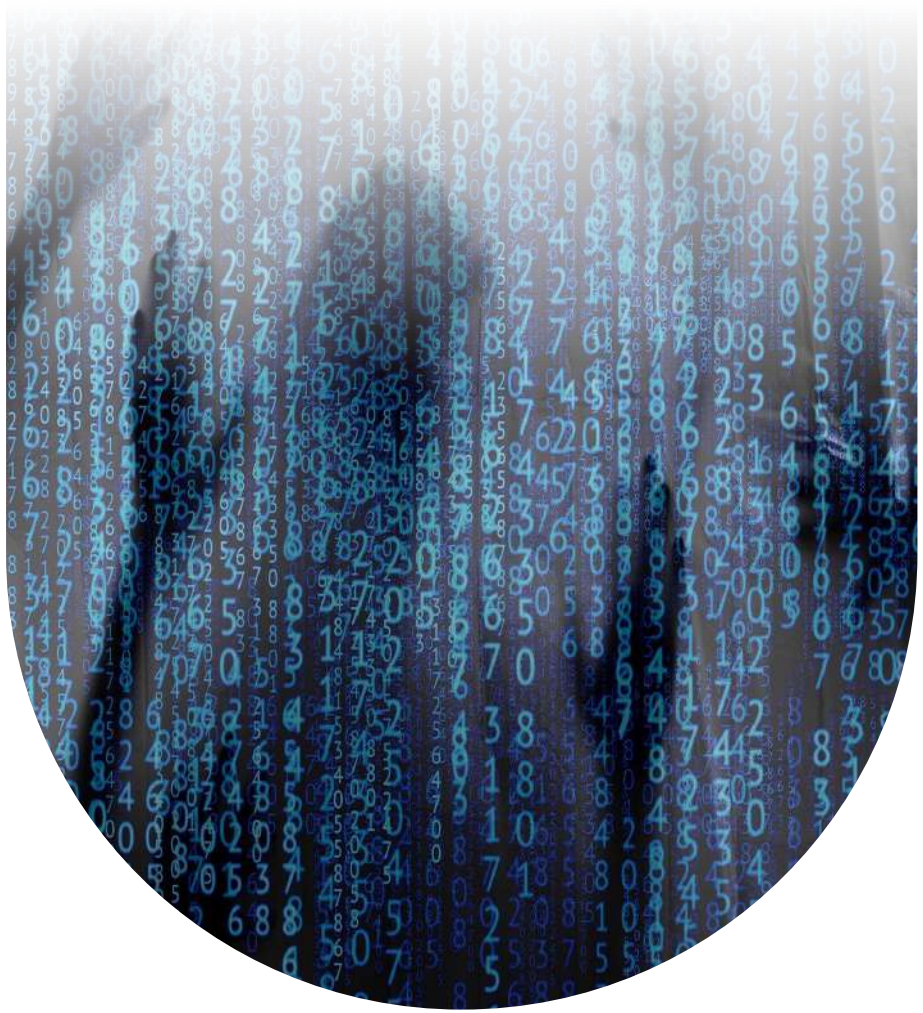
El 2023, els ciberatacs han augmentat un **1%** respecte del 2022.

El **79%** dels ciberatacs tenen motivació financera, seguida de l'espionatge i el *hacktivisme*.

1 de cada 10 empreses a escala mundial ha rebut intents d'atacs de *ransomware* durant el 2023, un augment del **33%**.

L'***email*** continua sent el principal vector d'atac per al ciberdelinqüents, amb el **90%** de les fuites de dades iniciades amb un atac de *phishing*.

El **sector sanitari** és un dels objectius preferits per les bandes de *ransomware,* és el segon sector més atacat per tercer any consecutiu darrere del sector industrial

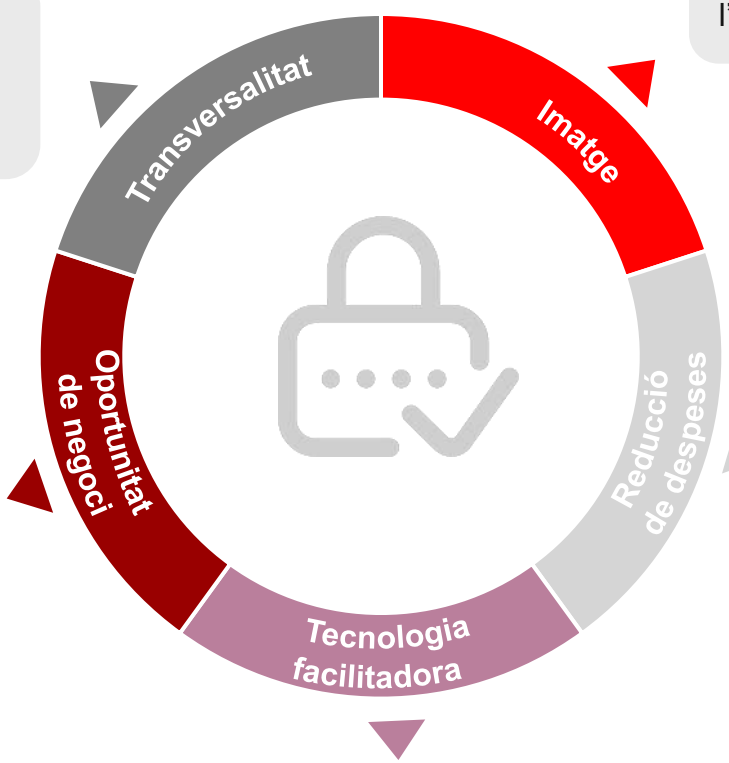


Fonts: Cybersecurity Ventures, Checkpoint, Verizon, Hackmageddon, Cofense i Crowdstrike

Importància de la ciberseguretat per a la indústria

La ciberseguretat afecta molts àmbits, des de governs i infraestructures fins a serveis financers, ciutats intel·ligents, processos productius i sistemes de salut.

Un atac important pot afectar de manera considerable la imatge i la reputació de l'empresa.



La implantació de bones mesures de ciberseguretat per evitar vulnerabilitats pot suposar un estalvi de despeses, gràcies a la disminució del nombre d'hores d'aturades i reinicis de sistemes, de reparació de dispositius, de fuites de dades que poden exposar informació privada o sensible i de repercussions legals.

Un entorn cada vegada més connectat permet generar empreses noves que desenvolupen tecnologies per a determinats tipus d'atacs i models de negoci nous basats en l'estudi de vulnerabilitats. Oportunitats per a startups, transformació d'empreses i creació de llocs de treball.

La ciberseguretat pot contribuir al ple desenvolupament d'altres tecnologies innovadores, com la IoT, el vehicle connectat, la indústria 4.0, la salut digital o el comerç electrònic.

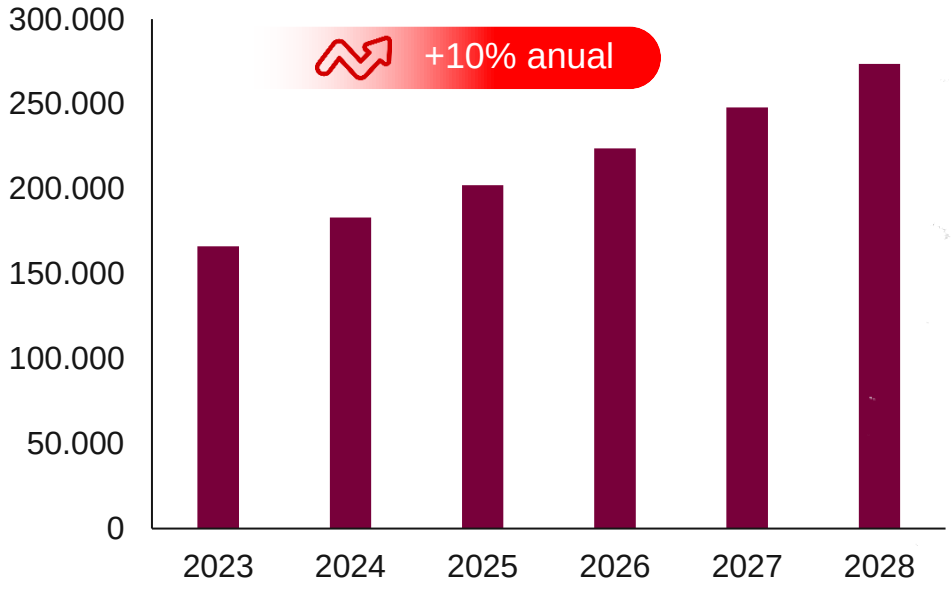
2. Principals magnituds mundials

Mercat mundial i perspectives de creixement de la ciberseguretat

La facturació mundial en ciberseguretat creixerà a un ritme del **10% anual** entre el 2023 i el 2028, fins als **275.000 M$**.

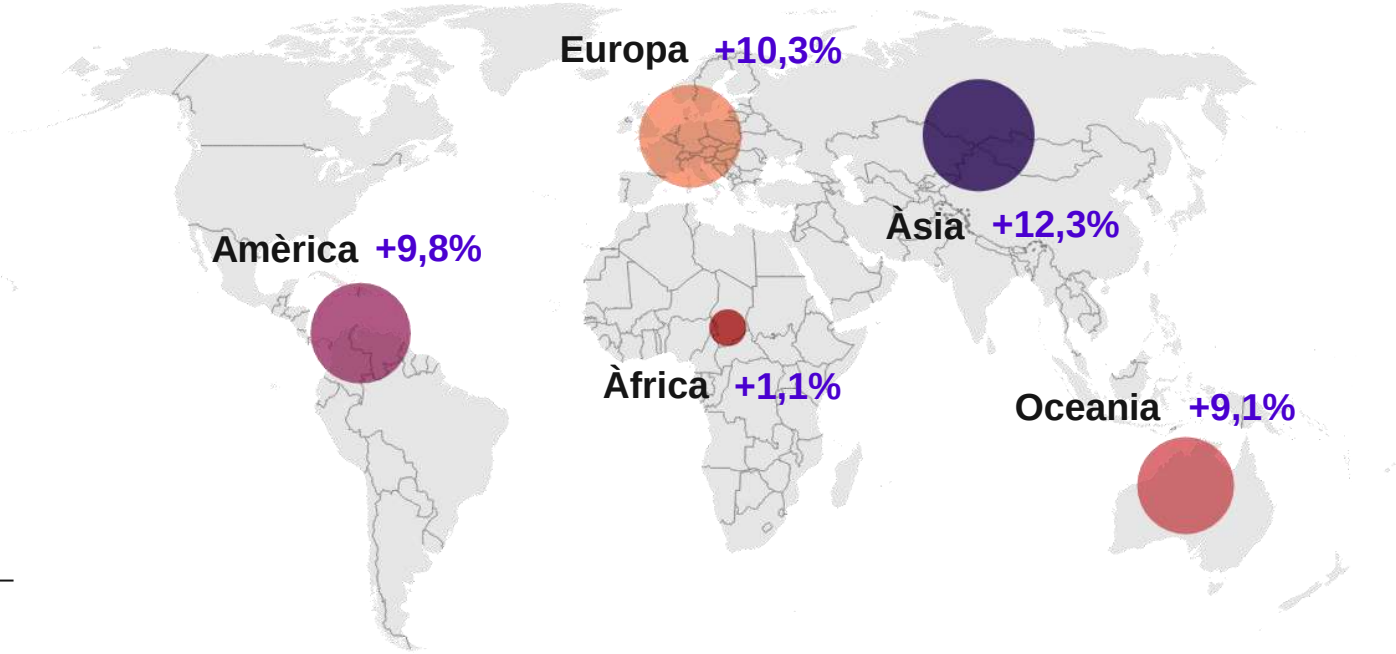
Facturació mundial de la ciberseguretat*

(2023-2028, M$)



Evolució de la facturació de la ciberseguretat, per regions

(2023-2028, %)



A la regió d'**Àsia** (12,3%) es produirà l'augment més gran en facturació de la ciberseguretat durant el període 2023-2028, seguit d'**Europa** (10,3%) i **Amèrica** (9,8%).

Font: Statista

Empreses líders en ciberseguretat

Estats Units

APPGUARD, BROADCOM, CISCO, CLOUDFLARE, CROWDSTRIKE, CYBERARK, DXC TECHNOLOGY, FORTINET, FUTUREX, IBM, imperva, KnowBe4, ManageEngine, Microsoft, okta, OneTrust, netskope, NordLayer, paloalto, proofpoint, RAPID7, Raytheon Technologies, RSA, SecurityHQ, Symantec, tenable, Trellix, VIPRE, UnderDefense, zscaler

Regne Unit

DARKTRACE, intruder, SAPPHIRE, SOPHOS

Alemanya

Avira, T

Israel

CHECK POINT, perimeter 81

Irlanda

accenture

Suïssa

Acronis

República Txeca

Avast

Espanya

cipher

Canadà

Genetec

França

THALES

Japó

TREND MICRO

Índia

INDUSFACE

Polònia

ANDERSEN

Presència a Catalunya

Font: elaboració pròpia a partir d'eSecurity Planet, fDi Markets, Indexsy i Software Testing Help

Inversió Estrangera Directa (IED) en ciberseguretat

La IED en ciberseguretat al món acumula més de **1.400 projectes** en el darrer quinquenni, que sumen una inversió superior als **31.000 milions d'euros** i **180.000 nous llocs de treball creats**.

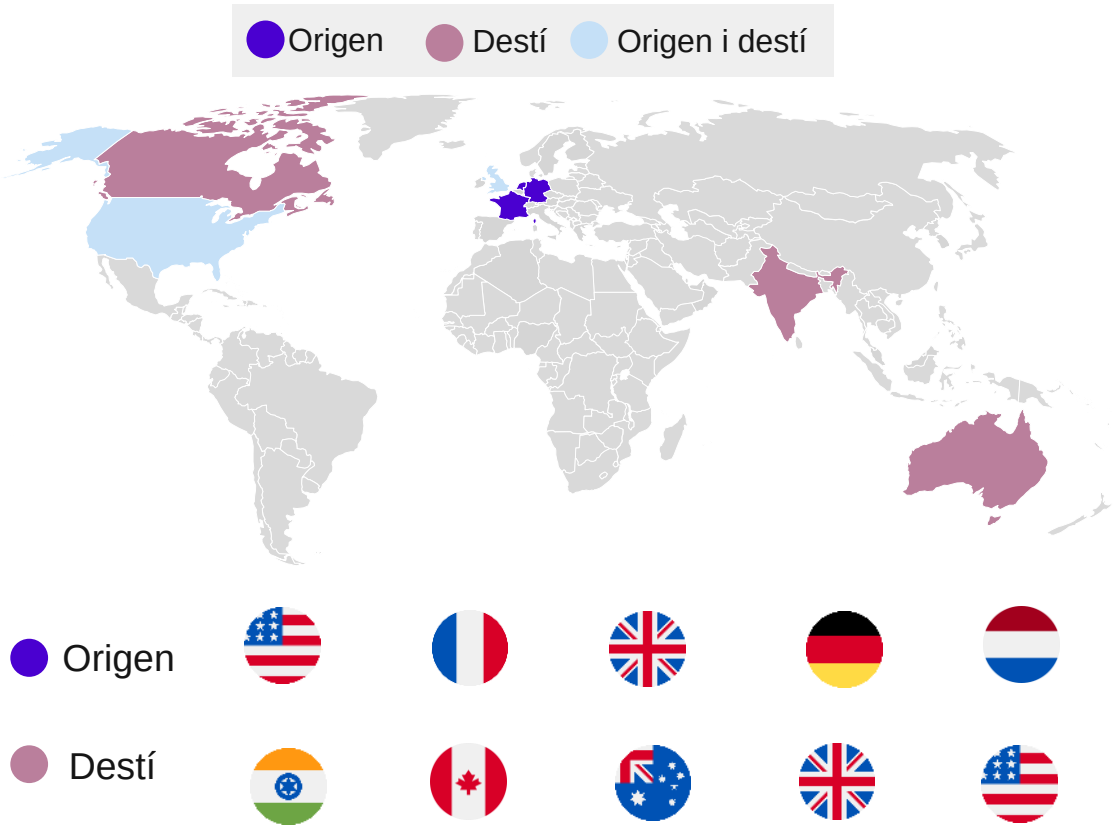
IED en ciberseguretat (2019-2023)

Any	Projectes	Capital invertit (M€)	Ocupació generada
2019	182	2.101	13.505
2020	152	4.014	11.949
2021	373	9.654	42.145
2022	450	8.992	69.978
2023	288	6.871	43.073

Principals empreses inversores (2019-2023)

CLOUDFLARE	netskope	THALES	DXC TECHNOLOGY	Microsoft
2.968 M€	1.780 M€	1.585 M€	1.241 M€	955 M€

Principals països d'origen i destí de la IED (2019-2023)



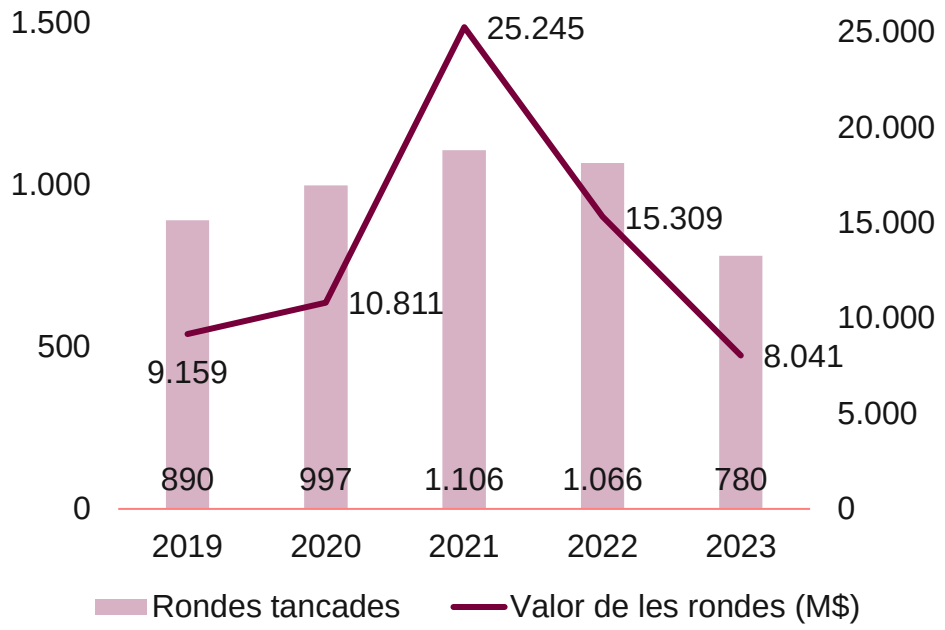
Font: elaboració pròpia a partir d'fDi Markets

Generalitat de Catalunya

Capital risc en startups de ciberseguretat

El 2023 ha tancat amb prop de **8.000 M$ en capital risc en startups de ciberseguretat** al món. Les startups nord-americanes lideren el rànquing de manera molt destacada.

Rondes d'inversió en ciberseguretat (2019-2023)



Nota: s'hi inclouen les rondes d'inversió «pre-seed», «seed» i les sèries A-J de les següents categories: «penetration testing», «network security», «intrusion detection», «identity management», «fraud detection», «e-signature», «cyber security» i «cloud security»; les dades fan referència al període 2019-2023.

