

Maig del 2024. Píndola tecnològica.

La ciberseguretat a Catalunya

La ciberseguretat a Catalunya. Píndola tecnològica.

ACCIÓ

Generalitat de Catalunya



Els continguts d'aquest document estan subjectes a una llicència Creative Commons. Si no s'indica el contrari, se'n permet la reproducció, la distribució i la comunicació públiques sempre que se'n citi l'autor, no se'n faci un ús comercial i no se'n distribueixin obres derivades. Podeu consultar un resum dels termes de la llicència a:

<https://creativecommons.org/licenses/by-nc-nd/4.0/>

L'ús de marques i logotips en aquest informe és merament informatiu. Les marques i els logotips esmentats pertanyen als seus respectius titulars i en cap cas són titularitat d'ACCIÓ. Aquesta és una representació il·lustrativa parcial de les empreses, les organitzacions i les entitats que formen part de l'ecosistema de la ciberseguretat. Hi pot haver empreses, organitzacions i entitats que no hagin estat incloses en l'estudi.

Realització

Unitat d'Estratègia i Intel·ligència Competitiva d'ACCIÓ

Agència de Ciberseguretat de Catalunya

Barcelona, maig del 2024

Resum executiu

1. Definició de ciberseguretat i importància per a la indústria
2. Principals magnituds mundials
3. Aplicacions prospectives per sector de demanda
4. Tendències en ciberseguretat i impacte en els ODS
5. La intel·ligència artificial i la ciberseguretat
6. Iniciatives en ciberseguretat
7. La ciberseguretat a Catalunya
8. Casos d'èxit a Catalunya

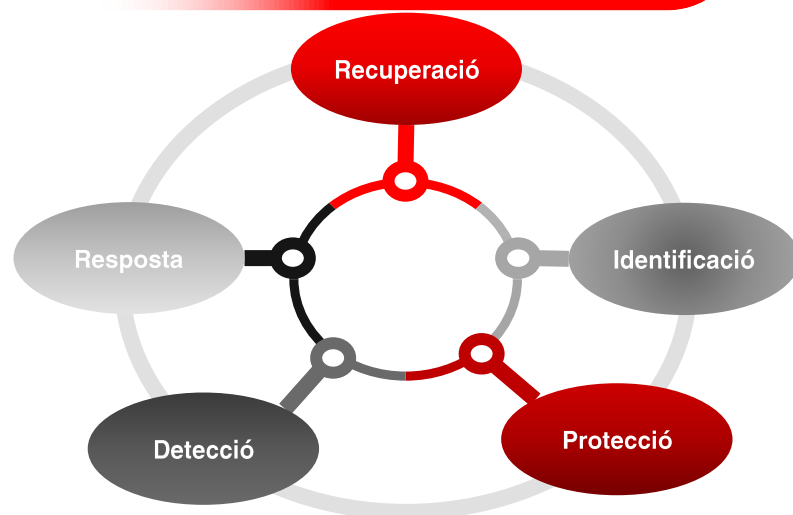
Resum executiu: la ciberseguretat a Catalunya (I)

4

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 | 🏥 Salut | 💻 Gestió de serveis TIC (B2B) |
| 🚗 Transport | 💧 Aigua potable | 🏛️ Administració pública |
| 🏦 Banca | 🚰 Aigües residuals | 🏠 Infraestructura digital |
| 🏢 Infraestructures del mercat financer | 🏢 Infraestructura digital | 🌐 Espai |



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 frauds
- El **sector sanitari** continua sent un objectiu preferent dels ciberatacs



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%)

Resum executiu: la ciberseguretat a Catalunya (II)

5

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



CENTRE DE COMPETÈNCIES I D'INNOVACIÓ EN CIBERSEGURETAT



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



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

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**.

