Maig del 2025. Píndola tecnològica.

La ciberseguretat a Catalunya

Generalitat de Catalunya

La ciberseguretat a Catalunya. Píndola tecnològica.

ACCIÓ
Generalitat de Catalunya

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

Barcelona, maig del 2025

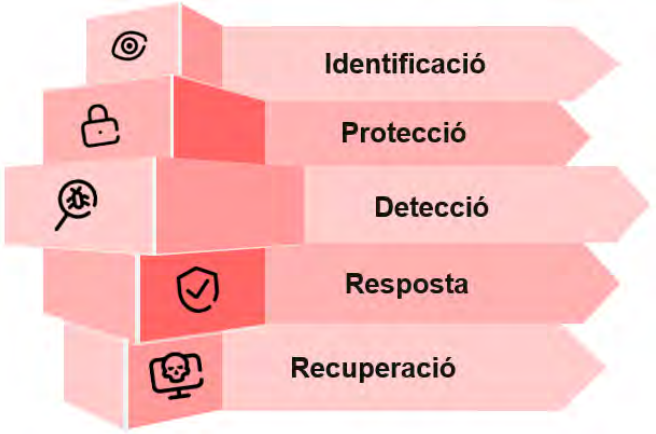
Generalitat de Catalunya

Índex de continguts

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.

Verticals



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

Impacte de les tecnologies quàntiques

Principals oportunitats en ciberseguretat:

- Criptografia de seguretat quàntica
- Comunicació ultrasegura
- Detecció d'amenaces millorada

Mercat mundial

La facturació mundial en ciberseguretat creixerà a un ritme del **8 % anual** durant els propers cinc anys, fins als **272.000 M$**.

Amèrica lidera de manera destacada el mercat de la ciberseguretat, mentre que **Europa** i Àsia es situen en segona i tercera posició, respectivament.

Els **serveis financers**, l'**administració pública** i el sector de la **salut** són els sectors més demandants de serveis de ciberseguretat.

En el darrer quinquenni, la **IED** en ciberseguretat acumula una inversió de **41.000 M€**, mentre que les startups de ciberseguretat han tancat **rondes de capital risc** per valor d'**11.000 M$**.

Resum executiu: la ciberseguretat a Catalunya (II)

557 empreses a l'ecosistema de la ciberseguretat

Augment del 7,9 % anual i del **58,2 %** des del 2018.

Facturació de **1.473 M€** (**+18,4 %**) i **10.672** llocs de treball (**+12,8 %**).

El **82,6 %** són PIMES i el **10,6 %** són startups.

Per segments, destaquen les empreses que es dediquen a **protegir** (**90,3 %**) i a identificar (**62,5 %**).

238 empreses (42,7 %) també desenvolupen solucions amb la **IA**

27 empreses (4,8 %) també desenvolupen solucions amb la **quàntica**

Catalunya, territori atractiu per la ciberseguretat

Els **projectes d'IED** en ciberseguretat a Catalunya s'han **doblat** durant el darrer quinquenni (de 6 a 12) i la **inversió** s'ha multiplicat **x9** (de 24 a 207 M€).

El **36 % dels 160 hubs tecnològics** d'empreses internacionals establerts a Catalunya es dedica a la ciberseguretat.

Catalunya és la **5a regió europea** en finançament a l'Horizon Europe (2022-2024), amb **15 projectes** i **11,3 M€**.

Talent en ciberseguretat

14 graus, màsters i postgraus de ciberseguretat, i **62 cursos** de formació professional en ciberseguretat.

La bretxa de talent augmenta un **12,8 %** anual i es situa en **13.500** persones.

Iniciatives per potenciar la ciberseguretat a Catalunya

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA · AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA · CENTRE DE COMPETÈNCIES I D'INNOVACIÓ EN CIBERSEGURETAT · BARCELONA CYBERSECURITY CONGRESS · CYBERSECURITY CAT · DIH4CAT Digital Innovation Hub de Catalunya · DCA Digital Catalonia Alliance · ASCICAT

Iniciatives quàntica – ciberseguretat

- **Qsunset**
- **6GQuiCryptoLab**
- **Qspace**
- **Full de ruta criptografia quàntica**
- **Qollserola**
- **Node Barcelona – Q-Network**

1. Definició de ciberseguretat i importància per a la indústria

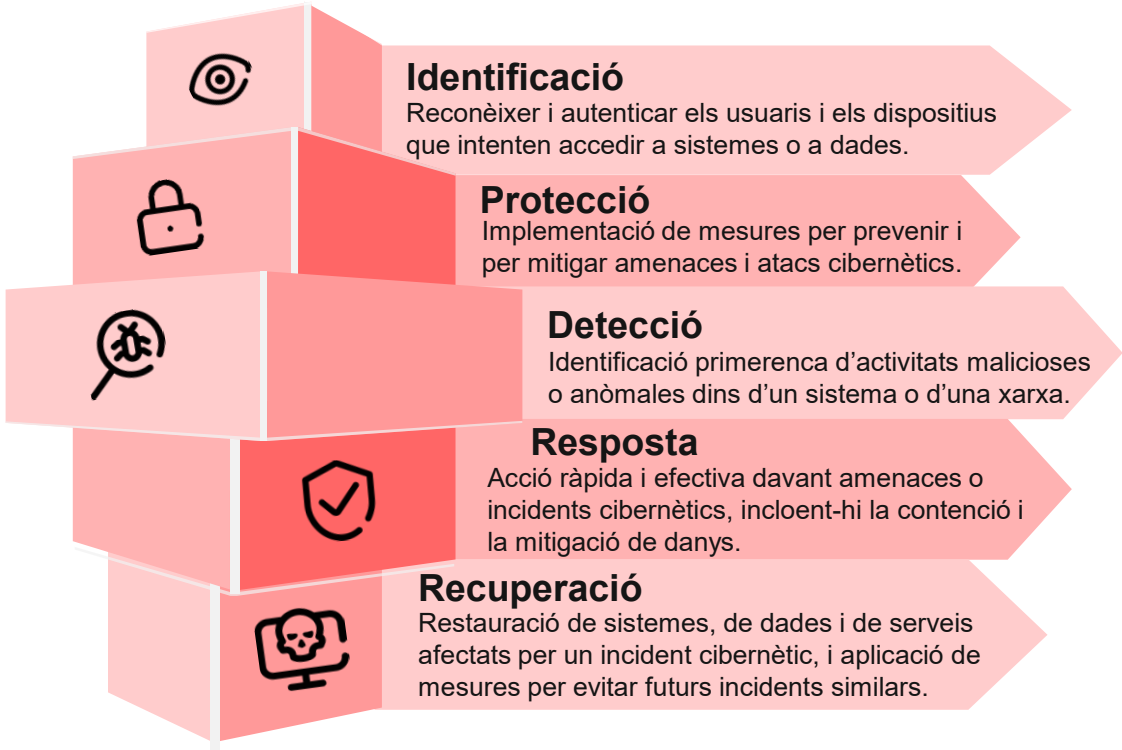
Definició de ciberseguretat

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.

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



Actua sobre:

Persones Processos Tecnologies

Magnituds dels cibercrims

A nivell mundial, per al 2024 es calcula que el cost econòmic provocat per l'activitat del cibercrim ha estat d'uns **9,5 bilions d'euros**.

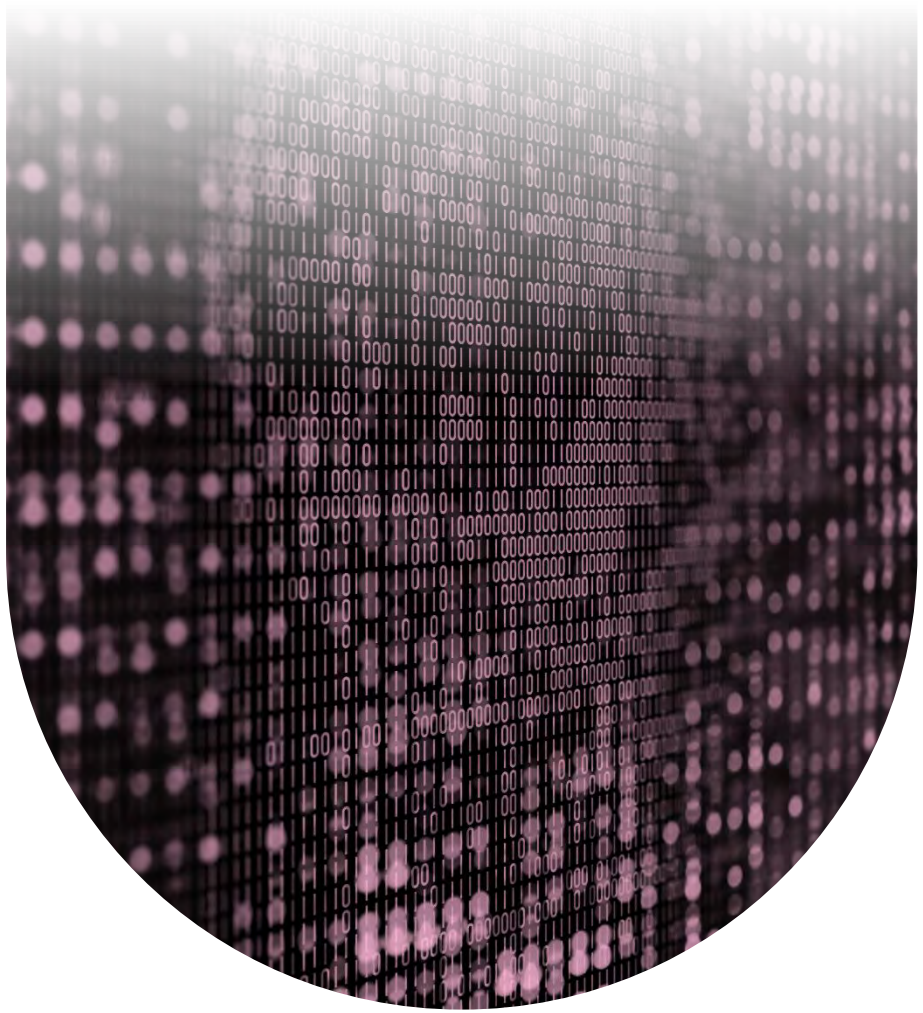
El 2024, els atacs de *ransomware* han augmentat un **11 %** a nivell global respecte de l'any anterior.

