Febrer del 2023. 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, febrer del 2023

Índex de continguts

1. Definició de ciberseguretat i importància per a la indústria

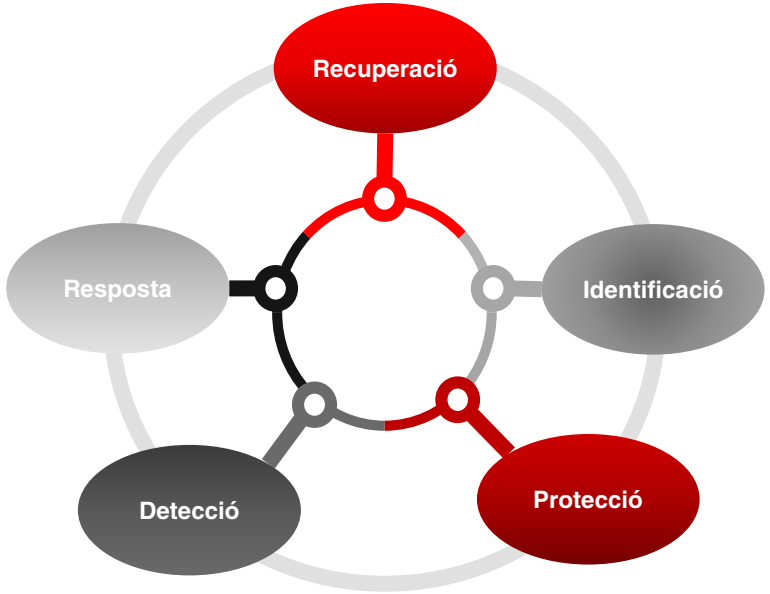
Definició de ciberseguretat

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 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 ser o bé confirma la font d'on 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 seva identificació, les accions de protecció, la detecció de ciberatacs, la resposta a incidents cibernètics i la recuperació.



Actua sobre:

Persones

Processos

Tecnologies

Magnituds del cibercrim

Es preveu que el cost del cibercrim a nivell mundial per al 2022 ha estat d'uns 7.000 M€.

El 2022, els ciberatacs han augmentat una mitjana d'un 50% respecte del 2021.

El 71% dels ciberatacs tenen motivació financera, seguida del robatori de propietat intel·lectual i l'espionatge.

Els cibercriminals han robat més de 3.000 M€ en criptovalors, sobretot d'*exchanges* i *bridges*.

El correu electrònic es consolida com el principal vector de distribució de *malware* i s'utilitza en l'inici del 84% dels ciberatacs.

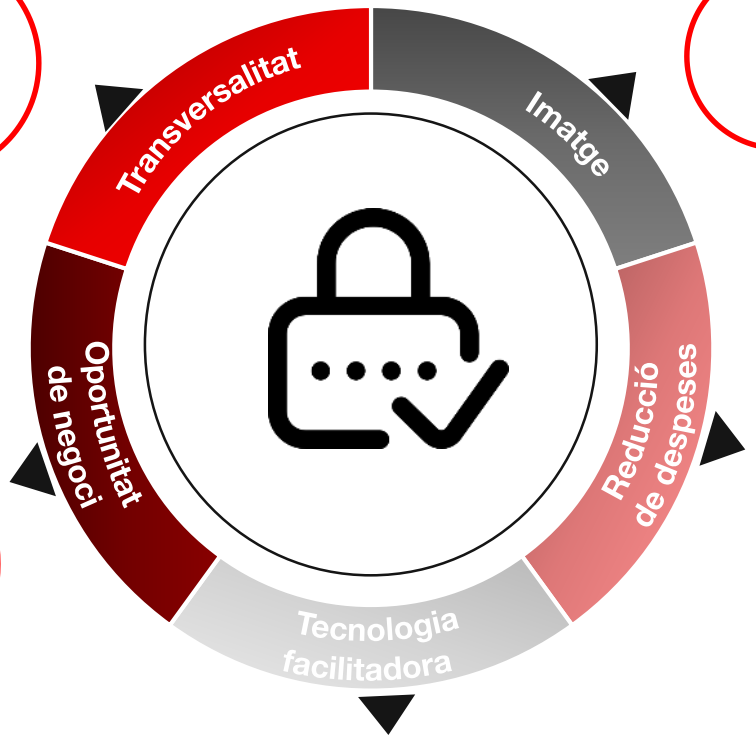
A la *dark web*, hi circulen 24.600 milions de credencials completes (usuari i contrasenya).

Fonts: Verizon, CheckPoint, Juniper i Cybersecurity Ventures

Importància de la ciberseguretat per a la indústria

La ciberseguretat afecta molts àmbits, des de governs i infraestructures fins a serveis financers, *smart cities*, processos productius i sistemes de salut.

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



Un entorn cada vegada més connectat permet generar noves empreses que desenvolupen tecnologies per a determinats tipus d'atacs i nous models de negoci basats en l'estudi de vulnerabilitats. 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 reinicis de sistemes, reparació de dispositius, fuites de dades que poden exposar informació privada o sensible i repercussions legals.

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

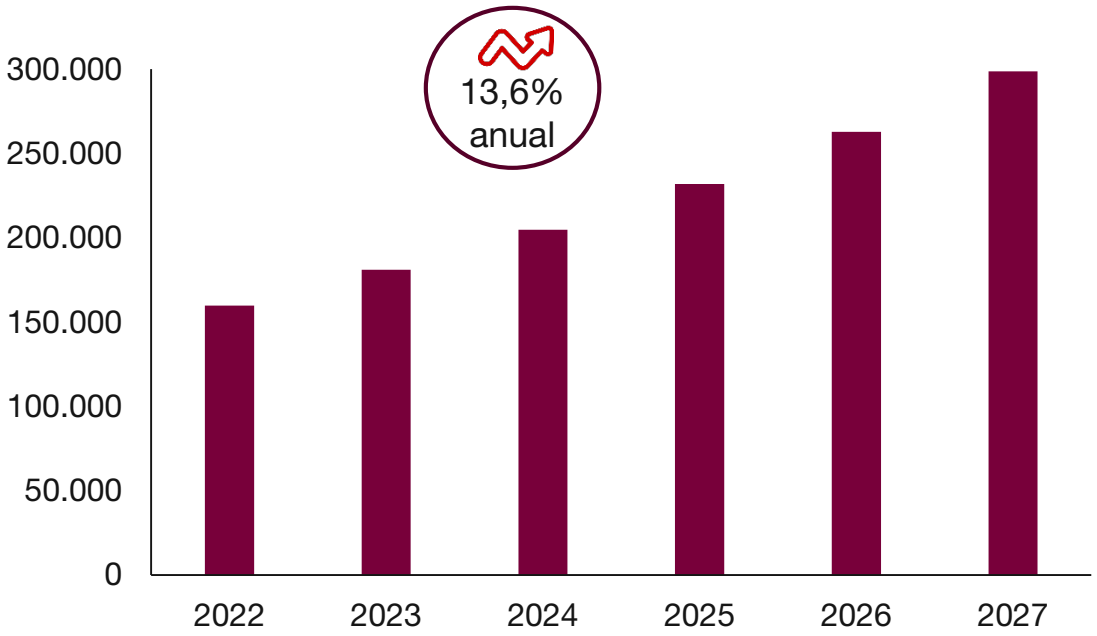
2. Principals magnituds mundials

Mercat mundial i perspectives de creixement de la ciberseguretat

La facturació mundial en ciberseguretat creixerà a un ritme del **13,6% anual** entre el 2022 i el 2027, fins els **298.700 M$**.

