Març del 2022. Informe tecnològic

La ciberseguretat a Catalunya

Generalitat de Catalunya

Fem avui l'**empresa** del demà

ACCIÓ
Generalitat de Catalunya

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

Barcelona, març del 2022

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 els trets característics de les dades i els sistemes d'informació.

Aquests trets característics són els següents:

- **Confidencialitat:** garanteix que només puguin accedir a aquestes dades les persones autoritzades.
- **Disponibilitat:** en garanteix plenament les funcions en el moment de fer una sol·licitud.
- **Integritat:** garanteix que no patiran cap alteració ni destrucció voluntària o accidental.
- **Autenticitat:** garanteix que una entitat és qui diu ser o bé que garanteix 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

Operacional

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

La Generalitat va patir un atac de DDoS que va afectar el funcionament de més de 2.000 aplicacions informàtiques de la institució durant unes 3 hores.

Econòmic

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

Segons l'asseguradora Hiscox, les empreses de l'Estat espanyol assumeixen de mitjana un cost anual de 30 000 euros per atacs cibernètics.

Legal

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

L'AEPD va sancionar la balear Air Europa amb 500 000 euros per una bretxa de seguretat arran d'un ciberatac, i 100 000 pel retard a notificar-ho.

Reputacional

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

Segons PwC, el 87 % dels consumidors i clients pensen a canviar de proveïdor si pateix una fuita de dades.

Font: diverses fonts com Hiscox o PwC

Actors	Motivacions	Vectors d'amenaça	Impacte
CIBERCRIM	▪ Enriquiment il·lícit a partir de ciberatacs directes ▪ Prestació de serveis cibercriminals a altres grups cibercriminals (Crime-as-a-Service)	▪ Credencials d'accés robades ▪ Explotació de vulnerabilitats ▪ Programari maliciós/*ransomware* ▪ Enginyeria social ▪ Atacs de DDoS ▪ Proveïdors tecnològics vulnerables	▪ Fuita de credencials i dades personals ▪ Pèrdua d'informació ▪ Interrupció de l'activitat ▪ Exigència d'un rescat ▪ Sancions
ESTATS	▪ Rivalitat geopolítica ▪ Protecció de la Seguretat nacional ▪ Ciberespionatge industrial ▪ Ciberguerra	▪ Grups APT patrocinats per estats ▪ Explotació de vulnerabilitats *0-day* ▪ Programari d'espionatge ▪ Programari maliciós/*ransomware* ▪ Enginyeria social ▪ Difusió de desinformació	▪ Interrupció de serveis essencials ▪ Afectació a l'estabilitat social i econòmica ▪ Filtració d'informació estratègica ▪ Pèrdua de reputació
CIBERTERRORISME	▪ Diferències ideològiques/polítiques/religioses ▪ Represàlies ▪ Desestabilització	▪ Atacs de DDoS ▪ Programari maliciós/*wiper* ▪ Explotació de vulnerabilitats ▪ Personal infiltrat	▪ Interrupció de serveis essencials ▪ Afectació a l'estabilitat social i econòmica ▪ Destrucció de dades
HACKTIVISME	▪ Ideologia ▪ Sociopolítiques ▪ Mediambientals ▪ Igualtat	▪ Atacs de DDoS ▪ Explotació de vulnerabilitats ▪ Personal intern ▪ Difusió d'informació en xarxes social	▪ Interrupció de l'operativa ▪ Pèrdua de dades confidencials ▪ Desfiguració (*defacement*) de web ▪ Pèrdua reputacional
HACKING ÈTIC	▪ Aprendre i ampliar capacitats ▪ Fer diners ▪ Diversió ▪ Progrés i carrera professional ▪ Protecció d'individus i negocis	▪ Explotació de vulnerabilitats ▪ Enginyeria social	▪ Revelació de vulnerabilitats ▪ Exigència d'una recompensa

El 2021, els **ciberatacs amb afectació a Catalunya** publicats als mitjans van créixer un **11%** respecte l'any anterior

S'estima que només es denuncia el **10% dels ciberdelictes** que es cometen cada any.

Al món, el 2021 es va produir **un atac de *ransomware* cada 11 segons** i es preveu que el 2031 els atacs es duran a terme cada 2 segons.

Més de la meitat dels ciberatacs es cometen contra les pimes, i el **60 %** fan fallida en els sis mesos següents de ser víctimes de piratejos.

Els costos mundials de la ciberdelinqüència creixeran fins els **9,5 bilions d'euros** anuals el 2025, davant els 2,7 bilions del 2015.

El frau publicitari digital causa pèrdues de **46 milions d'euros** al dia, i el 2023 aquesta xifra es disparará fins als 275 milions de dòlars diaris.

Font: Cybersecurity Ventures

Digitalització (DESI)

El DESI (*Digital Economy and Society Index*) és un índex compost publicat per la Comissió Europea que mesura el progrés dels països de la UE cap a una economia i societat digitals.

El DESI 2020 va atorgar a Catalunya el **5è** lloc en el conjunt d'estats de la UE

El DESI es calcula a partir de 5 dimensions:

Connectivitat

Capital humà

Ús de serveis d'Internet

Integració de tecnologia digital

Serveis públics digitals

Ciberseguretat (GCI)

El GCI (*Global Cybersecurity Index*) és un índex publicat per la ITU (*International Telecommunication Union*) que mesura el nivell de compromís dels països en matèria de ciberseguretat.

El GCI 2020 va atorgar a Catalunya el **8è** lloc en el conjunt d'estats de la UE

El GCI es calcula a partir de 5 pilars:

Mesures legals

Mesures tècniques

Mesures organitzatives

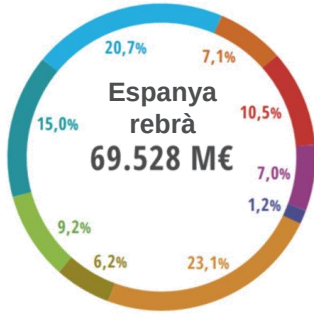
Mesures de capacitació

Mesures de coordinació

Font: Generalitat de Catalunya

El Pla NextGen EU impulsarà la digitalització de la indústria

El Pla s'estructura em 4 eixos i 10 palanques



Es tracta d'un pla de recuperació dotat en més de 800 mil milions d'euros per fer una UE post-pandèmia més ecològica, digital, resilient i adaptada als reptes actuals i futurs.

La palanca V "Modernització i digitalització de l'ecosistema de les nostres empreses" està dotada amb gairebé el 23,1% dels 69.528 milions d'euros que rebrà l'Estat espanyol.

Els fons per a l'Estat destinats al desenvolupament de la palanca V

Transformació digital de la indústria	Impulsar les pimes	Modernitzar el sector turístic	Potenciar el 5G i el talent en ciberseguretat
3.782 M€	**4.894 M€**	**3.400 M€**	**3.999 M€**

El Kit Digital, una subvenció de fins a 12.000 € per a la digitalització d'autònoms i pimes, inclou el desplegament solucions de ciberseguretat

La ciberseguretat esdevé un pilar essencial per a l'èxit del Pla NextGen

L'impuls per a la digitalització tindrà implicacions en matèria de ciberamenaces. Per una banda, augmentarà el valor dels actius digitals de les empreses, administracions i la societat en general, els quals esdevindran un reclam pel cibercrim. Per altra banda, les noves tecnologies vindran acompanyades de nous riscos cibernètics que plantejaran un gran repte per a la ciberseguretat.

Font: *Plan de Recuperación y Resiliencia*

Necessitat de confiança

La ciberseguretat és una palanca generadora de la confiança necessària per a promoure l'ús de les noves tecnologies, essencial per a l'èxit de la transformació digital i el bon funcionament de l'activitat econòmica.

81 % dels ciutadans europeus creu que Internet i les eines digitals exerciran un paper important en el futur.

13,8 % de la població de l'Estat espanyol té poca o cap confiança en Internet.

82 % dels ciutadans europeus considera útil la definició i promoció d'una visió europea comuna sobre drets i principis digitals.

Esquema de certificació en ciberseguretat

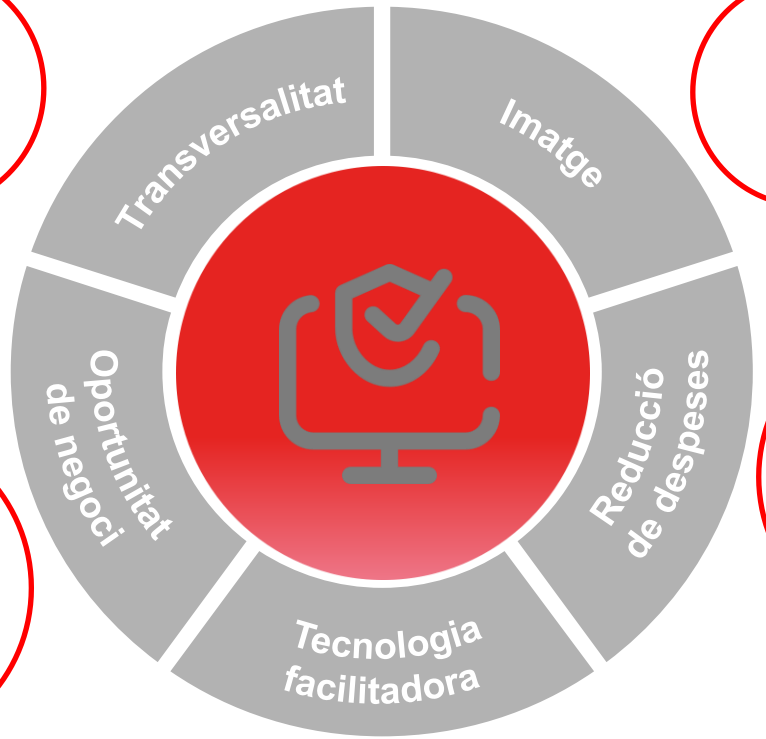
D'acord amb la Cybersecurity Act, la Unió Europea està desenvolupant diferents marcs de certificació que establiran un conjunt de regles, requisits tècnics, estàndards i procediments per a garantir que productes i serveis TIC compleixin uns requisits de ciberseguretat.

1. Incrementar la ciberseguretat i la confiança en els productes i serveis digitals de la UE
2. Incrementar la competitivitat i el creixement de les empreses europees
3. Millorar les condicions del mercat intern per evitar la dependència exterior en matèria de ciberseguretat

Fonts: Eurobaròmetre y Observaciber

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.

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.

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.

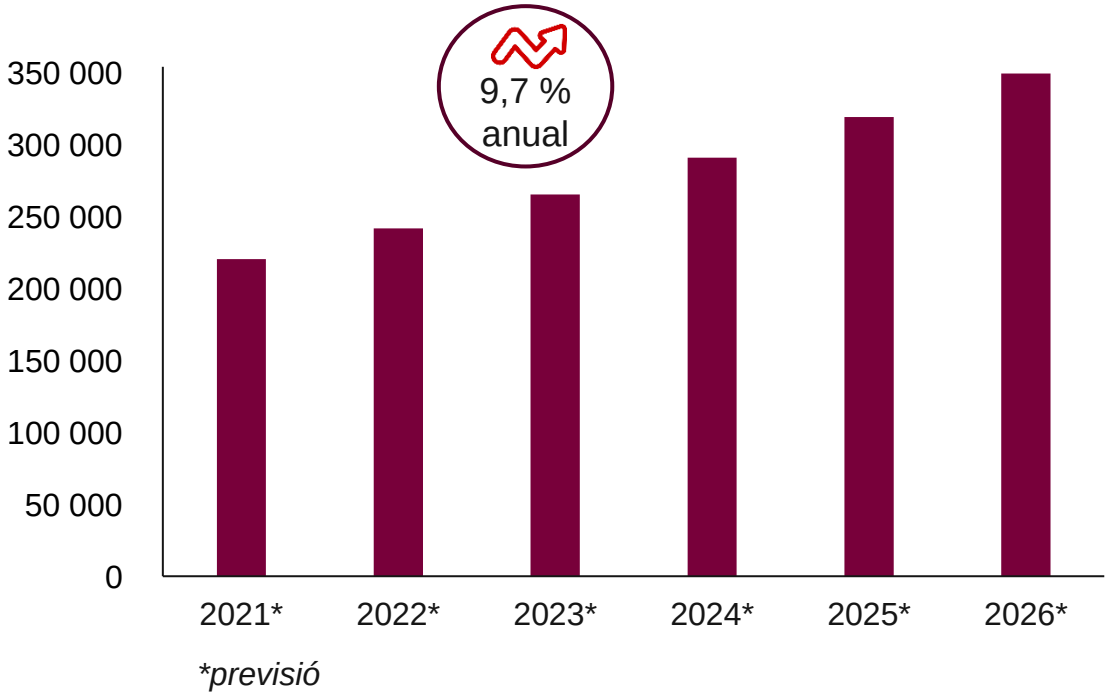
La ciberseguretat pot contribuir al ple desenvolupament d'altres tecnologies innovadores com la IoT, el vehicle connectat, la indústria 4.0, la salut digital o el comerç electrònic.