Les notícies sobre fraus amb suplantació han incrementat un **50 %** el 2024 respecte de l'any anterior.

El **91 %** dels atacs de *ransomware* del 2024 van incloure exfiltració de dades, un augment respecte del 75 % del 2023 i del 60 % del 2022.

Els cibercriminals han robat més de **2.000 M€** en criptovalors el 2024, un increment del **10 %** respecte de l'any anterior.

A Espanya, el 2024 els incidents de ciberseguretat han augmentat un **15 %** respecte de l'any anterior.

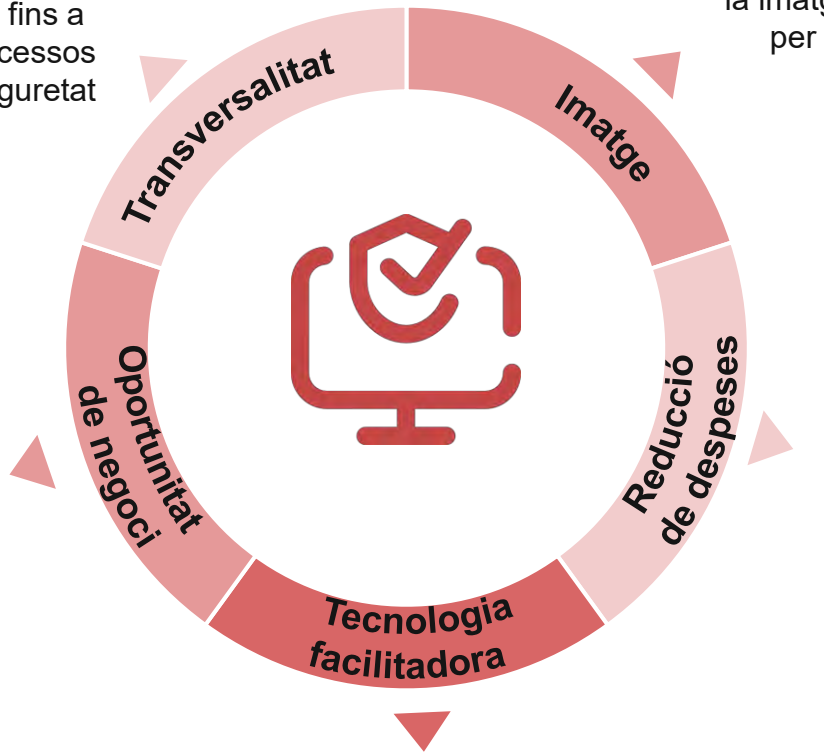


Fonts: Agència de Ciberseguretat de Catalunya, INCIBE, RansomDB, Blackfog

Importància de la ciberseguretat per a la indústria

Els atacs cibernètics afecten cada vegada més àmbits, des de governs i infraestructures fins a serveis financers, ciutats intel·ligents, processos productius i sistemes de salut. La ciberseguretat resulta fonamental per protegir-los.

Un atac cibernètic pot afectar de manera considerable la imatge, la confiança i la reputació de l'empresa, tant per part dels clients com per part dels inversors.



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

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 de reinicis de sistemes, de reparació de dispositius, de fuites de dades que poden exposar informació privada o sensible, de pagaments de rescats de dades i de repercussions legals.

La ciberseguretat és imprescindible per al ple desenvolupament i per a la hibridació d'altres tecnologies innovadores com la intel·ligència artificial, la internet de les coses o els bessons digitals. Sense ciberseguretat no hi ha indústria 4.0, mobilitat avançada ni salut digital.

Font: elaboració pròpia

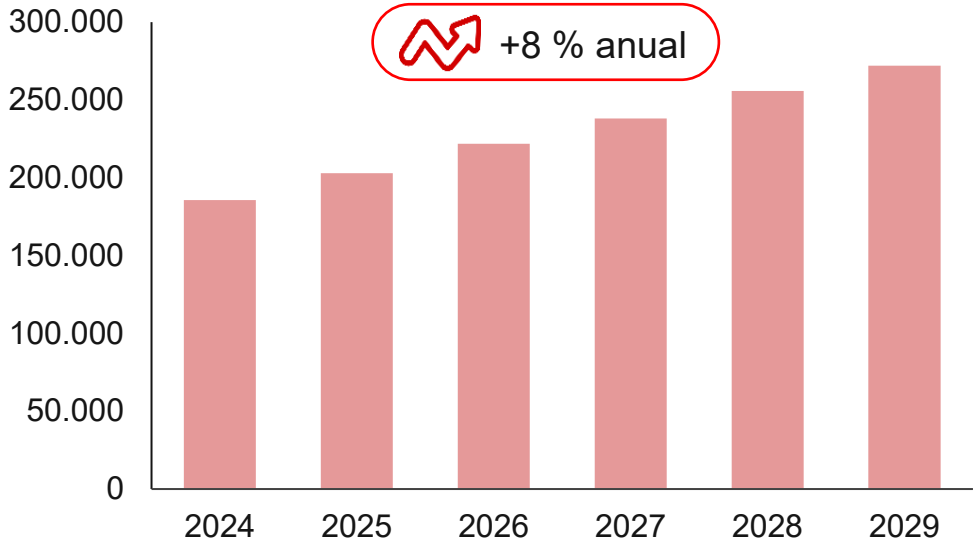
2. Principals magnituds mundials

Mercat mundial de la ciberseguretat

La facturació mundial en ciberseguretat creixerà a un ritme del **8 % anual** durant els propers cinc anys, fins als **272.000 milions de dòlars**.

Facturació mundial de la ciberseguretat

(2024-2029, milions de dòlars)



Factors clau del creixement del mercat de la ciberseguretat

- Ràpida adopció de noves tecnologies
- Increment general dels ciberatacs

Principals desafiaments del mercat de la ciberseguretat

- Escassetat de professionals en ciberseguretat
- Impacte de conflictes geopolítics

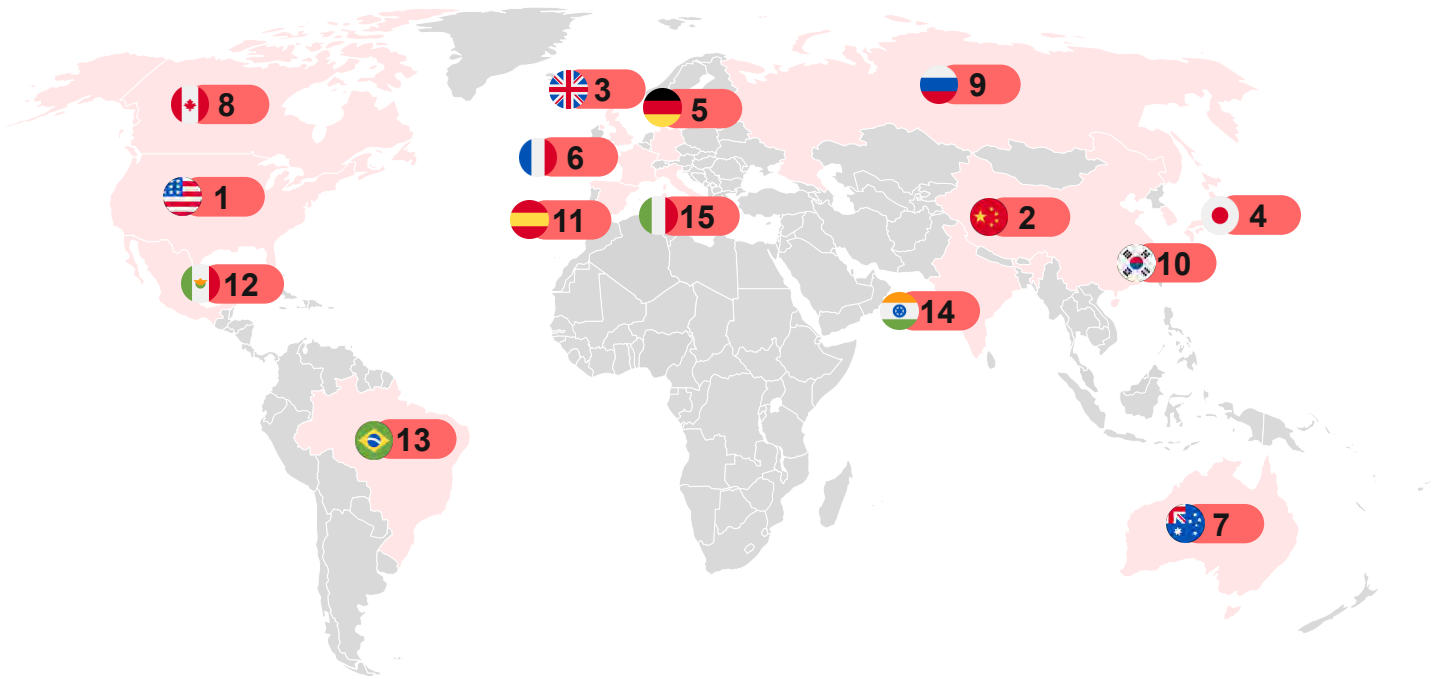
Font: Statista

Mercat mundial de la ciberseguretat, per països

Els **Estats Units** copen gairebé la meitat del mercat mundial de la ciberseguretat