Facturació mundial de la ciberseguretat*

2022-2027, M$



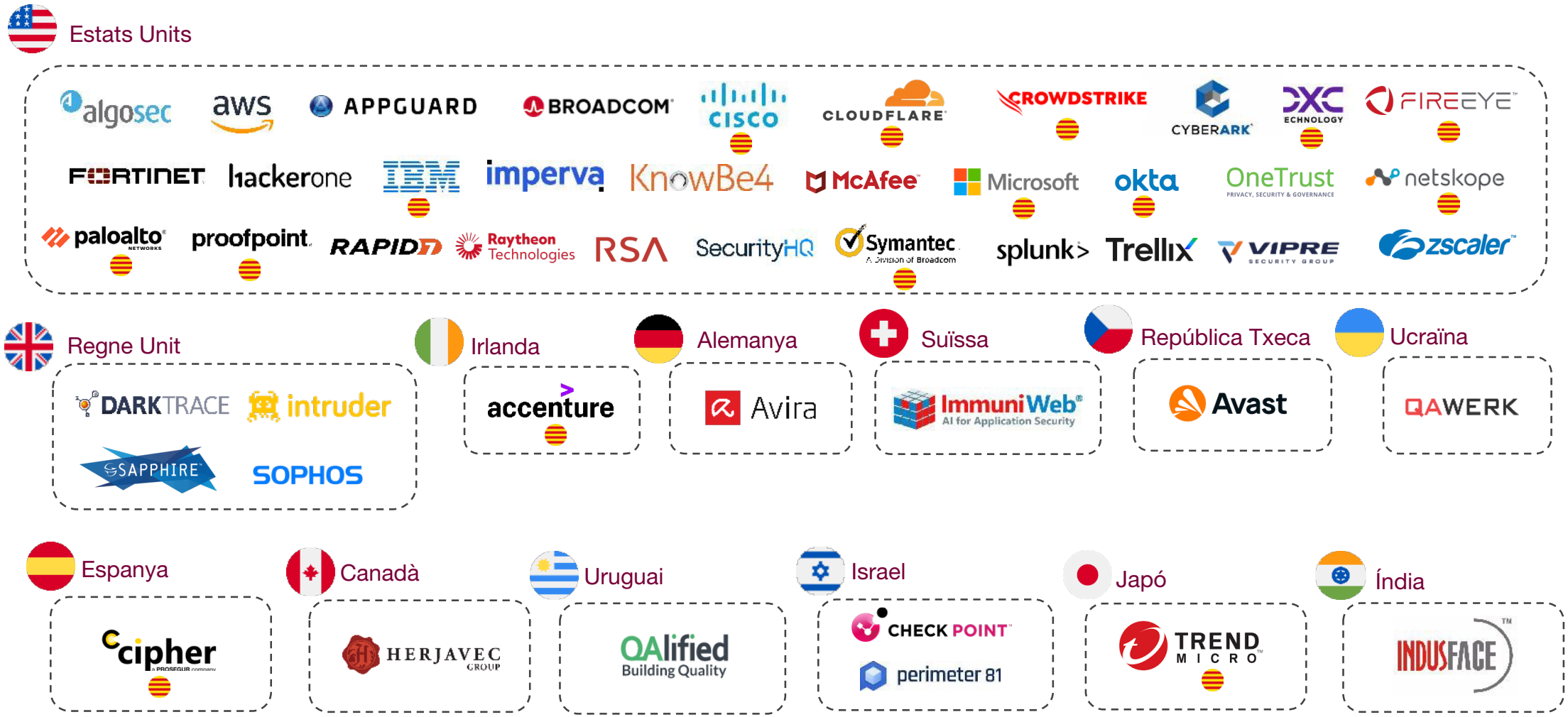
* *Previsió*

	Països	Facturació 2022 (M$)	Creixement anual 2022 – 2027 (%)
1	Estats Units	64.860	12,4%
2	Xina	14.050	17,5%
3	Japó	9.826	13,2%
4	Regne Unit	9.540	13,4%
5	Alemanya	6.436	12,8%
6	França	5.076	11,9%
7	Canadà	3.524	13,5%
8	Austràlia	3.519	13,3%
9	Rússia	3.215	8,4%
10	Corea del Sud	3.135	13,4%
11	Espanya	2.696	12,6%
12	Itàlia	2.439	11,5%
13	Brasil	2.369	15,1%
14	Països Baixos	2.295	12,9%
15	Índia	2.150	17,2%

Països ordenats per valor de mercat el 2022

Font: Statista

Empreses líders en ciberseguretat el 2022



Presència a Catalunya

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

Inversió Estrangera Directa (IED) en ciberseguretat

La IED en ciberseguretat durant el 2022 ha estat de **8.351 M€** i s'han creat **64.918 llocs de treball**. Durant el quinquenni 2018-2022, els Estats Units han estat el principal país d'origen de la IED, amb **19.817 M€**, i l'Índia, el principal receptor amb **3.835 M€**.

Inversió en ciberseguretat

Any	Projectes	Capital invertit (M€)	Ocupació generada
2018	183	8.163,1	16.695
2019	178	2.019,8	13.710
2020	147	3.837,1	12.163
2021	366	9.659,9	41.003
2022	398	8.351,3	64.918

Principals empreses inversores

CLOUDFLARE 7.957,8 M€

netskope 1.428,2 M€

DXC TECHNOLOGY 1.241,7 M€

Microsoft 959,2 M€

accenture 913,3 M€

Principals països d'origen de la IED

19.817,1 M€ | 1.451,0 M€ | 1.397,1 M€ | 1.369,0 M€ | 1.059,2 M€

999,7 M€ | 872,2 M€ | 750,0 M€ | 686,5 M€ | 588,7 M€

Principals països receptors de la IED

3.835,3 M€ | 2.687,1 M€ | 2.142,8 M€ | 2.094,9 M€ | 1.515,4 M€

1.289,3 M€ | 1.173,3 M€ | 930,7 M€ | 875,0 M€ | 844,6 M€

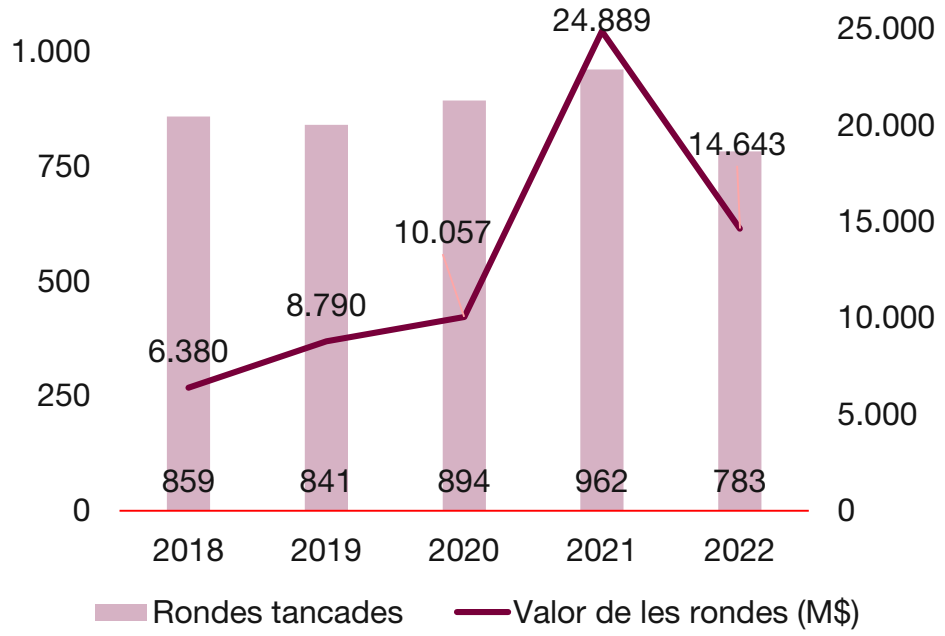
Nota: les dades fan referència al període 2018-2022

Font: elaboració pròpia a partir d'fDi Markets

Capital risc en startups de ciberseguretat

El 2022 ha tancat amb més de **14.600 M$ en capital risc en startups de ciberseguretat** al món, valor inferior al rècord marcat el 2021 però superior als anys anteriors. Les startups nord-americanes lideren el rànquing de manera molt destacada.