La ciberseguretat a Catalunya

1. Definició de ciberseguretat i importància per a la indústria

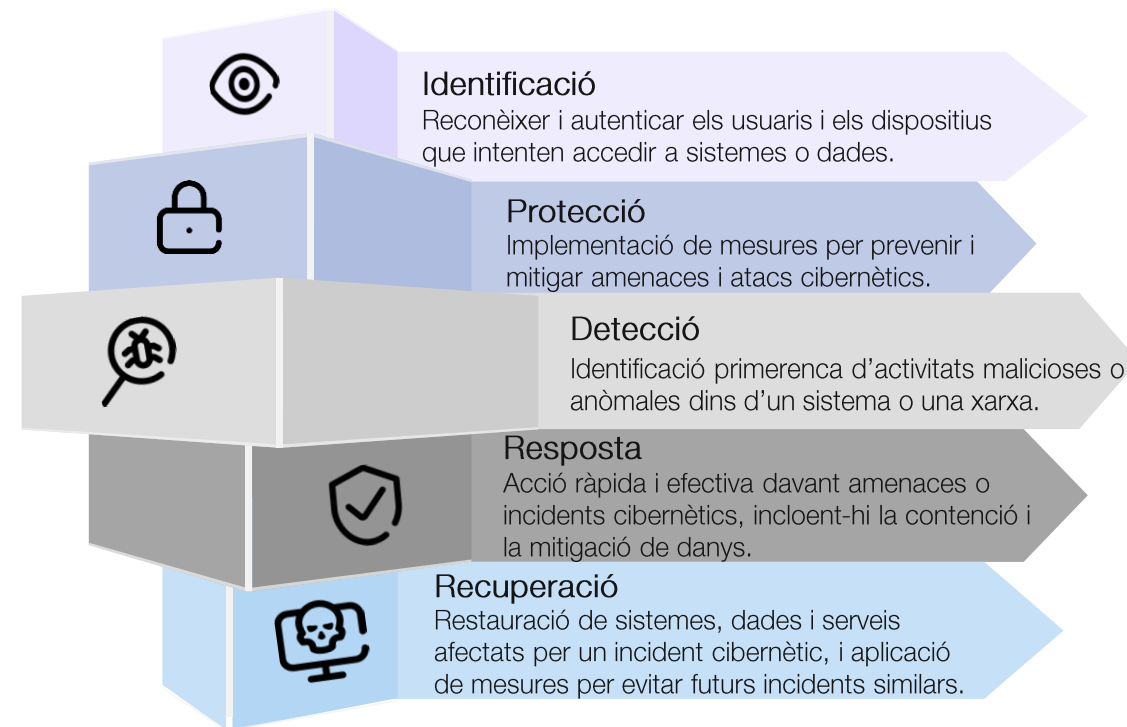
Definició de ciberseguretat

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:





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 paraitzar-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

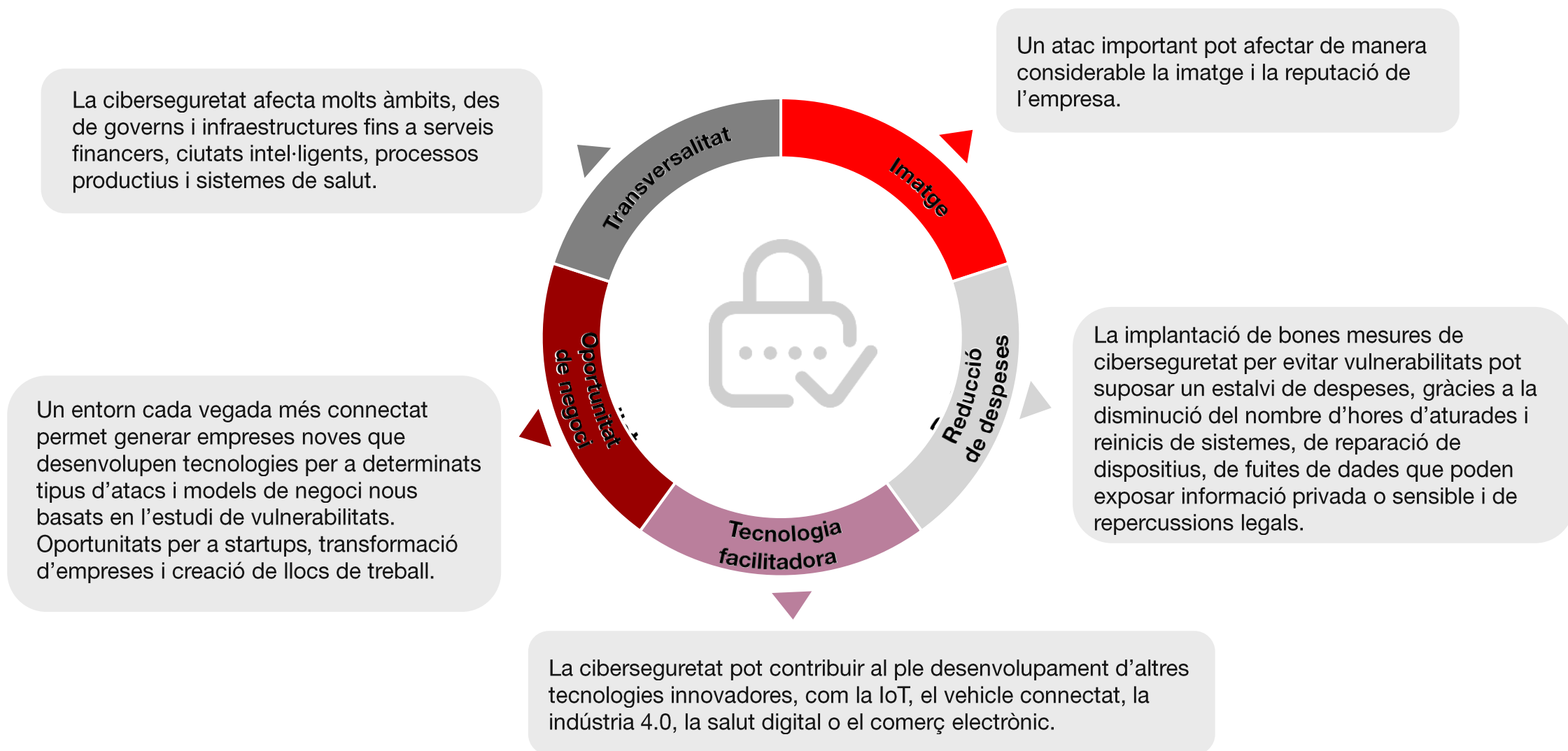
Un incident cibernètic pot afectar l'opinió que els clients o la ciutadania tenen d'una organització, d'una marca o bé d'un producte o servei, i això pot acabar impactant en el balanç econòmic. Recuperar la reputació després d'un incident pot representar un sobreesforç en termes econòmics i de temps.

