

Ciberseguretat a Catalunya, tecnologia necessària per garantir la seguretat de les nostres empreses

ACCIÓ
Catalonia
Trade & Investment



Generalitat
de Catalunya



AGÈNCIA DE
**CIBERSEGURETAT
DE CATALUNYA**

Barcelona, 22 d'abril 2021

Ciberseguretat a Catalunya, tecnologia necessària per garantir la seguretat de les nostres empreses

Programa

- 10:00h **Benvinguda** i presentació del seminari.
Imma Rodriguez, Màner d'Intel·ligència de Mercat, ACCIÓ
- 10:05h Presentació de l'informe: **La ciberseguretat a Catalunya**
Tomàs Roy, Director de l'Àrea d'Estratègia de la Seguretat a l'Agència de Ciberseguretat de Catalunya.
Ma. Dolors Núñez, Líder d'Equip d'Anàlisi i Detecció d'Oportunitats Tecnològiques. Unitat d'Estratègia i Intel·ligència Competitiva ACCIÓ.
- 10:30h **Casos d'èxit**
Lluís Vera, CEO, ACKENT.
Diana Navarro, Head of Research and Innovation, Fundació Privada Hospital Asil de Granollers.
Joan Mas, Director de l'Àrea de Tecnologies Digitals, EURECAT.
- 11:00h **Preguntes**
- 11:15h **Conclusions**

Moderador: Carles Gómara, ACCIÓ

Índex

- 1. Definició de ciberseguretat i importància per a la indústria**
- 2. Tendències en ciberseguretat**
- 3. Principals magnituds mundials**
- 4. La ciberseguretat a Catalunya**

1. Definició de ciberseguretat i importància per a la indústria



Definició de ciberseguretat

QUÈ ÉS LA CIBERSEGURETAT?



La ciberseguretat engloba el conjunt de mesures físiques, lògiques i administratives destinades a la protecció digital de les empreses, persones i sistemes (siguin dispositius, aplicacions o dades) davant d'atacs digitals que puguin comprometre'n la confidencialitat, disponibilitat o integritat.

EN QUÈ CONSISTEIX?



Els sistemes ciberfísics equipats amb la tecnologia d'Internet requereixen conceptes i tecnologies fiables per garantir la seguretat, la privacitat i la protecció del coneixement. Per tant, és crucial comptar amb unes comunicacions fiables i segures, juntament amb una identitat sofisticada i una gestió de l'accés de les màquines.

Sobre aquests actius, es defineixen i s'implementen diferents capes de protecció en diferents àmbits, així com de prevenció i resiliència. D'aquesta manera, es combinen diferents mesures per prevenir i mitigar atacs de forma efectiva.

QUINA IMPORTÀNCIA TÉ?



Avui en dia, les empreses tenen una gran presència digital, ja sigui exposada públicament a través d'Internet o internament mitjançant sistemes informàtics per gestionar les dades i processos interns. No ser capaç de protegir-se efectivament contra les noves amenaces exposa les empreses actuals a la pèrdua d'informació confidencial, a un impacte negatiu en la marca pròpia, a la incapacitat de desenvolupar l'activitat empresarial i a la vulneració de lleis específiques, com el nou Reglament de protecció de dades, l'incompliment del qual comporta sancions severes.

Impacte dels ciberatacs

EL CIBERCRIM ESTÀ EN EXPANSIÓ:

Es calcula que l'any 2021 cada **11 segons** hi haurà un ciberatac a nivell mundial. Aquesta dada ha augmentat significativament els últims anys: el 2016 la mitjana era de **40 segons**.

Cybersecurity Ventures estima que el cibercrim tindrà, l'any **2021**, un cost global de **6 bilions de dòlars anuals**, la qual cosa representa un 1% del PIB mundial.

El **99%** de les empreses espanyoles admet haver patit un ciberatac durant el 2020, amb una mitjana de **cinc ciberatacs** rebuts per empresa. El **43%** d'aquests atacs van dirigits a pimes.

El **79%** d'empreses a nivell mundial afirma que trobar el **talent** adequat en matèria de ciberseguretat és «molt difícil» o «extremadament difícil», una mitjana més elevada que en les mateixes categories per trobar talent en TIC (70%).

El sector públic, el de l'energia i la indústria manufacturera han estat els sectors que més ciberatacs han rebut en el darrer any. Un altre sector que ha patit l'atac de *hackers* arran de la pandèmia ha estat el de **proveïdors de salut**.

PRINCIPALS IMPACTES NEGATIS D'UN CIBERATAc PER A LES EMpRESSES:



El 45% dels atacs a Espanya provoquen danys per valor de més de **400.000 €**. El cost mitjà d'un atac a una pime és de **35.000 €**.



L'any passat, el 45% de les empreses va haver de gestionar una interrupció de més de **5 hores** a causa d'un ciberatac.



El 18% dels atacs a la seguretat han provocat que **més de la meitat dels sistemes de l'empresa** es vegin afectats.