Valor i nombre de rondes tancades als principals països

48.745 M$	**5.812 M$**	**2.298 M$**	**2.201 M$**	**1.932 M$**
2.552 rondes	343 rondes	334 rondes	131 rondes	132 rondes

Les startups europees representen el **10,5%** del total invertit

Principals startups per valor de rondes tancades

LACEWORK	snyk	Fireblocks	OneTrust	1Password
1.867 M$	**1.136 M$**	**1.039 M$**	**970 M$**	**920 M$**

Principals inversors en capital risc

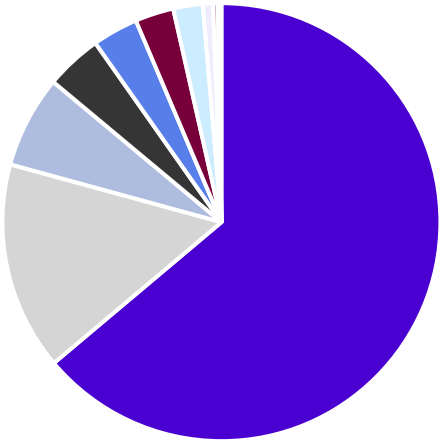
Y Combinator · techstars_ · MC MASSCHALLENGE · 500 · SOSV

Font: elaboració pròpia a partir de Crunchbase

Patents en ciberseguretat

L'augment del nombre de sol·licituds de patents de ciberseguretat mostra la gran quantitat d'inversió, investigació i desenvolupament per trobar noves maneres d'ajudar a prevenir els ciberatacs.

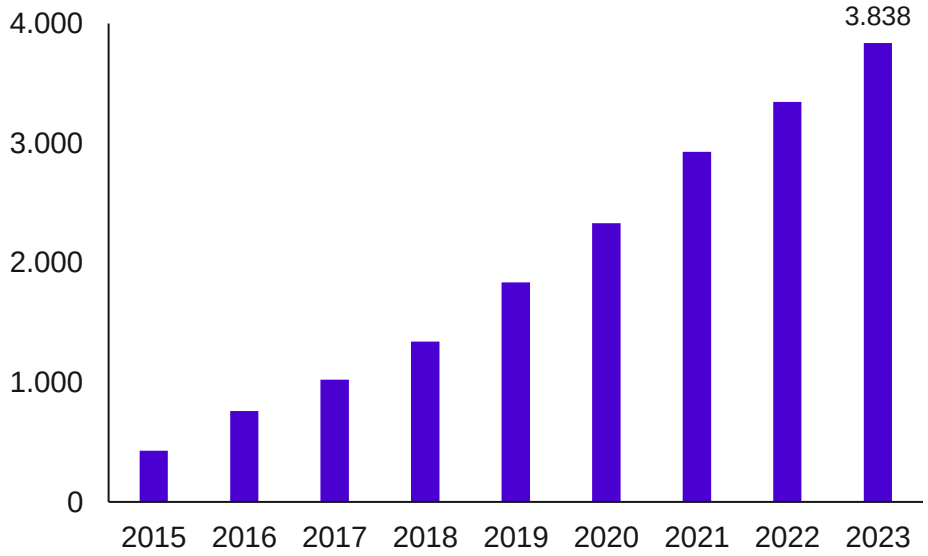
Distribució de patents per jurisdicció geogràfica (2015-2023)



- Estats Units d'Amèrica
- PCT
- EPO
- Índia
- Canadà
- Austràlia
- Xina
- Regne Unit
- República de Corea
- Singapur

Nota metodològica: sol·licituds de patents que mencionin el terme "cyber security" o "cybersecurity" a WIPO patentscope.

Evolució del nombre de patents (2015-2023)



Les principals àrees on es patenta son els **sistemes informàtics** basats en models computacionals específics, la **transmissió de dades** digitals i sistemes o mètodes de **processament de dades**.

Principals empreses sol·licitants de patents (2015-2023)

PURESTORAGE · IBM · Microsoft · Honeywell · UAB 360 IT · Strong Force · QOMPLX: · FIREEYE · BOEING · BANK OF AMERICA

Font: WIPO

Generalitat de Catalunya

3. Aplicacions prospectives per sector de demanda

Sectors de demanda (I)

La **Directiva europea NIS 2** determina **11 sectors essencials d'alta criticitat** i 7 sectors importants addicionals que constituiran nous sectors de demanda de productes i serveis de ciberseguretat. El 2024, els estats membres de la UE hauran de transposar la Directiva al dret intern.

11 sectors essencials d'alta criticitat, segons la Directiva europea NIS 2

Energia	Entitats dedicades a la producció i la transmissió d'electricitat, operadors de calefacció i refrigeració, i actors vinculats a l'extracció i la distribució de petroli, gas i hidrogen.
Transport	Autoritats, operadors i gestors d'infraestructura vinculada als transports aeri, ferroviari, marítim i de carretera.
Banca	Institucions de crèdit.
Infraestructures del mercat financer	Operadors de punts per al negoci i l'intercanvi, i entitats de contrapart centrals (en anglès, CCP).
Salut	Prestadors de serveis de salut, laboratoris de referència de la UE, entitats que duen a terme activitats de recerca i desenvolupament de productes medicinals, entitats que fabriquen productes farmacèutics bàsics i preparats farmacèutics, i entitats que fabriquen dispositius mèdics considerats crítics durant una emergència de salut pública.
Aigua potable	Proveïdors i distribuïdors d'aigua destinada al consum humà.
Aigües residuals	Empreses que recullen, eliminen o tracten aigües residuals urbanes, residuals domèstiques o residuals industrials, excloses les empreses per a les quals la recollida, l'eliminació o el tractament d'aigües residuals és una part no essencial de la seva activitat general.
Infraestructura digital	Proveïdors de punts d'intercanvi d'internet / Proveïdors de serveis DNS (exclosos els operadors de servidors de noms de domini arrel) / Registres de noms de TLD / Proveïdors de serveis de computació en núvol / Proveïdors de serveis de centres de dades / Proveïdors de xarxes de distribució de continguts / Proveïdors de serveis de confiança / Proveïdors de xarxes i serveis de comunicacions electròniques públicament disponibles.
Gestió de serveis TIC (B2B)	Proveïdors de serveis gestionats (en anglès, MSP) i proveïdors de serveis de seguretat gestionats (en anglès, MSSP).
Administració pública	Entitats de l'administració pública dels governs centrals, entitats de l'administració pública en l'àmbit regional.
Espai	Operadors d'infraestructures terrestres, propietats gestionades i operades per estats membres o per parts privades, que donen suport a la prestació de serveis basats en l'espai (exclosos els proveïdors de xarxes de comunicacions electròniques públiques).

Sectors de demanda (II)

7 sectors importants, segons la Directiva europea NIS 2

Serveis postals i de missatgeria	Proveïdors de serveis postals, inclosos els proveïdors de serveis de missatgeria.
Gestió de residus	Empreses que gestionen els residus, excloent-ne les empreses que no tenen la gestió de residus com a activitat econòmica principal.
Fabricació, producció i distribució de productes químics	Empreses que fabriquen i distribueixen substàncies químiques, incloent-hi les empreses que les utilitzen per produir articles a partir d'aquestes substàncies.
Investigació	Organitzacions de recerca.
Producció, processament i distribució d'aliments	Empreses alimentàries de producció i processament industrials.
Fabricació	Fabricació de dispositius mèdics i dispositius mèdics per a diagnòstics in vitro / Fabricació de productes informàtics, electrònics i òptics / Fabricació d'equips elèctrics / Fabricació de maquinària i equips no classificats en cap altra part / Fabricació de vehicles automotors, remolcs i semiremolcs / Fabricació d'altres equips de transport.
Proveïdors digitals	Proveïdors de mercats en línia, proveïdors de motors de cerca en línia i proveïdors de plataformes de serveis de xarxes socials.

Sectors de demanda impulsats pels Reglaments DORA i de Ciberresiliència

El **Reglament DORA** (*Digital Operational Resilience Act*) serà d'obligat compliment a partir del gener de 2025 per a qualsevol entitat financera que ofereixi serveis financers a la Unió Europea.

Entitats de crèdit	Institucions financeres, com per exemple bancs, caixes d'estalvis, cooperatives de crèdit, etc.
Entitats de pagament	Institucions financeres, com per exemple proveïdors de serveis de pagament, entitats de diners electrònics, etc.
Empreses de serveis d'inversió	Institucions financeres, com per exemple bancs d'inversió, societats de valors, empreses de gestió d'actius, etc.
Proveïdors de serveis de criptoactius	Institucions financeres, com per exemple plataformes d'intercanvi de criptomonedes, custòdia de criptoactius, etc.
Altres	Institucions que operen en el àmbit financer i exerceixen un paper crític en la economia i la societat, com per exemple fons de pensions, companyies d'assegurances, agències de qualificació de proveïdors de serveis d'infraestructura del mercat financer, etc.

El **Reglament de Ciberresilència** serà d'obligat compliment per a totes les empreses que fabriquen productes digitals, així com distribuïdors i importadors dins del marc de la Unió Europea. Una vegada aprovat, s'establiran 24 mesos per adaptar-se completament.

Fabricants de productes digitals	Tota entitat que desenvolupi productes, tant software com hardware, connectats directament o indirectament a un altre dispositiu o una xarxa.

Estan **exempts** de complir amb aquesta norma els fabricants per als quals ja existeixen requisits de ciberseguretat en els reglaments de la Unió Europea, com per exemple fabricants de vehicles, aviació, dispositius mèdics, agències policials, etc.

Convergència de tecnologies (I)

IA per a la producció audiovisual

S'ha observat un creixement en l'ús d'eines que fan servir la intel·ligència artificial per ajudar a crear fotografies i vídeos.
També s'ha constatat un increment en l'ús d'aquestes eines amb finalitats il·lícites, com la suplantació d'identitats per cometre fraus, la influència política o, fins i tot, per a interessos econòmics personals, com és el cas de la difusió de pornografia amb celebritats.

IA generativa

L'adopció de la intel·ligència artificial generativa, com ara el ChatGPT, està transformant diversos sectors de la nostra vida, i un d'aquests sectors és el camp de la ciberseguretat. Això es deu al potencial que té per facilitar anàlisis de seguretat, escriptura de codi, anàlisis de vulnerabilitats, etc. Ara bé, també se'n fa un ús delictiu per escriure codi maliciós, elaborar massivament missatges de *phishing*, etc.

Criptografia quàntica

A mesura que aquesta tecnologia avanci, al llarg de la dècada vinent, augmentarà el risc que alguns mètodes de xifratge utilitzats per protegir les dades en repòs i en trànsit quedin obsolets. És per això que les empreses han de començar a establir plans de migració vers algorismes de xifrat resistents a la computació quàntica.

Bessons digitals

Els bessons digitals (*digital twins*) esdevenen una eina clau per analitzar els riscos i els impactes d'un incident digital sobre entorns físics complexos que incloguin sistemes ciberfísics, IoT, persones, cadenes de subministrament, processos, etc. Els bessons digitals permetran simular entorns físics i entrenar, en temps real, la capacitat de reacció d'una organització davant d'un ciberatac.

Convergència de tecnologies (II)

Internet de les coses (IoT)

El concepte internet de les coses sorgeix de la idea que qualsevol objecte físic pot estar connectat a la xarxa i comunicar-se amb altres dispositius i altres sistemes. Aquesta idea aporta molts beneficis, encara que també s'hi ha d'anar amb compte, ja que, a l'hora de connectar dispositius, cal assegurar-se que s'implementen les mesures de protecció adients tant per als dispositius en si, com per a la xarxa que els uneix.

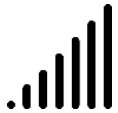
Seguretat al núvol

Les organitzacions esdevenen *cloudcèntriques*: necessitaran la flexibilitat de la ciberseguretat oferta des del núvol per mitjà d'arquitectures de seguretat SASE (*secure access service edge*) i controls d'accessos amb sistemes CASB (*cloud access security broker*). Són tecnologies que ja tenen uns quants anys, però és ara que ha arribat el seu moment.

Multifactor (MFA)

El 61% de les fuites de dades s'han originat a partir de l'ús de credencials robades; si s'hagués tingut un sistema MFA, aquestes fuites s'haurien evitat. Els fabricants i els proveïdors de serveis al núvol principals recomanen fer servir sistemes d'autenticació addicionals, com ara factors biomètrics, com la retina o la veu, elements que es posseeixen, com el telèfon mòbil, un *token*, o les contrasenyes d'un sol ús (OTP).

Connectivitat 5G



El desplegament de les tecnologies 5G, que promet ser un avenç significatiu pel que fa a velocitat, consum, eficiència i sensibilitat en les connexions de xarxa, presenta un repte significatiu en el paradigma de la ciberseguretat, ja que proporciona als atacants escenaris més potents per dur a terme atacs, com per exemple: *botnets*, denegació de serveis distribuïts (DDoS), atacs MiTM, etc.

4. Tendències en ciberseguretat i impacte en els ODS

Principals tendències en ciberseguretat del 2023

El robatori de dades alimenta un negoci lucratiu a la *dark web*. Els ciberdelinqüents roben i venen dades per perpetrar atacs nous, els quals acaben amb el robatori de més dades. Aquest cicle perpetua el mercat negre de dades robades i posa en perill la seguretat en línia.

Alerta global per atacs de *ransomware* a gran escala. Els cibercriminals exploten vulnerabilitats de dia zero i ataquen la cadena de subministrament de proveïdors de solucions TIC per desplegar atacs de *ransomware* de manera massiva entre els clients.

L'evolució del *ransomware*. Els operadors de *ransomware* adopten estratègies noves per aconseguir més afectacions, com l'automatització dels atacs per arribar a més víctimes, i l'especialització per aconseguir robar volums massius de dades.

Casos de doble *ransomware*. Més víctimes de *ransomware* reben un segon atac poc després d'haver-ne sofert un. Les causes: la venda dels mateixos accessos a diferents ciberdelinqüents i l'ús de diferents eines de xifratge per un mateix grup cibercriminal.

Augmenten els atacs a les cadenes de subministrament de *software*. Els atacs a les cadenes de subministrament de *software* permeten impactar múltiples víctimes amb un sol atac, per mitjà tant dels desenvolupadors com dels repositoris de llibreries.

Ciberseguretat a les eleccions. Els processos electorals són períodes propensos als ciberatacs: campanyes de *phishing*, atacs de DDoS als sistemes de votació en línia, manipulació de sistemes per difondre missatges ideològics i difusió de *deepfakes*.

Evolució dels atacs de DDoS en els conflictes geopolítics. L'ús de *botnets* formades amb recursos del núvol infectats permeten fer atacs més complexos i potents contra els serveis essencials en línia de l'adversari per desestabilitzar-lo.

Les tensions geopolítiques impulsen l'augment del ciberespionatge. Arran de la conflictivitat creixent entre diferents estats del món, s'han identificat nombrosos casos d'espionatge a treballadors públics o d'intrusions en xarxes governamentals.

Ciberatacs als serveis bàsics en conflictes geopolítics i escalada a tercers països. Els ciberatacs a serveis bàsics (com la distribució d'aigua i energia o les telecomunicacions) tenen el potencial d'afectar directament la població. Tenen un abast mundial, ja que es fan servir per atacar els rivals geopolítics i els seus aliats.

Preocupa l'ús de la IA per cometre fraus. Es disparen els casos en què s'utilitza la IA generativa per enganyar mitjançant la creació de missatges de text convincents i la suplantació de persones per mitjans audiovisuals.

El sector sanitari continua sent un objectiu preferent dels ciberatacs. La criticitat de l'activitat dels hospitals els converteix en objectius de *ransomware*, i les dades personals o de recerca que utilitzen esdevenen un objectiu cobejat pel cibercrim.

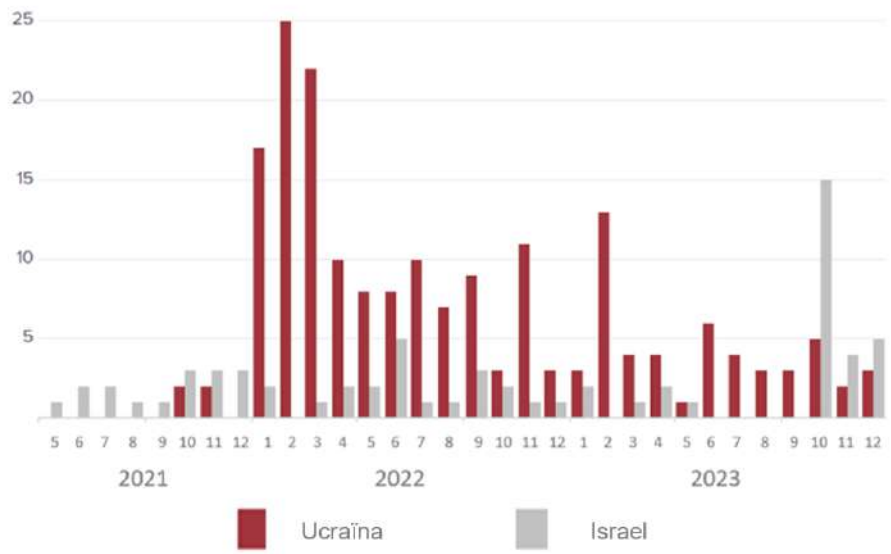
Risc cibernètic en períodes de consum elevat. El Nadal i les rebaixes atrauen ciberatacs dirigits a consumidors i empreses d'*e-commerce*. Els ciberdelinqüents aprofiten l'interès dels consumidors i l'activitat en línia per perpetrar fraus i robatoris de dades.

Principals tendències en ciberseguretat del 2023: els conflictes geopolítics incentiven una escalada cibernètica global que amenaça els serveis essencials

Els conflictes bèl·lics entre Ucraïna i Rússia, i entre Hamàs i Israel, han desencadenat una guerra cibernètica global. Els últims 3 mesos de 2023, les notícies de ciberatacs relacionades amb el conflicte al Pròxim Orient van traslladar el d'Ucraïna a un segon terme.

Notícies sobre ciberatacs relacionats amb conflictes geopolítics

2021-2023



Els conflictes cibernètics acaben esquitxant països que no estan directament relacionats amb la guerra.

Es constata que en els conflictes bèl·lics actuals es produeix una escalada cibernètica a través de l'ús de *wipers*, atacs de DDoS, la distribució de *sypwares*, campanyes de desinformació, etc.

El ciberespionatge ha emergit com una via il·lícita i altament efectiva per a l'obtenció d'informació sensible. Aquesta pràctica implica l'ús de recursos tecnològics avançats per infiltrar-se en els sistemes de l'objectiu, ja siguin de governs, empreses o individus, per tal d'accedir a informació confidencial.

Els ciberatacs relacionats amb els conflictes armats busquen pertorbar empreses o serveis essencials de l'adversari per a afectar la seva reputació o bé la seva estabilitat social i econòmica. Com a objectius freqüents d'aquests atacs es troben els entorns industrials vinculats a sectors com l'alimentari, i els subministraments d'aigua o energia.