2. Principals magnituds mundials

La facturació en ciberseguretat creixerà a un ritme del **9,7 % anual** entre 2021 i 2026, fins als **345 400 milions de dòlars**.

Facturació mundial de la ciberseguretat

2021-2026, milions de dòlars



**previsió*

	Països	% de creixement anual 2021 - 2026
1	Estats Units	7,6 %
2	Xina	19,5 %
3	Regne Unit	9,5 %
4	Japó	8,1 %
5	Alemanya	7,8 %
6	França	8,1 %
7	Austràlia	9,2 %
8	Corea del Sud	12,7 %
9	Canadà	9,2 %
10	Índia	17,7 %
11	Països Baixos	8,0 %
12	Itàlia	7,3 %
13	Espanya	9,2 %
14	Brasil	8,9 %
15	Suïssa	8,5 %

Països ordenats per valor de mercat el 2021

Font: Statista

Empreses líders en ciberseguretat

Nota: empreses ordenades per facturació. Les empreses s'inclouen segons els supòsits realitzats per la base de dades de la font. El llistat no és exhaustiu.

Presència a Catalunya

Font: Statista a partir de dades de Xignite

La IED en ciberseguretat ha estat rècord el 2021, tant en capital invertit (**9.421,6** milions d'euros) com en nombre de projectes (**345**). Canadà és el principal país receptor, amb més de 2.000 milions d'euros captats.

Inversió en ciberseguretat

Any	Projectes	Capital invertit (M€)
2017	151	3.542,7
2018	183	7.936,7
2019	176	1.946,8
2020	144	3.706,6
2021	345	9.421,6

Principals empreses inversores

2017 – 2021

CLOUDFLARE
8.695,7 M€

netskope
1.267,1 M€

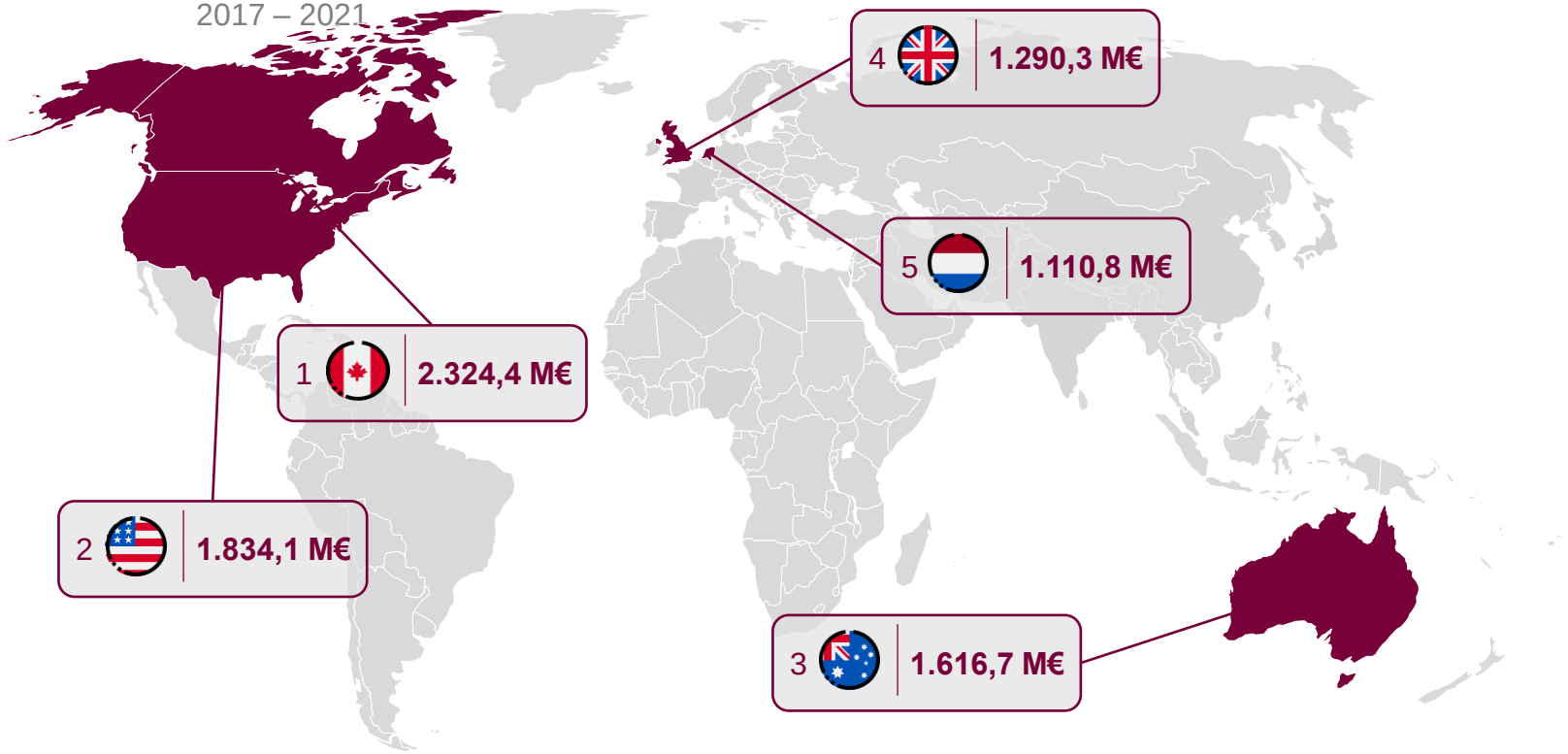
Microsoft
989,6 M€

accenture
821,9 M€

FUTUREX
763,3 M€

Principals països receptors d'inversió

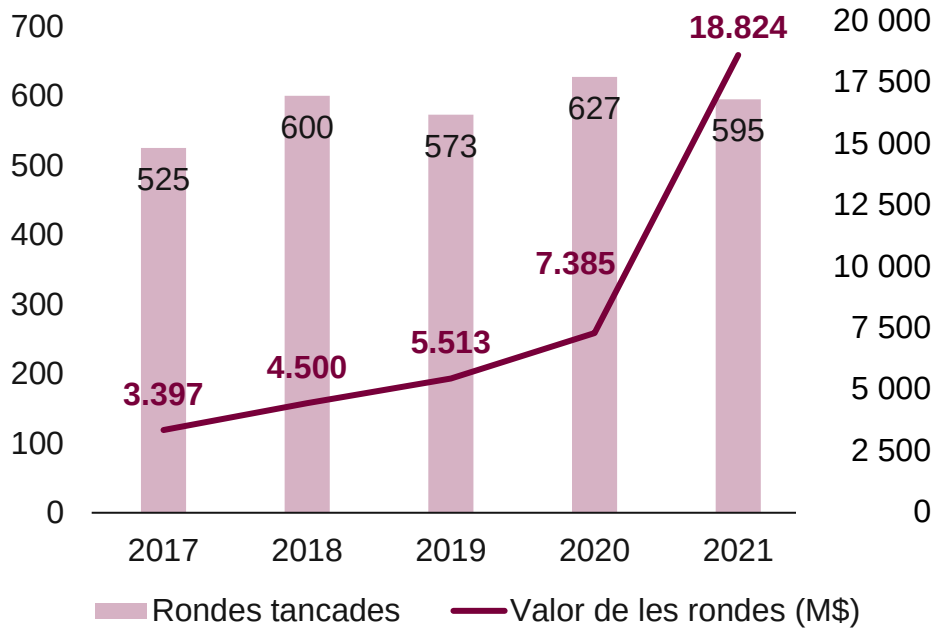
2017 – 2021



Font: fDi Markets

El 2021 ha estat un any rècord en capital de risc en startups de ciberseguretat al món, amb 18 824 milions de dòlars, la qual cosa ha més que doblat les dades de 2020. Les startups nord-americanes lideren el rànquing de manera molt destacada.

Rondes d'inversió en ciberseguretat



Nota: S'inclouen les rondes d'inversió pre-seed, seed i les sèries A-J. Les dades fan referència al període 2017-2021.

Valor i nombre de rondes tancades als principals països

31 046 M$	**3.086 M$**	**1.369 M$**	**1.063 M$**	**867 M$**
1.580 rondes	262 rondes	253 rondes	60 rondes	79 rondes

Principals startups per valor de rondes tancades

1.891 M$	**1.229 M$**	**1.039 M$**	**926 M$**	**910 M$**

Principals inversors en capital de risc

Font: Crunchbase

Hi ha **45** startups de ciberseguretat al món valorades en més de 1.000 milions de dòlars.

Principals unicorns en ciberseguretat

TANIUM 9.000 M$	snyk 8.600 M$	LACEWORK 8.300 M$
netskope 7.500 M$	1Password 6.800 M$	WIZ 6.000 M$
Socure 4.500 M$	ARCTIC WOLF 4.300 M$	Coalition 3.500 M$
FORTER 3.000 M$	illumio 2.750 M$	transmit security 2.740 M$
Acronis 2.500 M$	CATO NETWORKS 2.500 M$	AURA 2.500 M$

Nota: Unicorns ordenats per valoració.

Font: CB Insights

En els darrers 5 anys s'han produït **708 fusions i adquisicions** d'empreses de ciberseguretat