La **Xina** és el segon país per facturació i, juntament amb l'**Índia**, el que més creixerà en els propers anys

Cinc països europeus destaquen en el top-15: el **Regne Unit**, **Alemanya**, **França**, **Espanya** i **Itàlia**



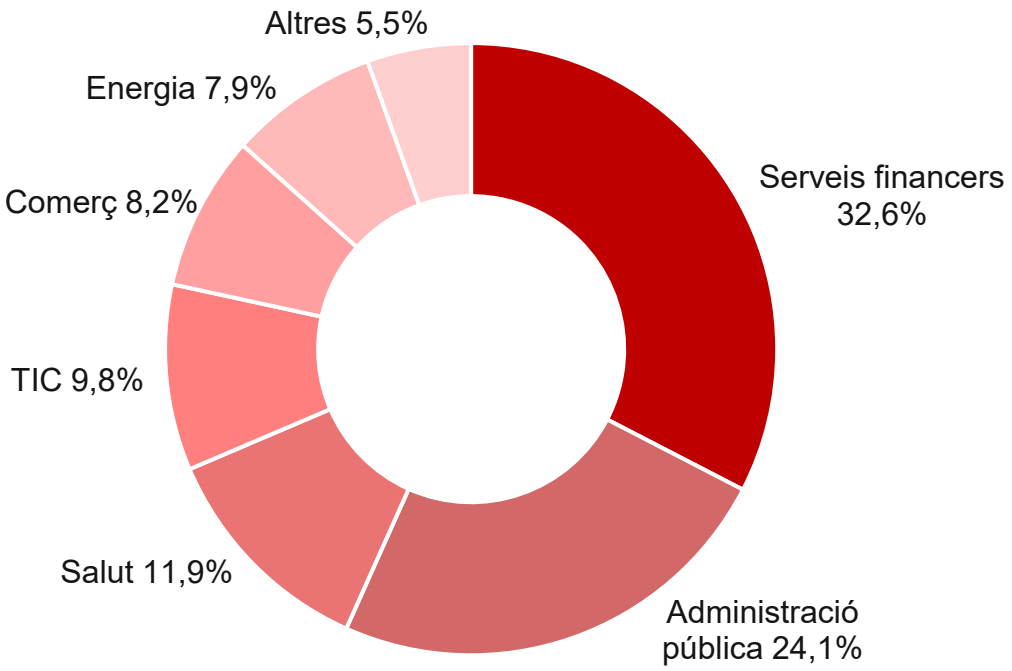
	Països	Facturació (M$, 2024)	% de creixement anual 24-29
1	Estats Units	81.370	7,4 %
2	Xina	14.750	10,8 %
3	Regne Unit	10.990	8,9 %
4	Japó	9.374	7,2 %
5	Alemanya	7.543	6,9 %
6	França	5.785	6,6 %
7	Austràlia	4.043	7,4 %
8	Canadà	3.834	8,2 %
9	Rússia	3.551	5,3 %
10	Corea del Sud	3.397	7,8 %
11	Espanya	3.075	6,7 %
12	Mèxic	3.018	7,5 %
13	Brasil	2.955	8,6 %
14	Índia	2.866	13,0 %
15	Itàlia	2.846	6,1 %

Font: Statista

Sectors més demandants de serveis de ciberseguretat

Els **serveis financers**, l'**administració pública** i el sector de la **salut** són els sectors més demandants de serveis de ciberseguretat.

Quota de mercat de la ciberseguretat, per sector demandant
(%, 2023)



Font: Statista

Empreses líders en ciberseguretat

Estats Units

APPGUARD · BROADCOM · CISCO · CLOUDFLARE · CROWDSTRIKE · CYBERARK · DXC TECHNOLOGY · FORTINET · f5 · 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 · Softcat · SOPHOS

Alemanya

Avira · secunet · T

Israel

CHECK POINT · perimeter 81

França

THALES · Capgemini · EXCLUSIVE NETWORKS

Suècia

yubico

República Txeca

Avast

Espanya

cipher

Canadà

Genetec

Irlanda

accenture

Japó

TREND MICRO

Índia

INDUSFACE

Polònia

ANDERSEN

Presència a Catalunya

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

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 17 d'abril del 2025 els estats membres han d'elaborar una llista amb les entitats impactades i revisar-la com a mínim cada 2 anys.

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

Energia	Entitats dedicades a la producció i a la transmissió d'electricitat, operadors de calefacció i refrigeració, i actors vinculats a l'extracció i a la distribució de petroli, de gas i d'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 per a 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 de 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)

Les **PIMES** emergeixen com a consumidores actives de ciberseguretat per fer front a les ciberamenaces emergents.

El 2024, el **74 %** dels atacs de *ransomware* es van dirigir a empreses de 1.000 empleats o menys. Ha suposat un augment de **7** punts percentuals respecte del 2023.

El *phishing* com a vector d'entrada s'utilitza en el **45 %** dels atacs dirigits cap a PIMES.

El **20 %** de totes les empreses no poden recuperar les dades després d'un ciberatac.

Les pèrdues per ciberatac arriben als **50.000 €** de mitjana per a les empreses més petites.

Durant el període de l'1 de gener al 30 d'abril del 2024, es van detectar un total de **2.402** casos de *malware* i de programari no desitjat ocult en productes de programari per a PIMES, tot representant un **8 %** més que el 2023.

Generalitat de Catalunya

Quins són els primers passos que s'han de seguir?

1. Sol·licitar el Kit Digital: És un programa dirigit a PIMES i a autònoms per acompanyar les organitzacions en el procés de transformació digital que inclou diverses solucions digitals com per exemple **comunicacions segures** i **ciberseguretat**.
2. Accessos segurs: Definir una política de **contrasenyes complexes,** implementar el **2FA** i definir una gestió d'identitats dins de l'organització.
3. Bons usos digitals a l'entorn digital: **Conscienciar i formar** els empleats sobre la necessitat de seguir un conjunt de **consells i de mesures preventives**, seguint els 10 consells de bons usos digitals a l'entorn de treball definit per l'Agència de Ciberseguretat de Catalunya.
4. Ús de la VPN: Crear una **xarxa privada virtual**, per permetre a l'usuari connectar-se de forma segura a la xarxa interna i a Internet.
5. Responsabilitat digital corporativa: Mantenir un entorn **digital sostenible** per mantenir una estratègia beneficiosa pel medi ambient, per la ciberseguretat i per la reputació de l'empresa.

Fonts: Coveware, Hodeitek, Hiscox, Futurum, Securelist

Convergència de tecnologies amb la ciberseguretat

La ciberseguretat evoluciona a mida que fa front a noves amenaces, i ho fa hibridant-se amb tecnologies complementàries.

- Intel·ligència artificial generativa
- Detecció i protecció de *zero day* amb IA
- IoT amb IA
- Xifratge post-quàntic

- Entorns híbrids
- Observabilitat
- Tecnologia biomètrica
- Connectivitat 6G

4. Tendències en ciberseguretat i impacte en els ODS

Principals tendències en ciberseguretat del 2024

Els *deepfakes* amenacen la integritat i l'estabilitat dels processos electorals. La unió entre la suplantació de celebritats a través de *deepfakes* i la facilitat de difusió de les xarxes socials s'ha convertit en una autèntica amenaça per la democràcia.

Creixement de l'ús de dades biomètriques: seguretat o preocupació? L'ús de dades biomètriques permet reforçar la seguretat a partir de la vigilància de les persones, però comporta preocupacions en matèria de privacitat i riscos de suplantació digital.

La pujada del valor de les criptomonedes atrau l'activitat cibercriminal. L'augment del valor de les criptomonedes ha disparat els ciberatacs per robar criptoactius, fent imprescindible reforçar la seguretat d'usuaris i de plataformes.

Els ciberatacs en el sector financer, en augment. El sector financer reuneix actius de valor, de manera que atrau ciberatacs dirigits tant a les mateixes entitats bancàries, amb atacs sofisticats, com usuaris, mitjançant troians bancaris avançats.

***Ransomware as a service* (RaaS): resistència als pagaments i tensions entre els ciberdelinqüents.** La resistència als pagaments de *ransomware* està provocant tensions en el model RaaS, impulsant el nombre d'atacs i la migració de ciberdelinqüents cap a altres grups.

Ciberatacs a les cadenes de subministrament provoquen fuites de dades massives a nivell global. 165 empreses afectades per la fuita de dades històrica a Snowflake, provocada per l'ús d'unes credencials robades i per l'absència d'autenticació de doble factor (2FA).

Augment dels fraus dirigits alimentats per les fuites de dades massives. Els fraus s'intensifiquen durant el període de vacances a través d'estafes que ofereixen ofertes atractives, però falses, d'entrades a esdeveniments o allotjaments estivals.

Aliances entre grups cibercriminals intensifiquen els ciberatacs amb afectacions directes a Catalunya. Les aliances entre grups cibercriminals, com la Holy League, han intensificat els atacs DDoS contra països europeus i aliats de l'OTAN.

Intensificació de la guerra cibernètica en el conflicte a l'Orient Mitjà. Els ciberatacs tradicionals (DDoS, *wipers* i desinformació) han deixat pas a atacs destructius amb impacte al món físic, com l'explosió dels buscapersones de Hezbollah.

Els ciberdelinqüents posen el dispositiu mòbil en el punt de mira de les estafes. Els fraus cibernètics tenen el mòbil com a vector d'entrada principal, combinant atacs per correu electrònic, SMS, xarxes socials o trucades de veu per enganyar les víctimes.

El robatori de dades continua sent un maldecap en el sector sanitari. Els robatoris de dades personals i mèdiques del sector sanitari, sovint a partir d'atacs de *ransomware*, suposen l'extorsió amb l'amenaça de publicar-les i la filtració de dades sensibles.