Qui hi ha al darrere del cibercrim? (I)

Agents	Motivacions	Vectors d'amenaça	Impacte
Cibercriminals	- Enriquiment il·lícit - Frau - Suplantació d'identitat	- Robatoris individuals d'identitat - Esquemes de dades i robatori de propietat intel·lectual - Persones infiltrades - Per mitjà de proveïdors tecnològics	- Pèrdua d'identitat - Pèrdues econòmiques - Pèrdua de propietat intel·lectual - Privacitat - Legislatiu
Estats/nacions	- Competició global - Seguretat nacional - Frau	- Cibercampanyes de llarga durada - Persones infiltrades - Proveïdors externs	- Pèrdua de propietat intel·lectual - Disrupció d'infraestructures crítiques - Pèrdues econòmiques - Legislatiu
Ciberterroristes/ hackers individuals	- Ideològiques - Polítiques - Privació de drets - Crear el caos	- Vulnerabilitats oportunistiques - Persones infiltrades - Per mitjà de proveïdors tecnològics	- Desestabilitzar, pertorbar i destruir actius d'institucions financeres - Legislatiu
Hacktivistes	- Causa política més que guany personal - Ideològiques	- Organitzacions que s'interposen a la seva causa - Persones infiltrades - Proveïdors externs	- Disrupció d'operacions - Desestabilització - Vergonya/imatge - Relacions públiques - Legislatiu

* Els cibercriminals són els principals agents que ataquen les indústries

Font: EURECAT

Qui hi ha al darrere del cibercrim? (II)

L'ENRIQUIMENT IL·LÍCIT COM A OBJECTIU FINAL DELS CIBERATACS:

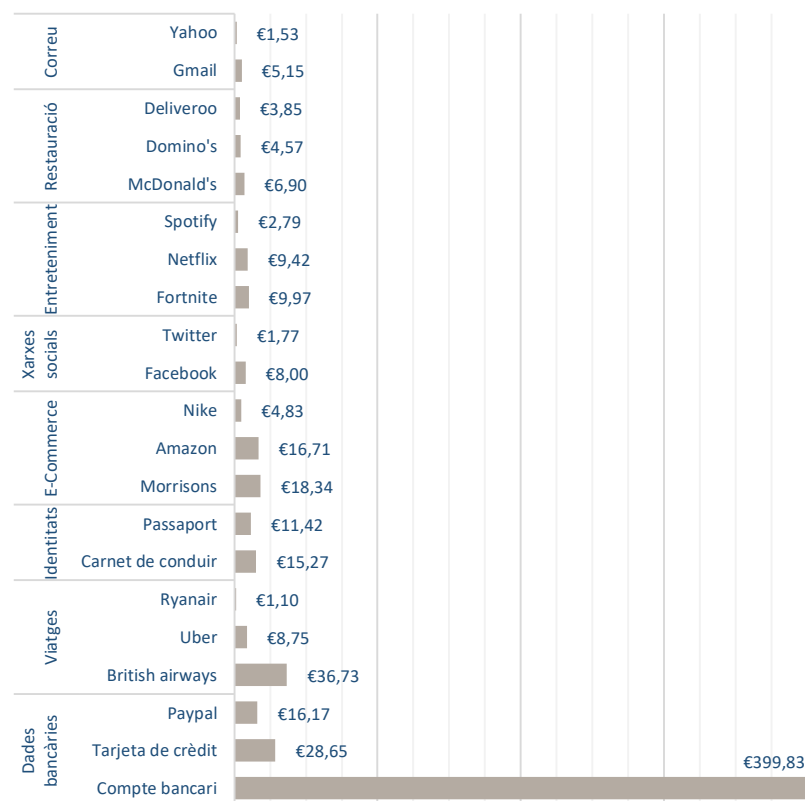
El *dark web* o *web fosc* s'utilitza per a tota una sèrie d'activitats il·lícites, especialment relacionades amb la venda de dades robades o l'oferta de serveis de *hacking* professionals amb finalitats delictives.

- L'anàlisi de Trend Micro mostra que 1,5 bilions de dòlars són generats a partir del subministrament de serveis de ciberdelinqüència oferts cada any als mercats del *dark web*.
- Segons Symantec, la venda dels detalls de només deu targetes de crèdit robades de llocs web compromesos podrien permetre obtenir fins a 2,2 milions de dòlars cada mes per als cibercriminals.



EXEMPLES DEL PREU DE LES CREDENCIALS ROBADES AL *DARK WEB*:

Cost de credencials robades al Dark Web



Font: Raconteur

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



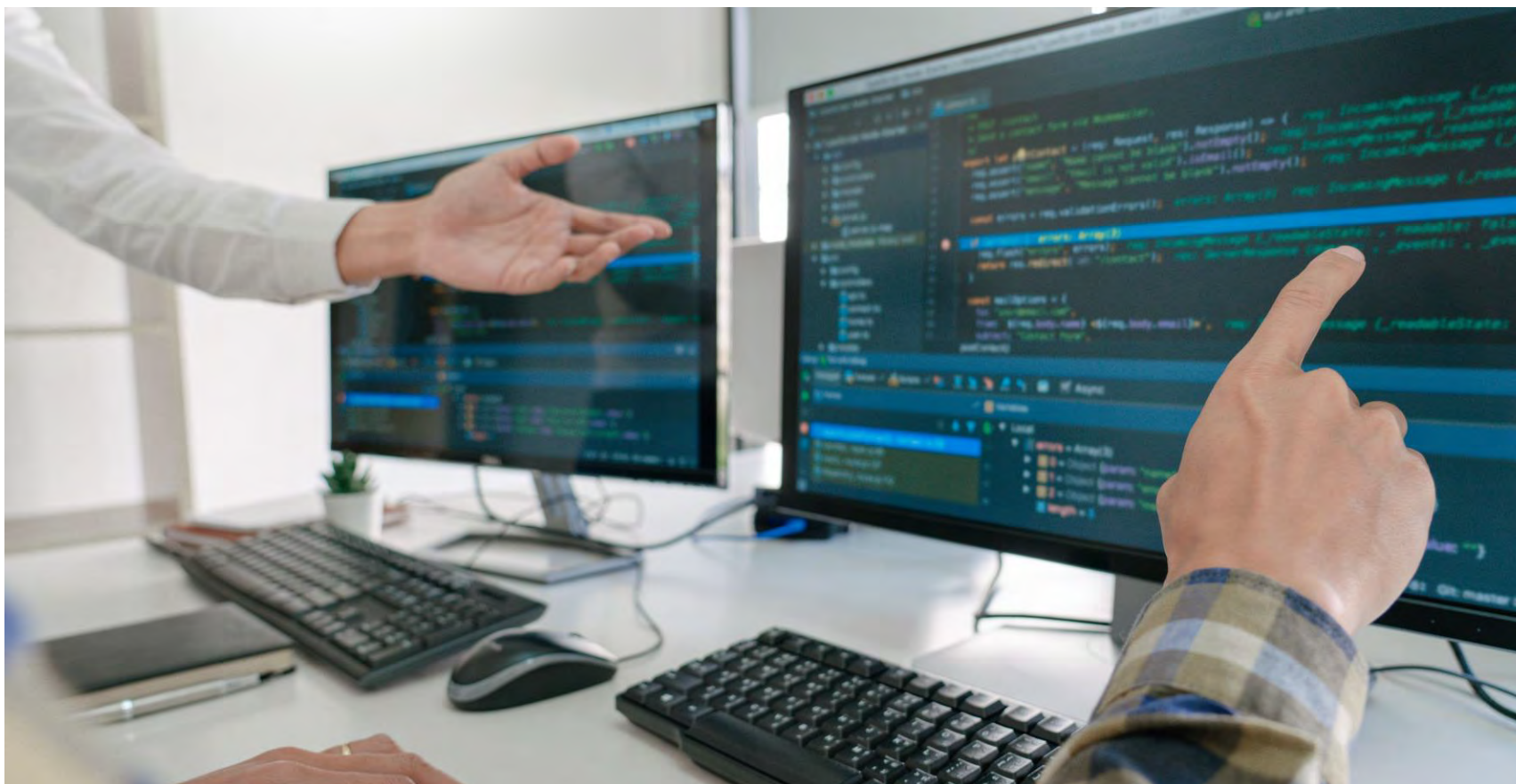
Un atac important pot afectar de manera considerable la imatge i la reputació de l'empresa.