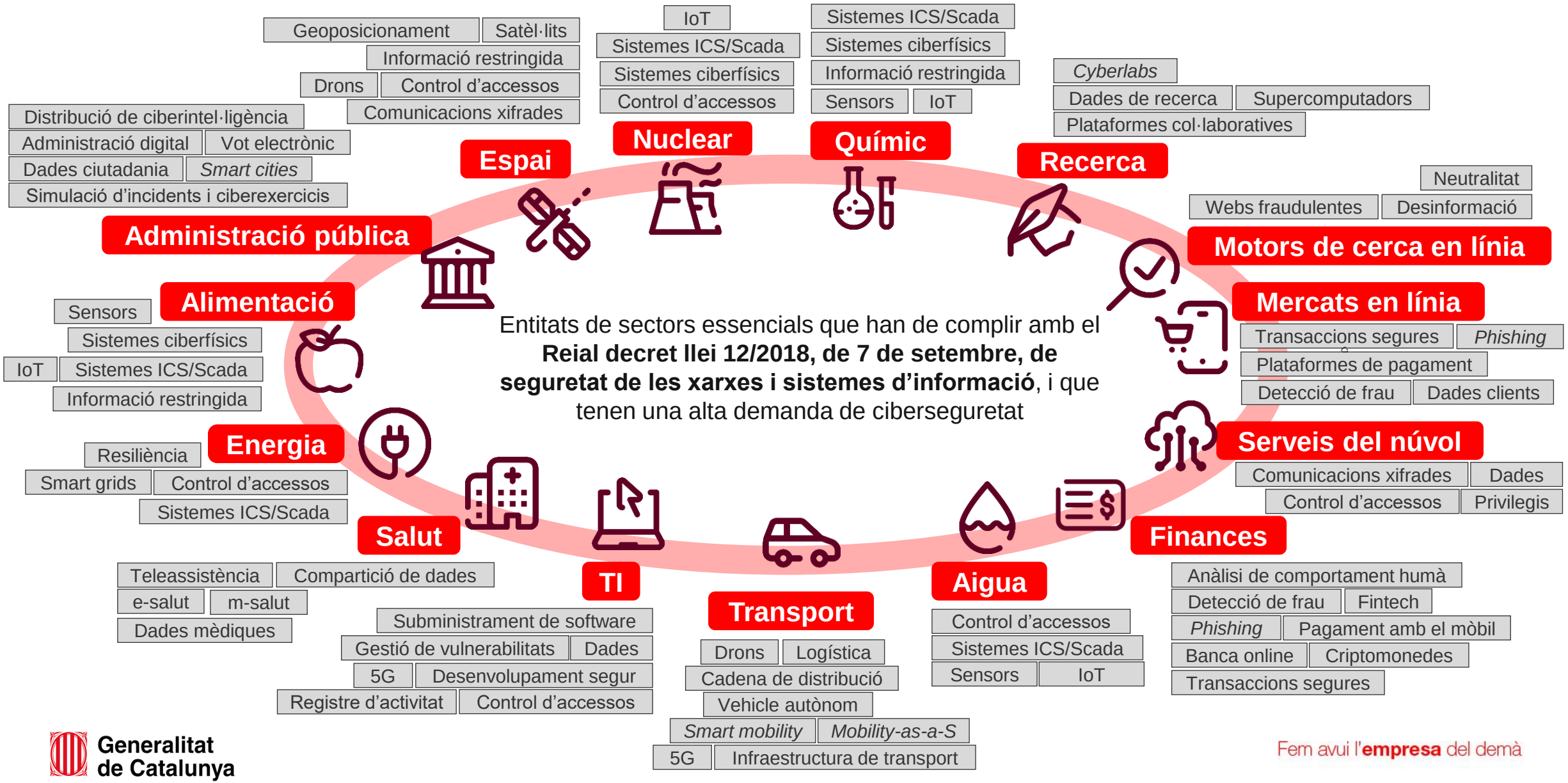
Principals fusions i adquisicions

2017 – 2021

Empresa adquirida	Empresa compradora	Import d'adquisició
Symantec ha desenvolupat un *software* de seguretat que consta de funcions antimalware, antiintrusió i tallafocs per a servidors i ordinadors.	Broadcom	10.700 M$
McAfee ofereix serveis i productes de xarxa i ciberseguretat.	Symphony Technology Group	4.000 M$
Sophos desenvolupa productes de seguretat de xarxes i gestió d'amenaces per protegir les organitzacions contra actes maliciosos.	Thoma Bravo	3.900 M$

Font: Crunchbase

3. Aplicacions prospectives per sector de demanda


Entitats de sectors essencials que han de complir amb el **Reial decret llei 12/2018, de 7 de setembre, de seguretat de les xarxes i sistemes d'informació**, i que tenen una alta demanda de ciberseguretat
Espai
Geoposicionament
Satèl·lits
Informació restringida
Drons
Control d'accessos
Comunicacions xifrades
Nuclear
IoT
Sistemes ICS/Scada
Sistemes ciberfísics
Control d'accessos
Químic
Sistemes ICS/Scada
Sistemes ciberfísics
Informació restringida
Sensors
IoT
Recerca
Cyberlabs
Dades de recerca
Supercomputadors
Plataformes col·laboratives
Administració pública
Distribució de ciberintel·ligència
Administració digital
Vot electrònic
Dades ciutadania
Smart cities
Simulació d'incidents i ciberexercicis
Motors de cerca en línia
Neutralitat
Webs fraudulentes
Desinformació
Alimentació
Sensors
Sistemes ciberfísics
IoT
Sistemes ICS/Scada
Informació restringida
Mercats en línia
Transaccions segures
Phishing
Plataformes de pagament
Detecció de frau
Dades clients
Energia
Resiliència
Smart grids
Control d'accessos
Sistemes ICS/Scada
Serveis del núvol
Comunicacions xifrades
Dades
Control d'accessos
Privilegis
Salut
Teleassistència
Compartició de dades
e-salut
m-salut
Dades mèdiques
TI
Subministrament de software
Gestió de vulnerabilitats
Dades
5G
Desenvolupament segur
Registre d'activitat
Control d'accessos
Transport
Drons
Logística
Cadena de distribució
Vehicle autònom
Smart mobility
Mobility-as-a-S
5G
Infraestructura de transport
Aigua
Control d'accessos
Sistemes ICS/Scada
Sensors
IoT
Finances
Anàlisi de comportament humà
Detecció de frau
Fintech
Phishing
Pagament amb el mòbil
Banca online
Criptomonedes
Transaccions segures

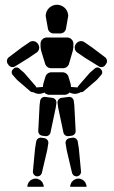
INTEL·LIGÈNCIA ARTIFICIAL

La IA esdevé un element clau per fer front a l'increment de la complexitat de les xarxes i de les ciberamenaces. Any rere any, té més rellevància en molts àmbits que requereixen l'anàlisi en temps real de volums de dades massa complexes per a un humà: detecció d'amenaces, vigilància de la xarxa, recerca de vulnerabilitats, etc .

METAVERS I WEB 3

L'aparició de l'experiència del metavers i el desplegament de la web 3 accentuaran la participació dels usuaris en entorns virtuals complexos on es comunicaran persones, empreses i màquines. S'elevarà l'ús de les dades personals i de la interacció digital a un altre nivell, amb l'aparició de nous ciberriscos.

DIGITAL TWINS



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

SISTEMES CIBERFÍSICS

Els sistemes ciberfísics disparà el desenvolupament de la Indústria 4.0, però al mateix temps acostarà la distància entre la seguretat física i la ciberseguretat, amb el creuament dels riscos i dels impactes dels mons físic i cibernètic. Els CPS (*cyber-physical systems*) hauran d'estar preparats perquè un incident informàtic no impacti el món físic, o a l'inrevés.

ZERO TRUST

Les organitzacions no poden confiar únicament en els controls de perímetre (tallafocs, VPN, etc.) per controlar els accessos a la xarxa, ja que el perímetre tradicional, després de la incorporació del teletreball, pràcticament s'ha esfumat. Els models de confiança zero esdevindran l'estratègia escollida per assegurar la xarxa interna.

SEGURETAT AL NÚVOL

Les organitzacions esdevenen *cloud-cèntriques*: necessitaran la flexibilitat de la ciberseguretat oferta des del núvol per mitjà d'arquitectures de seguretat SASE (*Secure Access Service Edge*) i controls d'accessos amb sistemes CASB (*Cloud Access Security Broker*). Són tecnologies amb alguns anys, però ara ha arribat el seu moment.

5G

Les xarxes 5G permetran el desenvolupament d'altres tecnologies emergents, com l'IoT, les comunicacions hologràfiques, l'e-salut, etc. Presenta un nou paradigma amb diferents mitjans de tractament de dades, establir connexions, etc. Que augmentaran la complexitat i la superfície d'atac de amb moltes més parts interactives i heterogènies. I el 6G ja està sobre la taula.

SMART CITIES

Les ciutats adopten noves tecnologies: sensors per a la recopilació de dades, sistemes de *big data* i intel·ligència artificial per optimitzar la presa de decisions en la gestió operativa i el govern de la ciutat, els sistemes d'*smart mobility*, etc. Ara bé, al mateix temps, incorporen nous factors de risc cibernètic, motiu pel qual les mesures de ciberseguretat passen a ser protagonistes.

4. Tendències en ciberseguretat i impacte en els ODS

Ransomware. Els atacs amb afectació a Catalunya publicats en els mitjans han augmentat un 200 % i incorporen factors d'extorsió com l'amenaça de filtració de dades robades i atacs de DDoS.

Atacs de DDoS. Han crescut un 29 % al món i augmenten en potència i complexitat per evitar ser bloquejats.

Atacs a la cadena de subministrament. S'han triplicat durant l'any i les empreses tecnològiques esdevenen l'objectiu principal.

Fuites de dades personals. S'han exposat 40 000 M de registres, més que mai. Els errors de configuració, vulnerabilitats en API i l'*scraping* en xarxes socials, les principals causes.

Criptomonedes. Han assolit valors de rècord i el cibercrim ha desplegat campanyes de *cryptojacking* i robatoris a usuaris i plataformes de canvi.

Ciberatacs contra el sector públic. Han augmentat un 80 % a Catalunya amb incidents de *ransomware* en ajuntaments i universitats i l'atac de DDoS a la Generalitat de Catalunya.

Vulnerabilitats de de *zero-day*. La seva explotació ha augmentat més d'un 100 % i ha arribat a registres històrics, i el cibercrim ja té la capacitat econòmica per a aprofitar-se'n.

Accessos remots. Les tecnologies de teletreball (RDP, VPN, correu electrònic, etc.) han estat objectiu de ciberatacs mitjançant l'explotació de vulnerabilitats o l'ús de credencials robades.

Cooperació global contra el cibercrim. Els estats s'alien per combatre el cibercrim, especialment el *ransomware*, com en la reunió de 32 estats per a fixar una estratègia comuna.

Accions policials. Les forces de l'ordre han actuat contra operadors de *ransomware* com REvil, Cl0p i s'ha forçat el tancament dels mercats negres més importants en la *dark web*.

Operadors de *ransomware.* S'han adaptat i han canviat estructura, models de negoci, objectius i tècniques, o han cessat la seva activitat per evitar ser enxampats per les forces de l'ordre.

Crime as a service. Ha evolucionat i els cibercriminals han adoptat l'*exploit as a service* (venda/lloguer d'*exploits*) i l'*access as a service* (venda d'accessos a xarxes d'organitzacions).

Font: diverses fonts

El 2021, any de rècords en matèria de ciberseguretat

+50 %

Més ciberatacs que mai
S'ha assolit el màxim històric de ciberatacs, segons Checkpoint, fins a un 50 % més respecte del 2020.

220 M€

El rescat més gran mai exigit
El 4t trimestre, MediaMarkt va patir un atac de *ransomware* amb una exigència de 220 M€.

3,47 Tbps

Atac de DDoS més potent de la història
El desembre, Microsoft va detectar i aconseguir bloquejar un atac de DDoS de 3,47 Tbps.

500 M€

Robatori de criptomonedes més gran
El protocol d'interoperabilitat entre cadenes de blocs PolyNetwork va patir un robatori superior als 500 M€ arran de l'explotació d'una vulnerabilitat.

12 250 M€

Major moviment il·lícit de criptomonedes
S'han comptabilitzat més de 12 000 M€ en moviments de criptomonedes d'adreces il·lícites, un 80 % més respecte **del** 2020.

746 M€

Màxima sanció per incompliment del RGPD
Amazon va rebre una sanció de 746 M€ de l'autoritat de protecció de dades de Luxemburg per incomplir el Reglament general de protecció de dades.

8.400 M de credencials

Recopilació de credencials històrica
En el 2n trimestre, es va identificar una base de dades de 8.400 M de credencials amb origen en diferents fuites.

40 000 M de registres

Major volum de dades personals filtrades
La quantitat de dades personals exposades supera qualsevol any anterior. Les fuites per sobre dels 1.000 M de registres de dades personals són cada cop més habituals.

Font: diverses fonts

Font: diverses fonts

- **Tancament d'Emotet i DarkMarket.** Una operació conjunta de la policia de sis països europeus, Canadà i els EUA va permetre prendre el control de la *botnet* Emotet, i la policia alemanya va tancar el mercat negre més gran del món, DarkMarket.

- **Conseqüències de SolarWinds.** El govern dels EUA va emetre una ordre executiva per revisar les cadenes de subministrament arran de l'impacte del ciberatac viscut per SolarWinds, que va afectar múltiples agències i entitats governamentals a tot el món.

- **Microsoft Exchange.** Un conjunt de vulnerabilitats de dia zero als servidors Exchange permetien a un atacant prendre'n el control sense necessitat de credencials. En el moment de la seva detecció, ja hi havia actors maliciosos que l'explotaven.

- **Tensions al ciberespai entre Iran i Israel.** Israel va confirmar haver dut a terme ciberatacs contra les instal·lacions del reactor nuclear de Natanz, a l'Iran, quan es pretenia accelerar la producció d'urani enriquit.

- **Colonial Pipeline.** La companyia, operadora d'un oleoducte dels EUA, va reiniciar les seves operacions després de pagar un rescat de 4 M€ per un atac de *ransomware*. L'FBI va atribuir l'atac al grup DarkSide que opera des de Rússia.

- **JBS.** L'empresa brasilera, una de les càrniques més importants del món, va ser víctima d'un atac de *ransomware* atribuït al grup Revil. Per evitar una llarga aturada en la producció, va anunciar que havia realitzat el pagament d'11 M€ en concepte de rescat.

- **Kaseya.** La companyia de software d'administració TI va ser víctima d'un atac de *ransomware* que es va propagar per la cadena de subministrament a unes 1.500 entitats de 17 països per la descàrrega d'una actualització maliciosa.