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.



Importància de la ciberseguretat per a la indústria

9



2. Principals magnituds mundials

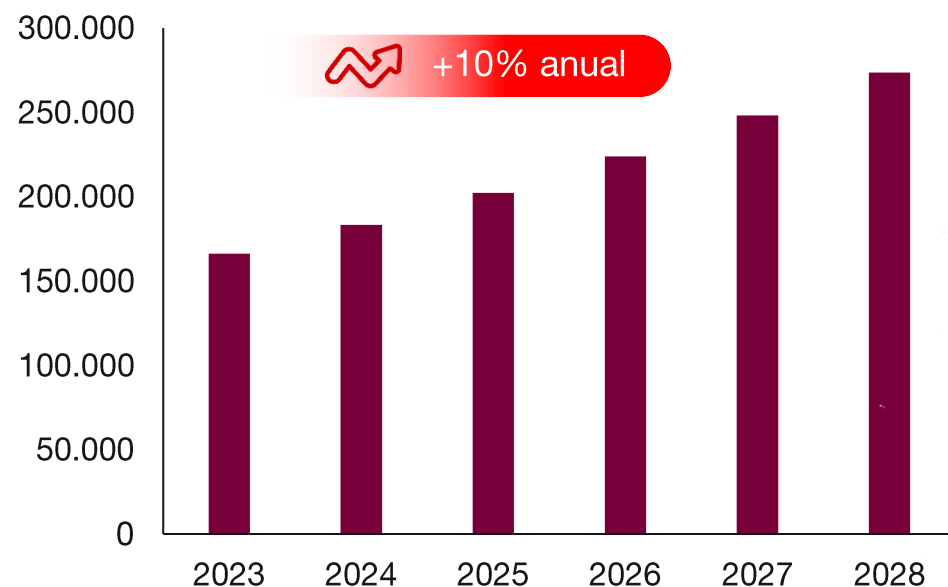
Mercat mundial i perspectives de creixement de la ciberseguretat