La implantació de bones mesures de ciberseguretat per evitar vulnerabilitats pot suposar un estalvi de despeses per 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.

Font: Elaboració pròpia

2. Tendències en ciberseguretat



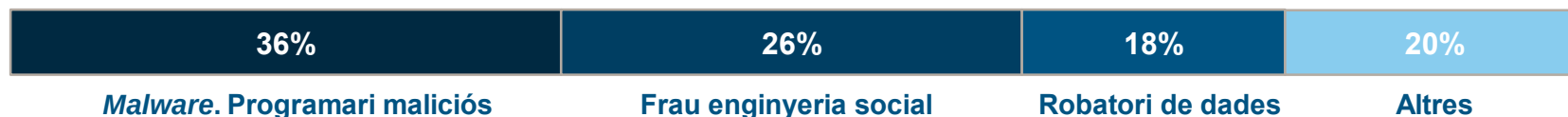
L'impacte de la COVID-19 en la ciberseguretat

IMPACTE I CONSEQÜÈNCIES DE LA PANDÈMIA

- La pandèmia de la COVID-19 ha afectat decisivament la realitat de la ciutadania, els sectors privat i públic, i el cibercrim mateix, i ha creat un context propici per als incidents de ciberseguretat.
- L'FBI va estimar un augment del 400% dels ciberatacs a partir de la pandèmia, al mateix temps que Proofpoint alertava que el 80% del total dels atacs cibernètics tenien una temàtica relacionada amb el coronavirus.



Incidents més freqüents arran de la COVID-19



Font: Elaboració pròpia

Principals tendències en ciberseguretat (I)

TECNOLOGIES

- Segons The Financial Times en el seu informe *Tech Cities of The Future for 2020/21*, Catalunya té la segona millor estratègia d'Europa per captar inversions en l'àmbit tecnològic. Barcelona se situa vuitena de tota Europa i primera del sud d'Europa com a ciutat tecnològica del futur.
- La inversió en TI a Europa ha baixat del 2019 al 2020: ha passat d'1,2 a 1,1 milions entre pimes, i de 74,1 milions a 54,3 milions entre grans empreses, segons Kaspersky. No obstant això, les inversions en ciberseguretat en el pressupost general de TI han passat del 23% al 26% entre les pimes, i del 26% al 29% entre les grans empreses.

Catalunya és una regió tecnològicament capdavantera en un món on la ciberseguretat esdevé un valor diferencial a l'alça.

							
Big Data i intel·ligència artificial	Blockchain	5G	Teletreball	Indústria 4.0	Salut digital	Computació al núvol	Autenticació biomètrica o multifactor
Potencia la capacitat de prevenció i detecció d' <i>Advanced Persistent Threats</i> (APT).	Aporta integritat de les dades i alta disponibilitat.	Possibilita la connectivitat segura d'un alt nombre de dispositius i comunicacions crítiques.	En condicions cibersegures, és imprescindible per a garantir la continuïtat de l'activitat econòmica.	Comporta la irrupció dels ciber riscos al sector industrial.	La ciberseguretat i la privacitat són elements clau en l'atenció sanitària i la supervisió dels malalts.	Suposa delegar la seguretat de dades i sistemes propis al núvol.	Assegura l'accés a dispositius, serveis i/o zones restringides.

Font: CybersecurityInsiders / Elaboració pròpia

Principals tendències en ciberseguretat (II)

TALENT

- Segons l'enquesta de població activa, el **sector TIC** ja ocupa **128.700 persones** a Catalunya, el **3,9%** de la població ocupada del país.
- La demanda de professionals de ciberseguretat a Catalunya pràcticament s'ha doblat. Segons Experis IT, a Barcelona, és on millor es recompensa el talent amb sous de **47.000 euros de mitjana**, un **76% superiors al sou mitjà interprofessional** de l'Estat.
- Segons l'ISC², la falta de professionals de la ciberseguretat arriba a **4 milions a tot al món** i el forat és de **291.000 tan sols a Europa**. Segons l'Associació de Seguretat de Sistemes d'Informació (ISSA) i l'empresa d'anàlisi Enterprise Strategy Group (ESG), el **74%** de les empreses no tenen cobertes les necessitats en seguretat cibernètica.