- **PolyNetwork.** Un hacker va explotar una vulnerabilitat per desviar les transferències dels usuaris de PolyNetwor, un protocol d'interoperabilitat entre *blockchains*. La suma desviada va superar els 500 M€, tot i que es va recuperar.

- **Impacte del *ransomware* a hospitals.** Una enquesta a 597 organitzacions sanitàries dels EUA va constatar que el *ransomware* afecta la capacitat assistencial, un fet que suposa un risc per la qualitat del tractament dels pacients.

- **Cimera contra el cibercrim.** El president dels EUA va convocar 32 països a una reunió amb l'objectiu de millorar la manera de combatre els atacs de *ransomware* mitjançant una estratègia comuna i global.

- **Rescat rècord a MediaMarkt.** Un atac amb el *ransomware* Hive va afectar les seves botigues de l'empresa alemanya Mediamarkt a Europa, a les portes del Black Firday. El reclam d'un rescat de 212 M€ ha estat la xifra més alta mai informada.

- **Log4Shell.** Es van publicar diferents vulnerabilitats de dia zero que, qualificades com a crítiques, afecten algunes versions de la biblioteca Log4J. Poden esdevenir les pitjors en la història per la quantitat d'equips vulnerables i la dificultat d'apedaçar-les.

Font: diverses fonts

- **Segrest de xarxes socials.** L'alcalde de Terrassa va ser víctima del robatori del seu compte d'Instagram. Els ciberdelinqüents exigien "quantitats elevades de diners" per recuperar-lo.

- **Proveïdor *cloud*.** Un atac amb el *ransomware* Ryuk a un proveïdor de serveis al núvol va xifrar la informació de desenes de despatxos professionals catalans que s'han quedat sense dades d'expedients, etc.

- **AMB.** L'Àrea Metropolitana de Barcelona va ser víctima d'un atac de *ransomware* que va afectar els serveis de tramitació electrònica i les instal·lacions que gestiona aquest ens.

- **The Phone House.** L'empresa de productes i serveis de telefonia mòbil va ser víctima d'un atac de *ransomware* amb el robatori d'informació. Es va negar a pagar el rescat i es van acabar filtrant més de 700.000 registres de clients catalans.

- **Campanyes de difusió de *malware* bancari.** Es van detectar diferents campanyes de difusió del troià bancari Bizarro afectant usuaris de l'Estat espanyol i Europa. El troià permet robar les credencials de clients de fins a 70 entitats bancàries.

- **Noves campanyes de *phishing*.** Es va alertar de campanyes de *phishing* dirigides a clients de les entitats BBVA, CaixaBank i Banco Santander. En el cas de CaixaBank, els correus utilitzaven l'anunci de la fusió amb Bankia com a esquer.

- **Ciberespionatge amb Pegasus.** Una filtració va revelar una llista d'objectius potencials de l'*spyware* Pegasus amb 50.000 contactes, de més de 50 països, espiats per 10 governs. La llista incloïa alguns polítics catalans.

- **Engany de falsos *hackers*.** La Policia Nacional va detenir 10 falsos hackers per estafar a més de 430 persones que havien contractat els seus serveis. Els agents van practicat registres a Barcelona, Girona i altres regions de l'Estat.

- **Olympus.** El gegant tecnològic va ser víctima d'un atac de *ransomware* del grup BlackMatter. Entre els seus clients hi havia centres sanitaris de Catalunya que van activar mecanismes d'alerta

- **UAB.** Un atac amb el *ransomware* Pysa va impactar la Universitat Autònoma de Barcelona. L'atac va obligar a desconnectar tots els sistemes i algunes fonts van especular amb la petició d'un rescat de 3 M€.

- **Damm.** Un atac informàtic va obligar l'empresa cervesera Damm a aturar la producció. L'empresa va activar el protocol de resposta que li va permetre restablir la producció.

- **Generalitat de Catalunya.** La institució va ser objectiu d'un atac de DDoS dirigit a col·lapsar el nus de telecomunicacions de la institució. El ciberatac va afectar l'operativa de múltiples serveis de la Generalitat de Catalunya.

Font: diverses fonts

Les vulnerabilitats Log4Shell poden esdevenir les més greus de la història: la llibreria Log4J està present en molts dispositius, servidors i aplicacions web, són complicades d'apedaçar, existeixen *exploits* i són fàcils d'explotar.

47% de les xarxes corporatives del món havien intentat ser explotades a final de 2021

9.000 IP 1,4% de les IP de Catalunya fan ús d'un servei Java i són potencialment vulnerables

- El 9 de desembre de 2021 es va publicar la vulnerabilitat crítica de dia zero Log4Shell (CVE-2021-44228), que afectava algunes versions de la biblioteca Log4J; pocs dies després se'n publicava una de nova (CVE-2021-45046), i més tard encara una altra, aquest cop qualificada com a alta (CVE-2021-45105).

- La llibreria Log4J, desenvolupada en Java l'Apache Software Fundation, permet escriure missatges de registre i el seu ús s'ha estès per centenars de milions de dispositius d'arreu del món.

Grups APT i organitzacions cibercriminals han explotat, i seguiran explotant, aquestes vulnerabilitats que permeten el robatori de dades, la instal·lació de *malware*, la denegació de servei (DoS), etc.

En aquest context, els models de gestió de vulnerabilitats àgils i efectius esdevenen cada cop més imprescindibles per a les organitzacions.

Font: Check Point i BitSight

Es redueix la bretxa mundial

Segons (ISC)[2], la bretxa de professionals en ciberseguretat se situa en 2,7 milions de vacants al món.

La bretxa global s'ha reduït un 13 % respecte de 2020, gràcies als 700 000 nous professionals en el mercat laboral.

Els països on creixen més els professionals de ciberseguretat són Alemanya (165 %), Singapur (61 %) i els EUA (30 %).

	2019	2020	2021
Europa	543 000	830 187	1 086 146
Regne Unit	289 000	365 823	300 087
França	121 000	118 302	146 808
Alemanya	133 000	175 159	464 782
Irlanda	N/A	14 212	15 028
Espanya	N/A	122 284	124 336
Països Baixos	N/A	34 406	35 106

Creix la bretxa a la UE i a Catalunya, tot i que es generen més professionals

Malgrat la millora global, a la UE i a Catalunya la bretxa continua creixent i se situa en 199 000 (+18 %) i més de 6.000 (+30 %) professionals respectivament.

A CATALUNYA ES GENEREN >600 NOUS PROFESSIONALS EN CIBERSEGURETAT

Institut de Formació Contínua-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	UOC 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	UPC Universitat Politècnica de Catalunya BarcelonaTech: Màster Cybersecurity Management	laSalle Universitat Ramon Llull: Màster en Ciberseguretat
uic barcelona: Postgrau en Compliance i Ciberseguretat	Universitat de Lleida: Màster en Ciberseguretat	telecos BCN: Màster en Ciberseguretat
unir La Universidad en Internet: Màster Universitari en Seguretat Informàtica	NUCLIO Digital School: Màster en Ciberseguretat	**28 centres de formació professional**

Font: diverses fonts com (ISC)[2] o l'Eurobaròmetre

La ciberseguretat, eix central en un món marcat pels efectes de la pandèmia

- La consolidació del teletreball exigirà reforçar la ciberseguretat.
- La dependència de les TIC posarà el focus en la ciberresiliència.
- Els pressupostos destinats a la ciberseguretat augmentaran per fer front a la proliferació de ciberatacs.
- Els conflictes armats, com el de Rússia i Ucraïna, derivaran en guerres híbrides.

Les TIC i la ciberseguretat, omnipresents en el dia a dia de la societat digital

- Creixerà l'ús d'Internet i la ciberseguretat serà present a tot arreu.
- La separació entre els mons físic i virtual es difuminarà i hi haurà transvasament de riscos i impactes
- Augmentarà la sensibilitat sobre la privacitat, i la ciutadania podrà accedir a nous serveis per preservar-la.
- La *e-health* integrarà la ciberseguretat en persones, processos i tecnologies.

Ciberamenaces evolucionades i majors impactes arran de l'impuls del negoci del cibercrim

- Els principals objectius dels ciberatacs seran els serveis essencials.
- Els ciberatacs a la cadena de subministrament provocaran afectacions a gran escala.
- Els operadors de *ransomware* industrialitzaran la seva activitat i incorporaran nous factors d'extorsió.
- Grans *botnets* perpetraran atacs de DDoS més devastadors per a l'extorsió.
- Un cibercrim econòmicament capacitat adquirirà els *exploits* de vulnerabilitats de dia zero.

Cooperació, ciberresiliència, sectors essencials i formació: pilars per a un ecosistema cibersegur

- Múltiples noves iniciatives materialitzaran l'Estratègia de ciberseguretat europea.
- Noves normes a la UE: NIS 2, ciberresiliència, DORA, Llei europea de xips, esquemes de certificació, etc.
- Naixeran noves formacions per a la capacitació de professionals en ciberseguretat.
- Les polítiques *zero-trust* es convertiran en prioritat i model de molts sistemes de gestió de la ciberseguretat.

Font: diverses fonts com la Comissió Europea o Hiscox

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

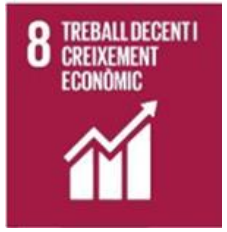
- Els ODS s'integren dins l'Agenda 2030 de Desenvolupament Sostenible de les Nacions Unides, la finalitat de la qual és millorar la qualitat de vida i el benestar social de tots els habitants del planeta, per tal de garantir el progrés i el desenvolupament econòmic de manera sostenible i respectuosa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

Font: Nacions Unides

Protegir dades mèdiques i permetre'n la compartició anonimitzada per a la recerca de vacunes i tractaments, tot preservant la privacitat dels pacients.
Desplegar dispositius mèdics interconnectats que comparteixin informació del pacient amb total seguretat i fiabilitat per garantir la monitorització i el tractament a distància.

Garantir una educació a distància de qualitat accessible per al conjunt de la ciutadania en condicions de seguretat, mitjançant eines informàtiques netes de programari maliciós i sota unes condicions de privacitat i llibertat.
L'accés a la informació ha de garantir que les fonts siguin fiables i íntegres.

Promocionar la presència de la dona en el 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.



En la construcció d'un sistema econòmic global més segur i fiable és necessari desenvolupar processos, protocols i estàndards. Això contribueix a desenvolupar un ecosistema empresarial en què tots els elements de la cadena (socis, proveïdors i clients) puguin confiar entre ells i en les tecnologies de comerç en línia.

Protegir tot el procés de digitalització, els entorns industrials i les infraestructures crítiques amb la corresponent diagnosi d'adequació i compliment.
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 a 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 de 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 concreta.

5. Ciberseguretat dels objectes connectats

L'impacte creixent dels ciberatacs impulsa el creixement del mercat de seguretat dels objectes connectats.

- Un nombre creixent de ciberatacs ha utilitzat dispositius de la internet de les coses com a punt d'entrada a la infraestructura informàtica de l'empresa o per infectar-los i crear grans botnets per dur a terme activitats il·lícites. Això exposa la internet de les coses com l'enllaç més feble de la seguretat empresarial.

- L'adopció de dispositius connectats augmenta ràpidament i, segons les estimacions de la indústria, hi haurà més de 75 000 milions de dispositius connectats al mercat l'any 2025. Tanmateix, això augmenta les preocupacions de seguretat. El 2019, gairebé el 70 % de les empreses que havien adoptat dispositius connectats van experimentar pèrdues comercials a causa dels pirates informàtics.

- Assegurar un dispositiu en cada fase del cicle de vida és clau. Les solucions basades en la identitat de dispositius que poden ajudar a protegir els dispositius de la internet de les coses (des de la seva producció a través d'operacions de camp i actualitzacions de seguretat) són essencials per a la seguretat de la internet de les coses.