Font: Agència de Ciberseguretat de Catalunya

Generalitat de Catalunya

Fets rellevants del 2023

INTERNACIONALS

A CATALUNYA

Gen. 23	Feb. 23	Mar. 23	Abr. 23	Mai. 23	Jun. 23	Jul. 23	Ago. 23	Set. 23	Oct. 23	Nov. 23	Des. 23
El bisbat de Girona, víctima d'un frau cibernètic *Frau*	Augmenten les deteccions del troià HoudRat a Catalunya *Malware*	L'Hospital Clínic, víctima d'un atac de *ransomware* que en paralitza l'activitat *Ransomware*	Creuers del Port de Barcelona experimenta un atac de *ransomware* de LockBit *Ransomware*	L'Agència de Ciberseguretat de Catalunya i el CTTI aturen un ciberatac *Ransomware*	Incident de *ransomware* a l'empresa del servei d'aigua de Lleida *Ransomware*	El Clínic confirma la filtració de dades robades durant el ciberatac *Fuita de dades*	La Guàrdia Civil deté una banda criminal dedicada a les ciberestafes *Frau*	Desarticulada una organització cibercriminal especialitzada *Frau*	Diversos hospitals afectats per un ciberatac a un proveidor *Ransomware*	Ciberatac a Junts per Catalunya coincidint amb la votació per a la investidura *Hacktivisme*	L'Ajuntament de Reus informa d'un ciberatac a Reus Mobilitat i Serveis *Fuita de dades*

S'exposen les dades de 37 M d'usuaris i usuàries de T-Mobile (EUA) *Fuita de dades*

Campanya de ransomware massiva contra servidors VMWare *Ransomware*

Cibercriminals utilitzen la IA per suplantar la veu de coneguts *Frau*

Ciberseguretat CheckPoint i universitats israelianes *DDoS*

Anonymous Sudan ataca l'empresa de gran de venda de credencials *Accions policials*

Desarticulada Genesis Market, la plataforma més dades i extorsionar els clients *Fuita de dades*

Explotació de vulnerabilitats de MOVEit per robar les dades de la clientela *Ransomware*

Diversos grups de ciberespionatge vinculats a la Xina dirigeixen les seves operacions a Europa i els EUA *Ciberespionatge*

Dues empreses de hosting daneses perden milers de milions de credencials *Fuita de dades*

L'empresa de ciberseguretat DarkBeam filtra per error més gran de la història *DDoS*

L'atac DDoS en peticions per segon instal·lacions d'aigua dels EUA *Sabotatge*

Ciberatacs amb vincles iranians dirigits a a hospitals alemanys durant la nit de Nadal *Ransomware*

Un atac de Lockbit interromp serveis mèdics

Font: diverses fonts

Generalitat de Catalunya

Fets rellevants del 2023 en l'àmbit internacional

- **S'exposen les dades de 37 M d'usuaris i usuàries de T-Mobile (EUA).** Les dades personals van quedar exposades per un atac maliciós a través d'una API. La informació compromesa inclou noms, dates de naixement, correus electrònics i adreces de facturació, però no dades financeres.

- **Campanya de *ransomware* massiva contra servidors VMWare.** El *ransomware* ESXiArg afecta servidors VMware ESXi i explota vulnerabilitats en servidors desactualitzats. S'evidencia un atac automatitzat, ja que en pocs dies milers de servidors han quedat afectats.

- **Cibercriminals utilitzen la IA per suplantar la veu de coneguts.** Una parella de 73 i 75 anys del Canadà van rebre una presumpta trucada del seu net. Informava que es trobava a la presó i que necessitava diners.

- **Anonymous Sudan ataca l'empresa de ciberseguretat CheckPoint i universitats israelianes.** Dos atacs de DDoS, l'últim més potent, deixen el web de l'empresa inactiu. Universitats com Tel Aviv, Hebrea de Jerusalem, Ben-Gurion i Weizmann també han estat afectades simultàniament.

- **Desarticulada Genesis Market, la major plataforma de venda de credencials a la *dark web*.** Una operació policial internacional ha culminat amb 119 persones detingudes que utilitzaven la informació subministrada en el mercat per a la suplantació d'identitats en serveis en línia.

- **Explotació de vulnerabilitats de MOVEit per robar dades i extorsionar els clients.** L'atac permet l'escalada de privilegis i l'accés no autoritzat als usuaris de la plataforma de compartició MOVEit. El grup cibercriminal Cl0p s'ha dedicat a robar dades i extorsionar les víctimes.

- **Dues empreses de *hosting* daneses perden totes les dades de clients/es en un atac de *ransomware*.** Els atacants van accedir als servidors i van xifrar les dades de clients, incloses les còpies de seguretat. Atès que no van pagar el rescat, van perdre les dades.

- **Diversos grups de ciberespionatge vinculats a la Xina dirigeixen les seves operacions a Europa i els EUA.** Utilitzen *phishing* i la falsificació de *tokens* per accedir a informació sensible. Microsoft ha bloquejat les operacions del grup Storm-0558 i dona consells per contrarestar el grup Storm-0978.

- **L'empresa de ciberseguretat DarkBeam filtra per error milers de milions de credencials dels seus clients.** El motiu: una configuració inadequada d'Elasticsearch i Kibana. Les dades filtrades inclouen correus electrònics i contrasenyes recopilades d'altres fuites per alertar clients sobre fuites.

- **Major atac DDoS en peticions per segon de la història.** Google Cloud, Amazon Web Services i Cloudflare van detectar i bloquejar un atac DDoS rècord de 398 Mrps (peticions per segon). L'atac explota una vulnerabilitat en HTTP/2 mitjançant la tècnica de "reseteig ràpid".

- **Ciberatacs amb vincles iranians dirigits a instal·lacions d'aigua dels EUA.** El govern dels EUA investiga ciberatacs de grups cibercriminals iranians que ataquen les tecnologies d'operació (OT) d'origen israelià utilitzades en instal·lacions de subministrament d'aigua.

- **Un atac de Lockbit interromp serveis mèdics a hospitals alemanys durant la nit de Nadal.** Durant la nit de Nadal, l'atac va interrompre serveis mèdics en tres hospitals alemanys de la xarxa KHO, xifrant dades i forçant el tancament de sistemes. Tot i això, l'atenció als pacients es va mantenir amb restriccions tècniques lleus.

Font: diverses fonts

Fets rellevants del 2023 en l'àmbit de Catalunya

- **El bisbat de Girona, víctima d'un frau cibernètic.** Els empleats reben correus electrònics fraudulents que semblen provenir de l'administrador diocesà. El correu sol·licita als treballadors que comprin targetes d'iTunes-Apple.

- **Augment en les deteccions del troià HoudRat a Catalunya.** Aquest *malware* RAT per a Windows roba informació, especialment dades financeres, i permet el control remot dels dispositius afectats. Es propaga principalment a través de suports extraïbles.

- **L'Hospital Clínic víctima d'un atac de *ransomware* que en paralitza l'activitat.** El grup de cibercriminal RansomHouse ha xifrat els sistemes de l'hospital i robat 4,5 TB de dades. Exigeix un rescat de 4,5M€ i, com que no s'ha pagat, s'han publicat part de les dades com a mesura de pressió.

- **Creuers del Port de Barcelona experimenten un atac de *ransomware* de LockBit.** LockBit ha xifrat sistemes i robat dades, de manera que exigeix un rescat de 299.999 €. També ofereix la possibilitat de pagar 1.000 € per ampliar el termini 24 hores.

- **L'Agència de Ciberseguretat de Catalunya i el CTTI aturen un ciberatac.** Durant el cap de setmana, les accions preventives han permès contenir l'atac i evitar un possible ciberincident de *ransomware*, després d'haver detectat i monitorat diferents accions d'un agent maliciós.

- **Incident de *ransomware* a l'empresa del servei d'aigua de Lleida.** L'atac afecta dades personals dels clients, però no s'ha detectat que hi hagi hagut cap publicació de dades. Els fets s'han comunicat a les autoritats de protecció de dades.

- **El Clínic confirma la filtració de dades robades durant el ciberatac.** El grup cibercriminal RansomHouse publica més dades. L'entitat sanitària i l'Agència de Ciberseguretat de Catalunya col·laboren per mitigar-ne les conseqüències, i recorden que la publicació de dades és un delicte.

- **La Guàrdia Civil deté una banda criminal dedicada a les ciberestafes.** Detingudes 14 persones a Catalunya per estafar i robar a través de ciberestafes com l'*smishing*, el *vishing* i també la sextorsió. Havien estafat a 16 veïns d'Osca per un total de 110.000 euros.

- **Desarticulada una organització criminal especialitzada en ciberdelinqüència amb detencions a Lleida.** Es detenen 54 persones d'un grup criminal que ha defraudat més de 150.000 euros en 80 delictes a tot el país mitjançant ciberatacs i estafes bancàries.

- **Diversos hospitals afectats per un ciberatac a la cadena de subministrament.** Diversos hospitals, inclòs el de la Seu d'Urgell, afectats per un ciberatac a l'empresa proveïdora de *software* de recursos humans. L'Hospital ha controlat l'atac i cap dada personal ha quedat compromesa.

- **Ciberatac a Junts per Catalunya coincidint amb la votació per a la investidura.** Durant la investidura de Pedro Sánchez, JxC va ser objecte d'un ciberatac coordinat, amb 70.000 "agressions planificades". Malgrat això, es va neutralitzar i es va garantir que no va afectar la votació telemàtica.

- **L'Ajuntament de Reus ha informat d'un ciberatac a Reus Mobilitat i Serveis.** S'han vist afectades l'aplicació APARCAR i els accessos als aparcaments municipals. Tot i això, les dades sensibles es van mantenir segures gràcies a una resposta ràpida.

Font: diverses fonts

Xifres dels ciberatacs amb impacte a Catalunya el 2023

70%

Protagonisme del *ransomware*

El 70% dels incidents de ciberseguretat publicats són a causa del *ransomware*.

+460%

El *ransomware* es dispara

El nombre d'incidents de *ransomware* publicats ha augmentat un 460% respecte de l'any anterior.

74%

Ciberatacs amb enginyeria social

Les notícies de ciberseguretat publicades destaquen temes relacionats amb el *phishing* (38%), la distribució de *malware* (25%) i el ciberfrau (11%).

81%

El sector sanitari, l'objectiu principal

El 81% dels ciberatacs fets públics han tingut afectacions al sector sanitari.

10%

Ciberatacs i denúncies

El 10% de les empreses catalanes han experimentat un ciberatac el darrer any, i el 46% d'aquestes ho han denunciat.

34%

Ciberassegurances

El 34% de les empreses catalanes tenen una assegurança per a incidents de ciberseguretat, un percentatge que creix amb la mida de l'empresa.

11%

***Malware* per a tots els sistemes operatius**

Els programaris maliciosos més detectats a Catalunya: RootSTV (Android), AMCleaner (MacOS) i Socks5Systemz (Windows).

36%

Vulnerabilitats a Apache

Les 23 vunerabilitats més presents a les IP de Catalunya afecten servidors Apache i representen el 36% del total de vulnerabilitats.

Fonts: Agència de Ciberseguretat, IDESCAT i Bitsight

Continua la falta de talent en ciberseguretat

Necessitat de professionals de la ciberseguretat

Segons (ISC)[2], el nombre de professionals de la ciberseguretat ha crescut un 8,7% al món, però la bretxa de professionals encara creix més: un 12,6%, fins als gairebé 4 milions de vacants al món.

A **Catalunya**, la tendència s'accentua més:

El nombre de professionals de la ciberseguretat creix en un **19%** i la bretxa, en un **23%**, de manera que la necessitat de professionals no coberta se situa en unes **12.000** persones

	Professionals de la ciberseguretat existents		Necessitat de professionals no coberta	
	vs. 2022	2023	vs. 2022	2023
MÓN	+8,7%	**5,4 M**	+12,6%	**4 M**
EMEA	+7,2%	**1,3 M**	+9,7%	**347 K**
CATALUNYA *	+19%	**31 K**	+23%	**12 K**

**Estimació*

Generalitat de Catalunya

Formació en ciberseguretat a Catalunya

13 màsters o postgraus de ciberseguretat

- Màster en Seguretat de la Informació Empresarial (OBS Business School)
- Postgrau en *Compliance* i Ciberseguretat (UIC Barcelona)
- Màster en Seguretat de les TIC (UOC Universitat Oberta de Catalunya)
- Màster en direcció de ciberseguretat (UPC Barcelonatech)
- Màster en Enginyeria de la Seguretat Informàtica i Intel·ligència Artificial (Universitat Rovira i Virgili)
- NEW Màster en Aprenentatge Automàtic i Ciberseguretat per a Sistemes Connectats a Internet (UPC Barcelonatech)
- Màster en Tècniques de Seguretat Informàtica. Ciberseguretat (Institut de Formació Contínua-IL3 Universitat de Barcelona)
- Màster en Ciberseguretat (Nuclio Digital School)
- Màster en Ciberseguretat (laSalle Universitat Ramon Llull)
- Màster Universitari en Seguretat Informàtica (UNIR La Universidad en Internet)
- Màster en Ciberseguretat (Universitat de Lleida)
- Màster en Ciberseguretat (telecos BCN)
- NEW Màster Universitari en Direcció i Gestió de la Ciberseguretat i Infraestructures Crítiques (laSalle Universitat Ramon Llull)

ENTi

1 GRAU DE NOVA CREACIÓ
S'AFEGEIX ALS 13 MÀSTERS I POSTGRAUS DE CIBERSEGURETAT

37 centres d'estudi ofereixen **47 cursos** de formació professional en ciberseguretat

Font: (ISC)2

Principals prospectives per al 2024

Els grups *hacktivistes* i cibercriminals es posicionaran i participaran activament en els conflictes geopolítics

- Els conflictes entre Rússia i Ucraïna, i també el d'Israel a Gaza han mostrat com diversos grups *hacktivistes* i cibercriminals han adoptat posicionaments ferms.
- La seva motivació geopolítica se centra a minar la confiança de la població i l'estabilitat de l'adversari mitjançant la desinformació a partir de notícies falses i els atacs cibernètics dirigits als serveis essencials.

La IA esdevindrà un element clau en una nova generació d'atacs cibernètics, però també per protegir-se

- Amb l'avenç de la IA, les capacitats dels cibercriminals per perpetrar atacs de suplantació es veuran ampliades: generaran correus *phishing* adaptats i, fins i tot, simularan veus o imatges per extreure diners o induir a creure situacions falses. Això demanarà una resposta més automatitzada per abordar la seguretat informàtica.
- La UE ha elaborat una regulació d'aquest ús de la IA, per garantir que es fa servir de manera ètica i segura.

Les tecnologies de *zero trust* i la innovació per fer front als nous reptes en ciberseguretat

- Els canvis recents, com el teletreball i els serveis al núvol, impulsen la solució de seguretat *zero trust*.
- Es preveu un augment de les empreses que migren les seves aplicacions al núvol.
- S'espera un auge de tecnologies com les arquitectures de seguretat SASE i els *digital twins* per avaluar riscos de ciberseguretat.
- També s'estan desenvolupant solucions criptogràfiques per resistir la computació quàntica.

Les noves legislacions de la UE activen els sectors públic i privat per garantir un procés digitalitzador segur amb marca pròpia

- Durant els pròxims anys, s'esperen diverses regulacions en l'àmbit de la ciberseguretat, incloent-hi la Directiva NIS 2 i el Reglament DORA per al sector financer.
- Així mateix, els serveis criptogràfics han de complir amb MiCA (*Markets in Crypto Assets*), mentre que tant el sector públic com el sector privat han de seguir l'ENS (Esquema Nacional de Seguretat), entre altres regulacions.

Font: diverses fonts

La ciberseguretat i els ODS (I)

- Els **Objectius de Desenvolupament Sostenible (ODS)** són el pla mestre per a aconseguir un futur sostenible per a tothom. S'interrelacionen entre si i incorporen els desafiaments globals als quals ens enfrontem dia a dia, com la pobresa, la desigualtat, el clima, la degradació ambiental, la prosperitat, la pau i la justícia.

- Els ODS s'integren dins l'Agenda 2030 de Desenvolupament Sostenible de les Nacions Unides, la finalitat de la qual és millorar la qualitat de vida i el benestar social de tots els habitants del planeta, per tal de garantir el progrés i el desenvolupament econòmic de manera sostenible i respectuosa amb el medi ambient.

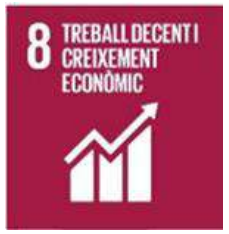
Font: Nacions Unides

La ciberseguretat i els ODS (II)

La creixent digitalització del sector de la salut aporta molts beneficis, però també exposa les dades mèdiques dels pacients a nous riscos i fa que els hospitals i altres proveïdors de serveis siguin vulnerables a atacs de *ransomware* i a altres intents de robatori i de manipulació de dades.

Les TIC ofereixen una millor distribució i escalabilitat dels productes educatius. Tanmateix, aquests productes i sistemes han de ser de confiança i segurs per protegir la privacitat dels estudiants. A més, les bones pràctiques a l'hora d'utilitzar ordinadors i tecnologies digitals són habilitats cada cop més importants.

És clau promocionar la presència de la dona al món de la ciberseguretat, tant en l'àmbit tècnic com en el de la gestió, mitjançant programes que en despertin la vocació, impulsin i incentivin l'emprenedoria en el sector i augmentin la protecció dels drets de les dones en aquesta indústria.



Cal desenvolupar processos, protocols i estàndards per construir un sistema econòmic global més segur i fiable. Això contribueix a desenvolupar un ecosistema empresarial on tots els elements de la cadena (socis, proveïdors i clients) puguin confiar entre ells i en les tecnologies de comerç en línia, inclosos els sistemes de pagament mòbil.

L'augment de l'accés a les TIC i a les noves tecnologies connectades sense gestionar els riscos de seguretat de les tecnologies pot fer-les perjudicials i dificultar-ne una adopció correcta. És necessari proveir ciberseguretat en el desenvolupament de noves tecnologies per a la indústria 4.0 i el desplegament de la internet de les coses (IoT).

El desenvolupament de conceptes com les *smart cities*, la sostenibilitat urbana, la gestió intel·ligent de les xarxes elèctriques o la revolució en la mobilitat només serà possible per complet si es té en compte la ciberseguretat per protegir els sistemes i la informació de la ciutadania.

Reforçar la ciberseguretat és millorar el funcionament de la societat, protegir la privacitat de la ciutadania, reduir el frau i minimitzar els riscos ambientals derivats dels ciberatacs dirigits contra infraestructures crítiques.

La ciberseguretat pren rellevància a l'hora d'evitar usos il·lícits dels sistemes informàtics (atacs DDoS, botnets, criptomineria furtiva, *spam*, etc.) que suposin un malbaratament energètic. Cal garantir l'eficiència i assegurar que cada dispositiu s'utilitzi per a la seva finalitat pertinent.