- Els coneixements de ciberseguretat que avui en dia requereixen les empreses s'han d'obtenir principalment a través d'**estudis postuniversitaris, certificacions i experiència laboral**. A Catalunya hi ha 10 titulacions.
- A Catalunya, **18 centres** imparteixen el cicle formatiu de grau superior en Administració de sistemes informàtics en xarxa, perfil professional en ciberseguretat. Recentment, el Govern espanyol ha aprovat **quatre nous títols** de FP de grau superior de Ciberseguretat.

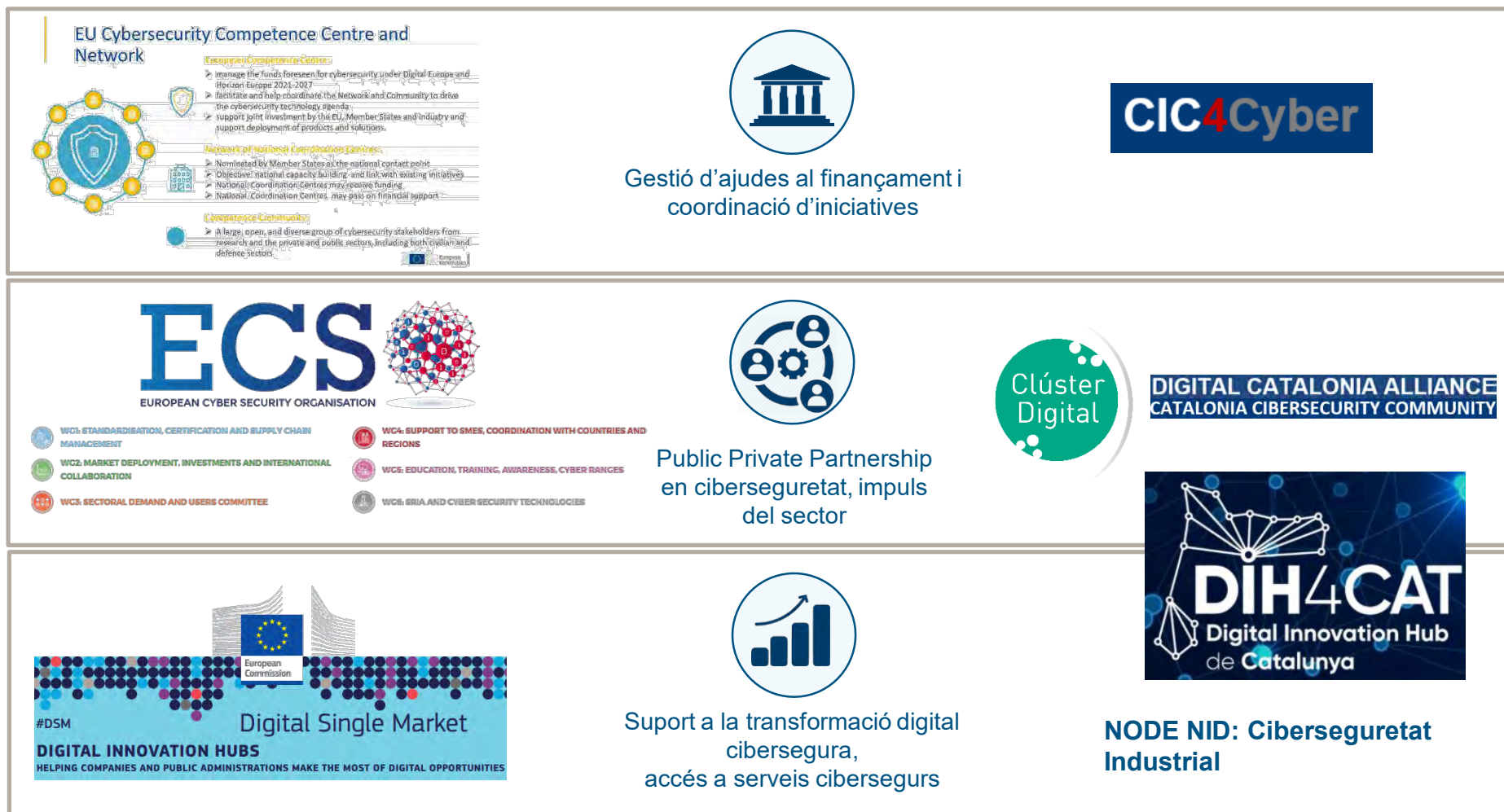
 Institut de Formació Continua-IL3 UNIVERSITAT DE BARCELONA	Màster en Tècniques de Seguretat Informàtica. Ciberseguretat	 UNIVERSITAT ROVIRA I VIRGILI	Màster Universitari en Enginyeria Informàtica: seguretat Informàtica i sistemes Intel·ligents
 Universitat Oberta de Catalunya	Màster Universitari en Seguretat de les Tecnologies de la informació i de les comunicacions	 OBS Business School	Màster en Seguretat de la Informació Empresarial
 UNIVERSITAT RAMON LLULL	Màster en Ciberseguretat	 UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH	Màster Cybersecurity Management
 Universitat de Lleida	Màster en Ciberseguretat	 UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH	Màster en Ciberseguretat
 Euncet Business School	Màster en Seguretat Informàtica i gestió del risc tecnològic	 Universitat de Girona	Curs de postgrau ciberseguretat



* Càlcul obtingut a partir de l'extrapolació de les dades de l'ISC².