Més del 30 % dels atacs identificats a les empreses implicaran dispositius connectats el 2020

Dels nous dispositius connectats intel·ligents, el 90 % requereixen capacitats avançades de protecció contra amenaces

2x

La quantitat de dispositius sense protecció a l'ecosistema connectat gairebé es va duplicar

Font: Frost&Sullivan

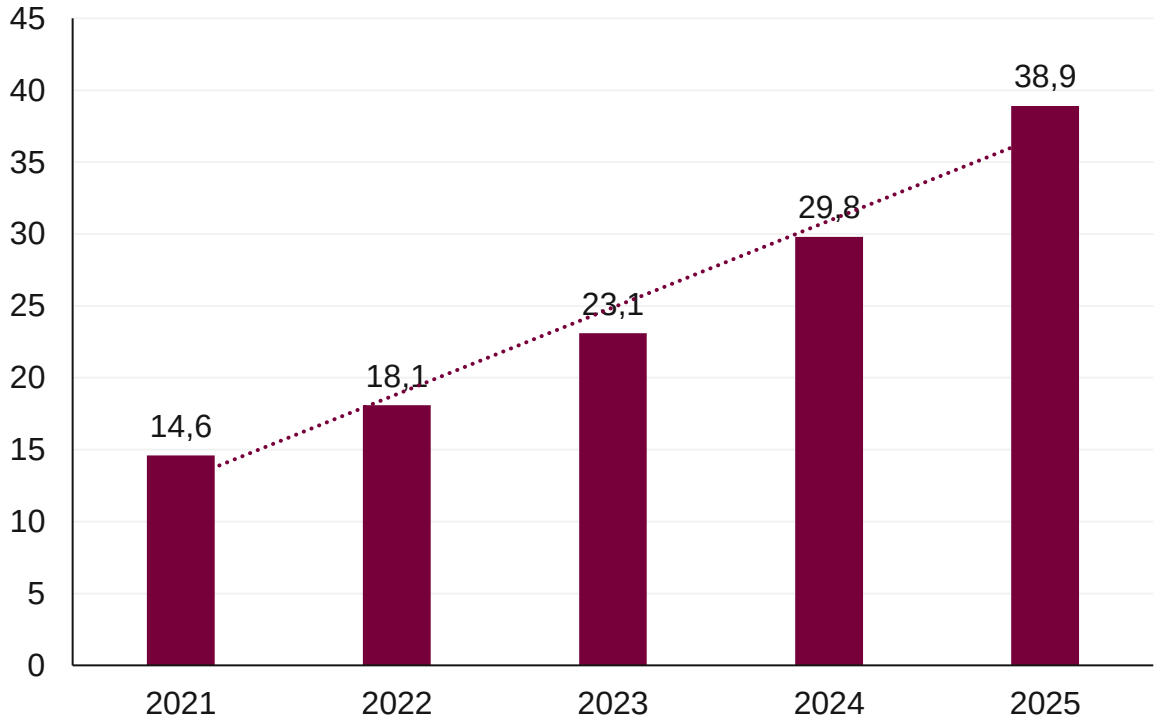
El mercat global de ciberseguretat d'objectes connectats passarà de **14 600** milions de dòlars el 2021 a **38 900** milions de dòlars el 2025, amb un creixement anual del **27,8 %**.

- Els dispositius i sensors intel·ligents de la internet de les coses en la fabricació estan transformant les fàbriques tradicionals, i els permeten estar més connectades i impulsar l'eficiència operativa. Aquests dispositius de la internet de les coses també creen nous punts d'atac per a ciberamenaces i requereixen seguretat.

- L'aparició dels cotxes autònoms i connectats, les ciutats intel·ligents i la digitalització d'infraestructures crítiques, com sistemes d'energia, d'aigua o hospitals, impulsa l'adopció de la seguretat dels objectes intel·ligents perquè utilitzen molts dispositius connectats per emmagatzemar i intercanviar dades que cal protegir.

Previsió de facturació de ciberseguretat dels objectes intel·ligents

2021-2025, milers de milions de dòlars



Font: Frost&Sullivan

Amèrica del Nord

Amèrica del Nord és un actor important al mercat global de seguretat d'objectes intel·ligents.
La ràpida evolució dels cotxes autònoms i la seva disponibilitat requereixen seguretat d'objectes intel·ligents per bloquejar les amenaces i mantenir la transmissió de dades segura. L'augment de la despesa del govern federal i del sector privat en l'espai de seguretat IoT també és un factor impulsor per al mercat.

Europa

Les empreses europees estan experimentant una digitalització ràpida i s'estan canviant cap a la força de treball mòbil i l'adopció d'infraestructures de núvol híbrid. Això està creant nous punts finals d'IoT que són vulnerables als ciberatacs. El sector sanitari és un altre dels principals adoptants de seguretat d'objectes intel·ligents a Europa, especialment després de la crisis de la COVID-19.

Àsia - Pacífic

El mercat de l'àrea Àsia – Pacífic serà un dels que experimentarà més ràpid creixement perquè les iniciatives governamentals cap a la digitalització industrial i les ciutats intel·ligents estan provocant un creixement exponencial dels dispositius connectats que s'han de garantir.
A més, la indústria 4.0 a diversos països representa un mercat important per a la seguretat d'objectes intel·ligents.

Font: Frost&Sullivan

Entre 2018 i 2020, s'han publicat **20.908 patents** a tot el món relacionades amb seguretat d'objectes connectats

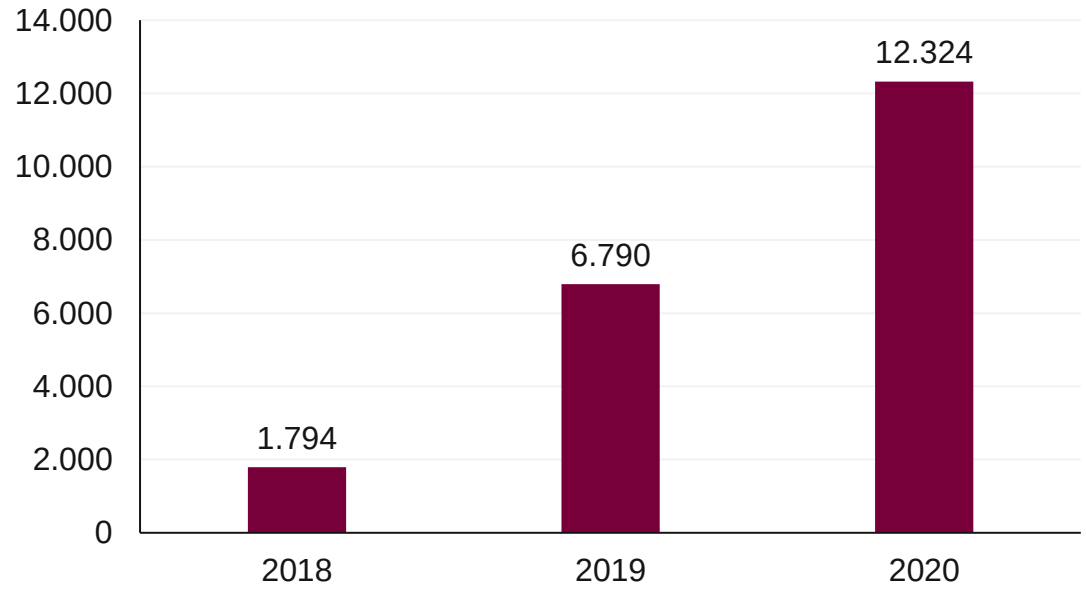
- Les publicacions de patents van augmentar gairebé un 80% interanual el 2020, cosa que indica un gran esforç en la investigació de seguretat d'objectes intel·ligents a causa de l'augment de la inversió en dispositius i sensors IoT en diverses indústries (com ara la fabricació avançada i l'automoció).

- Les patents presentades de seguretat d'objectes intel·ligents se centren en **vehicles intel·ligents, vehicles connectats, fabricació avançada, *smart city,* sanitat i electrònica de consum**.

- Els temes principals de les patents presentades són:

  - Dispositius de sensors IoT segurs
  - Verificació d'autoritzacions per a IoT
  - Transmissió i control de dades per a xarxes situades al núvol
  - Habilitar serveis M2M/IoT fiables i distribuïts

Patents publicades



Font: Frost&Sullivan

La **Xina** té el **44%** de les publicacions de patents per a la seguretat d'objectes connectats, seguida dels **EUA** amb un **17%**

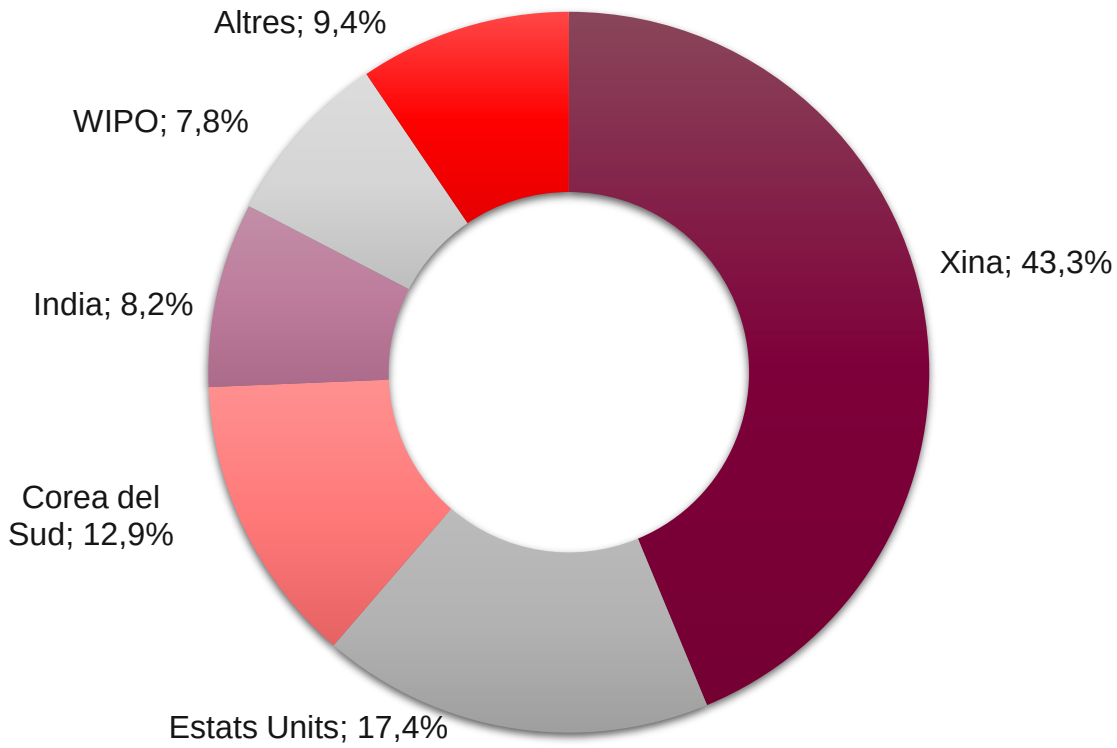
Àsia s'està convertint en un mercat important per a publicacions de recerca de patents, tant pel que fa a les jurisdiccions on es patenta com les pròpies empreses patentadores.

Principals propietaris de patents

SAMSUNG Qualcomm LG IBM HUAWEI ERICSSON intel Microsoft

Distribució de patents publicades per jurisdicció

2018 – 2020



Font: Frost&Sullivan

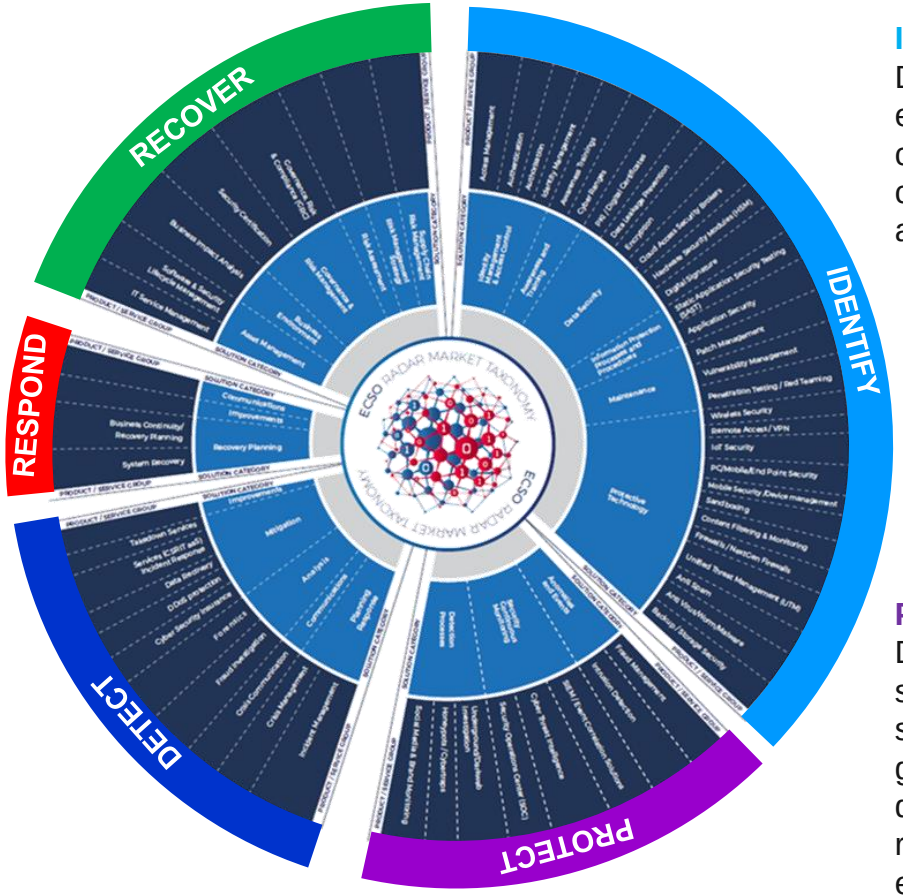
6. La ciberseguretat a Catalunya

L’ECSO (European Cybersecurity Organization) defineix el Market RADAR, una eina visual per a 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.