5. La intel·ligència artificial i la ciberseguretat

La intel·ligencia artificial (IA) i els seus usos empresarials

La IA és la capacitat d'una màquina per mostrar **capacitats semblants a la intel·ligència humana**, com ara el raonament, l'aprenentatge, la planificació i la creativitat

Exemples d'usos de la IA en el món empresarial:

- Anàlisi de grans volums de dades no estructurades
- Anàlisi de *big data* per extreure indicadors a temps real
- Automatització o assistència en la creació de documents
- Identificació de problemes operacionals
- Assistent en servei d'atenció al client
- Millora en el disseny de productes
- Resum de reunions o documentació
- Escriptura o revisió de codi (programació)
- Detecció de frau
- Màrqueting personalitzat

La IA per ciberatacar (I)

Les aplicacions de la IA generativa a l'abast de tothom han fet disparar l'**ús maliciós de la IA**:

- Escriptura de *malware*
- Escriptura de *phishing* i estafes més convincents
- Elaboració i venda de documentació no original

- Suplantació de veu per simular un segrest
- Suplantació de veu per demanar diners
- Missatges de veu de celebritats per perpetrar fraus

- *Deep fakes* per difondre desinformació
- Imatges generades amb IA per dur a terme *sextorsió*
- Vídeos pornogràfics falsos de famoses i *influencers*

La IA per ciberatacar (II)

Exemples d'aplicacions d'IA generativa maliciosa:

Chatbots maliciosos

Versions malicioses de l'IA generativa capaces de crear missatges fraudulents, codi maliciós o identificar vulnerabilitats per cometre frau.

Identitats falses/sintètiques

Eines que utilitzen l'IA generativa per crear fotografies o vídeos de persones que no existeixen, així com documents d'identitat falsos per usos fraudulents.

IA generativa per crear *deepfakes*

Utilització de la intel·ligència artificial per elaborar imatges, àudios o vídeos falsos però aparentment reals. Usats per cometre fraus o generar desinformació.

La IA per a la ciberseguretat (I)

Ciberassegurar la intel·ligència artificial i utilitzar la intel·ligència artificial per a la ciberseguretat són accions fonamentals per a un futur cibernètic segur

IDENTIFY

Anàlisi de riscos en temps real

Cerca i avaluació de vulnerabilitats

Analítica predictiva

Identificació d'usuaris falsos i continguts fraudulents

PROTECT

Conscienciació i recomanacions

Control d'accés biomètric (espais oberts)

Anti-DDoS

Anti*phishing/spam*

Anti *malware* polimòrfic i metamòrfic

Configuració de xarxes SDN

DETECT

Supervisió dels elements d'una xarxa

Detecció d'anomalies (intrusions / *insiders* / explotació de vulnerabilitats *zero-day)*

Honeypots adaptatius

Reducció de falsos positius

RESPOND

Automatització de les operacions de seguretat: *ransomware*, DDoS, cucs, etc.

Suport a la presa de decisions

Orquestració de xarxes SDN

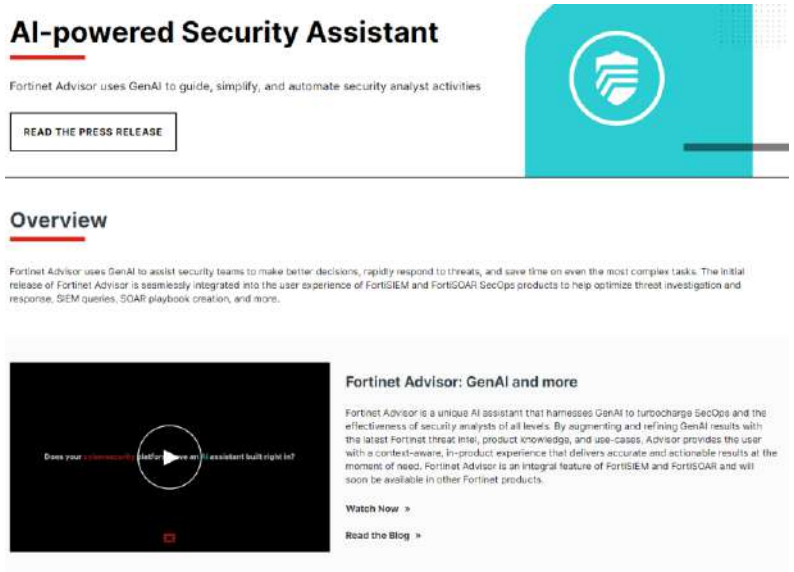
Anàlisi forense i recerca retrospectiva d'anomalies

RECOVER

La IA per a la ciberseguretat (II)

Exemples d'aplicacions de la IA per prevenir ciberatacs:

Eines de ciberseguretat amb assistent d'IA



S'incorpora la intel·ligència artificial com a capa addicional de seguretat, anant més enllà de la reactivitat tradicional i brindant una protecció proactiva en aprendre de forma contínua i adaptar-se a les tàctiques canviants dels ciberdelinqüents.

Detecció de *deepfakes*

Eines que utilitzen l'IA per detectar *deepfakes*, com AutoverifAI, creada per Telefónica.

La **Llei d'intel·ligència artificial europea** té com a objectiu garantir que els sistemes d'IA desplegats i utilitzats a la UE siguin segurs i respectin els drets fonamentals i els valors de la UE.

- La llei estableix diferents prohibicions o obligacions segons el nivell de risc del sistemes d'IA: **risc limitat** (amb obligacions de transparència i informar al consumidor); **alt risc** (que han de complir requisits estrictes de seguretat i tècnics per accedir al mercat), i prohibits o **risc inacceptable** (que no estan permeses, com per exemple la manipulació cognitiva-conductual).

- Aprovada el març del 2024, es preveu que entri en vigor el 2025.

Categorització i exemples d'obligacions dels proveïdors segons el nivell de risc dels sistemes d'IA

Limitat	Alt Risc	Inacceptable
Obligació de transparència	Acreditació de seguretat de la IA	Manipulació cognitiva-conductual
Reconeixement autoria IA	Garantia tècnica i drets fonamentals	Puntuació social i policia predictiva
Informació a l'usuari	Responsabilitats reforçades proveïdors	Reconeixement d'emocions i biometria

Font: Council of the European Union

6. Iniciatives en ciberseguretat

Ciberseguretat a la Unió Europea

La Unió Europea desplega les seves capacitats en ciberseguretat des de diversos enfocaments:

Estratègia Europea de Ciberseguretat

Presentada el 2020, descriu com la UE pot reforçar totes les eines i tots els recursos per ser tecnològicament sobirana i estratègicament autònoma.

Legislació i certificació

- RGPD
- Llei de ciberseguretat
- Reglament DORA NEW
- ENS (Estat espanyol) NEW
- Directiva NIS 2 NEW
- Reglament MiCA NEW
- Reglament de ciberresiliència (en curs)
- Reglament de cibersolidaritat (en curs)

Inversió

- Next Generation EU
- Horizon EU
- Programa Europa Digital
- InvestEU

Orientació de polítiques

- Pla de resposta coordinada als ciberatacs principals
- Unitat Cibernètica Conjunta
- Desplegament segur de 5G a la UE
- Assegurament del procés electoral

Comunitat cibernètica

- ENISA (Agència de la UE per a la Ciberseguretat)
- ISAC (Centres d'Intercanvi d'Informació i Anàlisi)
- JRC (Centre Comú de Recerca)
- CSIRT/CERT (equips de resposta a incidents de seguretat informàtica)
- ECSO (Organització Europea de Ciberseguretat)
- Women4Cyber

Altres àmbits de política cibernètica

- Ciberdelinqüència
- Ciberdiplomàcia
- Defensa
- Desenvolupament de capacitats cibernètiques en països tercers

Font: Comissió Europea

Nova normativa europea en ciberseguretat (I)

Directiva NIS 2 (sobre xarxes i sistemes d'informació)

La Directiva NIS 2 és una norma de la Unió Europea amb l'objectiu de **proporcionar un major nivell comú de ciberseguretat**, tenint en compte la importància dels sistemes de xarxes i informació per l'economia i la societat.

- Gestió de riscos
- Gestió d'incidents
- Seguretat de la cadena de subministrament

Aquesta norma afecta entitats mitjanes i grans de sectors crítics per l'economia i la societat incloent proveïdors de serveis públics de comunicacions electròniques, serveis digitals, gestió d'aigües residuals i residus, fabricació de productes crítics, serveis postals i de missatgeria, així com les administracions públiques, entitats de subministrament públiques de comunitats autònomes i també entitats de l'administració publica en l'àmbit local.

Els estats membre han de transposar la norma al dret intern abans d'octubre de 2024

Reglament DORA (Resiliència Operativa Digital)

El Reglament DORA és una norma de la Unió Europea per **regular** la forma en què les entitats financeres **gestionen el risc digital en les finances**. La norma impacta en els següents aspectes:

- Gestió de riscos
- Notificació d'incidents
- Proves de resiliència en l'operativa digital
- Intercanvi d'informació entre entitats financeres
- Monitorització continua del funcionament dels sistemes i eines

Aquesta norma afecta a les següents empreses (entre altres):

- Entitats de crèdit
- Entitats de pagament
- Proveïdors de serveis d'informació sobre comptes
- Entitats de diners electrònics
- Empreses de serveis d'inversió
- Proveïdors de serveis criptogràfics

El reglament serà plenament aplicable a partir del 17 de gener de 2025

Nova normativa europea en ciberseguretat (II)

Esquema Nacional de Seguretat

L'ENS és una norma de l'estat espanyol que té l'**objectiu** de:

- Crear les condicions necessàries de seguretat en l'ús de mitjans electrònics
- Promoure la gestió continuada de la seguretat
- Promoure la prevenció, detecció i correcció
- Promoure un tractament homogeni de la seguretat
- Servir de model de bones pràctiques

Aquesta norma afecta a tot el sector públic (segons l'article 2 de la llei 40/2025), així com als sistemes que manipulen informació classificada (sense perjudici de la llei 9/1968 de Secrets Oficials). També s'aplica als sistemes d'informació de les entitats del sector privat que ofereixen serveis o solucions a les entitats del sector públic.

L'esquema Nacional de Seguretat es regula pel Reial Decret 311/2022, del 3 de maig i els sistemes afectats han d'adequar-se 24 mesos després de l'entrada en vigor de la norma, per tant el 3 de maig de 2024

Reglament MiCA (Markets in Crypto Assets)

El Reglament MiCA és una normativa europea que regularà l'emissió i prestació de serveis relacionats amb criptoactius i *stable coins*, tot i que en deixa fora les DeFi (Descentralized Finance) i els NFT (Non Fungible Tokens).

- Construcció d'un marc legal sòlid, estableix normatives pels diferents actors del sector
- Determina requisits d'informació per a protegir consumidors i inversors
- Té per objectiu generar un ambient de confiança i promoure una competència lleial entre competidors

És la primera i única del tipus al món i, com en el cas de l'RGPD, marca el camí per a la resta de jurisdiccions.

Serà d'aplicació entre mitjans del 2024 i principis del 2025

Nova normativa europea en ciberseguretat (III)

Reglament de Ciberresiliència

El Reglament de ciberresiliència és una norma de la Unió Europea amb l'objectiu de **protegir als consumidors** i a les **empreses** que **comprin o utilitzin productes** amb un component digital.

El Reglament garanteix:

- Normes harmonitzades al comercialitzar productes o programes informàtics amb un component digital.
- Un marc de requisits de ciberseguretat que regeixin la planificació, el disseny, el desenvolupament i el manteniment dels productes, amb obligacions que s'han de complir en totes les fases de la cadena de valor.
- Obligació de vetllar per tot el cicle de vida dels productes.

Aquesta norma afecta als fabricants i minoristes de tots els productes connectats directament o indirectament a un altre dispositiu o xarxa, amb alguna excepció.

En fase d'aprovació. Els fabricants hauran d'aplicar les normes 36 mesos després de l'entrada en vigor

Reglament de Cibersolidaritat

Té per objecte reforçar les capacitats a la UE per **detectar**, **preparar-se i respondre** a amenaces i atacs de ciberseguretat significatius i a gran escala.

La proposta inclou:

- La creació d'un escut europeu de ciberseguretat, composat per centres d'operacions de seguretat interconnectats a tota la UE
- Mecanisme d'emergència de ciberseguretat global
- Un mecanisme de revisió d'incidents de ciberseguretat per avaluar i revisar incidents cibernètics específics
- L'Agència de ciberseguretat de la UE (ENISA) serà responsable de revisar incidents significatius o de gran escala i presentarà un informe amb les lliçons apreses i, si s'escau, recomanacions

En fase d'aprovació

Ciberseguretat a Espanya

Espanya ha posat el focus en la ciberseguretat amb diversos instruments i diverses inversions

Pla Nacional de Ciberseguretat

Dotat amb 1.000 M€, preveu prop de 150 iniciatives per al període 2022-2025, entre les quals destaca l'impuls per a la ciberseguretat de pimes, micropimes i autònoms.

ECTI 2021-2027

De les 23 línies estratègiques de l'Estratègia Espanyola de Ciència, Tecnologia i Innovació (EECTI) 2021-2027, destaca la línia específica per a la ciberseguretat.

España Digital 2026

Un dels 12 eixos cobreix la ciberseguretat, amb l'objectiu d'impulsar l'ecosistema empresarial del sector o posicionar Espanya com a node internacional de l'àmbit.

PRTR - Next Generation EU

El Component 15 (connectivitat digital, impuls de la ciberseguretat i desplegament del 5G) preveu una inversió estimada de 3.999 M€.

INCIBE

L'Institut Nacional de Ciberseguretat (INCIBE) és l'entitat pública de referència per al desenvolupament de la ciberseguretat en l'àmbit estatal.

KIT Digital

És un instrument que subvenciona la implantació a les empreses de solucions digitals, com per exemple la ciberseguretat, per aconseguir un avenç significatiu en el nivell de maduresa digital.

Component 15 - Inversió 7: Ciberseguretat

Inclou 27 actuacions diferents englobades en tres eixos amb un pressupost total de **524 M€**:

- Reforç de les capacitats en ciberseguretat de ciutadans, pimes i professionals. Inclou el reforç a la Línia telefònica d'Ajuda en Ciberseguretat, que incrementarà la capacitat fins a les 20.000 trucades al mes.
- L'impuls a l'ecosistema del sector de la ciberseguretat:
  - Programa INCIBE Emprende (**200 M€**): Per al desenvolupament i creixement d'empreses del sector.
  - Línia d'ajuts a l'R+D+I en ciberseguretat (**140 M€**)
  - Desenvolupament del talent: Programes autonòmics d'acceleració d'startups amb projecte ciber, creació d'un Centre Demostrador com a base de proves i creació de nous serveis en ciberseguretat, i creació d'un **Segell INCIBE-Acelera**
- Internacionalització: Participació a la xarxa de centres mirall o en projectes amb finançament europeu per al desenvolupament de capacitats comunes a nivell europeu.

Font: Plan de Recuperación y Resiliencia

El Pla NextGen EU: programa RETECH

El Ministeri d'Afers Econòmics i Transformació Digital llança la invitació pública a les comunitats autònomes per participar el programa **RETECH: Xarxes territorials d'especialització tecnològica**.

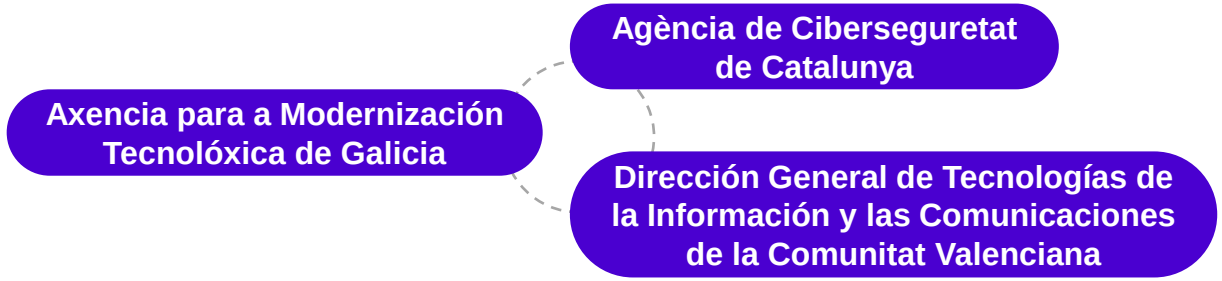
Mobilitza una inversió de **20.000 M€** per a la transformació digital del país (1a fase).

Aporta el **75%** del pressupost de cada iniciativa i les comunitats autònomes participants el 25% restant del pressupost del projecte.

Esperit col·laboratiu: promou la implicació de diferents agents del sector privat i públic.

Es valora positivament la mobilització d'inversió per part del **sector privat**.

L'**Agència de Ciberseguretat de Catalunya** ha liderat la proposta catalana en matèria de ciberseguretat de la iniciativa RETECH CIBERSEGURETAT.



L'objectiu de la proposta és impulsar xarxes de col·laboració públic-privada en les quals participin empreses i associacions empresarials, i entitats sense ànim de lucre per a enfortir les seves capacitats en matèria de ciberseguretat, enfortint la indústries amb impacte en **sectors com a ciències de la salut, transport, indústria i excel·lència operativa en ciberseguretat**.

Al desembre del 2023 es va signar el conveni d'adjudicació a Catalunya dels Fons, juntament amb 10 propostes més de tot l'Estat.

Font: Plan de Recuperación y Resiliencia

7. La ciberseguretat a Catalunya

L'ECSO i la metodologia utilitzada per al mapatge (I)

L'ECSO (European Cybersecurity Organization) defineix el **Market RADAR**, una eina visual per representar els proveïdors de productes, consultoria i serveis de ciberseguretat ubicats a Europa, segons 5 àmbits de capacitat principals. El mapatge de l'ecosistema empresarial català s'ha elaborat d'acord amb aquesta taxonomia.

IDENTIFY / IDENTIFICAR

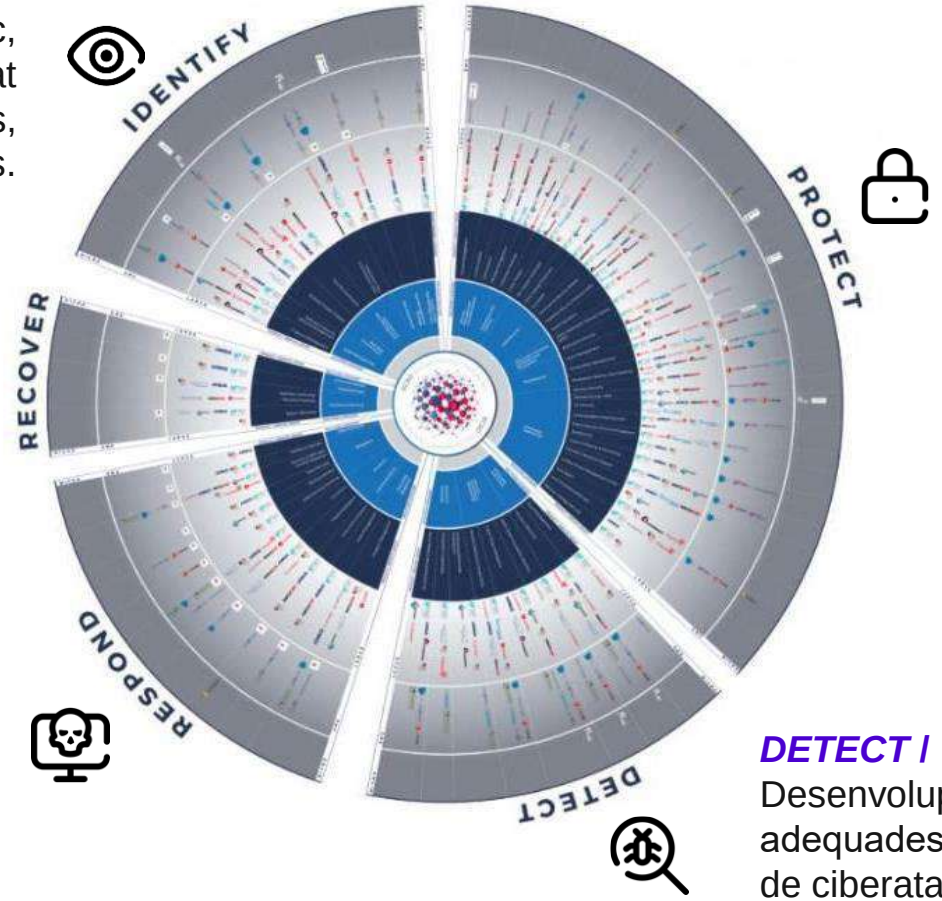
Desenvolupar, a nivell organitzatiu i estratègic, la infraestructura informàtica de ciberseguretat per gestionar els ciberriscos en sistemes, persones, actius, dades i capacitats.