Font: ISC² / Elaboració pròpia

Ecosistema en construcció



Font: Elaboració pròpia

Àmbits d'activitat de la ciberseguretat



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.

RECUPERAR

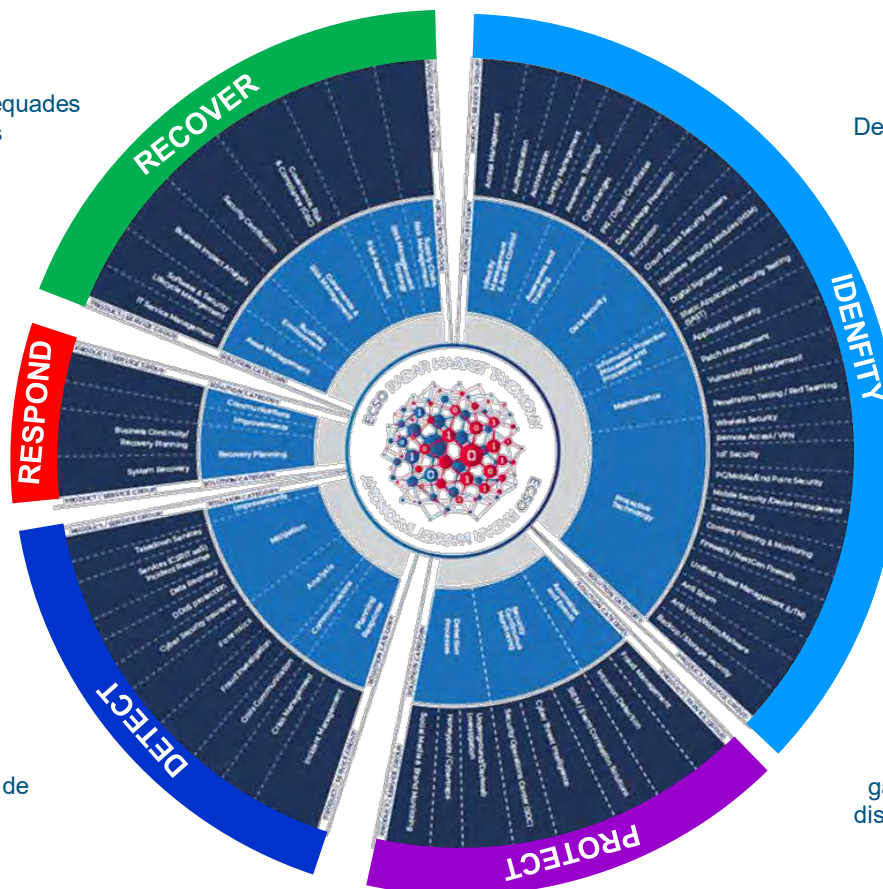
Desenvolupar i implementar activitats adequades per mantenir els plans, els processos i els recursos per a la resiliència de TI i per restaurar les capacitats o els serveis afectats a causa d'incidents cibernètics.

RESPONDRE

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

DETECTAR

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



IDENTIFICAR

Desenvolupar organitzativament i estratègica la infraestructura TI de ciberseguretat per gestionar els ciberriscos en sistemes, persones, actius, dades i capacitats.

PROTEGIR

Desenvolupar i implementar les solucions per a la reducció de la superfície d'atac a sistemes TI, i garantir la confidencialitat, integritat, disponibilitat i auditabilitat, així com el rendiment de serveis informàtics essencials.

Font: ECSO

3. Principals magnituds mundials

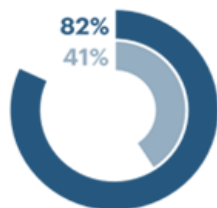


Mercat mundial de la ciberseguretat

DESPESA MUNDIAL EN CIBERSEGURETAT



Segons l'informe de l'estat de ciberseguretat d'Accenture, des de l'any 2017, el nombre d'empreses que **inverteixen més d'un 20% dels seus pressupostos** a la tecnologia digital i apliquen la ciberseguretat des de la fase de disseny **s'ha duplicat**.



■ Ara ■ Fa tres anys



Canalys al seu informe *Global cybersecurity 2021 forecast*, estima que la **despesa mundial en productes i serveis de ciberseguretat** creixerà entre un **6,6 i un 10%** durant l'any 2021.



Segons Gran View Research, el mercat mundial de seguretat cibernètica es va valorar en **156.500 milions de dòlars** el 2019 i es preveu un **creixement anual del 10% fins el 2027**.

PRESSUPOSTOS EN CIBERSEGURETAT



Segons Accenture, **la majoria d'organitzacions inverteix el 10,9%** dels pressupostos de TI en ciberseguretat.



El 31% dels CEOs preveuen **incrementar en més del 10% la seva inversió en ciberseguretat** i privacitat en els pròxims 3 anys. El 49% (56% en el cas d'Espanya) planeja realitzar un increment de la seva inversió en transformació digital superior al 10%.

TAXES DE CREIXEMENT

L'any 2021 les taxes de creixement previstes per tecnologia a escala mundial en els millors escenaris són les següents, segons Canalys.



Font: Canalys / Accenture / Gran View Research / PwC

Empreses líders mundials en ciberseguretat



Nota: L'ús d'aquestes marques és merament informatiu. Les marques esmentades en aquest informe pertanyen als seus respectius titulars i en cap cas són titularitat d'ACCIÓ. S'han inclòs les 12 empreses amb més facturació entre els llistats de "Best Cyber Security Companies" i "Hottest Cybersecurity Companies".