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

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

DETECTAR
Desenvolupar i aplicar les mesures adequades per a identificar l’aparició de ciberatacs.



IDENTIFICAR
Desenvolupar organitzativament i estratègica la infraestructura de 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 de TI, i garantir la confidencialitat, integritat, disponibilitat i auditabilitat, així com el rendiment de serveis informàtics essencials.

Font: ECSO

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

Identify	Protect	Detect	Respond	Recover
Asset Management	*Identity*	*Anomalies and Events*	*Response Planning*	*Recovery Planning*
Business Environment	*Awareness and Training*	*Security Continuous Monitoring*	*Communications*	*Improvements*
Governance & Risk Management	*Data Security*	*Detection Processes*	*Analysis*	*Communications*
Risk Assessment	*Information Protection Processes and Procedures*		*Mitigation*	
Risk Management Strategy	*Maintenance*		*Improvements*	
Supply Chain Risk Management	*Protective Technology*			

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

Font: ECSO

432 empreses

912,9 milions d'euros

8.188 llocs de treball

El **85,0 %** són pimes.

El **55,1 %** facturen **més d'un milió d'euros** i el **22,0 % més de 10 milions d'euros.**

El **29,6 %** són exportadores.

El **29,9 %** tenen menys de 10 anys.

El **18,1 %** són startups.

El **12,7 %** tenen dones en els llocs de direcció.

Per segments*, el **90,7 %** de les empreses es dediquen a la protecció, el **56,7 %** a la identificació, el **35,2 %** a la detecció, el **34,3 %** a la resposta i el **21,3 %** a la recuperació.

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

Font: ACCIÓ (dades d'empreses de 2021; facturació i nombre de treballadors de 2020)

Principals empreses de l'oferta de ciberseguretat a Catalunya (I)

Identificar

Identify

Principals empreses de l'oferta de ciberseguretat a Catalunya (II)

Protegir

Protect

Principals empreses de l'oferta de ciberseguretat a Catalunya (III)

Detectar

Detect

Principals empreses de l'oferta de ciberseguretat a Catalunya (IV)

Respondre

Respond

Recover

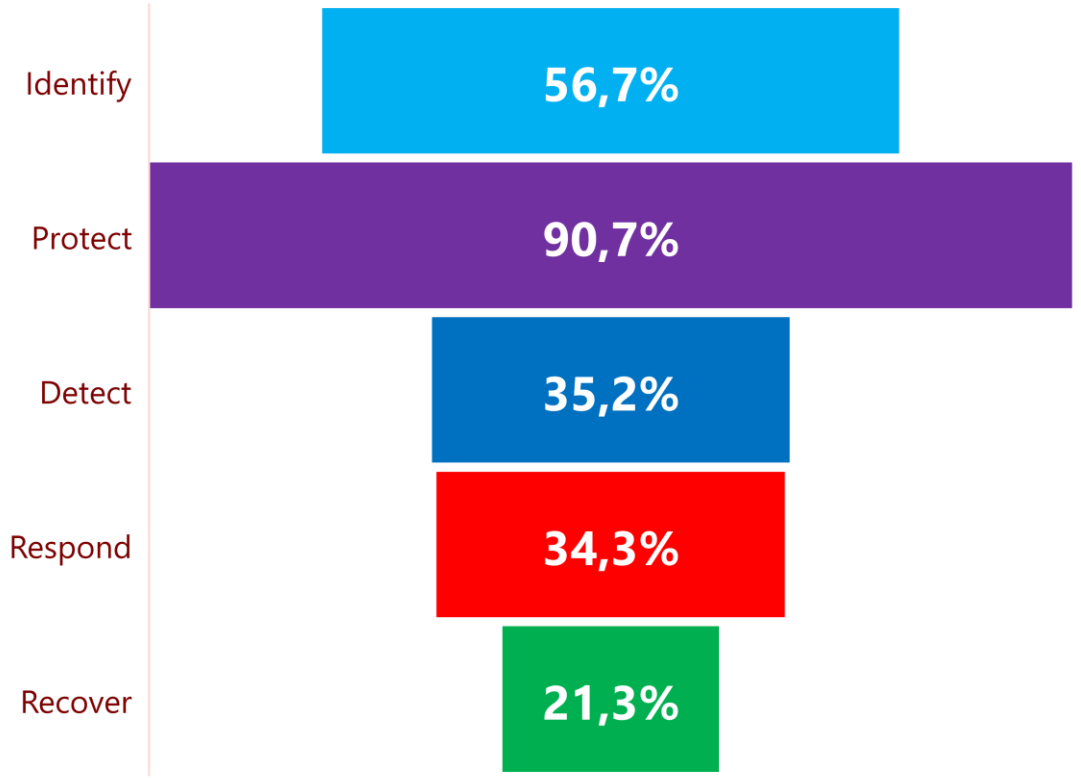

Telefónica
altran
ORACLE
Microsoft
T-Systems
NTT DATA
axians
Atos
izertis
it now
abast
accenture
GRUPO sermicro
S21 SEC
seidor
Bitdefender
NexTRet
opens
impala
dagram
PUNT informàtic
oylo
nexica
isec auditors
basetis
indra
wisesecurity
akcent
Inycom
getronics
AXA
claranet
Adam
Aiuken Cybersecurity
Avannubo
DETEINCO
I'LI'MI'T
AETECH
cisco
qupam
IBM
aggity
INDISEG
evolium
allenta
ABOX
ITGLOBAL
iTechGrup
Entelgy Innotec
VALORA DATA
trilogi
ESCUDA
Rockwell Automation
infoself
parlem
ARONTE
Opertek
3ASIDE Consultors
nearcrumbs
asnet
cipher
controlip
FlexVPC
TICsolutions
LAN
HITACHI
bytemaster
indigo
VILAmedi
grupo paradell
altercom 21
ene
SEVEN SECTOR
CROWDSTRIKE
DLTCode
Orednarbal
LightEyes
ProxymaTI
QUSIDE
Kerberosns
DEKRA
CCQ
innovaplanner
asartec
level4
kipmiOn
nae
ToBeIT
KPMG
sia
minsait
pwc
Qualitum
IoT PARTNERS

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

TOP 10
Categories de solució

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

Distribució de les capacitats



Al gran augment experimentat en el nombre d’empreses, facturació associada i llocs de treball se li sumen altres indicadors, com la proporció d’startups.

Empreses

Augment del 19,7% en el nombre d’empreses

Facturació

Augment de l’11,2%

Llocs de treball

Augment del 18,7%

PIMES

Lleuger augment de la proporció de pimes (85,0% el 2022 vs. 82,8% el 2021)

Startups

Creixement considerable del nombre d’startups (18,1% el 2022 vs. 13,0% el 2021)

Internacionalització

Lleuger repunt de la proporció d’empreses que exporten productes (29,6% el 2022 vs. 29,0% el 2021)

Solucions

Els productes i serveis de protecció continuen sent més presents en l’oferta de les empreses de ciberseguretat de Catalunya

Evolució

Malgrat l’aturada generalitzada en l’economia per la pandèmia, la ciberseguretat ha augmentat el seu pes

Agents de l'ecosistema de Ciberseguretat

Centres tecnològics i instituts de recerca

CYBERCAT, eurecat, ISG, ICFO, Cryptography & Graphs, CERCA, Institut d'Investigació en Intel·ligència Artificial - IIIA, Crises, i2cat, CTTC, CVC, BSC, Cryptography and Information Security for Open Networks, easy, TecnoCampus, laSalle Universitat Ramon Llull, inLab FIB, UPC, CIT UPC Technology Center

Estudis de màster i postgrau

Universitat Politècnica de Catalunya BarcelonaTech, telecos BCN, FIB, Nuclio Digital School, UOC Universitat Oberta de Catalunya, ulc barcelona, Universitat Rovira i Virgili, unir La Universidad en Internet, Universitat de Lleida, laSalle Universitat Ramon Llull, Institut de Formació Contínua IL3 Universitat de Barcelona, OBS Business School

Estudis d'FP

Institut Eugeni d'Ors Vilafranca del Penedès, INSTITUT ESTEVE TERRADAS I ILLA, Institut Caparrella, Institut Carles Vallbona, Institut F. Vidal i Barraquer Tarragona, ICB Institut Camps Blancs, CESF Centre d'Estudis Sant Francesc Grup Stucom, ites Escola Tècnica de Cicles Formatius d'Imatge i So, Institut Pedralbes, INSTITUT POBLENOU, EL CALAMOT, Institut Camí de Mar Calafell, Institut Lacetània, Joviat, Institut Tecnològic Barcelona, INSTITUT Badia del Vallès, Vedruna Vall Terrassa, Baix Camp, Jaume Vilaplana Centre Educatiu, Pere Martell Institut, Col·legi Cultural Barcelona, IFP Innovación en Formación Profesional, Pàlcam, Institut de l'Ebre Tortosa, Institució Cultural del CIC Fundació Privada, La Salle Manlleu

Associacions i esdeveniments

ISACA, itSMF, APCSD, informaTICs, Telecos.cat, Blockchain Solutions, IOT Solutions World Congress, APWG, NoN, ISMS, OWASP, Barcelona Digital Talent, World Trade Organization, secpho, (ISC)², apep, grausfit, coettc, GSMA MWC Barcelona, Barcelona Cybersecurity Congress, Trends.CAT, ITU, integrated systems europe, BCN BSIDES

CSIRT/CERT

Agència de Ciberseguretat de Catalunya, ESCERT, aokcent cybersecurity, incibe-cert, CSIRT.es, TF-CSIRT Trusted Introducer, LightEyes, CSUC, CaixaBank, cni-cert, FIRST

Institucions i administració pública

Generalitat de Catalunya Departament de la Vicepresidència i de Polítiques Digitals i Territori, ACCIÓ Generalitat de Catalunya, DIH4CAT Digital Innovation Hub de Catalunya, enisa, incibe_, ECSO, Agència de Ciberseguretat de Catalunya, DCA Ciberseguretat, AOC, apdcat, CCN, NESSI

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 la RDI en el període 2014-2020, amb un pressupost total de 77.028 M€.
- El 2021 ha estat substituït pel programa Horitzó Europa (HE) del qual encara no s'ha assignat projectes de ciberseguretat.

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

22 projectes
22 entitats
7.679.569 € d'inversió
357 socis de l'exterior

- Entitats participants en l'àmbit de ciberseguretat per ordre de volum d'inversió

Font: programa Horizon 2020

RIS3CAT

L'Estratègia de recerca i innovació per a l'especialització intel·ligent de Catalunya (RIS3CAT) és la resposta de Catalunya a l'exigència de la Comissió Europea que els estats i les regions de la Unió Europea elaborin estratègies de recerca i innovació per a l'especialització intel·ligent (*Research Innovation Strategies for Smart Specialisation*, RIS3) que s'ajustin al seu potencial d'innovació.