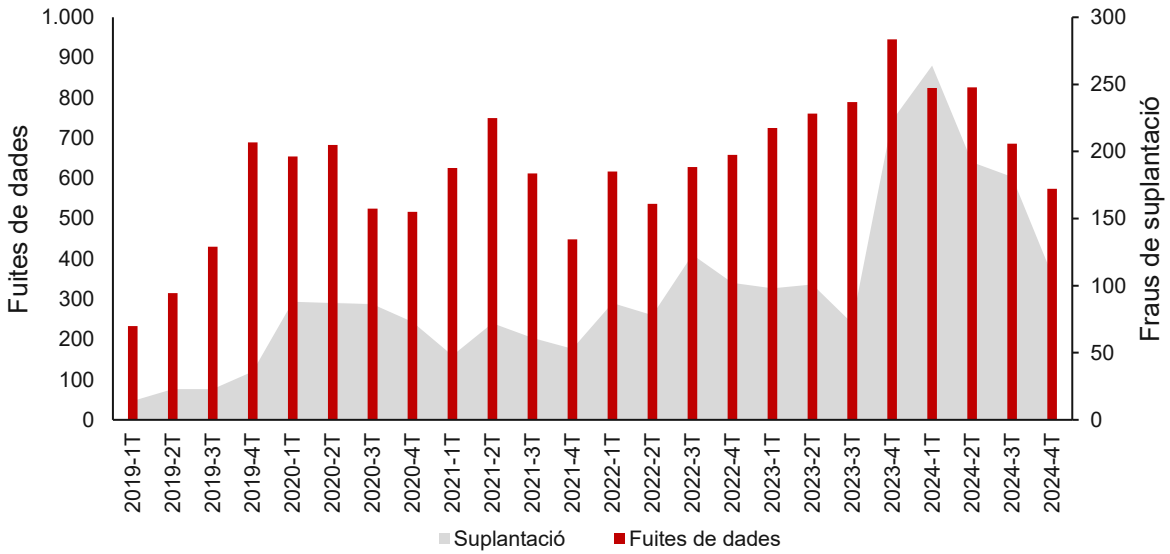
2024, any rècord en *ransomware*. El 2024 ha marcat un rècord d'incidents de *ransomware*, amb atacs centrats en sectors crítics i la demostració que els cibercriminals són capaços d'industrialitzar els atacs.

Font: Agència de Ciberseguretat de Catalunya

Principals tendències en ciberseguretat del 2024: les fuites de dades impulsen que els ciberfraus augmentin i es tornin més sofisticats

Les fuites de dades personals alimenten el mercat negre i permeten als ciberdelinqüents elaborar ciberestafes sofisticades, dirigides i creïbles.

Evolució del nombre de notícies de fuites de dades i dels ciberfraus a través de suplantacions (2019-2024)



Es constata una correlació entre el nombre de notícies de fuites de dades i el de suplantacions. Així, després d'un pic en les fuites de dades, hi ha un increment en els fraus de suplantació.

El 2024 hi ha hagut un augment de fuites de dades que ha proporcionat als atacants accés a grans quantitats d'informació sensible, com ara dades personals, financeres i empresarials.

Les dades compromeses són venudes a la *dark web* i permeten mecanismes de frau a través de diferents mitjans (estafes multicanal) o combinant el món físic i el món digital (estafes híbrides) per fer-los més creïbles.

Les dades compromeses s'utilitzen per enviar atacs de *phishing*, *smishing* i *vishing* amb l'objectiu d'obtenir credencials. Aquestes credencials s'empren per entrar als seus comptes personals per cometre suplantacions o robar actius de valor.

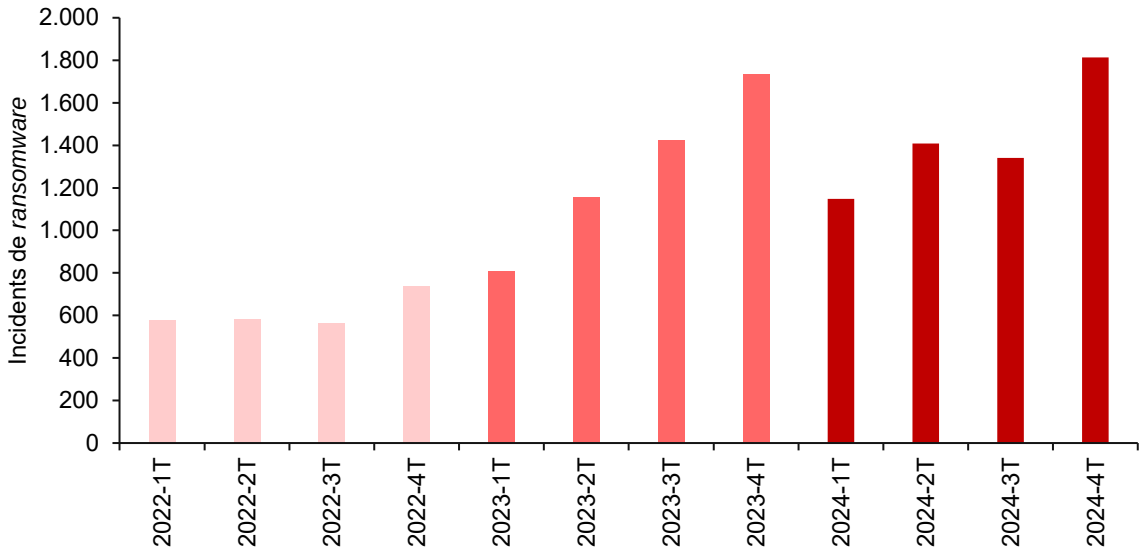
Els ciberdelinqüents fan servir la intel·ligència artificial generativa per elaborar de forma massiva missatges amb textos ben escrits, en qualsevol idioma i adaptats a cada víctima potencial per augmentar la probabilitat d'èxit.

Font: Agència de Ciberseguretat de Catalunya

Principals tendències en ciberseguretat del 2024: més incidents de *ransomware*, més grups cibercriminals i amb més robatoris de dades

La disminució del nombre de víctimes de *ransomware* que paguen rescat ha impulsat que els grups cibercriminals augmentin els atacs i explotin l'extorsió amb dades robades.

Evolució del nombre d'incidents de *ransomware* (2022 – 2024)



Durant el 2024 s'ha detectat un 11 % més d'incidents de *ransomware* que el 2023 i un 133 % més que el 2022.

Disminueix el percentatge de víctimes de *ransomware* que paguen rescats i, en resposta, els cibercriminals augmenten la seva activitat per preservar els ingressos.

La disminució del percentatge de pagaments ha creat tensions internes entre grups criminals que han derivat en la creació de nous grups. Aquest any s'han comptabilitzat fins a 48 nous grups de *ransomware*, més que qualsevol altre any.

Addicionalment, els grups de *ransomware* han potenciat els beneficis a partir del robatori de dades. Actualment, els actors del *ransomware* no només es limiten a xifrar les dades, sinó que les roben i posteriorment busquen lucrar-s'hi mitjançant l'extorsió i la venda a la *dark web*.

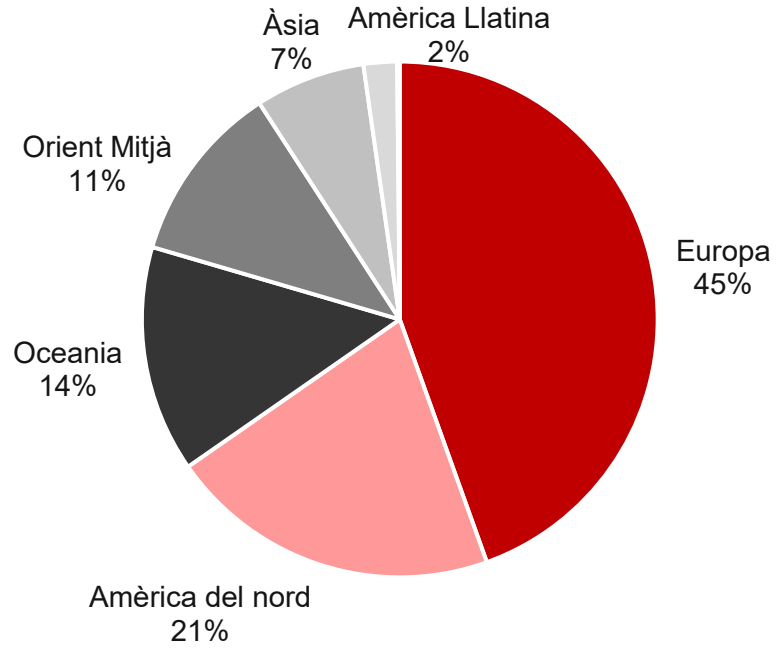
Els atacs de *ransomware* esdevenen massius i arriben a tot tipus d'organitzacions, fins i tot a les PIMES. Aquestes empreses sovint tenen menys recursos per invertir en ciberseguretat, fet que les pot convertir en objectius més vulnerables.

Fonts: Agència de Ciberseguretat de Catalunya, RansomDB

Principals tendències en ciberseguretat del 2024: les tensions geopolítiques a l'alça impulsen els atacs DDoS contra Europa

Els ciberatacs geopolítics han evolucionat de l'espionatge a les accions destructives i a la desinformació, afectant no només els països en conflicte, sinó també aquells que es posicionen ideològicament.

Distribució dels atacs DDoS per regió (2024)



Aquest 2024, Europa ha estat la regió més afectada per atacs DDoS, per sobre d'Amèrica del Nord, la regió més afectada fins al moment.

Els atacs amb motivacions geopolítiques són utilitzats per grups i per nacions per desestabilitzar adversaris, per mostrar poder mitjançant ressò propagandístic o per accedir a informació confidencial i personal.