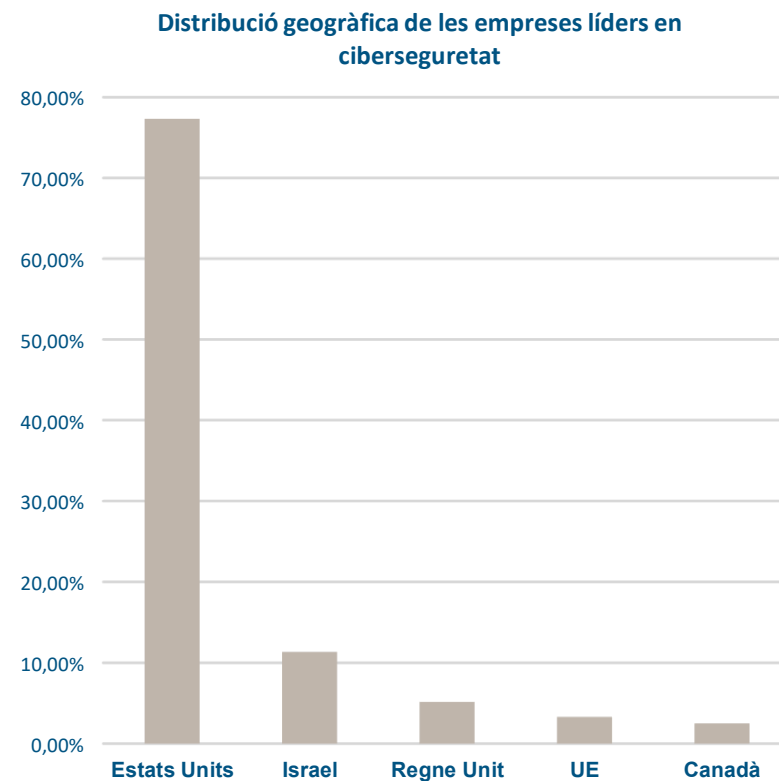
Font: SoftwareTestingHelp

Distribució d'empreses líders de ciberseguretat (I)

1 El mercat de la ciberseguretat està concentrat als EUA, amb el 77% de les 150 empreses líders a nivell mundial. Destaquen els pols d'atracció de San Francisco, CA (36% de empreses), la regió de Nova York, NY (12%) i Seattle, WA. (5%).

2 La segona potència mundial en ciberseguretat és Israel, que concentra l'11% de les empreses líders en ciberseguretat.

3 El Regne Unit se situa en tercera posició, amb més del 5% d'empreses líders. La UE només representa un 3,3%.

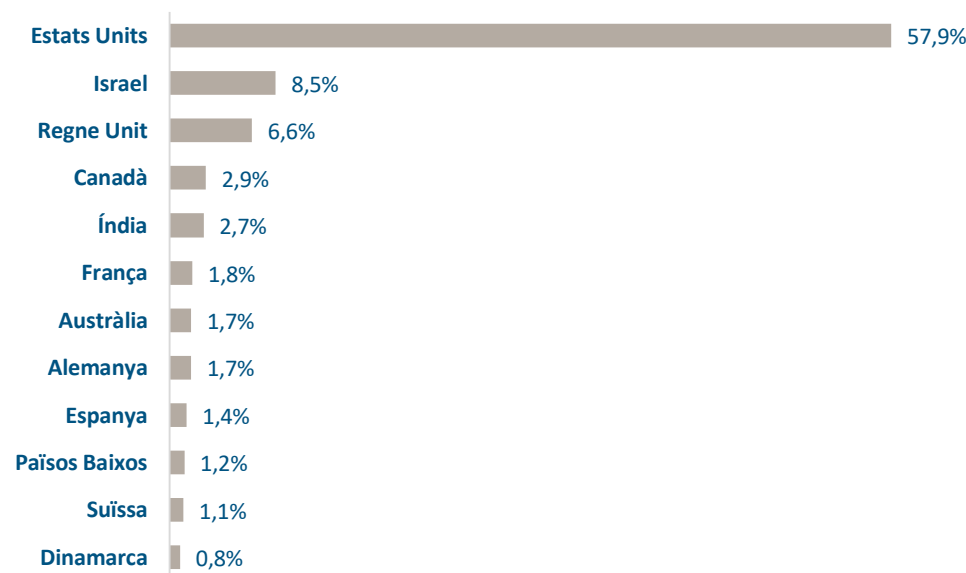


Distribució d'*startups* de ciberseguretat

S'han analitzat les 1105 *startups* (empreses amb menys de 10 anys de vida) amb una facturació superior a 1 milió de dòlars.

- La concentració de les principals *startups* de ciberseguretat també es troba als **Estats Units**. El país nord-americà concentra la majoria d'*startups* 57,9% del total, una tendència similar a la de les principals empreses.
- Es consolida la posició d'**Israel** com a *hub* tecnològic especialitzat en ciberseguretat amb un **8,5%**, seguit del **Regne Unit** en la tercera posició al podi de les principals seus d'*startups* en ciberseguretat, amb el **6,6%**.
- Els **països de la UE** continuen tenint un pes molt baix, i **Espanya** concentra poc més de l'**1,4%** d'*startups*.
- Del total d'*startups* d'Espanya, un **14% són a Catalunya**.