Impacte del programa RIS3CAT en l'àmbit de la ciberseguretat

4 projectes
8 entitats
3.080.411 € d'inversió
(sense socis de l'exterior)

Entitats participants per ordre de volum d'inversió

Diputació Tarragona
i2cat
altran
CETAQUA CENTRO TECNOLÓGICO DEL AGUA
eurecat Centre Tecnològic de Catalunya
gasNatural fenosa
ferrovial servicios

Projectes

utilities 4.0 SECUTIL

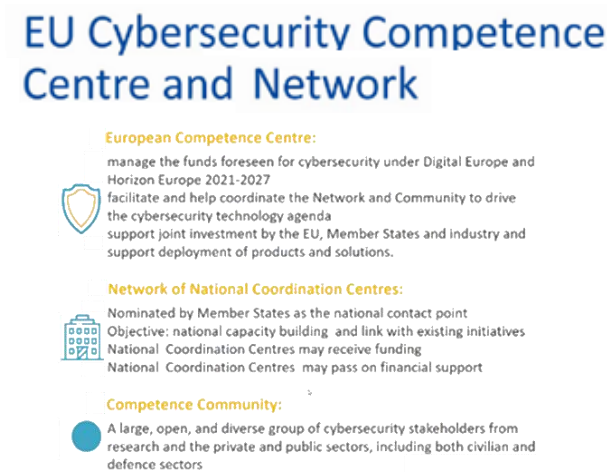
Vcsm_vehicle módul de comunicació segura

RuralLab - Baix Penedès Infraestructures tecnològica

TDACiberseguretat

Font: RIS3CAT

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



Gestió d'ajuts al finançament i coordinació d'iniciatives

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA | CENTRE D'INNOVACIÓ I COMPETÈNCIA EN CIBERSEGURETAT

www.ciberseguretat.cat

Impuls del sector de ciberseguretat de Catalunya

DCA Ciberseguretat

www.dca.cat

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

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

DIH4CAT Digital Innovation Hub de Catalunya

www.dih4cat.cat

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

CYBERSECURITY CAT

www.cybercat.cat

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

Universitat Rovira i Virgili · Universitat Oberta de Catalunya · Universitat de Lleida · Universitat Politècnica de Catalunya · Universitat Autònoma de Barcelona · Universitat Pompeu Fabra Barcelona

Línies de recerca

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

Font: CiberCAT

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

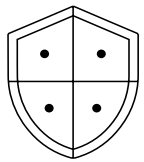
www.dca.cat

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

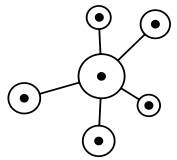
- Agrupar empreses actives de referència en innovació digital per tal de disposar d'un ecosistema dinàmic que contribueixi en l'economia digital.
- Resoldre reptes comuns de les empreses del sector, tant de les empreses petites com de les mitjanes.
- Donar suport a l'adopció dels canvis tecnològics per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

Comunitats:

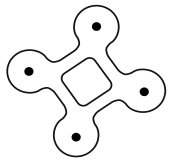
DCA Ciberseguretat



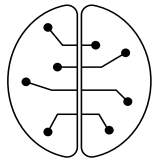
DCA IoT



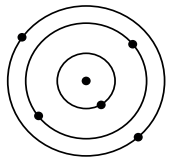
DCA Drons



DCA IA



DCA NewSpace



La DCA és una iniciativa de:

Generalitat de Catalunya
Departament de la Vicepresidència i de Polítiques Digitals i Territori

i2cat

Font: DCA

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

https://dih4cat.cat

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

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

Infraestructures digitals i tecnològiques

Marketplace de solucions

Acompanyament en el procés de transformació digital

Serveis

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

Font: DIH4CAT

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

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

www.ciberseguretat.cat

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

Funcions i serveis

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

Font: Agència de Ciberseguretat de Catalunya

El Catalonia Industry Suppliers és una plataforma en línia per a promoure la indústria a Catalunya a escala internacional.

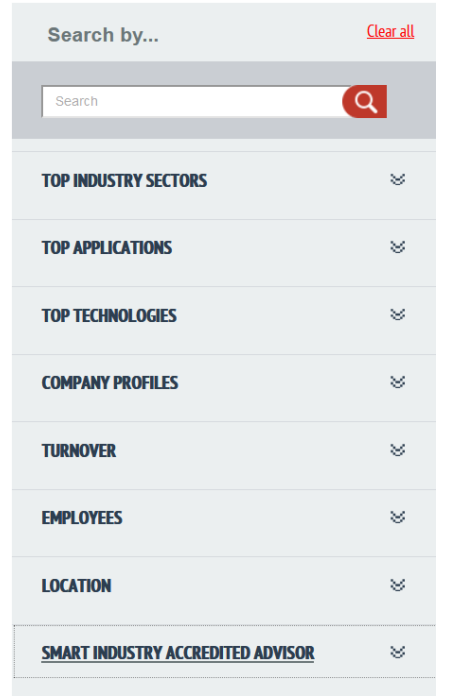
Catalonia Industry Suppliers

http://suppliers.catalonia.com/

- Posa a l'abast de les empreses informació sobre productes i d'empreses industrials i tecnològiques, i genera oportunitats de negoci, ja que permet que fabricants, distribuïdors, importadors, i inversors internacionals trobin proveïdors i socis a Catalunya.

- Permet fer cerques en línia de proveïdors industrials, tecnològics i de serveis a la indústria que tinguin activitat productiva a Catalunya i siguin exportadors, tinguin orientació internacional. Ofereix la possibilitat de fer cerques per sector, per productes, per aplicacions i per tecnologies.

- Possibilitats de cerca:
  - **Producte**
  - **Tecnologia**
    Big Data + Intel·ligència Artificial; DLT/Blockchain; Cloud/Edge; **Ciberseguretat**; Connectivitat; Fotònica, Quàntica; Robòtica;Fabricació Additiva; IoT; RA/RV; Nanotecnologia; Genòmica...
  - **Aplicacions**
  - **Perfils**
  - **Sectors**
  - **Mida i localització**
  - **Assessors acreditats**



Font: ACCIÓ

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

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

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

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

http://www.cttc.es/

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

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

https://i2cat.net/

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

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

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

https://eurecat.org/

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

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

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

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

https://www.centreeasy.com/

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

La Salle R&D desenvolupa projectes privats mitjançant subcontractació directa i participa activament en projectes competitius nacionals i internacionals. La Salle R&D ofereix als seus clients una amplia oferta en matèria d'R&D que inclou serveis de consultoria tecnològica i desenvolupament de projectes claus en mà. La capacitat La Salle R&D permet oferir un servei integral, des de la creació de la idea i prova de concepte, fins el desenvolupament del producte, tot això sota el paraigües d'una gestió integral conforme ISO9001.

https://www.salleurl.edu/

L'Institut de Ciències Fotòniques és un centre d'investigació ubicat en un edifici de 14 000 m2 al Parc Mediterrani de la Tecnologia de l'Àrea Metropolitana de Barcelona. Actualment acull més de 300 investigadors, inclosos caps de grup, investigadors postdoctorals, estudiants de doctorat, enginyers i personal, organitzats en 27 grups de recerca.

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

https://www.icfo.eu/

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

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

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

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

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

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

El Grup de Seguretat de la Informació (ISG) centra la seva activitat en el desenvolupament i proposta de serveis de seguretat, i el seu desplegament en xarxes de telecomunicacions.
El Grup de Seguretat de la Informació (ISG) es va crear a la Universitat Politècnica de Catalunya (UPC) l'any 2002. Des del primer moment, el principal objectiu estratègic del grup ISG va ser ser un grup de seguretat de referència.
Actualment, el grup està format per 9 professors i després de 15 anys de treball conjunt, els resultats són 163 articles en revistes classificades, 321 comunicacions en congressos, 60 projectes competitius, 20 tesis llegides, 17 llibres i capítols de llibres, 12 premis i 9 patents.
El grup lidera les tasques de seguretat i privadesa del projecte H2020 BIG IoT, inclosa la cadena de blocs per millorar la seguretat i la privadesa a l'IoT.

http://futur.upc.edu/ISG

CIT UPC, el Centre Tecnològic de la Universitat Politècnica de Catalunya és una entitat sense ànim de lucre, que posa la capacitat de recerca universitària al servei de la innovació en les empreses a partir del coneixement i els resultats dels centres de recerca i transferència de tecnologia de la UPC.
A l'àmbit de la ciberseguretat treballen en privadesa i protecció de dades, anàlisi de consultoria, auditoria i seguretat, cloud i big data, plans de continuïtat d negoci, seguretat d'infraestructures, serveis de confiança i seguretat, formació

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

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

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

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

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

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

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

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

https://www.bsc.es/ca

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

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

Cryptography and Information Security for Open Networks

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

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

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

TecnoCampus

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

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

Crises secure e-commerce

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

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

inLab FIB talent & tech

UPC

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

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

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

Principals oportunitats internacionals per a les empreses catalanes de ciberseguretat

Creix la necessitat de les empreses de protegir-se dels atacs cibernètics, sobretot les grans empreses financeres i d'assegurances.

Inversions per a accelerar la recuperació econòmica.
Entre les tecnologies destaca la ciberseguretat.

Indústria 4.0: robotització, intel·ligència artificial, ciberseguretat i impressió 3D.

Les TIC són crucials en el suport a les principals indústries de Hong Kong, i, per aquest motiu, la ciberseguretat cobra protagonisme.

Es crearan noves oportunitats per a empreses proveïdores de solucions relacionades amb la ciberseguretat, la internet de les coses o la IA.

Els Països Baixos reuneixen una infraestructura digital del més alt nivell amb una estratègia de digitalització de govern per a convertir el país en el líder digital d'Europa.

Oportunitats per a solucions de gestió de comerç electrònic en totes les fases de la cadena, des de solucions de pagament i ciberseguretat fins a logística i control d'estocs.

Kenya i les TIC: la Silicon Savannah.

Base d'expansió al sud-est asiàtic per a empreses tecnològiques.

Plataforma de llançament de tecnologies de l'era digital.

El sector de les TIC és un dels més dinàmics de l'economia xinesa.

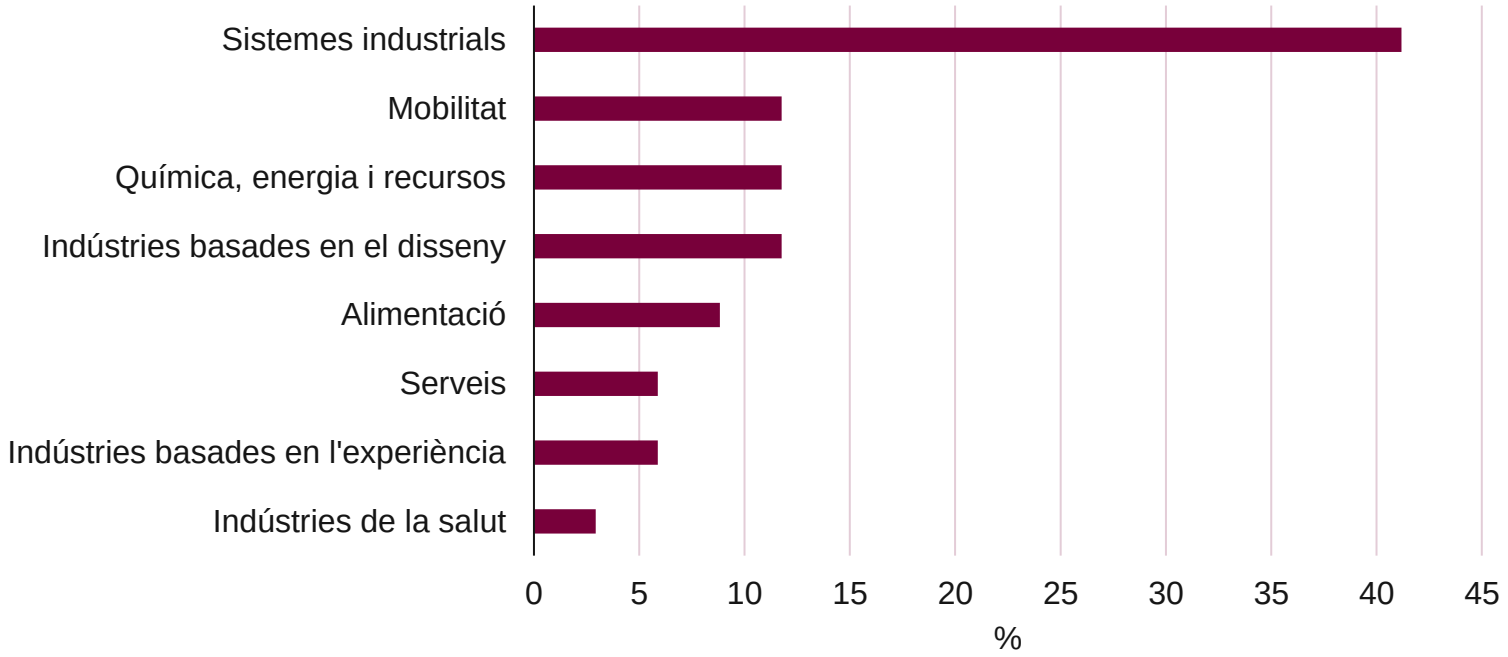
Font: ACCIÓ, *Mapa Global d'Oportunitats de Negocis Internacionals* de 2021

Sectors més demandants de solucions de ciberseguretat

La ciberseguretat suposa el **3,7 %** dels ajuts atorgats amb els Cupons Indústria 4.0. 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.