Rondes d'inversió en ciberseguretat



Nota: s'hi inclouen les rondes d'inversió «pre-seed», «seed» i les sèries A-J de les següents categories: «penetration testing», «network security», «intrusion detection», «identity management», «fraud detection», «e-signature», «cyber security» i «cloud security»; les dades fan referència al període 2018-2022.

Valor i nombre de rondes tancades als principals països

45 671 M$	**5.521 M$**	**2.340 M$**	**2.099 M$**	**2.093 M$**
2.307 rondes	336 rondes	317 rondes	119 rondes	131 rondes

Principals startups per valor de rondes tancades

LACEWORK	snyk	Fireblocks	Bolt	OneTrust
1.891 M$	**1.040 M$**	**1.039 M$**	**963 M$**	**933 M$**

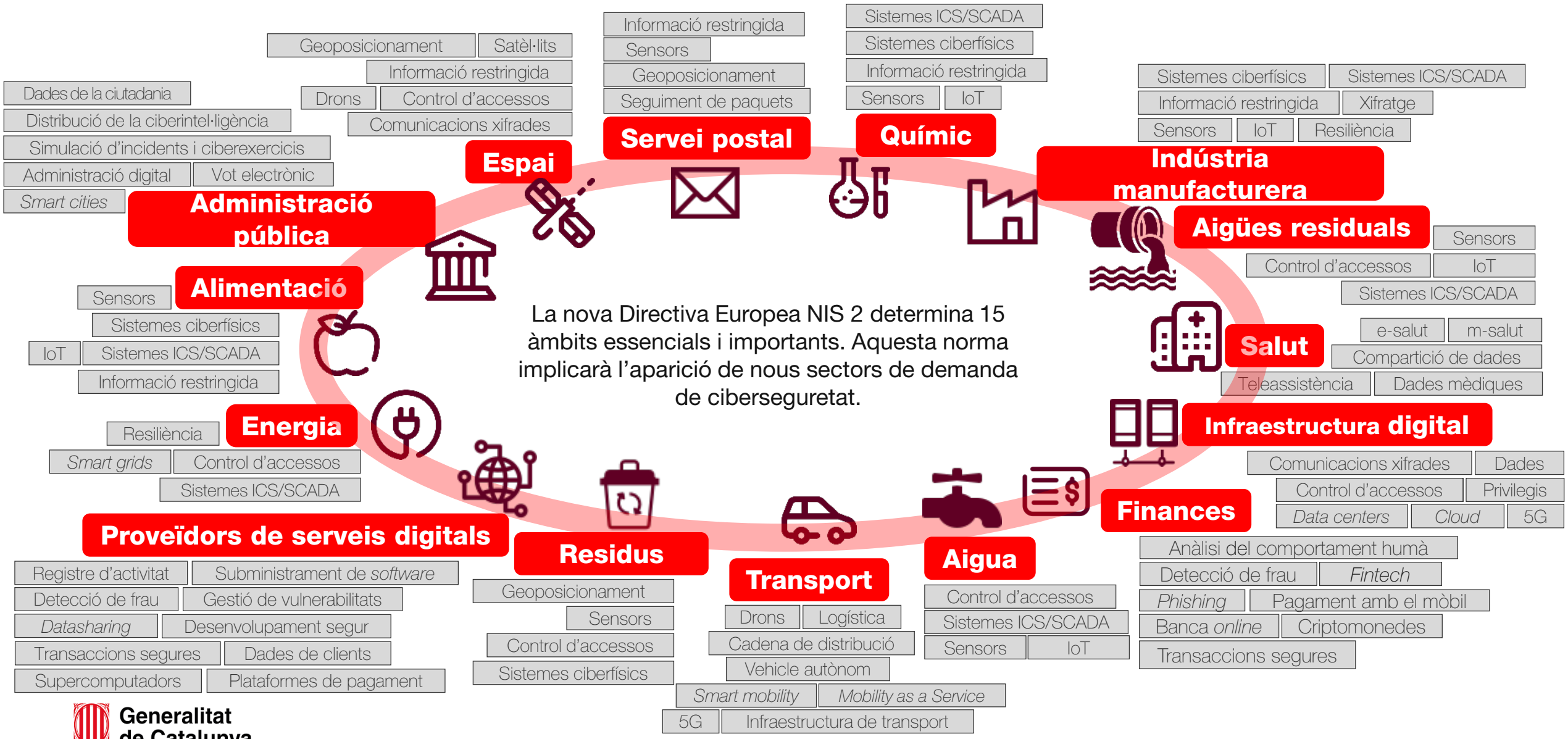
Principals inversors en capital risc

INSIGHT PARTNERS · ACCEL PARTNERS · Y Combinator · Bessemer Venture Partners · Lightspeed

Font: elaboració pròpia a partir de Crunchbase

3. Aplicacions prospectives per sector de demanda

Sectors de demanda



Generalitat de Catalunya

4. Tendències en ciberseguretat i impacte en els ODS

Principals tendències en ciberseguretat del 2022

La ciberguerra. El conflicte entre Rússia i Ucraïna ha fet el salt al ciberespai en forma de múltiples ciberatacs, no només entre els dos països, sinó que també ha afectat als seus aliats.

Atacs contra el sector energètic. En un context de crisi energètica a la UE, el sector energètic europeu ha estat objectiu de diversos ciberatacs que han posat en risc la seva operativa.

Evolució del *ransomware.* Les mesures de seguretat i l'aparició constant de nous operadors de *ransomware* augmenta la competència i els obliga a desenvolupar les seves capacitats.

Robatori de criptomonedes. S'han superat els 3.000 M€ en robatoris de criptomonedes explotant vulnerabilitats a plataformes de criptomonedes, el que constitueix un nou record històric.

Vulnerabilitats *zero-day*. S'han detectat més explotacions de vulnerabilitats de dia zero que mai. Els ciberatacants estan més capacitats per identificar i explotar aquestes vulnerabilitats abans que se'n publiquin els pedaços.

Ciberatacs contra el sector públic. Enguany, les publicacions de ciberatacs amb afectació al sector públic català han augmentat un 150% respecte del 2021.

L'hacktivisme a l'alça. Els ciberatacs amb motivació hacktivista han estat vinculats a conflictes com la guerra entre Rússia i Ucraïna, les protestes a l'Iran o els conflictes territorials de la Xina.

Atacs DDoS. Els atacs DDoS creixen en magnitud i complexitat, ja que cada cop són més destructius i difícils de bloquejar, i afecten el funcionament de serveis web o operadors de telecomunicacions.

Augment dels casos de BEC a Espanya. Durant el 2022, els casos de frau de correu professional publicats han augmentat un 300% respecte del 2021.

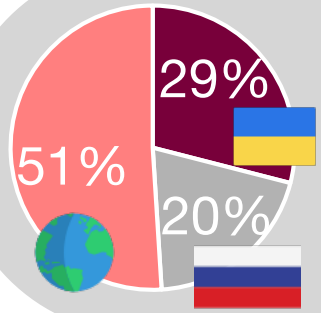
Accions policials. Durant el 2022, les publicacions d'operacions de les forces de l'ordre contra el grups cibercriminals han augmentat en un 30% respecte del 2021.

Fuites de dades personals. El cost mitjà d'una fuita de dades ha augmentat un 42% des del 2020 i, per dotzè any consecutiu, el sector sanitari és el sector on és més elevat.

Crime as a Service. Els preus dels serveis maliciosos oferts a la *dark web* han baixat, en part, gràcies a un mercat cada cop més competitiu: el 90% d'*exploits* a la venda estan per sota dels 10 €.