11

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

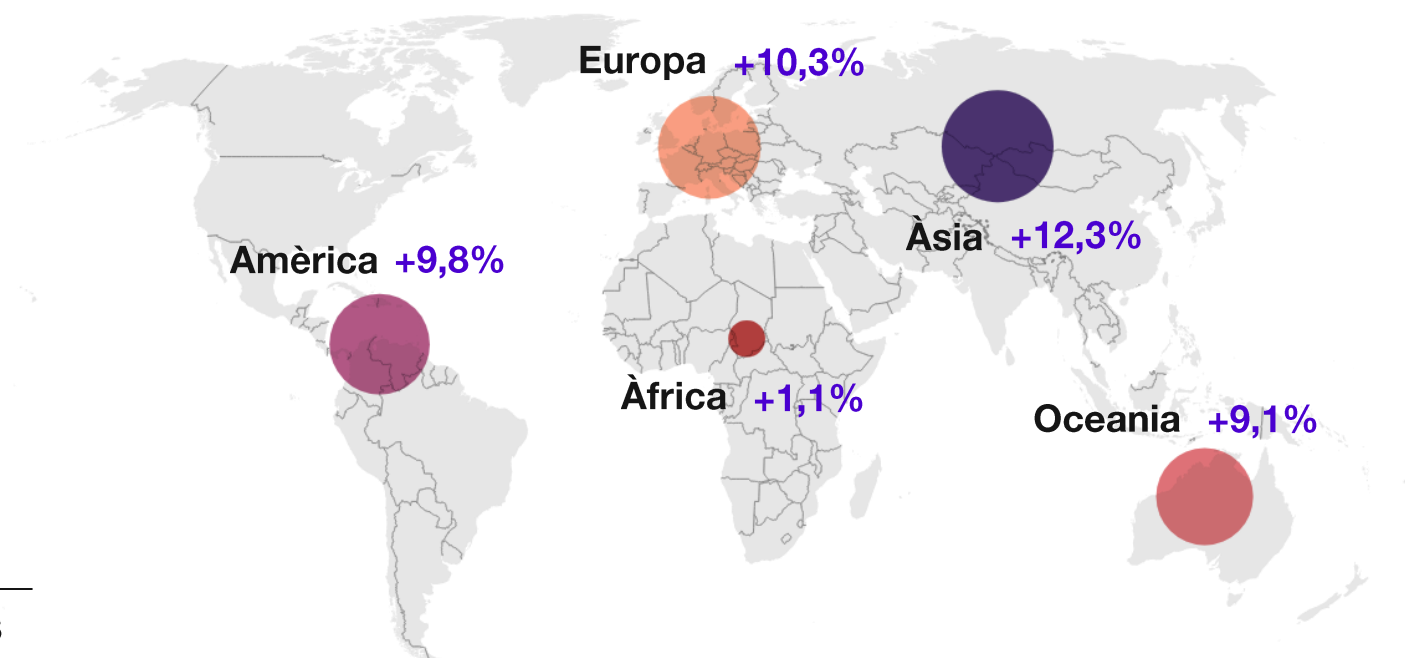
Facturació mundial de la ciberseguretat*

(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%).

Empreses líders en ciberseguretat

12



 Presència a Catalunya

3. Aplicacions prospectives per sector de demanda

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.		Aigües residuals	Empreses que recullen, eliminen o tracten aigües residuals urbanes, residuals domèstics 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.
	Transport	Autoritats, operadors i gestors d'infraestructura vinculada als transports aeri, ferroviari, marítim i de carretera.			
	Banca	Institucions de crèdit.		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.
	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.		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.
	Aigua potable	Proveïdors i distribuïdors d'aigua destinada al consum humà.		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).

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.



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 frauds, 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.

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

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 frau. 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 frau i robatoris de dades.



Fets rellevants del 2023

20

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

Desarticulada Genesis Market, la plataforma més gran de venda de credencials la dark web
Accions policials

Explotació de vulnerabilitats de MOVEit per robar dades i extorsionar els clients
Fuita de dades

Dues empreses de hosting daneses perden les dades de la clientela
Ransomware

L'empresa de ciberseguretat vinculats a la Xina dirigeixen les seves operacions a Europa i els EUA
Ciberespionatge

Ciberatacs amb vincles iranians dirigits a instal·lacions d'aigua dels EUA
Sabotatge

Un atac de Lockbit interromp serveis mèdics a hospitals alemanys durant la nit de Nadal
Ransomware

Ciberatacs en peticions per segon més gran de la història
DDoS

L'atac DDoS filtra per error milers de credencials dels seus clients
Fuita de dades

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 troia 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	organització cibercriminal especialitzada Frau	Desarticulada una Frau	Diversos hospitals afectats per un ciberatac a un proveïdor Ransomware	Ciberatac a Junts per Catalunya coincidint amb la votació per a la investidura Hacktivism
										L'Ajuntament de Reus informa d'un ciberatac a Reus Mobilitat i Serveis Fuita de dades	

Font: diverses fonts

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 ciberfraud (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 vulnerabilitats més presents a les IP de Catalunya afecten servidors Apache i representen el 36% del total de vulnerabilitats.