El **13 %** del assessors acreditats per ACCIÓ en Indústria 4.0 realitzen activitats relacionades amb la ciberseguretat.

Sectors demandants de solucions de ciberseguretat amb els Cupons d'ACCIÓ



Font: ACCIÓ a partir de dades relatives als 906 atorgaments dels ajuts de cupons per a la competitivitat empresarial (Cupons Indústria 4.0) que ha atorgat ACCIÓ durant les anualitats de 2019, 2020 i 2021

7. Casos d'èxit a Catalunya

Casos d'èxit a Catalunya

IThinkUPC, l'empresa de serveis digitals avançats de la Universitat Politècnica de Catalunya.

L'Ajuntament de Barcelona i **Cisco** provaran la plataforma de ciberseguretat IRIS.

CrowdStrike fixa a Barcelona la seva seu europea per al mercat *corporate*.

Impala, proveïdor de solucions IT amb seu a Barcelona.

Toni Pons, implementació de mesures tecnològiques i organitzacionals de ciberseguretat.

nebulaID, solució de videoautenticació i identificació remota amb valor legal probatori de **Vintegris**.

Opticks, detecció i prevenció de frau en anuncis online.

Build38, ciberseguretat per a aplicacions mòbils.

Evolutio, nou centre d'operacions de ciberseguretat a Barcelona.

Mars Intelligence, consultora de seguretat digital per a empreses i domicilis.

Nuclio, escola on cursar màsters en ciberseguretat, *data science i blockchain.*

Rockwell adquireix l'empresa de ciberseguretat catalana **Oylo**.

L'empresa de serveis digitals avançats de la Universitat Politècnica de Catalunya

- L'empresa ofereix diversos serveis digitals, entre ells ciberseguretat. Compten amb experiència i coneixement avançat per afrontar tots els reptes de ciberseguretat dels clients amb visió integral i serveis adaptats a cada necessitat.
- A més, l'empresa ajuda la UPC, universitat especialitzada en els àmbits de l'enginyeria i les ciències, en la seva missió de transferir el coneixement avançat de la ciència i la tecnologia a les empreses i la societat.

https://www.ithinkupc.com/

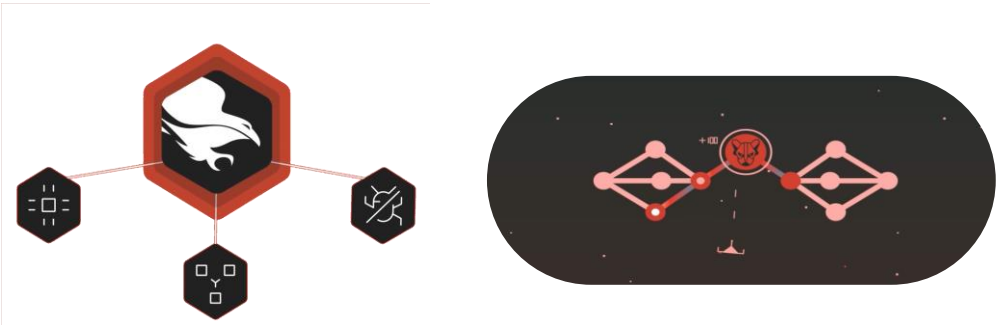
L'Ajuntament de Barcelona i Cisco provaran la plataforma de ciberseguretat IRIS

- L'Ajuntament de Barcelona i Cisco participen en un projecte europeu que busca la seguretat en l'entorn de l'IoT (Internet de les Coses). La plataforma de ciberseguretat IRIS es provarà a Barcelona per protegir les ciutats i comunitats de la Unió Europea.
- El projecte té com a objectiu oferir un marc que doni suport a les xarxes europees de resposta a incidents de seguretat. Servirà per detectar, compartir, respondre i recuperar-se de les amenaces i vulnerabilitats de ciberseguretat dels sistemes TIC impulsats per IoT i la Intel·ligència Artificial.

https://www.iris-h2020.eu/

CrowdStrike fixa a Barcelona la seva seu europea per al mercat *corporate*

- CrowdStrike, companyia de ciberseguretat especialitzada en la protecció *endpoint* des del núvol, ha anunciat l'elecció de Barcelona per fixar l'oficina des d'on donar servei al seu mercat *corporate*. L'empresa vol aprofitar el talent local per impulsar la demanda en el mercat de la seva plataforma CrowdStrike Falcon i en les seves solucions d'intel·ligència contra amenaces i serveis de resposta.
- La companyia, que ja compta a Espanya amb acords estratègics amb diverses empreses, segueix creixent i sumant clients de subscripció als seus serveis.



https://www.crowdstrike.com

ImpalaSEIDOR, un proveïdor de solucions IT amb seu a Barcelona

- ImpalaSEIDOR, amb seu a Barcelona, ofereix serveis i solucions de ciberseguretat per minimitzar riscos i amenaces. Tenen serveis per conèixer el nivell de risc, aplicar mesures de seguretat, i obtenir visibilitat, resposta i millora contínua.
- L'empresa també ofereix auditoria i consultoria en ciberseguretat, a més d'un servei d'IT amb el qual es pot contractar un projecte que inclou equips informàtics, llicències, serveis professionals i serveis gestionats alhora.

https://impala-net.com/

Toni Pons
caràcter mediterrani

Implementació de mesures tecnològiques i organitzacionals de ciberseguretat

- L'objectiu del projecte ha sigut la implementació de mesures tecnològiques i organitzacionals de ciberseguretat per minimitzar les probabilitats de sofrir un ciberatac o tenir un incident relacionat amb la ciberseguretat.
- El projecte ha passat per una fase inicial d'avaluació de l'estat actual de la ciberseguretat de la empresa, tant a nivell IT (tecnologies de la informació) com OT (tecnologies operacionals), la definició d'un pla d'accions a dur a terme en el curt, mitjà i llarg termini, i finalment la implementació d'algunes de les mesures tecnològiques i organitzacionals aplicables a curt termini per millorar la ciberseguretat de l'empresa.

eurecat
Centre Tecnològic de Catalunya

https://www.toniies.shop/

víntegris

nebulaID, solució de vídeo autenticació i identificació remota amb valor legal probatori

- Es tracta d'una eina de vídeo autenticació i identificació remota, amb valor legal probatori, dissenyada per facilitar la gestió de tota mena de tràmits eliminant la necessitat de presencialitat, però sense deixar de garantir la protecció total de les dades i identitats dels usuaris, i amb la màxima seguretat i compliment legal.
- nebulaID incorpora un sistema de "comparació facial" i "puntuació biomètrica facial" per comparar els trets facials del sol·licitant amb la foto del document d'identitat. També compta amb tecnologia de detecció de vida i intel·ligència artificial per detectar atacs de presentació biomètrica (PAD), així com mecanismes de detecció de manipulacions del document d'identitat i tecnologia OCR per a la recollida de dades del document.
- Compleix amb els estàndards del *Centro Criptológico Nacional* i la regulació eIDAS, a més d'alinear-se amb les normatives KYC i SEPBLAC.

nebulaID

https://www.vintegris.com/es/blog/vintegris-presenta-nebulaid-su-solucion-de-video-autenticacion/

Opticks

Detecció i prevenció de frau en anuncis online

- Opticks és una empresa fundada el 2018 i amb seu a Barcelona que es dedica a la detecció i prevenció del frau en anuncis online combinant l'experiència dels seus professionals amb el *machine learning* i la intel·ligència artificial, de manera que els beneficis vagin a l'anunciant i no al cibercriminal.
- Ha estat una de les empreses seleccionades en el 10è *Cyber Investors Days* que es va celebrar l'1 i 2 de desembre de 2021 a Helsinki.

https://optickssecurity.com/

build

Mobile Security

Ciberseguretat per a aplicacions mòbils

- Build38 és una empresa tecnològica amb seus a Alemanya, Barcelona i Singapur. Dins dels seus negocis hi ha una part important dedicada a la ciberseguretat. Ha desenvolupat un marc de seguretat per a aplicacions mòbils tant a nivell d'usuari com de desenvolupador.
- L'any 2020 va guanyar el Premi PwC en la categoria "Millor solució de ciberseguretat de l'any". També ha estat una de les empreses seleccionades en el 10è *Cyber Investors Days* que es va celebrar l'1 i 2 de desembre a Helsinki.

https://build38.com/

Un nou centre d'operacions de ciberseguretat a Barcelona

- Evolutio (antiga BT) és una empresa tecnològica en l'àmbit IT i de la ciberseguretat. Des de xarxes i tecnologia cloud fins a la consultoria i integració en ciberseguretat, la detecció d'amenaces i aplicacions d'intel·ligència artificial i big data.
- L'empresa ha inaugurat un nou Centre d'Operacions de Ciberseguretat (SOC) a Barcelona com a reforç del seu servei de protecció davant amenaces digitals. El centre comptarà amb 36 analistes de ciebrseguretat i pretén detectar fins al 1.500 amenaces digitals al mes i dur a terme 200 investigacions proactives.

https://www.evolutio.com/

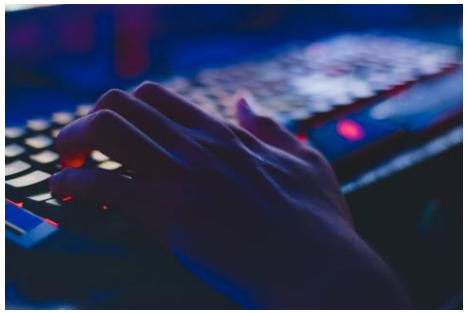
Consultora de seguretat digital per a empreses i domicilis

- Mars Intelligence és una consultora de seguretat integral que acompanya al client en el procés de la gestió del risc. Ara però, també han obert una nova divisió enfocada a la seguretat digital en el que posen a prova tot l'entramat tecnològic d'empreses i domicilis.
- Les properes passes de Mars Intelligence estan lligades a la tecnologia dels drons en usos com la localització de persones desaparegudes, la seguretat en el delivery o el suport a operatius terrestres en, per exemple, els controls d'accessos.

https://mars-intelligence.com/

Una escola on cursar màsters en ciberseguretat, Data Science i Blockchain

- Nuclio Digital School és una escola de negocis i incubadora de startups fundada a Barcelona el 2018. En l'àmbit de formació, la seva oferta compren màsters intensius en temàtiques TI on destaquen els màsters en ciberseguretat, Data Science i en Blockchain.
- El Banc Sabadell, a través de la seva divisió de capital risc Sabadell Venture Capital, hi ha invertit un milió d'euros en Nuclio, veient-la com una oportunitat per cobrir l'alta demanda de perfils tecnològics que la digitalització està creant.



https://nuclio.school/

Rockwell adquireix l'empresa de ciberseguretat catalana Oylo

- Rockwell, companyia d'Estats Units, ha adquirit la barcelonina Oylo. Es tracta d'un proveïdor privat de ciberseguretat industrial, amb seu al World Trade Center de la capital catalana, especialitzat en la vigilància de sistemes industrials i resposta a incidents.
- Entre els seus serveis, Oylo inclou avaluacions i implementacions de clau en mà, sempre enfocats a serveis i solucions de ciberseguretat de sistemes de seguretat industrials (ICS).

https://www.rockwellautomation.com/

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:

http://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