Principals tendències en ciberseguretat del 2022: la ciberguerra entre Rússia i Ucraïna

El conflicte entre Rússia i Ucraïna ha transcendit les fronteres del món físic i ha traspassat al ciberespai. Així, des de l'inici del 2022, s'ha observat com els ciberatacs han format part de l'estratègia dels dos països per generar desconfiança, desinformar o sabotejar serveis essencials.



Un **51%** dels ciberatacs vinculats al conflicte entre Rússia i Ucraïna han afectat **altres països**.

D'aquests, el **86%** han afectat països de l'OTAN.

- Polònia **22%**
- Lituània **12%**
- Letònia **10%**
- Espanya **1%**
- ...

- Durant el gener i el febrer, Ucraïna va ser l'objectiu de ciberatacs de desfiguració, DDoS i *wipers* per desestabilitzar el país i preparar-lo per a la invasió.
- Un cop esclata el conflicte bèl·lic, comença una guerra híbrida: *wipers* i atacs DDoS per destruir, i campanyes de *phishing* oportunistes.
- Diferents actors, tant cibercriminals com hacktivistes (com Conti, Anonymous, Killnet o la IT Army) s'han posicionat al costat d'un dels dos bàndols.
- El conflicte ha creat una batalla pel relat de la guerra que ha derivat en un allau de *fake news*. En aquest sentit, Rússia va restringir l'accés a Facebook o YouTube, i la UE va vetar les emissions de Russia Today (RT) i Sputnik.
- En aquest context bèl·lic en l'àmbit cibernètic, diverses administracions de tot el món han alertat sobre possibles ciberatacs com a represàlia al posicionament geopolític.

Fonts: CyberPeace Institute i d'altres

Fets rellevants del 2022

Font: diverses fonts

Xifres dels ciberatacs amb impacte a Catalunya el 2022

+30%

Augmenten els ciberatacs

S'ha detectat un augment superior al 30% dels ciberatacs amb afectació a Catalunya respecte del 2021.

+38%

Campanyes de *phishing* en augment

Les campanyes de correus de *phishing*, el vector d'atac més utilitzat en els ciberatacs, creix un 38% respecte del 2021.

20%

Protagonisme dels atacs de BEC

Els fraus de correu professional ja representen un 20% del total de ciberatacs amb afectació a Catalunya publicats enguany.

74%

Ciberatacs amb enginyeria social

El 74% dels incidents de ciberseguretat amb afectació a Catalunya publicats el 2022 han fet ús de tècniques d'enginyeria social.

+150%

El sector públic, objectiu dels ciberatacs

Les publicacions d'incidents cibernètics amb afectació al sector públic català han augmentat més d'un 150% respecte del 2021.

35%

***Ransomware* contra entitats públiques**

El *ransomware* és la principal causa dels ciberatacs contra el sector públic català, amb un 35% del total d'incidents publicats des del 2019.

11%

El troià RootSTV lidera les infeccions

Es tracta d'un troià *downloader* per a *smart TV* amb versions d'Android antigues. Representa un 11% del total de les infeccions a Catalunya.

48%

Predomini de *botnets* en les infeccions

Gairebé la meitat dels sistemes infectats a Catalunya han estat contagiats amb programaris maliciosos de tipus *botnet*.

Fonts: premsa i Bitsight

Continua la falta de talent en ciberseguretat

Necessitat de professionals de la ciberseguretat

Segons (ISC)², el nombre de professionals de la ciberseguretat ha crescut un 11% al món, però la bretxa de professionals encara creix més: un 26%, fins les 3,4 milions de vacants al món.

La tendència s'accentua més a Catalunya:

El nombre de professionals de la ciberseguretat creix un **23%** i la bretxa un **57%**, de manera que la necessitat de professionals no coberta arriba als **10.000**.

	Professionals de la ciberseguretat existents		Necessitat de professionals no coberta	
	vs. 2021	2022	*vs.* 2021	2022
MÓN	+11%	**4,6 M**	+26%	**3,4 M**
EMEA	+12%	**1,2 M**	+59%	**317 K**
CATALUNYA*	+23%	**26 K**	+57%	**10 K**

** Estimació*

Generalitat de Catalunya

Formació en ciberseguretat a Catalunya

11 màsters/postgraus de ciberseguretat

OBS Business School	Màster en Seguretat de la Informació Empresarial
UIC barcelona	Postgrau en *Compliance* i Ciberseguretat
UOC Universitat Oberta de Catalunya	Màster en Seguretat de les TIC
UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH	Màster en *Cybersecurity Management*
UNIVERSITAT ROVIRA I VIRGILI	Màster en Enginyeria de la Seguretat Informàtica i Intel·ligència Artificial
Institut de Formació Contínua-IL3 UNIVERSITAT DE BARCELONA	Màster en Tècniques de Seguretat Informàtica. Ciberseguretat
NUCLIO DIGITAL SCHOOL	Màster en Ciberseguretat
laSalle UNIVERSITAT RAMON LLULL	Màster en Ciberseguretat
unir LA UNIVERSIDAD EN INTERNET	Màster Universitari en Seguretat Informàtica
Universitat de Lleida	Màster en Ciberseguretat
telecos BCN	Màster en Ciberseguretat

37 centres d'estudi ofereixen 44 cursos de formació professional en ciberseguretat

A CATALUNYA ES GENEREN

>700

NOUS PROFESSIONALS EN CIBERSEGURETAT

Font: (ISC)²

Principals prospectives per al 2023

Les crisis globals esperonaran els ciberatacs

- La cibercriminalitat es consolidarà com una sortida a les dificultats econòmiques.
- La nova delinqüència serà de proximitat, estarà menys capacitada tècnicament i se centrarà en atacs d'enginyeria social.
- En plena crisi energètica i d'aigua, els ciberatacs es dirigiran als serveis de subministrament bàsics.
- Algunes bandes criminals desafiaran l'equilibri social i econòmic per mitjà de ciberatacs de gran impacte.

Els conflictes geopolítics irrompran al ciberespai

- Grups cibercriminals patriotes s'alinearan ideològicament amb alguna de les parts d'un món en conflicte.
- Del posicionament dels actors d'amenaces, naixeran conflictes paral·lels entre ells.
- La desconfiança i les precaucions entre bandes cibercriminals anirà en detriment de la seva col·laboració.
- La dificultat per identificar l'autoria i la motivació dels ciberatacs promourà els atacs de falsa bandera.

Espiral de digitalització, ciberamenaces i noves mesures legals mitigadores

- Començarà una nova era per a la ciberseguretat dels productes i serveis de la UE amb la *Cyber Resilience Act* i els futurs marcs de certificació.
- Creixerà l'ús dels *ratings* de ciberseguretat de tercers per planificar possibles inversions.
- La nova regulació europea promourà el potencial dels criptovalors i en frenarà les amenaces.
- Les regulacions europees en matèria de dades (*Data Act* i *Data Governance Act)* exigiran processos i estructures de compartició robustes.

El cibercrim mutarà per seguir optimitzant l'èxit

- Els atacs a la cadena de subministrament permetran provocar afectacions massives.
- El cibercrim dedicarà esforços a saltar-se les solucions de múltiples factors d'autenticació.
- Una nova generació de *botnets,* amb bots versàtils i potents en servidors al núvol infectats, elevaran els ciberatacs a un altre nivell.
- Els ciberatacs a entorns industrials (ICS/OT/IIoT) amenaçaran directament l'entorn físic.

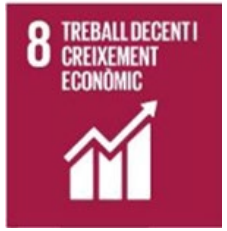
Font: diverses fonts

La ciberseguretat i els OBJECTIUS DE DESENVOLUPAMENT SOSTENIBLE

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

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

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



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

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

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

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

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

5. *Zero trust* i *cybersecurity mesh*

Zero trust, confiança zero

El *zero trust* és un enfocament estratègic de la ciberseguretat que protegeix una organització mitjançant l'eliminació de la confiança implícita i la validació contínua de cada etapa de la interacció digital.