Distribució geogràfica de les *Startups* líders en ciberseguretat

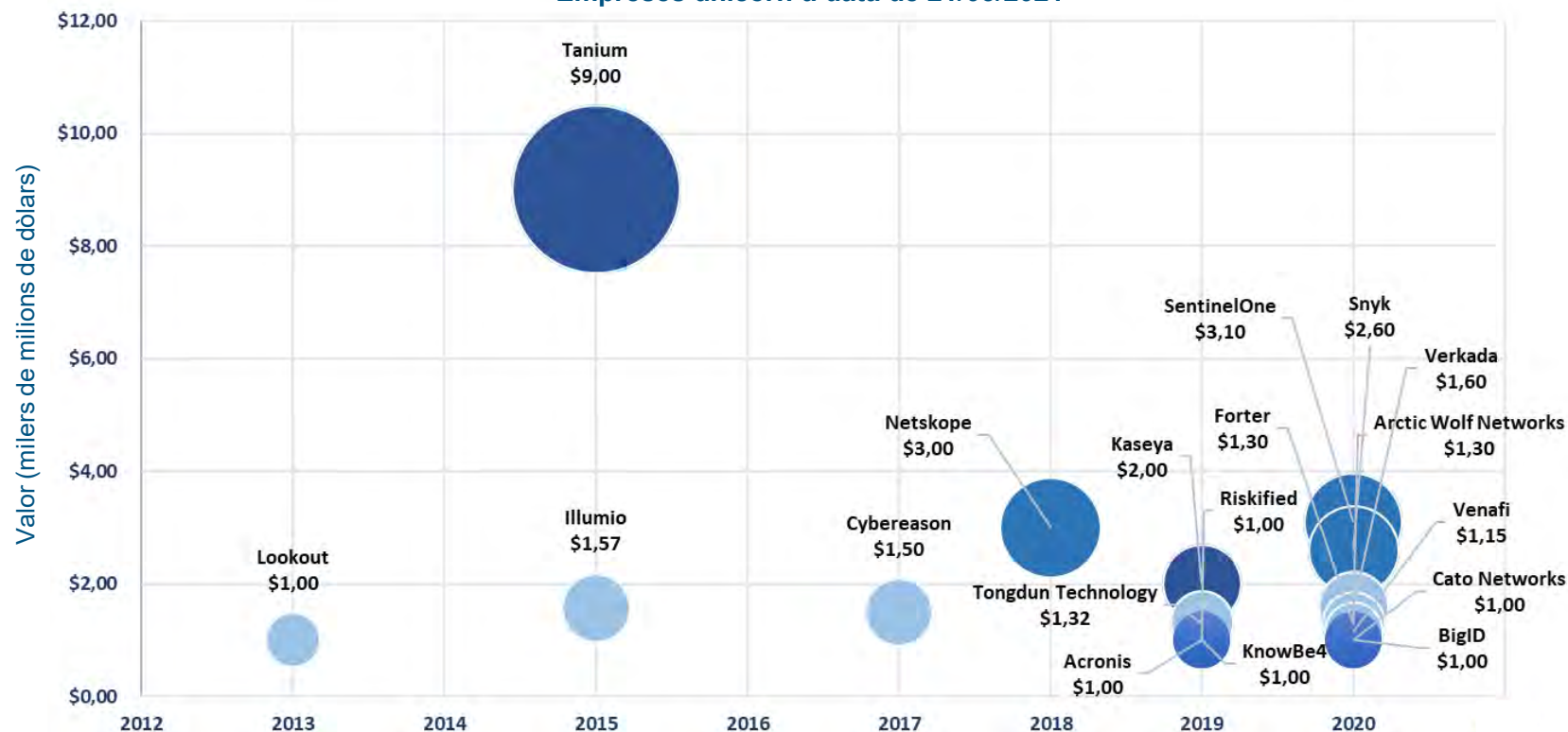


Font: *Crunchbase*

Unicorns líders mundials en ciberseguretat (I)

Una empresa unicorn és una *startup* tecnològica que ha aconseguit tenir una valoració superior als 1.000 milions de dòlars.

Empreses unicorn a data de 21/03/2021



Nota: l'ús d'aquestes marques és merament informatiu. Les marques esmentades en el present informe pertanyen als seus respectius titulars i en cap cas són titularitat d'ACCIÓ. Aquesta és una representació il·lustrativa parcial de les principals empreses que formen part de l'ecosistema del sector de la ciberseguretat, però hi pot haver altres empreses que no hagin estat incorporades a l'estudi.

Font: CB Insights

Principals inversors mundials



Nota: l'ús d'aquestes marques és merament informatiu. Les marques esmentades en el present informe pertanyen als seus respectius titulars i en cap cas són titularitat d'ACCIÓ. S'han inclòs en aquesta diapositiva els 10 principals inversors a tot el món des de principis del 2010, classificats segons el recompte de transaccions.

Font: PitchBook

Índex global de Ciberseguretat

CATALUNYA, 8NA D'EUROPA EN CIBERSEGURETAT

El *Global Cybersecurity Index* (GCI) que elabora l'Agència de Ciberseguretat de Catalunya en col·laboració amb PwC mesura 25 indicadors que permeten identificar i comparar el nivell de compromís dels països en matèria de Ciberseguretat. L'índex s'elabora segons:

	Mesures Legals	Aquelles que es basen en l'existència d'institucions i marcs legals que s'ocupen de la ciberseguretat i el ciberdelicte.
	Mesures tècniques	Aquelles que es basen en l'existència d'institucions tècniques i una agència que s'ocupa de la protecció nacional.
	Mesures organitzatives	Existència d'institucions de coordinació de polítiques i estratègies per al desenvolupament de la ciberseguretat a escala nacional.
	Mesures de captació	Existència de programes de recerca i desenvolupament, educació, conscienciació i captació, professionals, certificats i agències públiques interconnectades.
	Mesures de coordinació	Mesures basades en l'existència d'aliances, marcs cooperatius i xares d'intercanvi d'informació a escala internacional.