El 2024 han destacat els atacs DDoS: diferents grups cibercriminals organitzats, amb ideologia contrària a l'OTAN, han creat una aliança (Projecte DDoSia) per atacar la disponibilitat de pàgines web de diferents països per generar un ressò propagandístic.

En el context de conflictes geopolítics, els atacs cibernètics es dirigeixen tant als països en conflicte com a aquells que no hi estan directament implicats però que s'han posicionat públicament. Les guerres cibernètiques no tenen fronteres.

En l'àmbit geopolític, els atacs cibernètics destructius amb impacte en el món físic i en la vida de les persones han pujat de nivell. En són un exemple la detonació de dispositius electrònics a l'Orient Mitjà i els centenars de víctimes.

Font: Agència de Ciberseguretat de Catalunya

Fets rellevants del 2024

INTERNACIONALS		CATALUNYA
McAfee presenta un escut IA contra *deepfakes* d'àudio **IA**	**Gen. 24**	Veolia, propietària d'Aigües de Barcelona, víctima d'atac de *ransomware* ***Ransomware***
Estafadors utilitzen un *deepfake* per robar 25 milions de dòlars **Frau**	**Feb. 24**	Escaneig de l'iris a canvi de criptomonedes en centres comercials catalans **Privacitat**
Atac cibernètic sense precedents a 800 webs de ministeris francesos **DDoS**	**Mar. 24**	Alerta d'una campanya d'SMS fraudulents de l'Agència Tributària per retornar-te diners **Frau**
AT&T confirma la filtració de dades de 73 milions de clients **Filtració de dades**	**Abr. 24**	Un ciberatac compromet dades personals de famílies i dels centres educatius catalans **Filtració de dades**
La Universitat de Siena, víctima del *ransowmare* ***Ransomware***	**Mai. 24**	Desmantellament d'una xarxa de ciberdelinqüents a la Costa Daurada **Accions Policials**
El ciberatac a Snowflake provoca una fuita de dades històrica **Fuita de dades**	**Jun. 24**	Esquerra Republicana, objectiu dels ciberatacants **Filtració de dades**
Un ciberatac de *ransomware* paralitza 40 museus durant els Jocs Olímpics ***Ransomware***	**Jul. 24**	Grups afiliats al projecte DDoSia ataquen pàgines web d'institucions catalanes **DDoS**
L'FBI desmantella una granja de bots russos que difonia desinformació a nivell mundial **Accions policials**	**Ago. 24**	El servei sanitari català, paralitzat a causa de l'incident de CrowdStrike **Disponibilitat**
Un atac *ransomware* força el tancament temporal d'una escola al Regne Unit ***Ransomware***	**Set. 24**	L'Agència de Residus de Catalunya pateix un ciberatac ***Ransomware***
Desenvolupador de Pokémon, víctima d'un ciberatac que filtra més d'1 TB de dades **Filtració de dades**	**Oct. 24**	Una estafa de suplantació costa a la víctima un total de 23.000 € **Frau**
Memorial Hospital and Manor, víctima d'un atac de *ransomware* ***Ransomware***	**Nov. 24**	Investigació pel robatori de dades a l'aplicació La Meva Salut **Robatori de credencials**
Noves tàctiques per desplegar atacs de *ransomware* ***Ransomware***	**Des. 24**	Desmantellada a Osona una organització criminal que suplantava bancs **Accions policials**

Font: diverses fonts

Xifres dels ciberatacs amb impacte a Catalunya el 2024

4 %

Pugen els ciberincidents a Catalunya

Les notícies d'incidents de ciberseguretat a Catalunya han incrementat un 4 % respecte de l'any anterior.

3 %

Menys *ransomware* al sector públic

Segons l'APDCAT el registre de notificacions d'atacs *ransomware* ha passat del 19 % l'any anterior al 3 % aquest any.

35 %

Conscienciació ciutadana envers els seus drets

Aquest any l'APDCAT ha rebut un 35 % més de denúncies i de reclamacions per incompliments de la normativa de protecció de dades.

60 %

Majoria de fuites de dades per errors humans

Segons l'APDCAT el 60 % de les filtracions de dades en institucions públiques catalanes han estat causades per errors humans.

1a

Catalunya, líder en denúncies de ciberestafes

Catalunya ha destacat per ser la comunitat autònoma amb més denúncies d'estafes informàtiques, amb un total de 71.772.

95 %

Les estafes informàtiques predominen

Les estafes informàtiques denunciades a Catalunya representen el 95 % de tota la cibercriminalitat enregistrada.

67 %

Els càrrecs bancaris fraudulents són les ciberestafes més habituals

Les notícies de fraus financers cap a la ciutadania incrementen un 55 % respecte de l'any anterior.

24 %

IP infectades a Catalunya

El 24 % de les IP infectades de Catalunya tenen origen en el *malware* RootSTV dissenyat per a Smart TV amb versions antigues d'Android.

Fonts: APDCAT, Bitsight, Mossos d'Esquadra, Agència de Ciberseguretat de Catalunya

Principals prospectives per al 2025

Ciberestafes

- Les fuites de dades personals s'han succeït de manera alarmant, una situació que presagia un 2025 ple d'estafes cibernètiques que, gràcies a l'ús d'aquestes dades, esdevindran cada vegada més sofisticades. I gràcies a la intel·ligència artificial (IA), les estafes podran ser personalitzades i massives.

Intel·ligència artificial

- L'IA també serà clau en la ciberseguretat per lluitar contra ciberatacs complexos, ja que pot aportar eines avançades per a la detecció i per a la resposta automàtica. Aquesta tecnologia permetrà una millora en la seguretat de les xarxes i la detecció precoç de comportaments sospitosos.

Cadenes de subministrament

- L'increment de la connectivitat i la complexitat de les cadenes de subministrament fomentaran els riscos cibernètics. Fabricants i organitzacions continuaran apostant per l'adopció de models de ciberseguretat de confiança zero (*zero trust*).

Geopolítica

- El creixent nombre de conflictes geopolítics potenciarà una nova onada de ciberatacs destructius, incloent-hi DDoS i *wipers* i altres variants que evidenciaran la capacitat de causar danys reals en el món físic.

Ransomware

- El *ransomware* és probablement la ciberamenaça més important per a les organitzacions i continuarà evolucionant per tal d'aconseguir mantenir els ingressos. L'extorsió a través del robatori de dades, en què no només s'encripta la informació sinó que també s'amenaça de divulgar-la, suposarà una pràctica eficaç.

Normatives

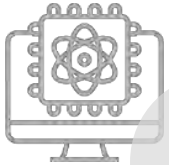
- La regulació en ciberseguretat exigirà noves peticions en matèria de ciberseguretat, en línia amb les amenaces cibernètiques emergents. Per a tota mena d'organitzacions, el 2025 serà un any clau per a l'adaptació a noves regulacions significatives en ciberseguretat.

Font: Agència Catalana de Ciberseguretat

5. La quàntica i la ciberseguretat

Tecnologies quàntiques

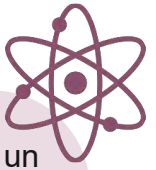
Les **tecnologies quàntiques** són un conjunt de tecnologies emergents que aprofiten els principis de la mecànica quàntica, una branca de la física que descriu el comportament de la matèria a nivell atòmic i a nivell subatòmic.



La **computació quàntica** és una tecnologia emergent que aprofita les lleis de la mecànica quàntica per resoldre problemes massa complexos per als ordinadors clàssics. Els problemes complexos són problemes amb moltes variables que interactuen de maneres complicades. Aquestes màquines són molt diferents dels ordinadors clàssics que existeixen des de fa més de mig segle.

La **comunicació quàntica** és un camp de la física quàntica aplicada estretament relacionada amb el processament de la informació quàntica. Es tracta de codificar la informació en estats quàntics de la llum per a la transmissió d'informació i per habilitar aplicacions disruptives en criptografia.

La comunicació quàntica abasta una àmplia gamma de tecnologies i d'aplicacions que van des d'experiments de laboratori d'última generació fins a la realitat comercial. Té algunes de les tecnologies quàntiques més madures en distribució de claus quàntiques (QKD) i generadors de nombres aleatoris quàntics (QRNG).



Dins de la tecnologia quàntica, un **sensor quàntic** utilitza propietats de la mecànica quàntica, com ara l'entrellaçament quàntic, la interferència quàntica i l'estrenyiment de l'estat quàntic, que han optimitzat la precisió i que superen els límits actuals de la tecnologia del sensor. Aquesta tecnologia detecta amb molta precisió els canvis de moviment, així com els camps magnètics i elèctrics, tot millorant enormement la capacitat de mesurar i de comprendre l'entorn.

Font: elaboració pròpia a partir d'IBM, MIT Technology review, Quside i PwC: Quantum Technology Monitor

Impacte de les tecnologies quàntiques en la ciberseguretat

Les tecnologies quàntiques poden suposar una amenaça per al xifratge de les dades actuals, però també poden fer millorar la ciberseguretat.

Els ordinadors quàntics representen una amenaça important per als estàndards de xifratge actuals com RSA i ECC, que actualment protegeixen moltes comunicacions i moltes dades.

Algorismes com el de Shor permeten als ordinadors quàntics trencar aquests mètodes de xifratge, cosa que podria comprometre dades sensibles a tot el món.

Les tecnologies quàntiques poden millorar la ciberseguretat mitjançant innovacions com la distribució de claus quàntiques (QKD) i la generació de nombres aleatoris quàntics (QRNG), que proporcionen una comunicació ultrasegura i mètodes criptogràfics més forts. Per la seva banda, els algorismes post-quàntics protegeixen l'emmagatzematge de dades.

Solucions per al risc quàntic

Criptografia postquàntica

Desenvolupament i implementació d'algorismes de seguretat quàntica que siguin segurs contra atacs quàntics suportats per ordinador.