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

Formació en ciberseguretat a Catalunya

13 màsters o postgraus de ciberseguretat

	Màster en Seguretat de la Informació Empresarial		Màster en Tècniques de Seguretat Informàtica. Ciberseguretat
	Postgrau en Compliance i Ciberseguretat		Màster en Ciberseguretat
	Màster en Seguretat de les TIC		Màster en Ciberseguretat
	Màster en direcció de ciberseguretat		Màster Universitari en Seguretat Informàtica
	Màster en Enginyeria de la Seguretat Informàtica i Intel·ligència Artificial		Màster en Ciberseguretat
	Màster en Aprenentatge Automàtic i Ciberseguretat per a Sistemes Connectats a Internet		Màster en Ciberseguretat
			Màster Universitari en Direcció i Gestió de la Ciberseguretat i Infraestructures Crítiques



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

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 fermes.
- 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 ampliadades: 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 a Catalunya

5. La intel·ligència artificial i la ciberseguretat

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 convincts
- 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 frauds



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

La IA per a la ciberseguretat

26

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



La ciberseguretat a Catalunya

6. Iniciatives en ciberseguretat

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.

Orientació de polítiques

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

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)

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

Inversió

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

Altres àmbits de política cibernètica

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

Font: Comissió Europea



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.

La ciberseguretat a Catalunya

7. La ciberseguretat a Catalunya

Mapatge de l'ecosistema de ciberseguretat a Catalunya

31



 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.

* 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.



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

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

32

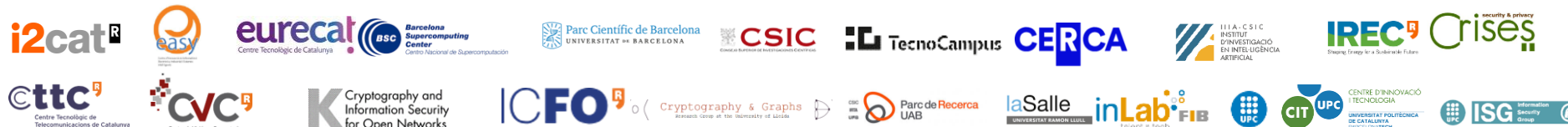


Agents de l'ecosistema de la ciberseguretat

33



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

Iniciatives per potenciar la ciberseguretat a Catalunya

34



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.



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



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.



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.



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.



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

Hubs tecnològics a Catalunya enfocats a la ciberseguretat el 2023

35



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:



Deloitte.