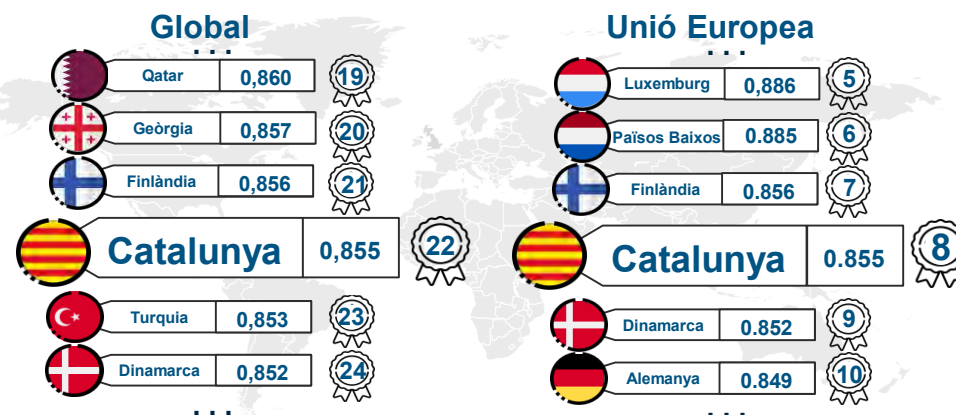
ÀMBIT GLOBAL

Qui lidera és **Regne Unit** amb una puntuació de 0,931 per sobre d'**Estats Units** (0,926) i **França**.

ÀMBIT EUROPEU

L'índex està liderat per **França** amb una puntuació de 0,918, seguida de **Lituània i Estònia**, amb 0,908 i 0,905 respectivament.

Comparativa Internacional



Catalunya ha obtingut la màxima puntuació pel que fa a les **mesures legals**. El compromís en matèria de ciberseguretat es constata en la **Llei 15/2017** de creació de l'**Agència de Ciberseguretat de Catalunya** com a entitat encarregada d'executar i de comandar les polítiques públiques de la Generalitat de Catalunya, esdevenint l'òrgan encarregat de vetllar per la ciberseguretat al territori.

Font: Agència de Ciberseguretat de Catalunya

4. La ciberseguretat a Catalunya



Principals conclusions del mapatge

La ciberseguretat a Catalunya



361 empreses

6.896 treballadors vinculats a la ciberseguretat

Facturació de 820,6 M€ directament vinculats a la ciberseguretat

El 82,8% de les empreses són pimes

El 31,8% de les empreses tenen menys de deu anys

El 14,8% de les empreses tenen presència femenina als Consells d'Administració

El 13% de les empreses de l'ecosistema són *startups*

El 55,9% factura més d'1 € i el 22,9% més de 10 M€

Un 29% de les empreses són exportadores

A l'ecosistema català destaquen les empreses que treballen en els següents àmbits d'activitat:

- Protegir
- Identificar
- Respondre

Nota: Les dades de facturació i treballadors corresponen a les darreres dades econòmiques disponibles per a les empreses (2019 en la majoria de casos).

Font: Elaboració pròpia

Agents de l'ecosistema de ciberseguretat a Catalunya



Centres
tecnològics i
de recerca



Universitats i
màsters



Formació
tècnica



Associacions i
Fires



CSIRT/CERT



Institucions i
Administració
pública

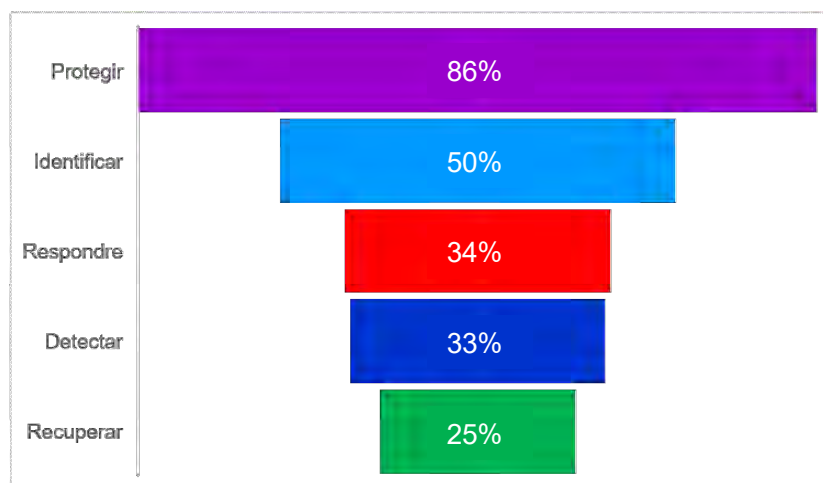


Font: Elaboració pròpia

Capacitats i solucions de les empreses

Les empreses de ciberseguretat amb presència a Catalunya estan principalment especialitzades en la capacitat de **PROTEGIR**.

DISTRIBUCIÓ DE LES CAPACITATS



TOP 5

CATEGORIES DE SOLUCIÓ

1. *Backup / Storage Security* (PROTEGIR)
2. *PC/Mobile/End Point Security* (PROTEGIR)
3. *IT Service Management* (IDENTIFICAR)
4. *Firewalls / NextGen Firewalls* (PROTEGIR)
5. *Identity Management* (IDENTIFICAR)

Les solucions de **CÒPIES / EMMAGATZEMATGE DE SEGURETAT** són els productes i serveis més presents en l'oferta de les empreses de ciberseguretat de Catalunya.

Empreses de ciberseguretat a Catalunya (I): IDENTIFY



Empreses de ciberseguretat a Catalunya (II): PROTECT (I)



Empreses de ciberseguretat a Catalunya (III): PROTECT (II)



DETECT



Empreses de ciberseguretat a Catalunya (IV): RESPOND



RECOVER



Mapeig de la ciberseguretat a Catalunya

ciberseguretat.gencat.cat



La ciberseguretat a Catalunya 2020

AGÈNCIA DE
CIBERSEGURETAT
DE CATALUNYA

ACCIÓ
Catalonia Trade & Investment

Consulta l'informe complet aquí:

<http://www.accio.gencat.cat/ca/serveis/banc-coneixement/cercador/BancConeixement/la-ciberseguretat-a-catalunya>



Més informació sobre el sector, notícies i oportunitats:

www.accio.gencat.cat/ca/sectors/tic/