Considerada la solució líder per a les amenaces quàntiques al xifratge per la seva familiaritat com a extensió dels sistemes actuals.

Segura contra atacs quàntics coneguts.

Implementable dins de la infraestructura existent.

Els esquemes PQC coneguts tenen inconvenients de rendiment, com ara claus llargues i temps de processament prolongat.
Els desenvolupaments en criptoanàlisi poden afectar la seva seguretat en el futur.

Distribució de claus quàntiques (QKD)

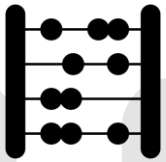
La QKD permet a dues parts crear una clau secreta compartida per xifrar i desxifrar missatges. Qualsevol intent d'interferir amb la comunicació quàntica serà detectat.

Augment de la protecció contra atacs de *recol·lecció ara i desxifrat posteriors*, ja que el protocol d'intercanvi de claus no és vulnerable als atacs quàntics.

Es pot combinar amb altres esquemes per a més seguretat.

No es poden desenvolupar algorismes per accedir a les claus intercanviades.

Alta inversió en maquinari especialitzat.
Limitacions potencials de distància pendents del desenvolupament del repetidor quàntic/QKD per satèl·lit.
Necessita un canal d'autenticació separat, afegint complexitat.



Generadors de Nombres Aleatoris i Xifratge (QRNG)

Els QRNG generen nombres veritablement aleatoris mitjançant processos indeterministes, tot oferint una seguretat superior en el xifratge de dades.

Mentre que els RNG (generadors de nombres aleatoris) clàssics es deriven d'alguna font d'entropia (com ara el soroll tèrmic), els QRNG són inherentment aleatoris.

La possibilitat de prova de l'aleatorietat (aleatorietat certificable) per a algunes implementacions.

Algunes aplicacions requereixen repetibilitat, cosa que no és possible per a QRNG.
Difícil quantificar la millora de la seguretat.

Font: elaboració pròpia a partir de KPMG, Deloitte, CEPS (Centre for European Policy Studies), Telefónica i World Economic Forum

Conscienciar sobre l'amenaça quàntica i entendre el risc

01.

Criptografia

Revisar els sistemes criptogràfics per crear una infraestructura dinàmica, adaptable a les canviants necessitats empresarials i de seguretat.

02.

Cripto-agilitat

Crear eines per actualitzar de manera eficient els algorismes, els paràmetres i les tecnologies criptogràfics quan sigui necessari.

03.

Ecosistema de ciberseguretat

Col·laboració amb administració, associacions i indústria per conèixer els avenços en computació quàntica, criptografia i riscos.

04.

Higiene de ciberseguretat

Protegir les dades sensibles de totes les amenaces, inclosos els futurs riscos de la computació quàntica. Tot i que l'amenaça pot semblar llunyana, les organitzacions han d'equilibrar les inversions en mitigació del risc quàntic amb altres prioritats de ciberseguretat.

Font: elaboració pròpia a partir de KPMG, Deloitte, CEPS (Centre for European Policy Studies), Telefónica i World Economic Forum

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, l'Estratègia de Ciberseguretat de la UE reforça la resposta col·lectiva davant ciberatacs, protegeix serveis essencials, promou l'autonomia tecnològica i impulsa la cooperació internacional per garantir la seguretat al ciberespai.

Legislació i certificació

- Directiva sobre la seguretat de les xarxes i sistemes d'informació (Directiva SRI)
- Reglament de Ciberresiliència
- Llei de Ciberseguretat
- Reglament de Cibersolidaritat

Inversió

- Next Generation
- R+D+I: Horizon Europe
- Programa Europa Digital
- InvestEU

Orientació normativa

- Pla director per a una resposta coordinada als principals ciberatacs
- Unitat Cibernètica Conjunta
- Desplegament segur de la 5G a la UE
- Garantir processos electorals

Habilitats i sensibilització

Davant la manca d'experts en ciberseguretat, la Comissió Europea està prenent mesures per estimular el desenvolupament de capacitats en matèria de ciberseguretat, com la Cybersecurity Skills Academy posada en marxa el 2023.

Comunitat cibernètica

- ENISA
- 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

Ciberpolítica

- Ciberdiplomàcia
- Ciberdefensa
- Desenvolupament de capacitats en tercers països
- Diàlegs cibernètics amb socis com els EUA, Ucraïna o el Japó.

Font: Comissió Europea

Reglament de Ciberresiliència

El Reglament de Ciberresiliència és una norma de la Unió Europea que té l'objectiu de protegir els consumidors i les empreses que comprin o que utilitzin productes amb un component digital.

La llei garanteix el següent:

- Normes harmonitzades en 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 els minoristes de tots els productes connectats directament o indirectament a un altre dispositiu o a una altra xarxa, amb alguna excepció.

El reglament va entrar en vigor el 10 de desembre del 2024 i serà aplicable de forma general des de l'11 de desembre del 2027.

Reglament de Resiliència Operativa Digital (DORA)

El Reglament 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 del risc TIC, propi i de tercers.
- Incidents i notificacions d'incidents relacionats amb les TIC.
- Proves de resiliència operativa digital, que comprenen una varietat d'avaluacions, de proves, de metodologies, de pràctiques i d'eines.
- Intercanvi d'informació entre entitats financeres.
- Monitorització contínua del funcionament dels sistemes i de les eines.

Aquesta norma afecta, entre altres, les següents empreses:

- Entitats de crèdit.
- Entitats de pagament i de diners electrònics.
- Entitats de serveis d'inversió.
- Proveïdors de serveis de criptoactius.
- Altres entitats financeres: gestors de fons, asseguradores, etc.

El reglament és plenament aplicable des del 17 de gener del 2025.

Esquema Nacional de Seguretat (ENS)

L'ENS és una norma de l'Estat espanyol amb 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, la detecció i la correcció.
- Promoure un tractament homogeni de la seguretat.
- Servir de model de bones pràctiques.

Aquesta norma afecta tot el sector públic (segons l'article 2 de la llei 40/2025), així com els 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 hagut d'adequar-se 24 mesos després de l'entrada en vigor de la norma, el 3 de maig del 2024.

Directiva sobre xarxes i sistemes d'informació 2 (NIS2)

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 la informació per a l'economia i per a la societat.
La Directiva engloba procediments que inclouen la:

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

Aquesta norma afecta entitats mitjanes i grans de sectors crítics per a l'economia i per a 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 pública en l'àmbit local.

Fins al 17 d'abril del 2025 els estats membres han d'elaborar una llista amb les entitats impactades i revisar-la almenys cada 2 anys.

7. La ciberseguretat a Catalunya

Mapatge empresarial de la ciberseguretat a Catalunya (I)

557 empreses

+7,9 %[1]

1.473 milions d'euros

+18,4 %[1]

10.672 llocs de treball

+12,8 %[1]

- El **82,6 %** són PIMES.
- El **57,1 %** facturen més d'1 milió d'euros i el **26,2 %** més de 10 milions d'euros.
- El **26,0 %** tenen menys de 10 anys.
- El **10,6 %** són startups.
- El **26,4 %** són exportadores.
- El **16,9 %** són filials d'empreses estrangeres.

Per **segments**, les empreses se situen a:

Protegir	**90,3 %**
Identificar	**62,5 %**
Detectar	**41,8 %**
Respondre	**35,5 %**
Recuperar	**23,0 %**

238 empreses (42,7 %) també desenvolupen solucions lligades amb la **intel·ligència artificial**

[1] els creixements són respecte de les dades del mapatge elaborat l'any anterior.

Nota: les dades de les empreses fan referència al 2024; les de facturació i nombre de treballadors, al 2023 (o darreres disponibles).

Font: ACCIÓ

Generalitat de Catalunya

Mapatge empresarial de la ciberseguretat a Catalunya (II)