Una arquitectura *zero trust* és un model de seguretat que se centra en la verificació de cada usuari i dispositiu, tant dins com fora del perímetre d'una organització, abans de concedir-hi accés. És a dir, no pressuposa que els entorns dins de l'organització són entorns segurs.

- Suposa que els atacants ja estan a l'aguait a la xarxa.
- No confia en un entorn més que en un altre.
- Suposa que no hi ha confiança implícita.
- Analitza i avalua contínuament els riscos.
- Mitiga els riscos.

L'enfocament de la *zero trust* se centra principalment en la protecció de dades i serveis, però cal ampliar-la per incloure-hi tots els actius de l'empresa (dispositius, components d'infraestructura, aplicacions i components virtuals i del núvol) i els subjectes (usuaris finals, aplicacions i altres entitats no humanes que sol·liciten informació dels recursos).

«Mai confiar, sempre verificar»

Verificar cada usuari

Validar els seus aparells

Limitar intel·ligentment els seus accessos

Fonts: Microsoft; F5, IBM, Paloalto

Com es desplega un model de confiança zero?

Fer un inventari dels actius

Determinar la superfície d'atac a través de la identificació dels actius digitals de més valor: dades sensibles, aplicacions crítiques, serveis corporatius, còpies de seguretat, etc.

Analitzar el trànsit de dades

Supervisar i entendre el tràfic de dades a través de la xarxa per decidir quins són els controls que cal desplegar i on s'ubiquen.

Desplegar una arquitectura de malla de seguretat

Dissenyar i implementar una arquitectura adequada a través de la segmentació de la xarxa, tallafocs de propera generació (NGFW) i autenticació multifactor (MFA).

Crear polítiques de confiança zero

Dissenyar i implementar polítiques de seguretat en què es validi, per a cada usuari, dispositiu o xarxa que sol·liciti accés: qui, què, quan, on, per què i com.

Monitoritzar la xarxa

Observar l'activitat de la xarxa per corregir problemes potencials i millorar el rendiment de la xarxa mitjançant *logs*, alertes i altres mètriques recollides.

Font: diverses fonts

La *cibersecurity mesh*, indispensable per a la *zero trust*

La malla de ciberseguretat *(cybersecurity mesh)* és un component clau d'una filosofia de xarxa de confiança zero.

La malla de ciberseguretat és un enfocament/arquitectura innovador de ciberseguretat que permet que les empreses implementin solucions de seguretat, que garanteixen de manera independent cada punt d'accés amb perímetres individuals creats a mida, com ara tallafocs i eines de protecció de la xarxa. Proporciona diverses solucions de seguretat integrades per millorar la seguretat d'extrem a extrem, mentre apropa els punts de control als actius que han de protegir.

La malla de ciberseguretat té un paper crucial en la construcció d'una arquitectura de seguretat de xarxa segura de confiança zero que protegeixi completament els usuaris, els seus dispositius i les aplicacions a les quals s'accedeix mitjançant una gestió avançada d'identitats, independentment d'on es trobin.

Disrupció tecnològica

La malla de ciberseguretat transformarà el panorama de la seguretat per reforçar la postura de seguretat, millorar l'agilitat i augmentar la interoperabilitat.

Fonts: Frost & Sullivan i Gartner

Característiques clau de la malla de ciberseguretat

La malla de ciberseguretat és una eina molt crítica per detectar anomalies a xarxes empresarials àmpliament esteses sense límits definits.

Esquema basat en la identitat

La malla de ciberseguretat crea un sistema de control d'accés mitjançant la identitat digital en lloc de la ubicació de la xarxa. Crea perímetres de xarxa més petits basats en diversos punts de dades, que inclouen una combinació dinàmica de persones/usuaris, dispositius utilitzats i aplicacions a les quals s'accedeix.

La malla de ciberseguretat ofereix capacitats superiors per interactuar i treballar de manera eficient amb xarxes existents que poden tenir diferents arquitectures de seguretat. Proporciona una passarel·la sòlida que permet establir connexions segures entre xarxes internes i externes.

Interoperabilitat amb xarxes existents

Operació multisalt

La malla de ciberseguretat està dissenyada per oferir serveis de xarxa sense interrupcions. En cas d'atac cibernètic o si algun punt d'accés únic està fora de servei, proporcionarà accés a un altre camí per garantir que no hi hagi interrupcions.

La malla de ciberseguretat permet que les empreses despleguin punts d'accés ràpids a la xarxa, que són conscients del context i es poden autocurar en cas d'avaria. La malla es desenvolupa de manera intel·ligent amb capacitats d'autorecuperació, per estalviar temps i esforç.

Capacitat d'autocuració avançada

Fonts: Frost & Sullivan i Gartner

6. Iniciatives en ciberseguretat

Ciberseguretat a la Unió Europea

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

Estratègia Europea de Ciberseguretat

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

Legislació i certificació

- Llei de ciberresiliència NEW
- Reglament DORA NEW
- Directiva NIS 2 NEW
- Llei de ciberseguretat

Inversió

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

Orientació de polítiques

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

Comunitat cibernètica

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

Altres àmbits de política cibernètica

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

Font: Comissió Europea

Ciberseguretat a Espanya

Espanya ha posat el focus en la ciberseguretat, especialment a partir de la crisi de la COVID-19, amb diversos instruments i 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 de 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 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 a nivell estatal.

KIT Digital

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

7. La ciberseguretat a Catalunya

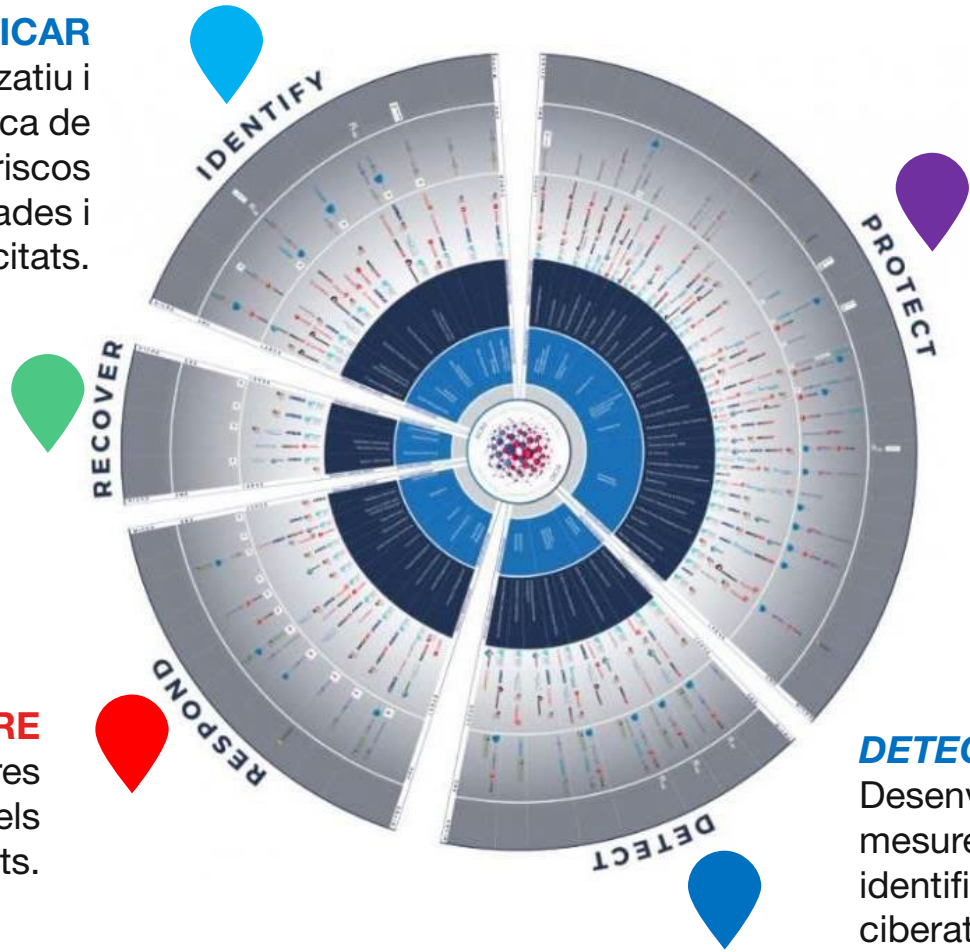
L'ECSO i la metodologia utilitzada per al mapatge

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

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

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

***RESPOND* / RESPONDRE**
Desenvolupar i implementar mesures per actuar adequadament en els incidents de ciberseguretat detectats.