RECOVER / RECUPERAR

Desenvolupar i implementar activitats adequades per mantenir els plans, els processos i els recursos per a la resiliència dels sistemes informàtics i per restaurar les capacitats o els serveis afectats a causa d'incidents cibernètics.

RESPOND / RESPONDRE

Desenvolupar i implementar mesures per actuar adequadament en els incidents de ciberseguretat detectats.



PROTECT / PROTEGIR

Desenvolupar i implementar les solucions per reduir la superfície d'atac a sistemes informàtics i garantir-ne la confidencialitat, integritat, disponibilitat i auditabilitat, així com el rendiment dels serveis informàtics essencials.

DETECT / DETECTAR

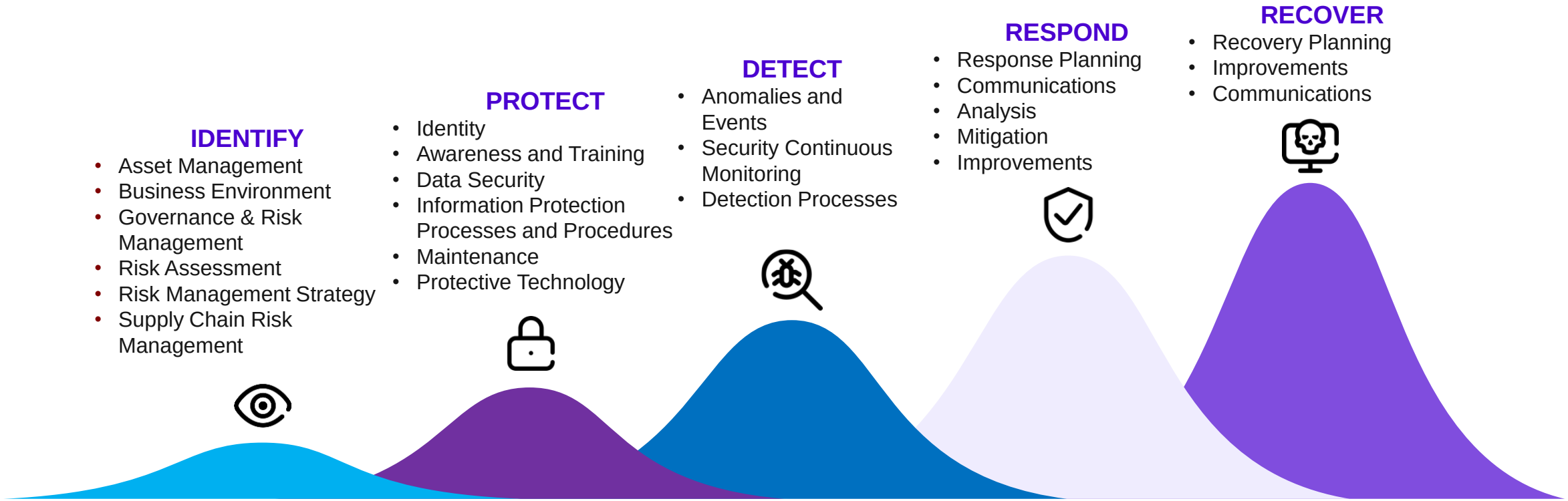
Desenvolupar i aplicar les mesures adequades per identificar l'aparició de ciberatacs.

Font: ECSO

Generalitat de Catalunya

L'ECSO i la metodologia utilitzada per al mapatge (II)

El RADAR representa la situació del sector de la ciberseguretat basant-se en una taxonomia única i la mida de les empreses d'acord amb la definició de la UE



Per a cadascuna de les 5 «capacitats» principals definides, el RADAR estableix diferents «categories de solució» i, per a cadascuna d'elles, classifica les empreses per «grups de producte/servei».

Font: ECSO

Mapatge de l'ecosistema de ciberseguretat a Catalunya

516 empreses
+4,2%*

1.243,9 milions d'euros
+16,1%*

9.458 llocs de treball
+0,5%*

El **85,3%** són pimes.

El **26,9%** tenen menys de 10 anys.

El **16,7%** són startups.

El **54,5%** facturen **més d'1 milió d'euros** i el **24,2%, més de 10 milions d'euros**.

El **27,5%** són exportadores.

Per segments**, el **89,9%** de les empreses es dediquen a la protecció; el **58,7%,** a la identificació; el **39,0%,** a la detecció; el **34,3%,** a la resposta, i el **20,7%,** a la recuperació.

Font: ACCIÓ (dades d'empreses de 2023; facturació i nombre de treballadors de 2022)

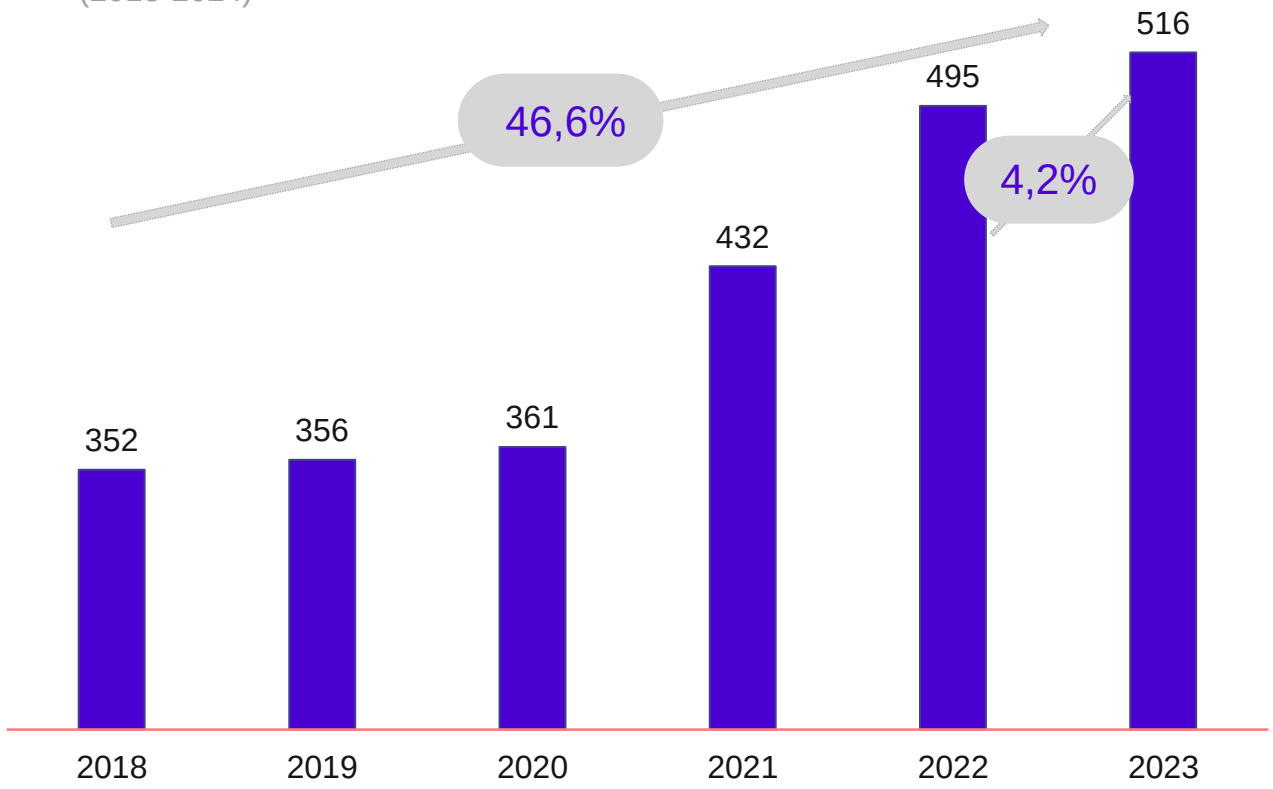
** Respecte de les dades del mapatge fet el 2023.*

***Les empreses es poden classificar en més d'un segment dins de la taxonomia de la ciberseguretat.*

Evolució de l'ecosistema de la ciberseguretat a Catalunya (I)

Des del 2018, el nombre d'empreses que ofereixen serveis de ciberseguretat a Catalunya ha crescut un 46,6%.

Evolució del nombre d'empreses de ciberseguretat a Catalunya
(2018-2024)

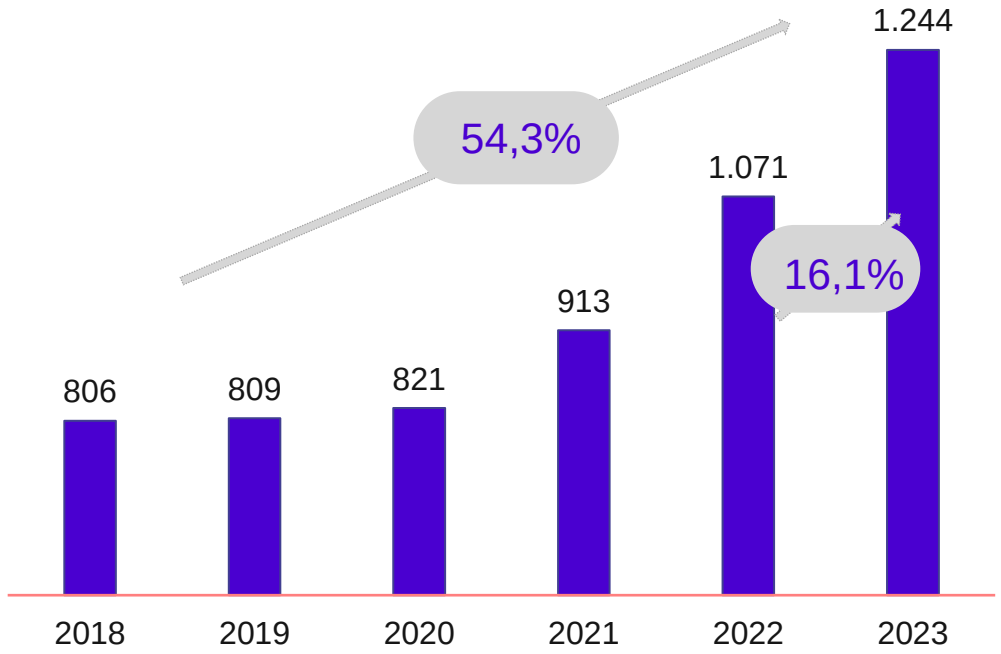


Font: ACCIÓ

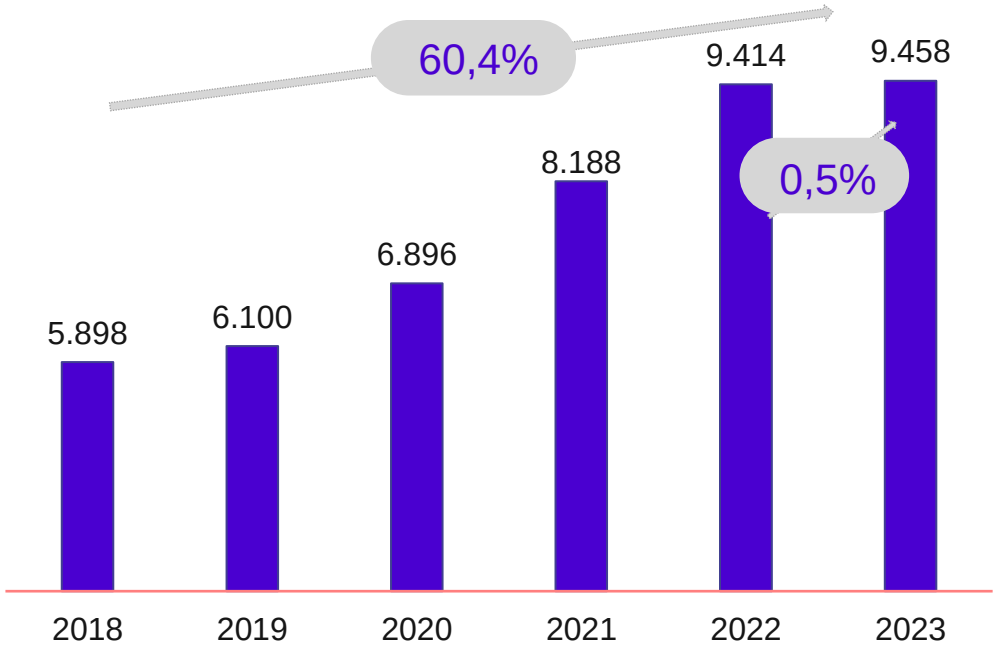
Evolució de l'ecosistema de la ciberseguretat a Catalunya (II)

La facturació de les empreses de ciberseguretat ha augmentat un **54,3%** en el període 2018-2024, mentre que el nombre de treballadors ha crescut un **60,4%**.

Evolució de la facturació de les empreses de ciberseguretat a Catalunya (2018-2024)



Evolució del nombre de treballadors de les empreses de ciberseguretat a Catalunya (2018-2022)



Nota: la facturació i el nombre de treballadors fan referència a l'any anterior

Font: ACCIÓ

Empreses de l'ecosistema de la ciberseguretat a Catalunya: mapatge complet

Empreses de l'ecosistema de la ciberseguretat a Catalunya: segment identificar

Identificar

Generalitat de Catalunya

Empreses de l'ecosistema de la ciberseguretat a Catalunya: segment protegir

Protegir

Generalitat de Catalunya

Empreses de l'ecosistema de la ciberseguretat a Catalunya: segment detectar

Detectar

Empreses de l'ecosistema de la ciberseguretat a Catalunya: segment respondre

Respondre

Empreses de l'ecosistema de la ciberseguretat a Catalunya: segment recuperar

Recuperar

Generalitat de Catalunya

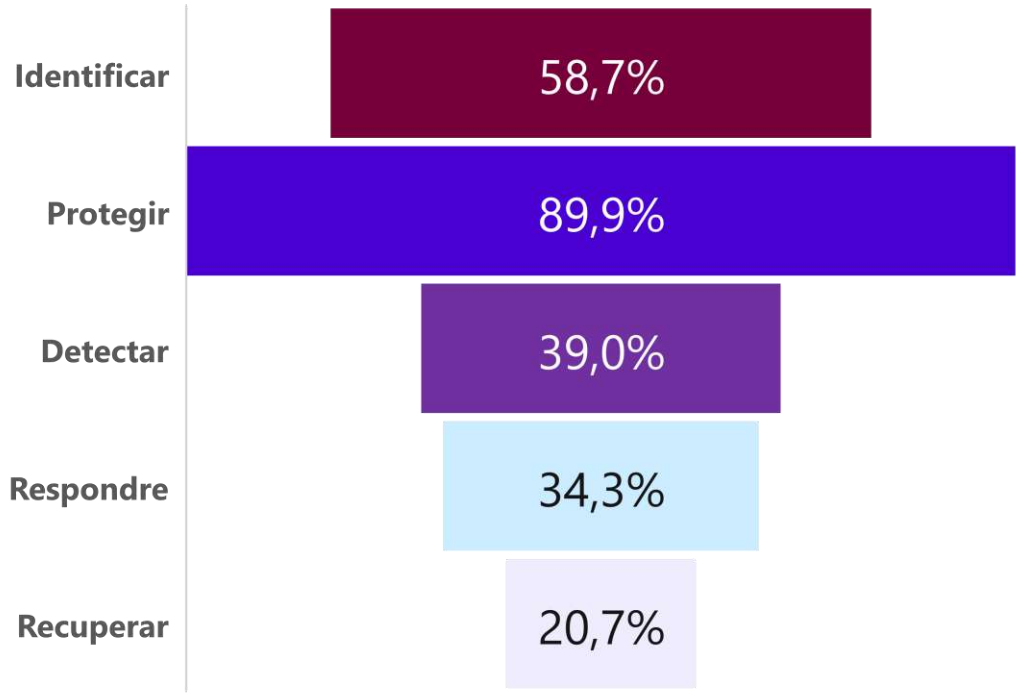
Capacitats i solucions de l'ecosistema empresarial català

Les empreses de ciberseguretat amb presència a Catalunya estan principalment especialitzades en la capacitat de "Protegir".

TOP 10
Categories de solució

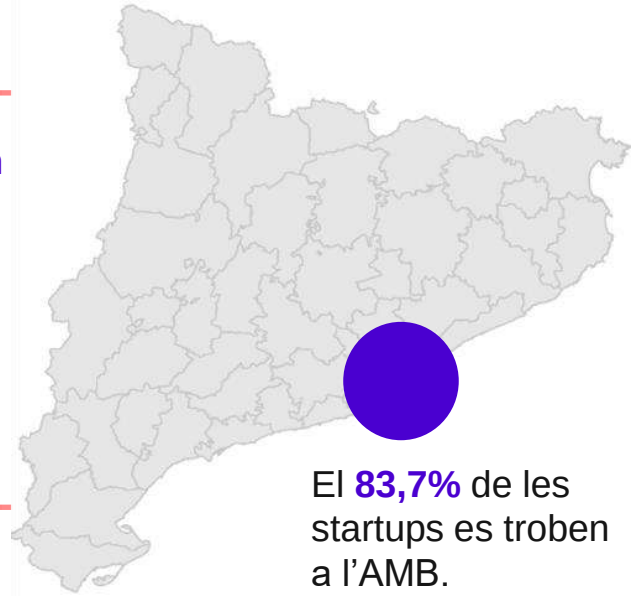
1. Backup / Storage Security (Protegir)
2. IT Service Management (Identificar)
3. Anti Virus / Worm / Malware (Protegir)
4. Firewalls / NextGen Firewalls (Protegir)
5. IoT Security (Protegir)
6. Risk management strategy development & consulting (Identificar)
7. Access Management (Protegir)
8. Authentication (Protegir)
9. Identity Management (Protegir)
10. Risk Management solutions & services (Identificar)

Distribució de les capacitats



Anàlisi de l'ecosistema de la ciberseguretat a Catalunya: ubicació de les empreses

Un **83,7% de les empreses es troben a l'Àrea Metropolitana de Barcelona** (AMB). La comarca que concentra més empreses dedicades a la ciberseguretat és el Barcelonès (63,2%), seguida pel Vallès Occidental (12,0%) i el Baix Llobregat (6,6%).