Mapatge complet

557 empreses

Generalitat de Catalunya

Mapatge empresarial de la ciberseguretat a Catalunya: segment identificar

Identificar

348 empreses

Generalitat de Catalunya

Mapatge empresarial de la ciberseguretat a Catalunya: segment protegir

Protegir

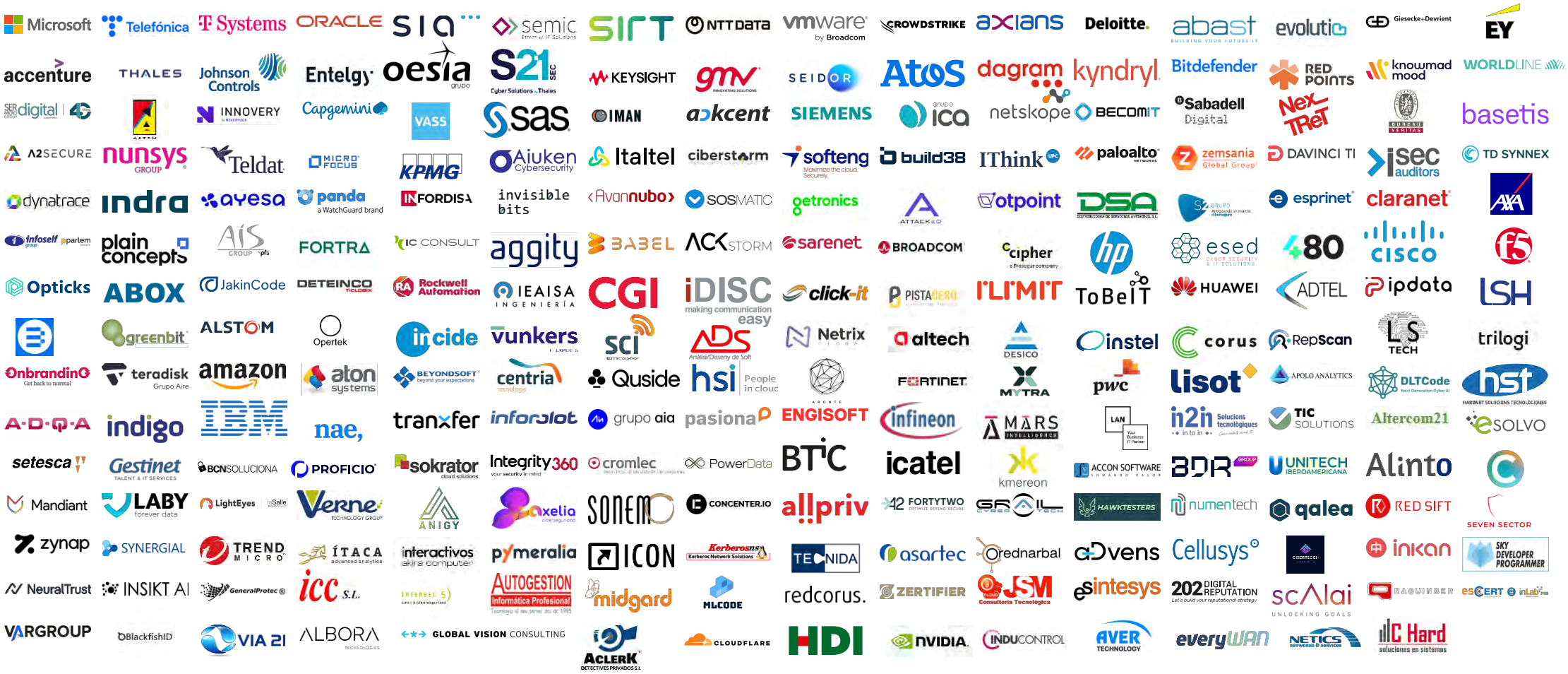
503 empreses

Generalitat de Catalunya

Mapatge empresarial de la ciberseguretat a Catalunya: segment detectar

Detectar

233 empreses



Generalitat de Catalunya

Mapatge empresarial de la ciberseguretat a Catalunya: segment respondre

Respondre

198 empreses

Generalitat de Catalunya

Mapatge empresarial de la ciberseguretat a Catalunya: segment recuperar

Recuperar

129 empreses

Generalitat de Catalunya

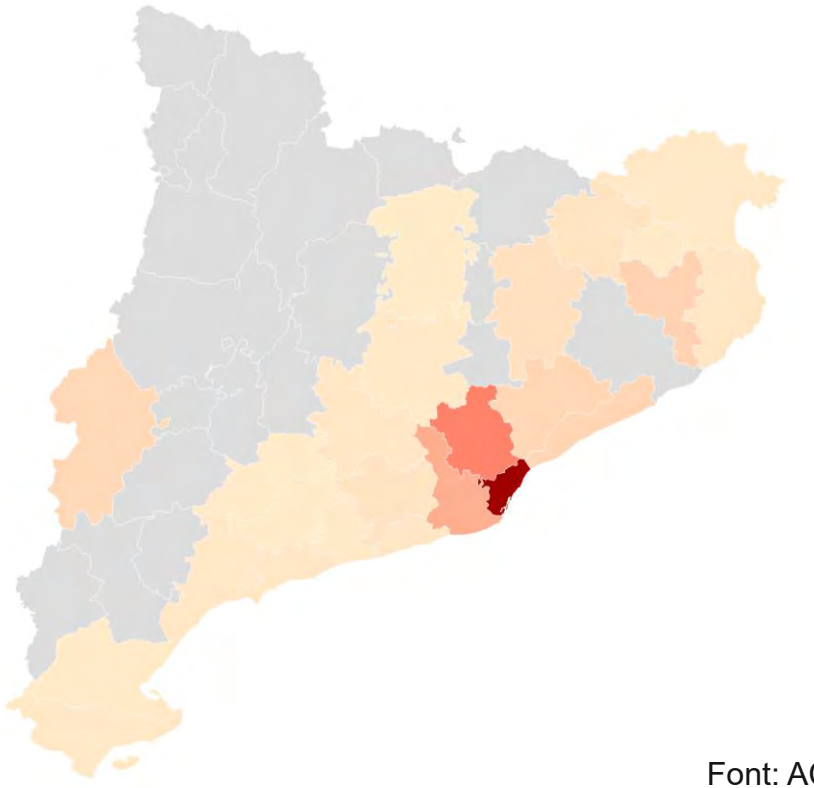
Localització de les empreses catalanes de ciberseguretat

El 64,7 % de les empreses de ciberseguretat es troben a l'Àrea Metropolitana de Barcelona (AMB).

Per ciutats, destaquen Barcelona (322), Sant Cugat del Vallès (22), Terrassa (15), Lleida (12), l'Hospitalet de Llobregat (11), Sabadell (11) Girona (10) i Cerdanyola del Vallès (9).

Comarca	Nombre d'empreses	% sobre el total
Barcelonès	340	61,0 %
Vallès Occidental	69	12,4 %
Baix Llobregat	41	7,4 %
Gironès	17	3,1 %
Vallès Oriental	15	2,7 %
Maresme	14	2,5 %
Segrià	12	2,2 %
Resta	49	8,7 %
Total	**557**	**100 %**

Repartiment comarcal de les empreses de ciberseguretat



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

Font: ACCIÓ

Empreses catalanes que fusionen la ciberseguretat amb la intel·ligència artificial

Intel·ligència artificial

La intel·ligència artificial està transformant la ciberseguretat, millorant la protecció de dades, optimitzant els algoritmes per a una resposta més ràpida davant les amenaces i desenvolupant solucions per fer front a ciberatacs cada cop més precisos, amb les empreses catalanes a l'avantguarda d'aquesta revolució.

238 empreses, el **42,7 %** del total d'empreses de ciberseguretat

Principals aplicacions per segments:

Identificar	ANKO, CROWDSTRIKE, NexTRet, otpoint, paloalto NETWORKS
Protegir	FORTINET, FUJITSU, Mitek, netskope, RED SIFT
Detectar	APOLO ANALYTICS, BlackfishID, NeuralTrust, RED POINTS, WISE SECURITY
Respondre	asnet, f5, JakinCode, MLCODE, T Systems
Recuperar	aggity, Bitdefender, build38, NTT DATA, RepScan

Nota: imatge il·lustrativa parcial. Les empreses poden estar ubicades en més d'un dels segments.

Font: ACCIÓ

Empreses catalanes que fusionen la ciberseguretat amb tecnologies quàntiques

Tecnologies quàntiques

Les tecnologies quàntiques milloren la ciberseguretat amb criptografia quàntica, pràcticament impenetrable gràcies a la superposició i a l'entrellaçament quàntic, i ajuden a contrarestar els riscos de la computació quàntica, que podria desxifrar la criptografia tradicional, i així garantir la protecció de les dades en el futur.

27 empreses, el **4,8 %** del total d'empreses de ciberseguretat

Principals empreses:

cellnex · gmv INNOVATING SOLUTIONS · IBM · KEYSIGHT · LUXQUANTA · oesia grupo · Quside · SATELIOT Space · Connecting · 5G IoT · scAlai UNLOCKING GOALS · sener

Nota: imatge il·lustrativa parcial.

Font: ACCIÓ

Agents de l'ecosistema de la ciberseguretat

Centres tecnològics i instituts de recerca

Estudis de grau, de màster i de postgrau

Estudis d'FP

Associacions i esdeveniments

CSIRT/CERT

Institucions i administració pública

Generalitat de Catalunya

Iniciatives per potenciar la ciberseguretat a Catalunya

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

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

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, de les tecnologies, del coneixement i de l'experiència als àmbits d'actuació de l'Agència.

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 per a expositors.

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

DCA Digital Catalonia Alliance

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

ASCICAT
ASSOCIACIÓ DE CIBERSEGURETAT DE CATALUNYA

Entitat sense ànim de lucre formada per empreses de la cadena de valor del sector de la ciberseguretat a Catalunya.

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 per a 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 de 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 per augmentar el nivell de seguretat de les xarxes i dels 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 del 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

Inversió estrangera directa (IED) en ciberseguretat a Catalunya

La IED en ciberseguretat a Catalunya ha augmentat exponencialment durant el darrer quinquenni arrel de la creixent digitalització provocada per l'esclat de la pandèmia de la COVID-19.

	2015-2019	2020-2024	
Projectes	6	**12**	**x2**
Capex (M€)	24	**207**	**x9**
Llocs de treball	267	**976**	**x4**

Empreses inversores durant el darrer quinquenni

netskope · T Systems · Schneider Electric · CROWDSTRIKE · RED SIFT · veriff · getronics · dynatrace · FUJITSU · build38 · relyens · aDvens

Font: elaboració pròpia a partir d'fDi Markets

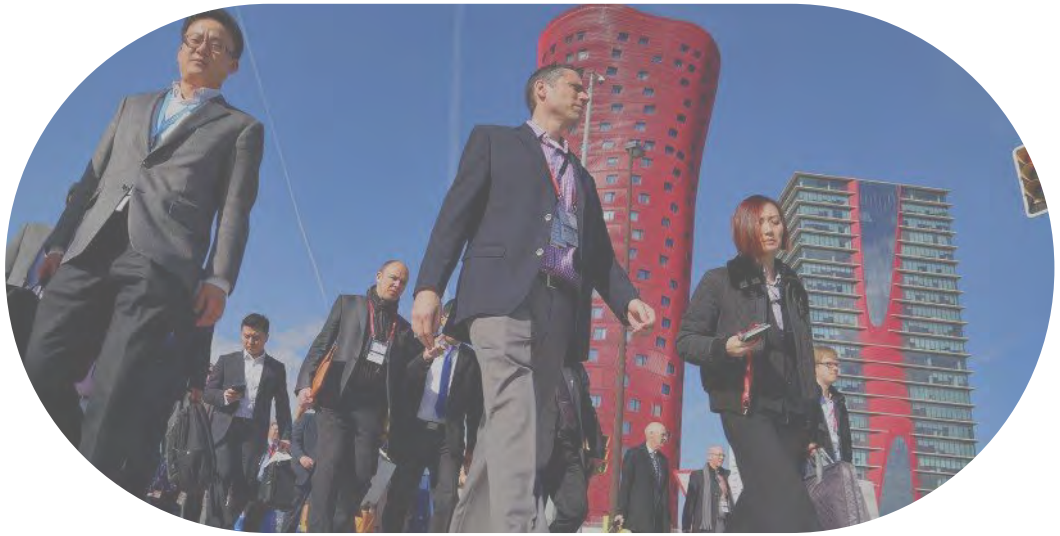
Hubs tecnològics a Catalunya enfocats a la ciberseguretat

160 *hubs* tecnològics
d'empreses estrangeres

+9 % respecte de l'any anterior

6.200 nous llocs de treball

Impacte econòmic de **2.879 M€**



El 36 % dels *hubs* es dediquen a la ciberseguretat

La ciberseguretat és la **segona tecnologia més implantada pels nous *hubs***, amb el 29 % del total.