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

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

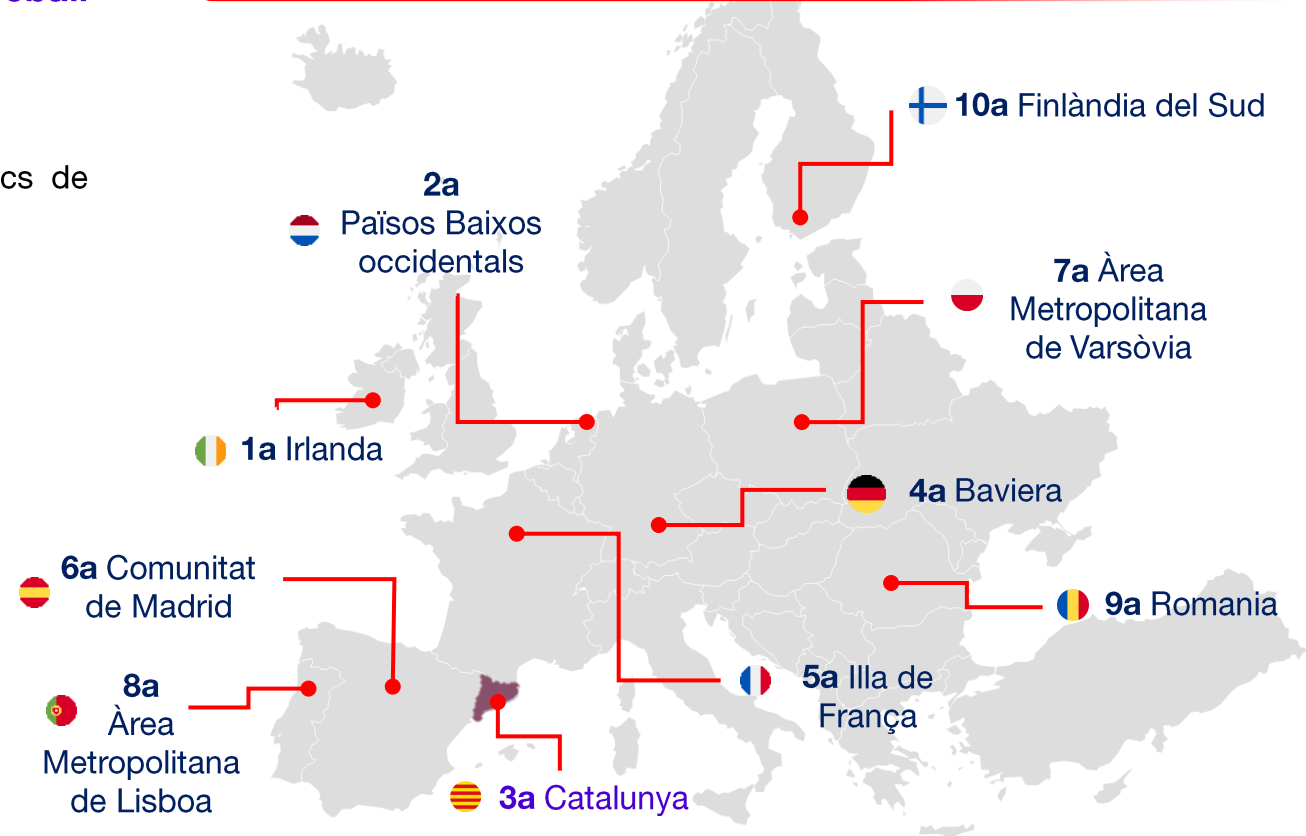
El 2023, Catalunya ha estat la **3a regió de la UE en nombre de projectes estrangers** de ciberseguretat, la **5a en llocs de treball creats** i la **6a en captació d'inversió estrangera**.

- 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

37

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).

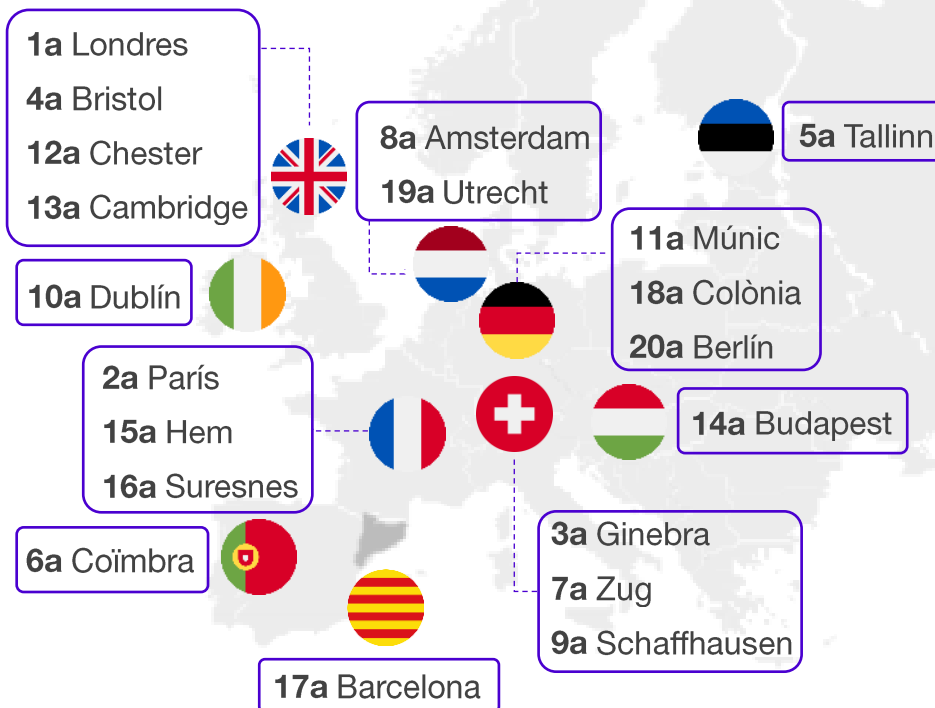
L'startup catalana que ha rebut més finançament és **Red Points**, que ha tancat 2 rondes per valor de més de 58 milions de dòlars en els darrers 5 anys.