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

***DETECT* / DETECTAR**
Desenvolupar i aplicar les mesures adequades per identificar l'aparició de ciberatacs.

Font: ECSO

Mapatge de l'ecosistema de ciberseguretat a Catalunya

495 empreses
+14,6%*

1.071,1 M€
+17,3%*

9.414 llocs de treball
+15,0%*

El **85,0%** són pimes.

El **53,6%** facturen **més d'1 M€** i el **21,7%** **més de 10 M€**.

El **28,7%** són exportadores.

El **29,1%** tenen menys de 10 anys.

El **9,5%** són startups.

El **13,8%** tenen dones als càrrecs directius.

Per segments**, el **89,7%** de les empreses es dediquen a la protecció, el **58,7%** a la identificació, el **37,0%** a la detecció, el **33,6%** a la resposta i el **20,6%** a la recuperació.

** Respecte de les dades del mapatge realitzat el 2021*

*** Les empreses poden estar classificades en més d'un segment dins de la taxonomia de la ciberseguretat*

Font: ACCIÓ (dades d'empreses del 2022; facturació i nombre de treballadors el 2021)

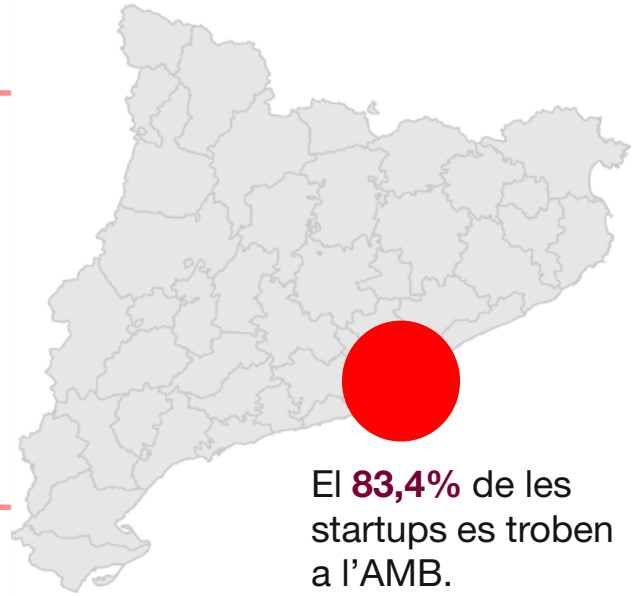
Generalitat de Catalunya

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

Generalitat de Catalunya

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

Un **83,4% de les empreses es troben a l'Àrea Metropolitana de Barcelona** (AMB). La comarca que concentra més empreses dedicades a la ciberseguretat és el Barcelonès (62,2%), seguida pel Vallès Occidental (12,7%) i el Baix Llobregat (5,7%).



El **83,4%** de les startups es troben a l'AMB.

Comarca	Núm. d'empreses en ciberseguretat	% d'empreses en ciberseguretat
Barcelonès	308	62,2%
Vallès Occidental	63	12,7%
Baix Llobregat	28	5,7%
Maresme	14	2,8%
Segrià	13	2,6%
Gironès	12	2,4%
Vallès Oriental	11	2,2%
Osona	7	1,4%
Anoia	5	1,0%
Garrotxa	4	0,8%
Tarragonès	4	0,8%
Baix Camp	4	0,8%
Alt Penedès	3	0,6%
Garraf	3	0,6%
Baix Empordà	3	0,6%
Baix Penedès	2	0,4%
Alt Camp	2	0,4%
Alt Empordà	2	0,4%
Pla de l'Estany	1	0,2%
Baix Ebre	1	0,2%
Moianès	1	0,2%
Montsià	1	0,2%
Bages	1	0,2%
Berguedà	1	0,2%
Conca de Barberà	1	0,2%
Total	**495**	**100,0%**

Accés directe a les empreses de ciberseguretat de Catalunya

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

Agents de l'ecosistema de la ciberseguretat

Centres tecnològics i instituts de recerca

Estudis de màster i postgrau

Estudis d'FP

Associacions i esdeveniments

CSIRT/CERT

Institucions i administració pública

Barcelona, 6a ciutat de la UE en valor de rondes de finançament tancades per a startups

- Barcelona és la **6a ciutat de la UE i la 13a europea** en valor de rondes tancades per a startups de ciberseguretat, amb 103,3 M$ en 17 rondes (2018-2022).
- L'startup catalana que ha rebut més finançament és **Red Points**, que ha tancat 3 rondes per valor de més de 70 M$ en els darrers 5 anys.

Startups de Barcelona amb rondes tancades

RED POINTS · unnax · Signaturit · Blueliv. · numentech · CAMIUM · Bigle Legal · Validated ID

Top 15 de ciutats europees per valor de rondes d'inversió tancades en startups de ciberseguretat (2018-2022)

Nota: s'inclouen les rondes d'inversió «pre-seed», «seed» i les sèries A-J de les següents categories: «penetration testing», «network security», «intrusion detection», «identity management», «fraud detection», «e-signature», «cyber security» i «cloud security». Les dades fan referència al període 2018-2022.

Font: elaboració pròpia a partir de Crunchbase

Catalunya, tercera destinació a Europa occidental per a la IED en ciberseguretat el 2022