El **83,7%** de les startups es troben a l'AMB.

Comarca	Núm. d'empreses en ciberseguretat	% d'empreses en ciberseguretat
Barcelonès	326	63,2%
Vallès Occidental	62	12,0%
Baix Llobregat	34	6,6%
Segrià	14	2,7%
Vallès Oriental	13	2,5%
Gironès	12	2,3%
Maresme	10	1,9%
Osona	6	1,2%
Garraf	5	1,0%
Anoia	4	0,8%
Tarragonès	4	0,8%
Alt Penedès	4	0,8%
Baix Camp	3	0,6%
Baix Empordà	3	0,6%
Garrotxa	3	0,6%
Resta	13	2,5%
Total	**516**	**100,0%**

Nota: l'Àrea Metropolitana de Barcelona inclou 36 municipis de les comarques del Barcelonès, el Baix Llobregat, el Vallès Occidental i el Maresme

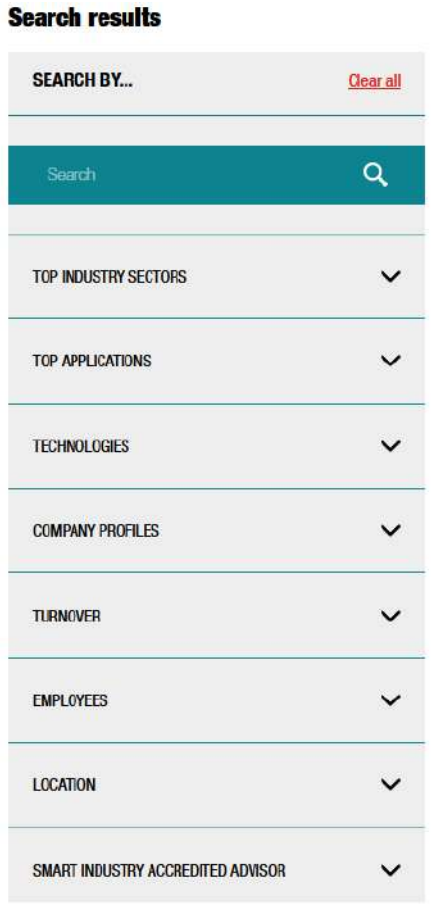
Catalonia Industry Suppliers

Les empreses catalanes de ciberseguretat es troben al **Catalonia Industry Suppliers**, una plataforma en línia per a promoure la indústria i les capacitats tecnològiques catalanes a escala internacional.

Catalonia Industry Suppliers

suppliers.catalonia.com

- Posa a l'abast de les empreses informació sobre productes i d'empreses industrials i tecnològiques, i genera oportunitats de negoci, ja que permet que fabricants, distribuïdors, importadors, i inversors internacionals trobin proveïdors i socis a Catalunya.
- Permet fer cerques en línia de proveïdors industrials, tecnològics i de serveis a la indústria que tinguin activitat productiva a Catalunya i tinguin orientació internacional. Ofereix la possibilitat de fer cerques per sector, per productes, per aplicacions i per tecnologies.



Accés directe a les empreses de ciberseguretat a Catalunya

Generalitat de Catalunya

Agents de l'ecosistema de la ciberseguretat

Centres tecnològics i instituts de recerca

Estudis de grau, màster i postgrau

Estudis d'FP

Associacions i esdeveniments

CSIRT/CERT

Institucions i Administració pública

Generalitat de Catalunya

Centres tecnològics i instituts de recerca que treballen en l'àmbit de la ciberseguretat (I)

El **Centre Tecnològic de Telecomunicacions de Catalunya (CTTC)** és un centre públic d'R+D+i creat per la Generalitat de Catalunya a Castelldefels (BCN).

La recerca, innovació i transferència tecnològica que fa el CTTC es basa en tecnologies dels nivells físic, d'enllaç i xarxa de sistemes de comunicacions, en els serveis i la infraestructura de xarxa, i en la geomàtica. Les activitats s'organitzen en quatre divisions: sistemes, xarxes, tecnologies de comunicacions i geomàtica, i compten amb l'assessorament d'un comitè científic extern internacional.

En l'àmbit de la ciberseguretat, algunes de les publicacions que han realitzat han estat Security in Internet of Things, Impact on Security of Enabling SDN in VANETs i Detection of Malicious Users in Cognitive Radio Ad Hoc Networks.

http://www.cttc.es/

La **Fundació i2CAT** és una institució de recerca aplicada en l'àmbit d'Internet, de les tecnologies digitals avançades i de la societat digital. És l'entitat de recerca i innovació de Catalunya que participa en més projectes europeus de TIC, en les línies d'Internet of Things (IoT), 5G, arquitectura de xarxes i gestió i tecnologies immersives i interactives; també incorpora noves àrees, com les d'open big data, intel·ligència artificial i ciberseguretat.

i2CAT disposa d'aliances estratègiques amb la IOT Catalan Alliance, Agència de Ciberseguretat de Catalunya, CTTI i 5GBarcelona, per tal de vertebrar projectes tractors i d'impacte en el teixit industrial i social.

https://i2cat.net/

Eurecat, Centre Tecnològic de Catalunya (membre de TECNIO), aplega l'experiència de més de 600 professionals i dona servei a més de 1000 empreses.

L'R+D aplicat, els serveis tecnològics, la formació d'alta especialització, la consultoria tecnològica i els esdeveniments professionals són alguns dels serveis que Eurecat ofereix tant per a grans com per a petites i mitjanes empreses de tots els sectors.

La Unitat d'IT & OT Security d'Eurecat està formada per un grup d'enginyers i matemàtics de perfil mixt (investigadors i hackers ètics), i com a tal realitzen una doble funció: d'una banda, la investigació i la innovació en assumptes de seguretat informàtica i, de l'altra, l'abordatge dels temes més inquietants de la ciberseguretat.

https://eurecat.org/

Font: elaboració pròpia a partir de les webs del centres tecnològics

Centres tecnològics i instituts de recerca que treballen en l'àmbit de la ciberseguretat (II)

El **Centre Easy** està especialitzat en intel·ligència artificial i *machcrowd*, en tecnologies digitals intel·ligents i en transferir-les a la indústria.

En relació amb les Tecnologies digitals intel·ligents, el centre és expert en monedes virtuals (un tipus de diners no regulat, digital, que normalment és emès i controlat pels seus desenvolupadors, i és utilitzat i acceptat pels membres d'una comunitat virtual específica) i en preservació digital (un esforç formal per a assegurar que la informació digital de valor continuï sent accessible i utilitzable). El Centre Easy connecta aquestes tecnologies amb la indústria.

https://www.centreeasy.com/

La missió de **La Salle R&D** és impulsar l'ús de les TIC i aportar valor afegit i competitivitat a les empreses mitjançant la recerca aplicada i el desenvolupament de noves solucions innovadores i úniques.

La Salle R&D desenvolupa projectes mitjançant subcontractació directa i participa activament en projectes competitius nacionals i internacionals. La Salle R&D ofereix als seus clients una amplia oferta en matèria d'R+D que inclou serveis de consultoria tecnològica i desenvolupament de projectes claus en mà. La seva capacitat els permet oferir un servei integral, des de la creació de la idea i prova de concepte fins al desenvolupament del producte.

https://www.salleurl.edu/

L'Institut de Ciències Fotòniques és un centre d'investigació ubicat en un edifici de 14 000 m^2 al Parc Mediterrani de la Tecnologia de l'Àrea Metropolitana de Barcelona. Actualment acull més de 300 investigadors, inclosos caps de grup, investigadors postdoctorals, estudiants de doctorat, enginyers i personal, organitzats en 27 grups de recerca.

En el camp de la ciberseguretat destaquen les seves spin-offs Luxquanta, criptografia segura quàntica per al món digital; QuSide desenvolupa tecnologies quàntiques per als camps de ciberseguretat i supercomputació.

https://www.icfo.eu/

L'Institut de Recerca en Energia de Catalunya (IREC), creat al 2008, és un centre d'investigació referent a nivell nacional i europeu en recerca i desenvolupament tecnològic (R+D), dins el sector de l'energia. L'IREC compta amb una línia d'investigació dedicada a la ciberseguretat en el sector de l'energia amb, entre d'altres, la participació en projectes finançats per la Unió Europea (H2020: SDN-microSENSE 833955, FP7: PREEMPTIVE 607093).

www.irec.cat

Font: elaboració pròpia a partir de les webs del centres tecnològics

Centres tecnològics i instituts de recerca que treballen en l'àmbit de la ciberseguretat (III)

El **Centre de Visió per Computador** és un centre de recerca sense finalitats de lucre, fundat el 1995 per la Generalitat de Catalunya i la Universitat Autònoma de Barcelona (UAB).

La seva missió és dur a terme una investigació capdavantera en el camp de la visió per computador i aconseguir un gran impacte internacional. També promou la transferència de coneixement a la indústria i a la societat.

El CVC compta amb més de 130 investigadors multidisciplinaris i tècnics de diferents nacionalitats.

http://www.cvc.uab.es/

El **Grup de Seguretat de la Informació (ISG)** centra la seva activitat en el desenvolupament i proposta de serveis de seguretat, i el seu desplegament en xarxes de telecomunicacions. El Grup de Seguretat de la Informació es va crear a la Universitat Politècnica de Catalunya l'any 2002. Des del primer moment, el principal objectiu estratègic del grup ISG va ser ser un grup de seguretat de referència.

El grup lidera les tasques de seguretat i privadesa del projecte H2020 BIG IoT, inclosa la cadena de blocs per millorar la seguretat i la privadesa a l'IoT.

http://futur.upc.edu/ISG

CIT UPC, el Centre Tecnològic de la Universitat Politècnica de Catalunya és una entitat sense ànim de lucre, que posa la capacitat de recerca universitària al servei de la innovació en les empreses a partir del coneixement i els resultats dels centres de recerca i transferència de tecnologia de la UPC.

En l'àmbit de la ciberseguretat treballen en privadesa i protecció de dades, l'anàlisi de consultoria, auditoria i seguretat, cloud i big data, plans de continuïtat de negoci, seguretat d'infraestructures, serveis de confiança i seguretat, i formació.

https://cit.upc.edu/ca/ciberseguretat/

Font: elaboració pròpia a partir de les webs del centres tecnològics

Centres tecnològics i instituts de recerca que treballen en l'àmbit de la ciberseguretat (IV)

El **Centre d'Investigacions en Intel·ligència Artificial (IIIA)** del Consell Superior d'Investigacions Científiques (CSIC). IIIA es va crear el 1994.
Amb experiència en moltes àrees de la intel·ligència artificial, com ara l'aprenentatge automàtic, la representació del coneixement, els sistemes multiagent, les tecnologies d'acord, el processament del llenguatge natural, el raonament, l'optimització i la semàntica.
Lideren més d'un centenar de projectes de recerca sobre aspectes fonamentals de la IA i sobre l'aplicació de resultats teòrics a molts dominis diferents com l'educació, la salut o la fabricació. IIIA també és un actor actiu de l'ecosistema industrial català, participant en un gran nombre de projectes de transferència de tecnologia.

https://www.iiia.csic.es/

El **Grup de Recerca en Criptografia i Gràfics (C&G)** de la Universitat de Lleida constitueix un equip de recerca consolidat amb una trajectòria de més de 15 anys d'activitats científiques. Els membres de l'equip del grup C&G formen part del Departament de Matemàtiques i de l'Institut Politècnic de Recerca i Innovació en Sostenibilitat (InsPIReS).
Els interessos de recerca dels membres del grup C&G es troben entre la teoria i les aplicacions, principalment en les dues àrees següents: Criptografia i Teoria de gràfics.
A l'àrea de criptografia, la nostra recerca se centra en els aspectes computacionals de la criptografia de corbes algebraiques i el disseny de protocols criptogràfics segurs per a la tecnologia RFID, targetes intel·ligents i sistemes de vot electrònic. A l'àrea de la teoria de gràfics, la nostra investigació es refereix a problemes oberts sobre dígrafs densos i excèntrics, problemes extrems i anàlisi de dades de xarxes socials que preserven la privadesa.

http://www.cig.udl.cat/

El **Barcelona Supercomputing Center-Centro Nacional de Supercomputación (BSC-CNS)** és el centre nacional de supercomputació a Espanya. Estem especialitzats en computació d'altes prestacions (HPC) i gestionem el MareNostrum, un dels supercomputadors més potents d'Europa, ubicat a la capella de la Torre Girona.
Amb un equip total de més de 725 experts i professionals en R+D, el BSC-CNS és un centre que aconsegueix atraure talent. La nostra recerca es focalitza en quatre camps: Ciències Computacionals, Ciències de la Vida, Ciències de la Terra i Aplicacions Computacionals en Ciència i Enginyeria.

https://www.bsc.es/ca

Font: elaboració pròpia a partir de les webs del centres tecnològics

Centres tecnològics i instituts de recerca que treballen en l'àmbit de la ciberseguretat (V)

Cryptography and Information Security for Open Networks

La línia de recerca del grup **KISON** se centra en la compatibilitat de la seguretat de les xarxes descentralitzades (xarxes ad hoc i d'igual a igual [P2P]) i la protecció de la propietat intel·lectual dels continguts digitals a internet amb el dret a la privacitat dels usuaris:

- Seguretat i privacitat de les xarxes obertes
- Seguretat i privacitat dels continguts multimèdia

https://www.uoc.edu/portal/ca/in3/recerca/grups/kriptography_and_information

TecnoCampus

El grup de **Processament de Senyals de TecnoCampus** es va crear l'any 1995 a l'Escola Universitària Politècnica de Mataró. Inicialment només es dedicava als senyals de parla (codificació, reconeixement d'altaveus), però durant els darrers anys els temes de recerca també s'han estès al processament d'imatges i comunicacions. Línies de recerca: Biometria per a la salut i la seguretat (cara, geometria mà, signatura en línia, parla, empremta digital), codificació de la parla, Beamforming per a senyals de parla, imatge tèrmica.

https://www.tecnocampus.cat/grups-de-recerca-del-tecnocampus/grup-de-recerca-tractament-del-senyal-i-dades-tsd

Crises secure e-commerce

Crises és un centre de recerca de la Universitat Rovira i Virgili.
L'interès del grup i la seva contribució a l'entorn socioeconòmic se centra en la creació de tecnologies que facin compatibles tres objectius: seguretat per a empreses, governs i persones de la societat de la informació; privadesa de les persones usuàries o subjectes passius de la societat de la informació; utilitat dels sistemes informàtics subjacents.
Les principals línies de recerca són: privacitat de dades i comerç electrònic; privacitat i seguretat en entorns mòbils; recuperació d'informació privada i codis; anonimització de dades.

https://crises-deim.urv.cat/web/

inLab FIB talent & tech

UPC

inLab FIB UPC és el laboratori d'innovació i recerca de la Facultat d'Informàtica de Barcelona de la UPC amb una trajectòria de més de 40 anys de col·laboració amb entitats i empreses. La seva missió és innovar i transferir coneixement a la societat en l'àmbit de les TIC, mitjançant el desenvolupament del talent humà i la realització de projectes R+D+I multidisciplinars, sobretot en temes relacionats amb el *Data Science and Big Data*; la *Smart Mobility*; el *Knowledge and Service Engineering*; la Ciberseguretat; la Modelització, Simulació i Optimització; i els Entorns i Serveis TIC de Suport a l'Aprenentatge.

https://inlab.fib.upc.edu/

Font: elaboració pròpia a partir de les webs del centres tecnològics

Iniciatives per potenciar la ciberseguretat a Catalunya

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

Organisme que governa la ciberseguretat a Catalunya i vetlla per una societat digital segura per al conjunt de la societat catalana i la seva Administració pública.

BARCELONA CYBERSECURITY CONGRESS

Esdeveniment que, durant tres dies, reuneix els actors principals de la ciberseguretat a escala internacional en un espai per a conferències i expositors.

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA
CENTRE DE COMPETÈNCIES I D'INNOVACIÓ EN CIBERSEGURETAT

Centre que té com a objectiu promoure solucions innovadores per millorar la ciberseguretat per mitjà de l'aprofitament dels processos funcionals, les tecnologies, el coneixement i l'experiència als àmbits d'actuació de l'Agència.

DCA Digital Catalonia Alliance

Iniciativa que agrupa sis tecnologies emergents del territori català, entre les quals la ciberseguretat, en una aliança de comunitats tecnològiques innovadora, visionària, disruptiva i col·laborativa.

CYBERSECURITY CAT

Primer centre de recerca de ciberseguretat de Catalunya creat per sis universitats públiques catalanes amb l'ambició de constituir-se com un centre de referència en la recerca en ciberseguretat i privadesa.

DIH4CAT Digital Innovation Hub de Catalunya

Xarxa connectada d'actius, infraestructures i coneixement a Catalunya orientada al testatge i l'experimentació de tecnologies digitals avançades, entre les quals la ciberseguretat.

Agència de Ciberseguretat de Catalunya

L'Agència de Ciberseguretat de Catalunya vetlla per una societat digital segura per al conjunt de la societat catalana i la seva Administració Pública.

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

www.ciberseguretat.cat

- L'Agència de Ciberseguretat de Catalunya és l'encarregada d'executar les polítiques públiques en matèria de ciberseguretat i desenvolupar l'estratègia de ciberseguretat de la Generalitat de Catalunya. És l'organisme que governa la Ciberseguretat a Catalunya.
- L'Agència és l'encarregada d'establir el servei públic de ciberseguretat i treballa per garantir i augmentar el nivell de seguretat de les xarxes i els sistemes d'informació a Catalunya, així com la confiança digital dels ciutadans.
- Com a organisme competent en matèria de ciberseguretat, es responsabilitza de l'establiment i el seguiment dels programes d'actuació en matèria de ciberseguretat, sota la direcció estratègica del Govern de la Generalitat de Catalunya, en coordinació amb les entitats del sector públic de l'Administració de la Generalitat de Catalunya, i col·laborant amb governs locals de Catalunya, sector privat i societat civil.

Funcions i serveis

- Governança de la ciberseguretat
- Resposta a incidents
- Protecció i prevenció
- Conscienciació

Font: Agència de Ciberseguretat de Catalunya

Barcelona Cybersecurity Congress

El Barcelona Cybersecurity Congress, organitzat per Fira de Barcelona i l'Agència de Ciberseguretat de Catalunya, és un esdeveniment que durant tres dies reuneix els principals actors de ciberseguretat a nivell internacional en un espai per a conferències i expositors.

- El 2024, el Congrés celebra la seva cinquena edició sota el lema "Secure today, safeguard tomorrow" i tornarà a posar el focus en la necessitat d'augmentar els nivells de seguretat a tota la indústria per evitar o minimitzar els efectes dels ciberatacs, cada cop més habituals.

- En el marc del Congrés, s'organitza la 3a edició dels *Cyber Investor Days* organitzat per l'Organització Europea de Ciberseguretat (ECSO), on start-ups especialitzades podran presentar els seus projectes davant inversors europeus.

- El Congrés també contarà amb un Hacking Village on experts en hacking ètic posaran en pràctica les seves habilitats i compartiran els seus coneixements.