Startups de Barcelona amb rondes tancades:



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

Activitats de recerca catalana en ciberseguretat a l'Horizon Europe

38

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

15 projectes

5,5 milions d'euros

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

6a

regió europea en
finançament a
l'Horizon Europe



13 institucions

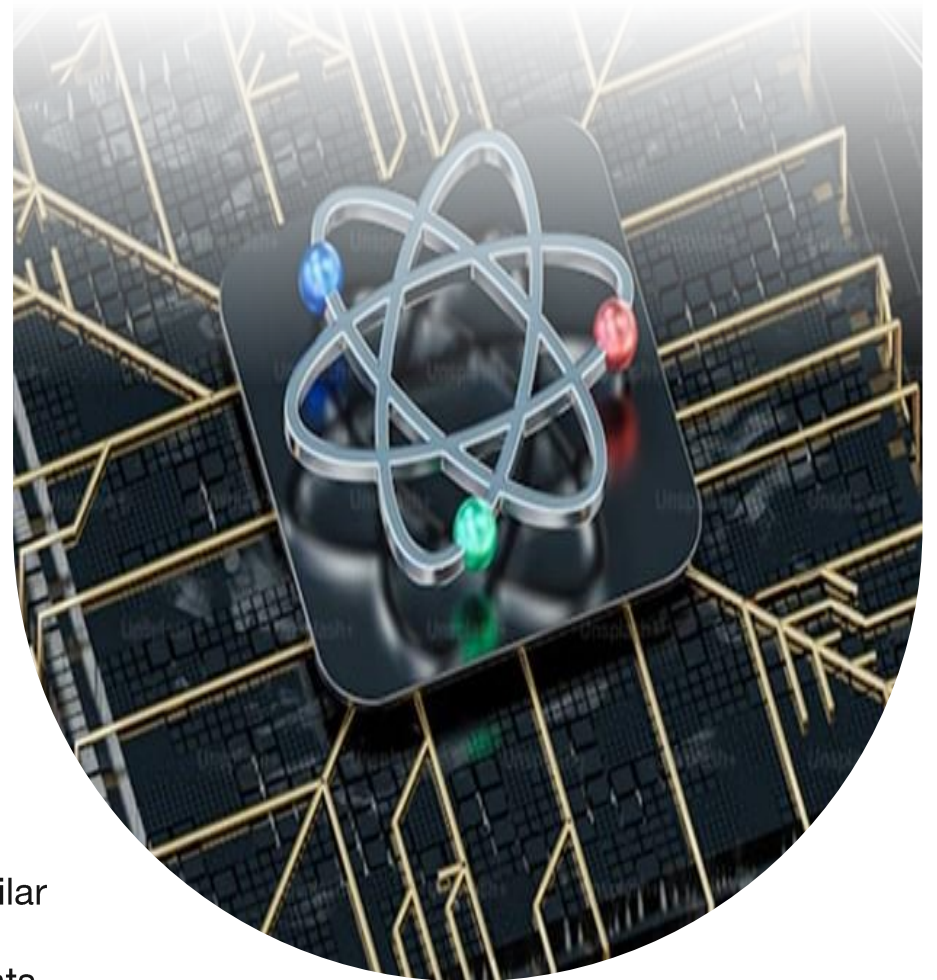


Nota: s'hi inclouen els projectes de l'Horizon Europe (2022-2023) relacionats amb la ciberseguretat (*computer security* i *network security*).



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.



EuroQCI, European Quantum Communications Infrastructures

40

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.



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.



El node d'Espanya té com a partners:



 **Partners catalans en el projecte:**



Fonts: European Comission i Digital Strategy

La ciberseguretat a Catalunya

8. Casos d'èxit a Catalunya

Casos d'èxit a Catalunya

42



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.

Gràcies!



Passeig de Gràcia, 129
08008 Barcelona

[accio.gencat.cat](https://accio.gencat.cat/catalonia.com)
[catalonia.com](https://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>