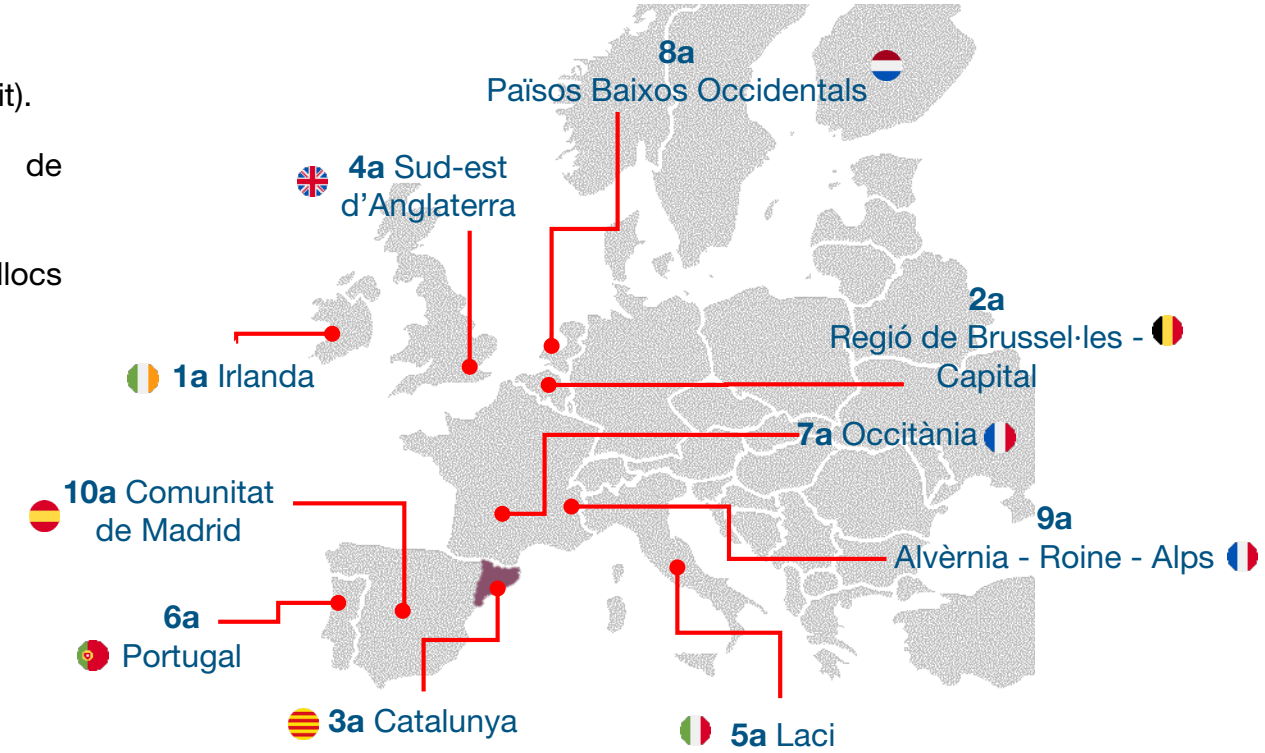
El 2022, Catalunya ha estat la **3a regió d'Europa occidental en captació d'inversió estrangera**, la 8a en nombre de projectes i l'11a en llocs de treball creats.

- La inversió ha estat de **163,6 M€** (7,0% del total invertit).
- Ha rebut **4 projectes** (2,5% del nombre total de projectes).
- S'han creat **313 llocs de treball** (2,4% del total de llocs de treball creats).

Empreses inversores a Catalunya (2022)

netskope	**76,0 M€**	**46 llocs de treball**
Boehringer Ingelheim	**61,0 M€**	**60 llocs de treball**
Schneider Electric	**25,2 M€**	**200 llocs de treball**
relyens	**1,4 M€**	**7 llocs de treball**

Principals regions d'Europa occidental en captació d'inversió estrangera (2022)



Font: elaboració pròpia a partir d'fDi Markets

La innovació en ciberseguretat a Catalunya – H2020

European Commission | Horizon 2020 European Union funding for Research & Innovation

- HORITZÓ 2020 (H2020) és el programa marc de la Unió Europea per al finançament de l'RDI en el període 2014-2020.
- El 2021, ha estat substituït pel programa Horitzó Europa (HE) del qual encara no hi ha dades significatives en projectes de ciberseguretat.

Impacte del programa H2020 a Catalunya en l'àmbit de la ciberseguretat

31 projectes

40 entitats

11.514.961 € d'inversió (representa el **17,1%** del finançament a l'Estat i l'**1,9%** de la UE).

Principals entitats participants en l'àmbit de ciberseguretat per ordre de volum d'inversió

i2cat · UPC Universitat Politècnica de Catalunya BarcelonaTech · eurecat · Schneider Electric · Scytl · Insikt Intelligence · Hospital General de Granollers · World Sensing · IREC · herta security · Australo Marketing Lab · eticas Foundation · teclib' · Altran part of Capgemini · LS Tech · Ficosa · IMI Institut Municipal d'Informàtica · BSC Barcelona Supercomputing Center · PildoLabs move smart · FACTUAL

Font: programa Horizon 2020

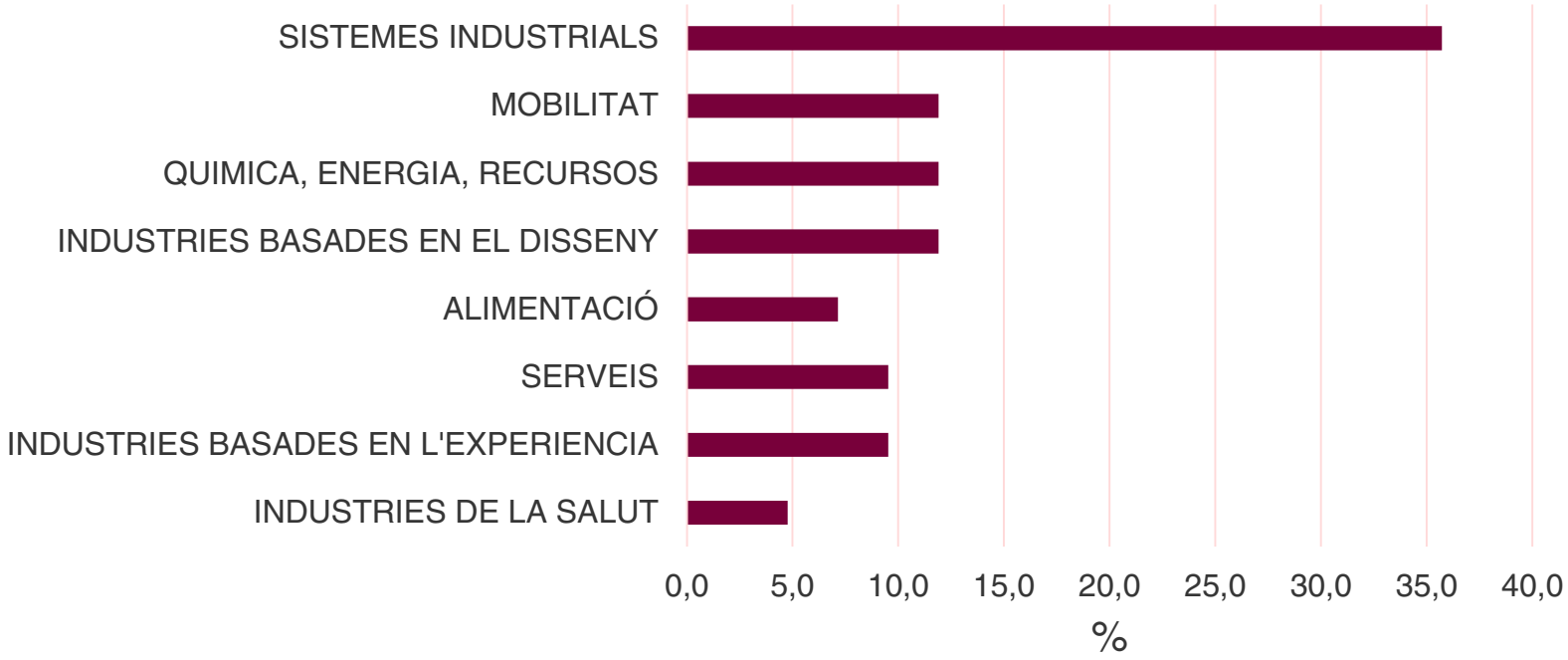
Sectors més demandants de solucions de ciberseguretat

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

assessor acreditat ACCIÓ Generalitat de Catalunya Fins a 09/07/2022

20 assessors tecnològics acreditats per ACCIÓ realitzen activitats relacionades amb la ciberseguretat.

Sectors demandants sol.lucions de Ciberseguretat. CUPONS ACCIÓ



Font: ACCIÓ a partir de dades relatives als 1.209 atorgaments dels ajuts de cupons per a la competitivitat empresarial (Cupons Indústria 4.0) que ha atorgat ACCIÓ durant les anualitats de 2019, 2020, 2021 i 2022

8. Casos d'èxit a Catalunya

Casos d'èxit a Catalunya

Red Points ha tancat una nova ronda de finançament de 19,3 M€.

Neskope ha posat en marxa un centre de dades a Barcelona, que amplia la seva xarxa NewEdge.