Conferències


Hacking village


Exposició

BARCELONA CYBERSECURITY CONGRESS

www.barcelonacybersecuritycongress.com

Eixos temàtics de les conferències

- Formació i sensibilització dels empleats
- Intel·ligència i monitorització d'amenaces
- Mesures de seguretat robustes
- Simulacions de gestió de compliment
- Govern de dades i privacitat
- Tecnología reguladora

Font: Barcelona Cybersecurity Congress

Centre de Competències i d'Innovació en Ciberseguretat (CCI)

El centre de competència (CC) identifica, desenvolupa i aprofita els processos funcionals, el coneixement i l'experiència que beneficien als àmbits d'actuació de l'Agència, amb l'objectiu de promoure solucions pràctiques i innovadores (I) per millorar la ciberseguretat.

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

CENTRE DE COMPETÈNCIES I D'INNOVACIÓ EN CIBERSEGURETAT

El CCI neix en el marc de la xarxa de Centres Nacionals de Competència (NCC) europeus per donar suport a la innovació i la política industrial en ciberseguretat.

Entre els seus objectius hi ha:

- Desenvolupar competències funcionals i tecnològiques
- Impulsar la Innovació
- Promoure la transferència tecnològica

De forma més específica, treballa per a:

- La generació de coneixement
- La transferència de coneixement
- Les solucions innovadores
- La capacitació
- La investigació i la recerca

Línies de servei:

Competències per àmbits
Desenvolupar habilitats tècniques
Difondre competències per àmbits
Promoure posicionament estratègic

Innovació
Incrementar innovació
Disposar d'eines innovadores
Generar y mantenir coneixement intern

Ciència i analítica de dades
Analitzar dates
Dissenyar estratègia de dades
Generar intel·ligència global i sectorial

Font: Agència de Ciberseguretat de Catalunya

Generalitat de Catalunya

Digital Catalonia Alliance

La Digital Catalonia Alliance (DCA) és una iniciativa que agrupa els principals sectors tecnològics emergents del territori català en una aliança de comunitats tecnològiques innovadora, visionària, disruptiva i col·laborativa.

DCA Digital Catalonia Alliance

www.dca.cat

La DCA vol esdevenir impulsora dels sectors econòmics digitals de Catalunya i, per aquest motiu, la DCA treballa en les següents línies:

- Agrupar empreses actives de referència en innovació digital per tal de disposar d'un ecosistema dinàmic que contribueixi en l'economia digital.
- Resoldre reptes comuns de les empreses del sector, tant de les empreses petites com de les mitjanes.
- Donar suport a l'adopció dels canvis tecnològics per part de les empreses i la societat.
- Alinear-se amb els Objectius de Desenvolupament Sostenible (ODS) i amb els reptes estratègics del territori.

La DCA està formada per 6 verticals tecnològiques amb **528 membres**:

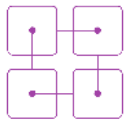

Drons


IoT


IA


Ciberseguretat


NewSpace


Blockchain

La DCA és una iniciativa de:

Generalitat de Catalunya

i2cat

La DCA-Ciberseguretat és una peça clau de l'estratègia de Ciberseguretat de la Generalitat de Catalunya, i està impulsada i esponsoritzada:

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

Font: DCA

Cybercat: centre de recerca de ciberseguretat a Catalunya

Sis universitats catalanes investiguen les tecnologies de seguretat i la privadesa de dades informàtiques a través del CYBERCAT.

www.cybercat.cat

- Sis universitats públiques catalanes han creat el primer centre de recerca de ciberseguretat de Catalunya. Les sis universitats aportaran al Cybercat els grups de recerca que actualment treballen en tecnologies de la seguretat i privacitat de la informació.
- La missió és impulsar la recerca en ciberseguretat i privadesa de la informació a Catalunya i enfortir la seva projecció internacional, així com reforçar i estendre la formació d'alt nivell en aquest àmbit i consolidar les relacions de recerca existents entre les sis universitats que hi participen.
- L'ambició del centre és constituir-se com un centre de referència en l'àmbit nacional i internacional en la recerca en ciberseguretat i privadesa.

Línies de recerca

- Seguretat i privadesa en l'automòbil connectat
- Privadesa en xarxes socials
- Privadesa en grans volums de dades
- Privadesa en el núvol
- Privadesa en ciutats intel·ligents
- Privadesa en xarxes socials
- Privadesa en entorns col·laboratius
- Privadesa en mineria de dades
- Privadesa de la localització
- Automatització de dades
- Seguretat i privadesa en la Internet de les coses

Font: Cybercat

Digital Innovation Hub de Catalunya (DIH4CAT)

Digital Innovation Hub de Catalunya (DIH4CAT) és una xarxa connectada d'actius, infraestructures i coneixement a Catalunya orientada al testeig i experimentació de tecnologies digitals avançades, per accelerar la transformació digital de la indústria catalana.

https://dih4cat.cat

El DIH4CAT es constitueix seguint el model dels *digital innovation hubs* establert per la Comissió Europea i es configura com una comunitat de serveis en xarxa través de la qual la indústria i les administracions públiques poden accedir a un conjunt de serveis, infraestructures, capacitats i solucions tecnològiques i no tecnològiques per impulsar la seva transformació digital i tecnològica; alhora, actua com a connector avançat entre l'oferta i la demanda que existeix en el conjunt de Catalunya.

Connecta 7 àmbits tecnològics estratègics: la Intel·ligència Artificial, la Supercomutació, la **Ciberseguretat**, l'Smart Connectivity, la Fabricació additiva i la impressió 3D, la Robòtica i la manufactura avançada i la Fotònica

Infraestructures digitals i tecnològiques

Marketplace de solucions

Acompanyament en el procés de transformació digital

Serveis

- Consultoria Tecnològica
- Testeig i experimentació / solucions
- Formació transversal i tecnològica
- Serveis preparatoris
- Divulgació i sensibilització
- Diagnosi, reflexió estratègica i definició d'actuacions
- Accés a finançament
- Cerca de socis i ecosistema d'innovació

Font: DIH4CAT

Alineament amb els organismes europeus en ciberseguretat

Catalunya s'alinea amb les estratègies europees d'impuls, capacitació i innovació en l'àmbit de la ciberseguretat.

DIGITAL INNOVATION HUBS
Helping companies and public administrations make the most of digital opportunities

Gestió d'ajuts al finançament i coordinació d'iniciatives

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

CENTRE DE COMPETÈNCIES I D'INNOVACIÓ EN CIBERSEGURETAT

www.ciberseguretat.cat

Impuls del sector de ciberseguretat de Catalunya

DCA Ciberseguretat

www.dca.cat

Suport a la transformació digital cibersegura de la demanda i accés als serveis de ciberseguretat

DIH4CAT Digital Innovation Hub de Catalunya

www.dih4cat.cat

Generalitat de Catalunya

Hubs tecnològics a Catalunya enfocats a la ciberseguretat el 2023

140 *hubs* tecnològics
d'empreses estrangeres

+11% respecte de l'any anterior

5.200 llocs de treball nous

Facturació de **500 M€**

Principals *hubs* a Catalunya enfocats a la ciberseguretat:

Boehringer Ingelheim · Cisco · Deloitte. · Fujitsu · getronics · GFT · IBM · KPMG · Lufthansa · Nestlé · Novartis · Oracle · PepsiCo · Schneider Electric · T-Systems · Zurich

Els Estats Units
(amb el 28% dels *hubs*) és el principal país d'origen de la inversió en aquests centres, seguit d'Alemanya (17%).

El 59% dels *hubs*
prové d'empreses de països europeus.

La ciberseguretat (36%)
és una de les tecnologies d'especialització predominants dels *hubs* del territori català.

Font: Mobile World Capital Barcelona, ACCIÓ, Ajuntament de Barcelona: Tech hubs overview

Generalitat de Catalunya

Catalunya, 3a regió de la UE en captació d'IED en ciberseguretat el 2023

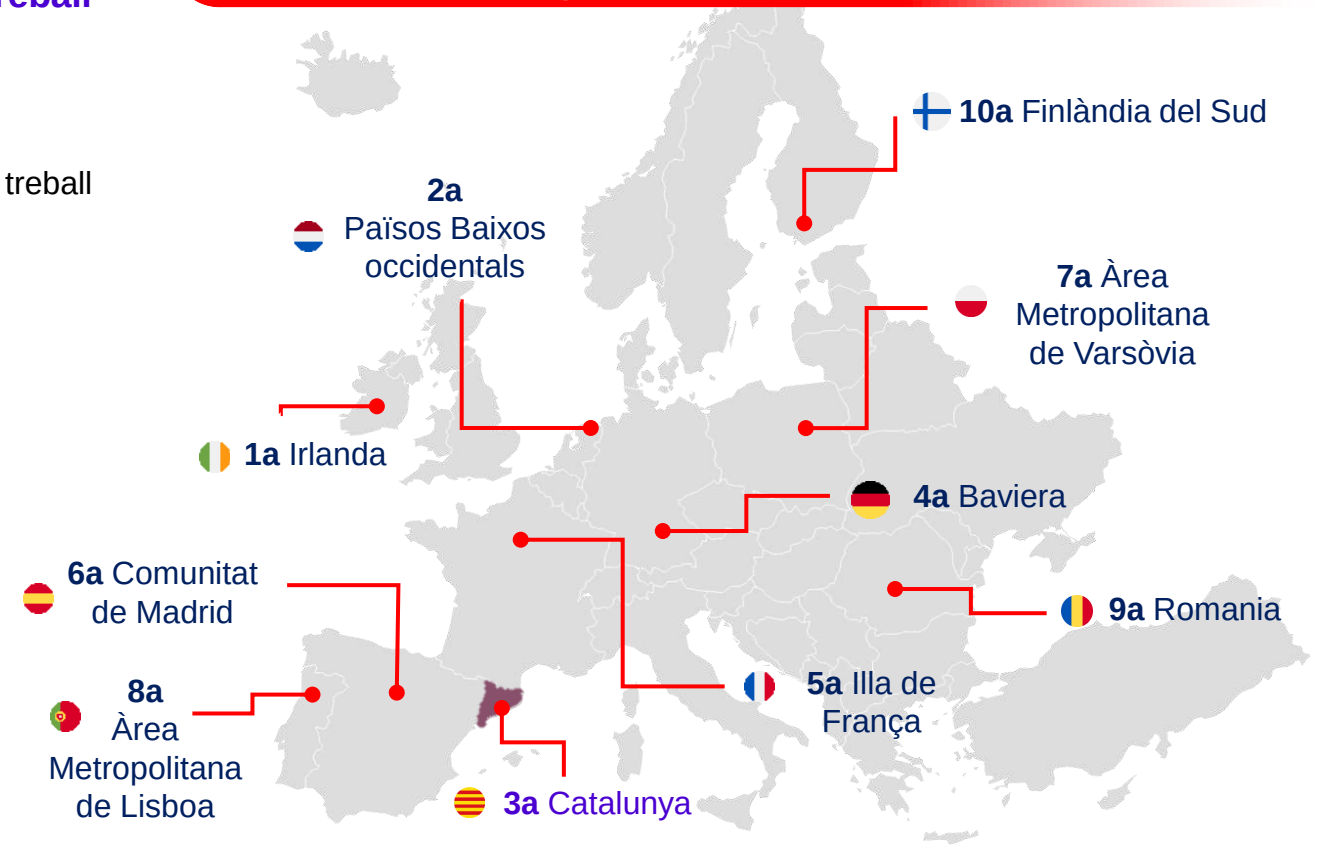
El 2023, Catalunya ha estat la **3a regió de la UE en nombre de projectes estrangers** de ciberseguretat, la **5a en llocs de treball creats** i la **6a en captació d'inversió estrangera**.

- Ha rebut **4 projectes** (4,3% del nombre total de projectes).
- S'han creat **407 llocs de treball** (3,7% del total de llocs de treball creats).
- La inversió ha estat de **66,4 M€** (2,4% del total invertit).

Empreses inversores a Catalunya (2023)

getronics	5,9 M€	127 llocs de treball
Advens – Security for the greater good	0,6 M€	15 llocs de treball
T-Systems	58,1 M€	250 llocs de treball
FUJITSU	1,8 M€	15 llocs de treball

Principals regions de la UE en nombre d'inversions estrangeres de ciberseguretat (2023)



Font: elaboració pròpia a partir d'fDi Markets

Barcelona, 10a ciutat de la UE en valor de rondes de finançament tancades per a startups

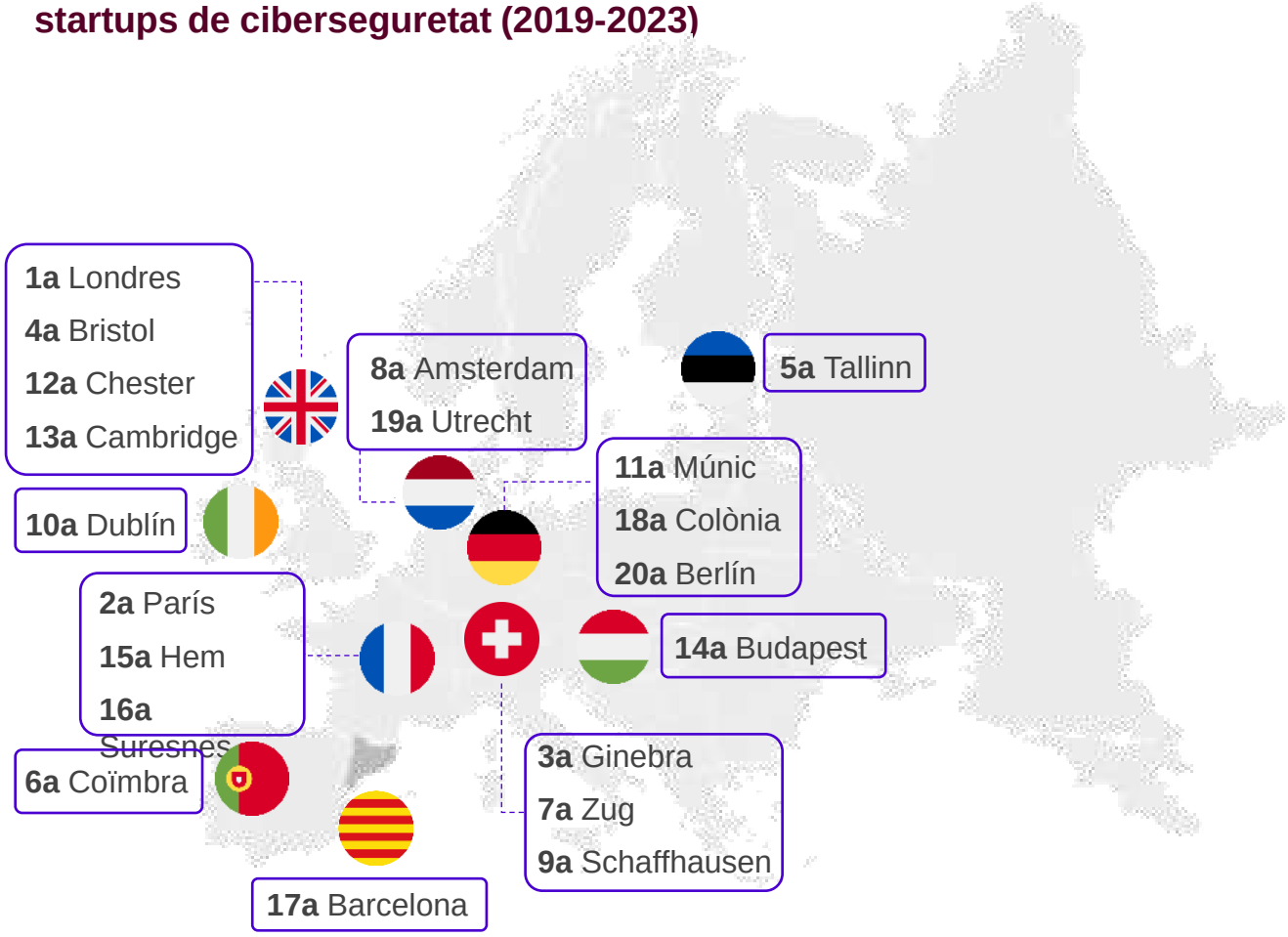
- Barcelona és la **10a ciutat de la UE i la 17a europea** en valor de rondes tancades per a startups de ciberseguretat, amb 85,2 milions de dòlars en 14 rondes (2019-2023).
- L'startup catalana que ha rebut més finançament és **Red Points**, que ha tancat 2 rondes per valor de més de 58 milions de dòlars en els darrers 5 anys.

Startups de Barcelona amb rondes tancades:

RED POINTS · unnax · Signaturit · BlackfishID · numentech · CAMIUM · Bigle Legal · Validated ID

Nota: s'hi inclouen les rondes d'inversió «pre-seed», «seed» i les sèries A-J de les categories següents: «penetration testing», «network security», «intrusion detection», «identity management», «fraud detection», «e-signature», «cyber security» i «cloud security». Les dades fan referència al període 2019-2023.

Top 20 de ciutats europees per valor de rondes d'inversió tancades en startups de ciberseguretat (2019-2023)



Font: elaboració pròpia a partir de Crunchbase

Generalitat de Catalunya

Activitats de recerca catalana en ciberseguretat a l'Horizon Europe

Recerca en ciberseguretat a Catalunya en el marc de l'Horizon Europe

15 projectes

6a regió europea en finançament a l'Horizon Europe

5,5 milions d'euros

3,2% del total europeu
21,3% del total a l'Estat espanyol

Horizon Europe

13 institucions

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH
eurecat Centre Tecnològic de Catalunya
beawre
CVC
i2cat
ttc Centre Tecnològic de Telecomunicacions de Catalunya
FGC Ferrocarrils de la Generalitat de Catalunya
WORLD SENSING
FICOSA
Schneider Electric
Applus IDIADA
IThink UPC
PAL ROBOTICS

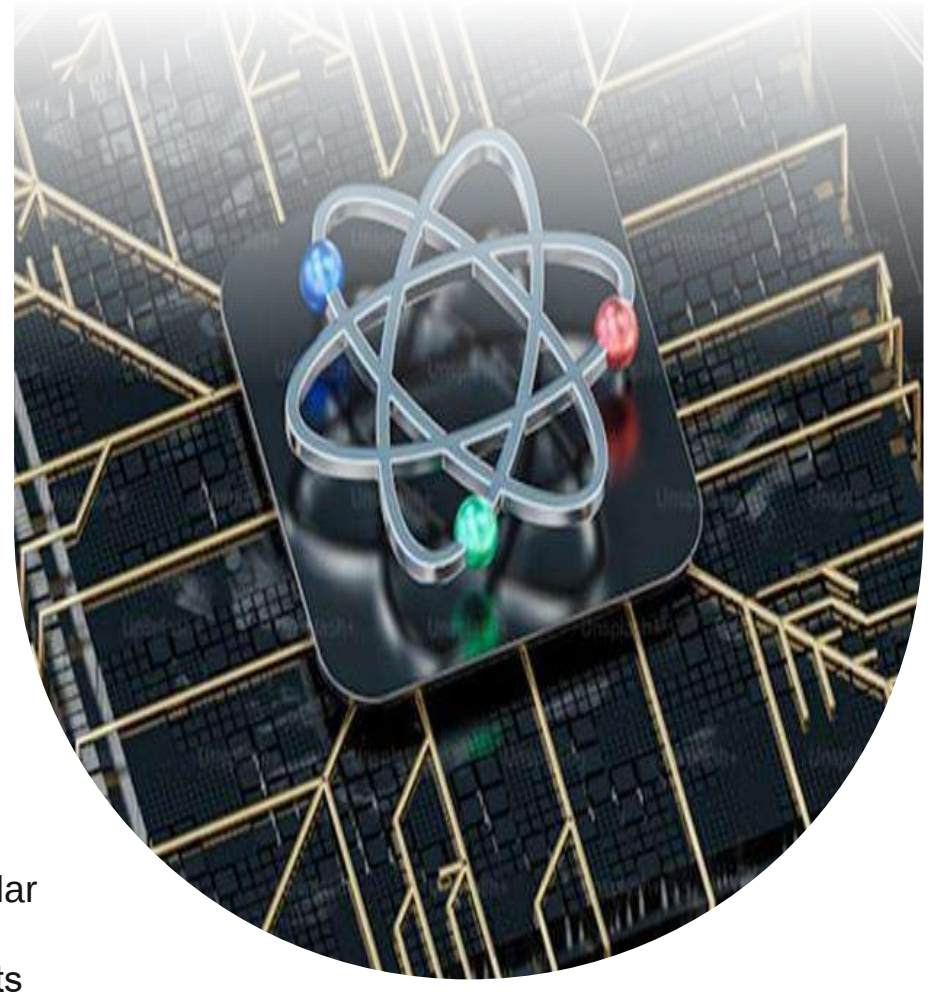
Nota: s'hi inclouen els projectes de l'Horizon Europe (2022-2023) relacionats amb la ciberseguretat (*computer security* i *network security*).