La ciberseguretat es troba **entre els tres perfils professionals més sol·licitats** als *hubs*.

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

Nota: les dades fan referència al 2024.

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

Activitats de recerca catalana en ciberseguretat a l'Horizon Europe

15 projectes

11,3 milions d'euros

3,2 % del total europeu

26,1 % del total a l'Estat espanyol

20 institucions

5a regió europea en finançament a l'Horizon Europe

Nota: s'hi inclouen els projectes de l'Horizon Europe (2022-2024) relacionats amb la ciberseguretat (*computer security* i *network security*).

Font: Horizon Europe

Continua la falta de talent en ciberseguretat

Necessitat de professionals de la ciberseguretat

Segons (ISC)[2], el nombre de professionals de la ciberseguretat es manté estable al món i la bretxa de professionals creix en un **19 %**: més de 4 milions de vacants al món.

A **Catalunya**, com a Europa, s'estima que la bretxa augmenta en un **12,8 %**, de manera que la necessitat de professionals no coberta augmenta i es situa en unes **13.500** persones.

	Professionals de la ciberseguretat existents		Necessitat de professionals no coberta	
	vs. 2023	2024	vs. 2023	2024
MÓN	+0,1 %	**5,45 M**	+19 %	**4,76 M**
EUROPA	-0,7 %	**1,3 M**	+12,8 %	**392 K**
CATALUNYA*	-0,7 %	**28 K**	+12,8 %	**13,5 K**

**Estimació*

Font: (ISC)2

Formació en ciberseguretat a Catalunya

45 centres d'estudi ofereixen **62 cursos** de formació professional en ciberseguretat

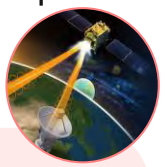
14 graus, màsters i postgraus de ciberseguretat

- ENTi — Grau en Ciberseguretat
- Institut de Formació Contínua IL3 UB — Màster en Ciberseguretat. Àmbit de la transformació digital
- OBS Business School — Màster en Seguretat de la Informació Empresarial
- ULC Barcelona — Postgrau en *Compliance* i Ciberseguretat
- Nuclio Digital School — Màster en Ciberseguretat
- telecos BCN — Màster en Ciberseguretat
- UOC Universitat Oberta de Catalunya — Màster en Ciberseguretat i Privadesa; Ciberseguretat en xarxes i sistemes
- Universitat Rovira i Virgili — Màster en Enginyeria de la Seguretat Informàtica i Intel·ligència Artificial
- UPC Universitat Politècnica de Catalunya BarcelonaTech — Màster en Direcció de Ciberseguretat; Màster en Aprenentatge Automàtic i Ciberseguretat per a Sistemes Connectats a Internet
- laSalle Universitat Ramon Llull — Màster en Ciberseguretat; Màster Universitari en Direcció i Gestió de la Ciberseguretat i Infraestructures Crítiques

Iniciatives quàntica – ciberseguretat a Catalunya

La quàntica pot impactar en diversos àmbits, especialment en el de la ciberseguretat. A Catalunya, s'estan desenvolupant iniciatives que integren aquestes tecnologies per reforçar la seguretat en les comunicacions.

QSunset



Sistema de distribució de claus quàntiques i *entanglement* mitjançant un satèl·lit d'òrbita baixa, que inclou pay-load per al satèl·lit i un telescopi receptor a l'estació terrestre.

6GQuCryptoLab

Instal·lació d'I2CAT per simular distribució de claus quàntiques (QKD) punt a punt i amb nodes de confiança, integrant protocols de variables discretes (DV) i contínues (CV) i escenaris de xarxes satèl·lit.

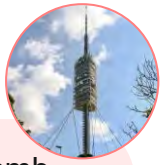
Qspace

Infraestructura per desenvolupar distribució de claus quàntiques i *entanglement* via satèl·lit, centrada en nanosatèl·lits i LEO amb càrrega útil quàntica i serveis 5G/6G.

Full de ruta criptografia quàntica

La Generalitat de Catalunya impulsa un projecte de 2 M€ per preparar la transició a la criptografia quàntica a les seves solucions TIC. El projecte inclou monitoritzar sistemes i crear normativa per a la criptografia quàntica.

Qollserola



Anell de ciberseguretat amb distribució de claus quàntiques (QKD) al voltant de l'àrea metropolitana de Barcelona.

ICFO · cellnex · Quside · LUXQUANTA

Node Barcelona – Q-Network

La Comissió Europea i l'Agència Espacial Europea estan impulsant l'EuroQCI, una xarxa de comunicació quàntica europea amb elements terrestres i espacials. Inicialment, es crearan nodes a ciutats com Barcelona, que es connectaran entre si en una segona fase.

EuroQCI · EUROQCI SPAIN · ICFO · cellnex

Font: ACCIÓ

8. Casos d’èxit a Catalunya

Casos d'èxit empresarials en ciberseguretat

BRONTOBYTE és una empresa especialitzada en la protecció de dades crítiques i en la continuïtat del negoci, gràcies a les seves plataformes de *backup* immutable i Disaster Recovery as a Service (DRaaS).

ZYNAP és una empresa especialitzada en solucions de protecció de dades crítiques i garantia operativa per a les empreses.

SONICWALL ajuda a crear, a escalar i a gestionar la seguretat en qualsevol combinació d'entorns tradicionals, híbrids i en el núvol, gràcies a la seva plataforma de tallafocs d'última generació.

SECRETS VAULT ha desenvolupat una eina que permet protegir i compartir informació sensible a partir de l'ús d'imatges en lloc de contrasenyes tradicionals.

QUSIDE és una empresa de tecnologia quàntica especialitzada en la generació, monitorització i processament d'aleatorietat, amb aplicacions en ciberseguretat i computació d'alt rendiment.

ZEROD ofereix un *marketplace* amb hackers ètics d'arreu del món que ofereixen els seus serveis cibernètics i d'assessoria a les empreses.

NEURALTRUST ofereix una plataforma que detecta vulnerabilitats, bloqueja atacs i monitoritza el rendiment i garanteix el compliment normatiu per a aquelles aplicacions d'IA generativa.

WISE SECURITY ofereix un catàleg de serveis en ciberseguretat que van des de la tecnologia *blockchain* fins a la ciberseguretat ofensiva, passant per signatura electrònica i la gestió de les vulnerabilitats de programari.

LUXQUANTA ofereix solucions de ciberseguretat basades en criptografia quàntica. El senyal quàntic transmès per fibra òptica genera claus criptogràfiques segures segons la física quàntica.

MITEK SYSTEMS està especialitzada en solucions tecnològiques per verificar identitats digitals i la veracitat de documents, utilitzant intel·ligència artificial, anàlisi biomètrica, visió per computació i aprenentatge profund.

Catalunya, ecosistema dinàmic en ciberseguretat

El **36 % dels 160 hubs tecnològics** d'empreses internacionals establerts a Catalunya es dedica a la ciberseguretat.

La ciberseguretat es troba entre els **tres perfils professionals més sol·licitats**.

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

Ecosistema empresarial local

557 empreses dedicades a la ciberseguretat, un creixement del **7,9 %** anual i un **58,2 %** més respecte del 2018.

Facturació de **1.473 M€** (+18,4 %) i **10.672 llocs de treball** (+12,8 %).

Hubs internacionals especialitzats

Aplicació de tecnologies emergents

238 empreses (42,7 %) desenvolupen **eines d'IA** i **27 empreses** (4,8 %) **tecnologies quàntiques**.

6 iniciatives per potenciar el desplegament de la **quàntica** lligada a la **ciberseguretat**.

Territori atractiu per desplegar la ciberseguretat

Els projectes d'**inversió estrangera** s'han **doblat** i la inversió s'ha multiplicat **x9** durant el darrer quinquenni.

netskope · T-Systems · Schneider Electric · CrowdStrike · Red Sift · veriff · getronics · dynatrace · Fujitsu · build38 · relyens · Devens

Ampli ecosistema de suport

Iniciatives que potencien la ciberseguretat a Catalunya

Agència de Ciberseguretat de Catalunya · Agència de Ciberseguretat de Catalunya – Centre de Competències i d'Innovació en Ciberseguretat · Barcelona Cybersecurity Congress · CYBERCAT · DIH4CAT Digital Innovation Hub de Catalunya · DCA Digital Catalonia Alliance · ASCICAT

Generalitat de Catalunya

Gràcies!

ACCIÓ Catalonia Trade & Investment

Generalitat de Catalunya

Passeig de Gràcia, 129
08008 Barcelona

accio.gencat.cat
catalonia.com

@accio_cat
@Catalonia_TI

/acciocat/
/invest-in-catalonia/

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

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:

Generalitat de Catalunya