Schneider Electric escull Barcelona pel seu nou *hub* digital internacional, amb la ciberseguretat com a protagonista.

L'empresa catalana **Sosmatic** farà el salt als EUA amb una nova oficina a Miami.

Icatel proporciona auditories per detectar les vulnerabilitats cibernètiques de les empreses.

Granollers, referent en l'àmbit de la ciberseguretat.

Omnios, empresa guanyadora del Cyber Investor Days.

Catalunya Auxiliars, una de les pimes que es beneficia del Kit Digital.

Vottun ha creat una eina per verificar la procedència de criptomonedes confiscades pels cossos policials.

Boehringer reforça el seu *hub* digital, que s'ha especialitzat en ciberseguretat.

Relyens amplia la seva activitat a Barcelona amb la ciberseguretat entre els seus objectius.

Parlem compra Infoself per accelerar la digitalització i la protecció a les pimes del territori.

Invoport amplia el seu servei amb la creació d'Invoport Smart Security, especialitzat en *pentesting*.

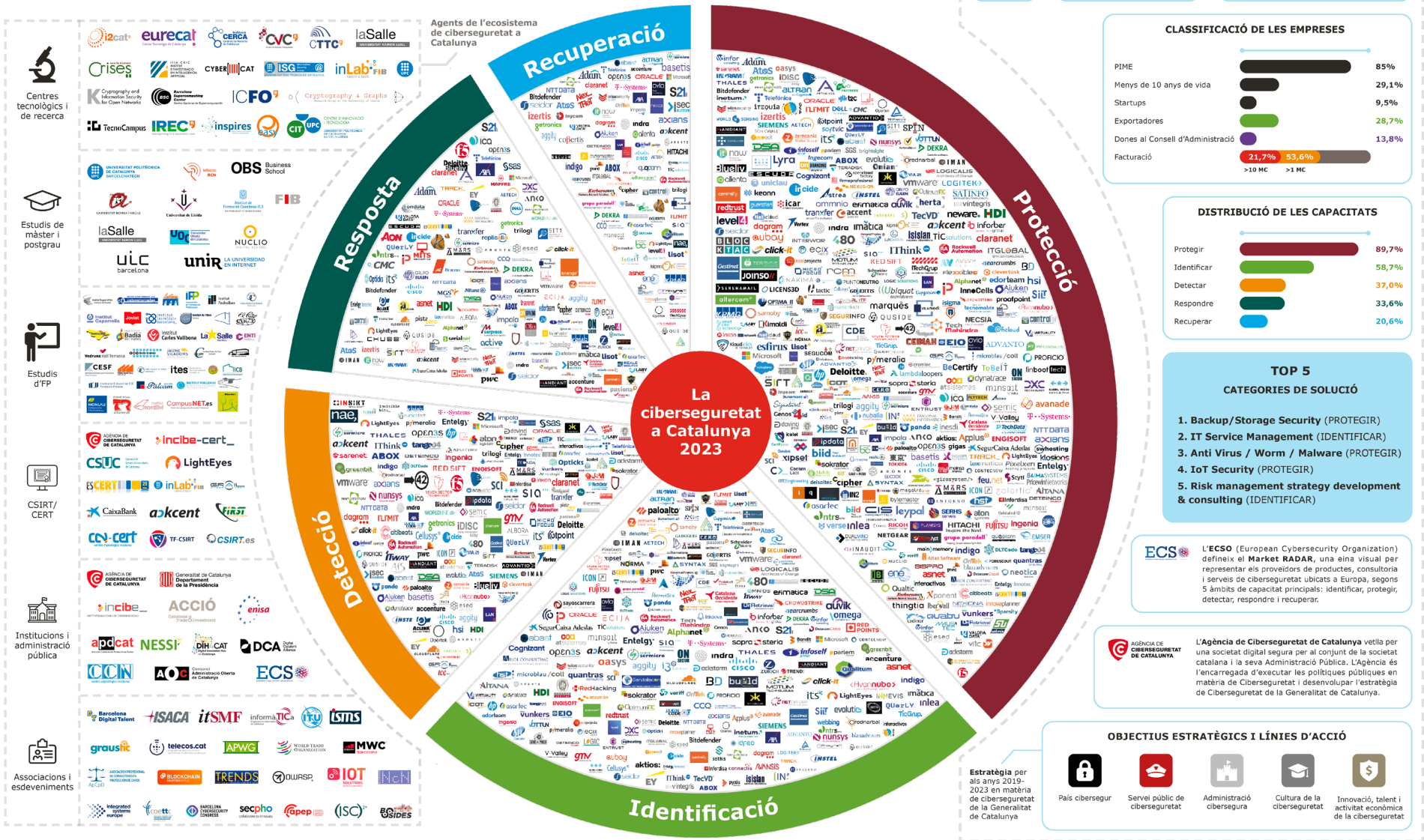
L'Agència Catalana de Turisme lidera el projecte europeu **TOURBIT**, per impulsar la digitalització de les pimes turístiques.

Circe, empresa guanyadora dels Cyber Investor Days.

La ciberseguretat a Catalunya el 2023

Principals conclusions del mapatge de l'ecosistema de ciberseguretat a Catalunya

495 empreses	9.414 treballadors vinculats a la ciberseguretat	Facturació de 1.071 M € directament vinculats a la ciberseguretat



CLASSIFICACIÓ DE LES EMPRESES

PIME	85%
Menys de 10 anys de vida	29,1%
Startups	9,5%
Exportadores	28,7%
Dones al Consell d'Administració	13,8%
Facturació	21,7% >10 MC · 53,6% >1 MC

DISTRIBUCIÓ DE LES CAPACITATS

Protegir	89,7%
Identificar	58,7%
Detectar	37,0%
Respondre	33,6%
Recuperar	20,6%

TOP 5
CATEGORIES DE SOLUCIÓ

1. **Backup/Storage Security** (PROTEGIR)
2. **IT Service Management** (IDENTIFICAR)
3. **Anti Virus / Worm / Malware** (PROTEGIR)
4. **IoT Security** (PROTEGIR)
5. **Risk management strategy development & consulting** (IDENTIFICAR)

ECS

L'**ECSO** (European Cybersecurity Organization) defineix el **Market RADAR**, una eina visual per representar els proveïdors de productes, consultoria i serveis de ciberseguretat ubicats a Europa, segons 5 àmbits de capacitat principals: identificar, protegir, detectar, respondre i recuperar.

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

L'Agència de Ciberseguretat de Catalunya vetlla per una societat digital segura per al conjunt de la societat catalana i la seva Administració Pública. L'Agència és l'encarregada d'executar les polítiques públiques en matèria de Ciberseguretat i desenvolupar l'estratègia de Ciberseguretat de la Generalitat de Catalunya.

OBJECTIUS ESTRATÈGICS I LÍNIES D'ACCIÓ

Estratègia per als anys 2019-2023 en matèria de ciberseguretat de la Generalitat de Catalunya

- País cibersegur
- Servei públic de ciberseguretat
- Administració cibersegura
- Cultura de la ciberseguretat
- Innovació, talent i activitat econòmica de la ciberseguretat

Generalitat de Catalunya

Gràcies!

ACCIÓ Catalonia Trade & Investment

Generalitat de Catalunya

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

Passeig de Gràcia, 129
08008 Barcelona

accio.gencat.cat
catalonia.com

@accio_cat

@catalonia_ti

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

ecosistema@ciberseguretat.cat
ciberseguretat.gencat.cat

@ciberseguracat

@ciberseguracat

Consulteu l'informe aquí:
https://www.accio.gencat.cat/ca/serveis/banc-coneixement/cercador/BancConeixement/eic-la-ciberseguretat-a-catalunya

Més informació sobre el sector, notícies i oportunitats:
https://www.accio.gencat.cat/ca/sectors/tic/