Font: Horizon Europe

Criptografia quàntica en comunicacions crítiques

La Generalitat de Catalunya impulsa la continuïtat del pilot de criptografia quàntica en comunicacions crítiques, liderat per l'ICFO, mitjançant l'anàlisi de la implantació de la criptografia quàntica a les seves xarxes de comunicacions

- El pilot de criptografia quàntica és l'embrió d'una futura xarxa que es connectarà a la internet quàntica estatal i a l'europea, i que es vol convertir en un «anell» que encercli Barcelona amb l'objectiu de transmetre informació crítica de manera *quantum-safe*.
- L'anell físic envoltarà Barcelona i connectarà diverses infraestructures i diversos equipaments de la ciutat. En fases posteriors, es connectarà per via terrestre i per satèl·lit amb altres localitzacions estatals i internacionals.
- Utilitza un sistema de comunicació segura basat la distribució de claus quàntica, un mètode de xifratge per generar una clau «completament segura» davant els avanços en la capacitat de còmput ordinària i quàntica.
- Aquest projecte està alineat amb l'estratègia quàntica Euro-QCI, que és un pilar estratègic de ciberseguretat europeu, i en les iniciatives en què participen activament l'ecosistema català d'empreses, els centres de recerca i les entitats públiques.



Generalitat de Catalunya

EuroQCI, European Quantum Communications Infraestructures

La iniciativa **EuroQCI** té com a objectiu establir una infraestructura de comunicació quàntica segura a tota la UE i els seus territoris d'ultramar.

- Constarà de segments tant terrestres com espacials, i integrarà sistemes quàntics a les infraestructures de comunicació existents.
- La iniciativa reforça la ciberseguretat, perquè protegeix dades confidencials i infraestructures crítiques, com institucions governamentals, centres de dades, hospitals i xarxes energètiques.
- La col·laboració amb els socis de la indústria europea i les pimes és crucial per desenvolupar components EuroQCI basats en les tecnologies europees.
- La implementació inclou finançament per a projectes industrials, xarxes nacionals de comunicació quàntica, accions de coordinació i infraestructures de proves.
- Els enllaços transfronterers entre xarxes nacionals i les interconnexions amb el segment espacial compten amb el suport del mecanisme Connecting Europe.
- Es preveu que la infraestructura de proves i avaluació de tecnologies i serveis basats en QKD estigui disponible a partir de mitjan 2024.
- Les especificacions per a una constel·lació de satèl·lits EuroQCI de primera generació s'estan desenvolupant en col·laboració amb l'ESA, amb l'objectiu de llançar-se a finals de 2025 o principis de 2026.

EuroQCI

L'EuroQCI és un pas cap a la sobirania i la competitivitat digitals europees, i s'alinea amb els objectius de la dècada digital de la UE per al 2030.

EUROQCI SPAIN

El node d'Espanya té com a partners:

POLITÉCNICA · indra · CSIC · tecnobit grupo oesía · Telefónica

Partners catalans en el projecte: ICFO · cellnex

Fonts: European Comission i Digital Strategy

Oportunitats internacionals en ciberseguretat

Canadà

La digitalització de la indústria ha fet créixer la demanda de solucions innovadores de ciberseguretat i intel·ligència artificial.

Bolívia

La indústria i els serveis del país andí demanen solucions tecnològiques per modernitzar l'economia productiva i de serveis.

Estats Units

Solucions TIC amb demanda als EUA: desenvolupament i programació, IA per domòtica, agricultura i indústria, realitat augmentada per educació i salut, comerç electrònic i ciberseguretat.

Bèlgica

Estratègia Digital Europea: pilar a la UE i a Bèlgica.

Suècia

Suècia, la plataforma de llançament a l'era digital.

Portugal

La transformació digital és una de les principals prioritats del govern.

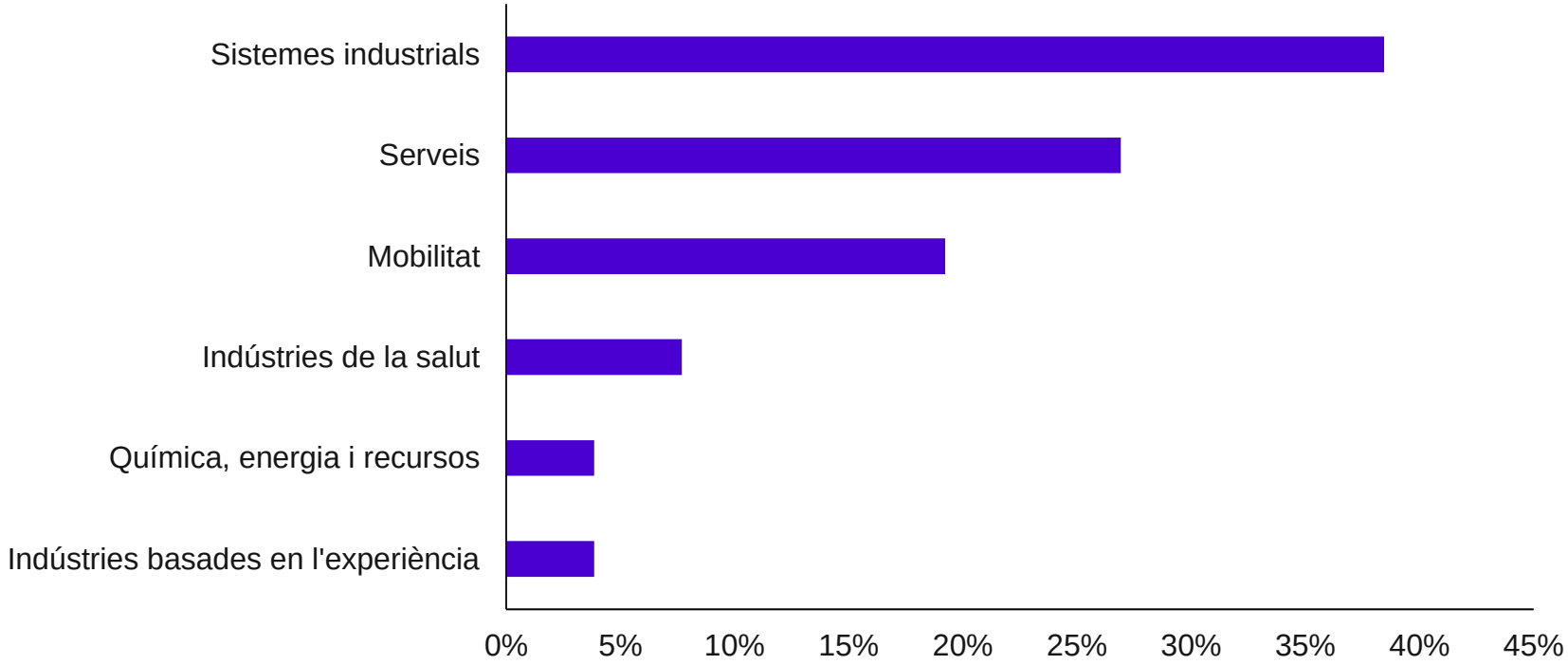
Font: Mapa global d'oportunitats de negoci internacionals 2024

Sectors més demandants de solucions de ciberseguretat

26 empreses han rebut ajuts atorgats amb els Cupons Indústria 4.0 per a realitzar projectes de ciberseguretat. Per àmbits sectorials, destaquen els sistemes industrials com a principal demandant, seguits de serveis, la mobilitat, les indústries de la salut, la química, l'energia i els recursos, i les indústries basades en l'experiència.

27 assessors tecnològics acreditats per ACCIÓ realitzen activitats relacionades amb la ciberseguretat. (un 14,36% del total d'assessors (2024)

Sectors demandants sol·lucions de ciberseguretat: CUPONS ACCIÓ



Font: ACCIÓ a partir de dades relatives als ajuts de cupons per a la competitivitat empresarial (Cupons Indústria 4.0) que ha atorgat ACCIÓ durant el 2022 i el 2023

8. Casos d’èxit a Catalunya

Casos d'èxit a Catalunya

SIRT, líder en ciberseguretat per a l'Administració pública i les empreses privades, consolida el seu negoci.

Getronics reinverteix a Barcelona i duplica la mida del seu centre mundial de ciberseguretat.

LuxQuanta és una *spin-off* de l'ICFO, i lidera un projecte europeu per implementar una xarxa de seguretat quàntica a Europa.

Fujitsu obre un *hub* a Barcelona destinat a la ciberseguretat en el sector de la salut.

Build38 obté 13 milions d'euros d'una ronda de finançament destinats a fer créixer la seva presència a Barcelona.

Zerod ha creat un *marketplace* per connectar les empreses amb els millors *hackers* ètics del món.

Inetum inaugura oficines noves a Tarragona amb el compromís de potenciar l'ecosistema tecnològic.

La **UAB** i la **UOC** s'uneixen per desenvolupar solucions per protegir les xarxes de contingut fals i reduir els ciberatacs.

Casos d'èxit (I)

SIRT, líder en ciberseguretat per a l'administració pública i les empreses, consolida el seu negoci

Sirt, líder reconegut en el camp de la ciberseguretat per a l'administració pública i les empreses, celebra 25 anys amb la consolidació del negoci a nivell nacional i internacional amb una amplia cartera de clients, com la Generalitat de Catalunya. L'empresa factura més de 20 milions d'euros en ciberseguretat.

L'empresa és responsable de valorar i identificar les necessitats personalitzades de cada escenari i empresa per millorar el seu grau d'exposició i nivell de ciberseguretat global. Desenvolupa solucions tecnològiques innovadores per a sectors com l'administració pública, la banca, la salut o la logística.

Serveis de seguretat en:

- Llocs web
- Connectivitat IoT
- *Cloud computing*
- Gestió d'infraestructures IT

www.sirt.com

LuxQuanta és una *spin-off* de l'ICFO, i lidera un projecte europeu per implementar una xarxa de seguretat quàntica a Europa

LuxQuanta ofereix solucions de criptografia per reforçar la seguretat de les empreses i xarxes de telecomunicacions. El seu producte principal consisteix en sistemes de distribució de claus quàntiques d'alt rendiment. La seva tecnologia es basa en la investigació duta a terme per l'Institut de Ciències Fotòniques (ICFO).

Amb una visió ambiciosa i compromesa amb la seguretat digital, LuxQuanta encapçalarà el projecte europeu Quarter, amb l'objectiu d'implementar una xarxa de seguretat quàntica per a les comunicacions a Europa. Desenvoluparà les eines necessàries per protegir les infraestructures de xarxes de tots els estats membres de la Unió Europea, prevenir atacs i salvaguardar les dades més sensibles. LuxQuanta serà el principal beneficiari de fons, amb un total de 3,2 milions d'euros.

Solucions del projecte:

- Seguretat de les dades
- Protecció de les xarxes de telecomunicacions

www.luxquanta.com

Fonts: The New Barcelona Post, ICFO i On Economia

Casos d'èxit (II)

Build38 obté 13 milions d'euros d'una ronda de finançament destinats a fer créixer la seva presència a Barcelona

Build38, una startup germano-catalana dedicada a la protecció d'aplicacions mòbils empresarials per mitjà d'IA, ha obtingut 13 milions d'euros d'una ronda de finançament de sèrie A que destinarà a potenciar les oficines a Barcelona. Tikehau Capital, a través del seu fons europeu centrat en ciberseguretat, ha liderat l'operació.

Build38, amb presència també a Alemanya però amb la capital catalana com a nucli innovador, s'ocupa de blindar les dades de les aplicacions, l'accés a *backends* i les dades personals, i assessora empreses per fer front a la regulació en matèria de seguretat informàtica, especialment en el disseny d'aplicacions mòbils. L'startup va ser finalista del Cyber Investor Days 2023.

Solucions de protecció per a:

- Aplicacions mòbils
- Llocs web

www.build38.com

Inetum inaugura oficines noves a Tarragona amb el compromís de potenciar l'ecosistema tecnològic

Inetum és una empresa de tecnologies de la informació que ofereix serveis i solucions digitals per a empreses i institucions. Va inaugurar noves oficines a la ciutat de Tarragona, apostant per convertir Catalunya en seu de l'ecosistema tecnològic, fet que suposarà també l'atracció de nous professionals que contribuiran al desenvolupament econòmic i tecnològic de la zona.

Els professionals d'Inetum desenvolupen projectes per a la Generalitat de Catalunya i el sector privat català, vinculats a solucions col·laboratives per a la gestió intel·ligent i avançada del lloc de treball, canals digitals, automatització i millora de processos i aplicacions, cultura digital i gestió del canvi, dades i ciberseguretat.

Algunes de les solucions de seguretat per a *blockchain*:

- Certificats
- Credencials
- *Wallets*
- Pagaments

www.inetum.com

Fonts: The New Barcelona Post, Internet Segura i Computing

Casos d’èxit (III)

Getronics reinverteix a Barcelona i duplica la mida del seu centre mundial de ciberseguretat

Getronics és una consultora especialitzada en tecnologies de la informació i la comunicació, amb presència a la ciutat de Barcelona, reconeguda com a *hub* tecnològic d'excel·lència.

Recentment ha inaugurat el Centre d’Operacions de Seguretat a Barcelona, on un equip de 30 professionals ofereix serveis ininterromputs de ciberseguretat a empreses de tot el món, amb un èmfasi especial en la gestió del cicle de vida de les amenaces (TLM) i, sobretot, en la detecció i resposta. D’aquesta manera, també amplia les seves capacitats per garantir solucions innovadores i afrontar les amenaces de seguretat dels clients amb eficàcia.

Serveis digitals principals:

- Emmagatzematge al núvol
- Ciberseguretat
- Gestió i anàlisi de dades

www.getronics.com

Fujitsu obre un *hub* a Barcelona destinat a la ciberseguretat en el sector de la salut

El 2023 l’empresa japonesa Fujitsu, especialitzada en TIC i seguretat de la informació, va establir el primer Healthcare Cybersecurity Center del món a Barcelona. La capital catalana va ser escollida gràcies al dinamisme en el sector tecnològic de la salut del territori. L’empresa preveu també explorar possibles col·laboracions amb startups *healthtech*, universitats i centres de recerca a Catalunya.

El *hub* és el responsable de detectar les demandes específiques del sector i establir mecanismes específics de seguretat de les dades. A més, el centre preveu oferir solucions per a la gestió dels riscs sanitaris davant qualsevol atac.

Solucions del hub:

- *Digital health*
- Ciberseguretat

www.fujitsu.com

Fonts: ElPeriódico, The New Barcelona Post i web corporativa

Casos d'èxit (IV)

Zerod ha creat un *marketplace* per connectar les empreses amb els millors *hackers* ètics del món

Zerod és una plataforma que no només connecta empreses amb el món del *hacking*, sinó que també verifica rigorosament les habilitats i l'experiència dels *hackers* registrats. Aquests professionals han de demostrar les seves habilitats a través dels *bug bounties*, programes que ofereixen certes companyies amb la finalitat de recompensar a aquells *hackers* que les hi reportin errors de ciberseguretat. A més, els *hackers* han de tenir entre 10 i 15 anys d'experiència i les certificacions apropiades.

Zerod compta amb més de 150 *hackers* registrats, els quals han detectat més de 1.500 vulnerabilitats en sistemes d'empreses com Microsoft, Meta o Google. L'empresa també està explorant en el desenvolupament d'un model de *hacker* ètic que utilitza IA per millorar els processos de recerca en ciberseguretat, combinant aquesta tecnologia amb l'expertesa humana per fer front a les amenaces cibernètiques.

Serveis de l'empresa:

- Auditories i assessorament
- Formació en ciberseguretat
- *Penetration Testing*

www.zerod.io

La UAB i la UOC s'uneixen per desenvolupar solucions per protegir les xarxes de contingut fals i reduir els ciberatacs

Un equip d'investigadors coordinat des del Departament d'Enginyeria de la Informació i les Comunicacions de la Universitat Autònoma de Barcelona (UAB) i amb la participació de la Internet Interdisciplinary Institute (IN3) de la Universitat Oberta de Catalunya (UOC), ha iniciat el projecte DANGER (Ciberseguretat per a la detecció, anàlisi i filtratge de continguts falsos o maliciosos en entorns d'hiperconnectivitat).

L'objectiu principal del projecte, que es desenvoluparà durant els propers dos anys, és millorar la seguretat de les xarxes mitjançant eines que analitzin la informació i permetin la identificació maliciosa per a fer-ne un filtratge posterior. L'equip de recerca treballarà en diverses àrees de la ciberseguretat, potenciant la valorització i transferència dels resultats a la societat i als sectors productius, així com la divulgació a diferents tipus de públic.

Abast del projecte:

- Gestió i anàlisi de dades
- Protecció de la informació
- Transferència i divulgació

www.uab.cat

Fonts: ViaEmpresa, 30 Virtual i web corporativa

Gràcies!

ACCIÓ Catalonia Trade & Investment

Generalitat de Catalunya

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

Passeig de Gràcia, 129
08008 Barcelona

accio.gencat.cat
catalonia.com

@accio_cat
@Catalonia_TI

linkedin.com/company/acciocat/
linkedin.com/company/invest-in-catalonia/

Carrer de Salvador Espriu, 51
08908 L'Hospitalet de Ll.

ecosistema@ciberseguretat.cat
ciberseguretat.gencat.cat

@ciberseguracat

@ciberseguracat

Més informació sobre el sector, notícies i oportunitats:
https://www.accio.gencat.cat/ca/serveis/banc-coneixement/cercador/BancConeixement/eic-la-ciberseguretat-a-catalunya

Generalitat de Catalunya