AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

Protecció de dades personals i ciberseguretat

Març 2023

LA CIBERSEGURETAT A CATALUNYA

Diari de Girona
Un virus informàtic afecta el laboratori que treballa per a sis hospitals catalans
Només atendrà analítiques urgents a través d'un circuit alternatiu que protegeix les dades

El ciberatac contra l'Hospital [illegible]

Broggi afecta 13 centres sanitaris més

Un atac informàtic bloqueja els ordinadors de l'Ajuntament de Lloret
- Un virus segresta les dades del sistema, que recuperarà la normalitat dues se[illegible] després
- El sabotatge alenteix l'atenció ciutadana i la contractació

El virus informàtic dels ajuntaments arriba a la Diputació i empreses privades
REDACCIÓN | LLEIDA Actualitzada 26/09/2019 a les 08:55

CIBERESTAFA
Detectados numerosos intentos de 'phishing' a empresas suplantando a la Seguridad Social

Font: Premsa en línia

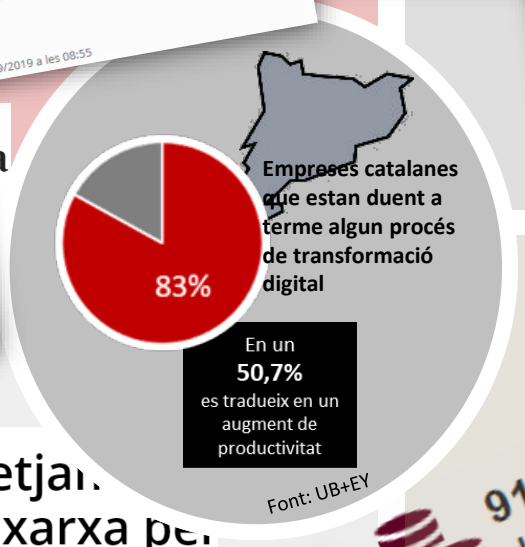
Fraud costs the global economy over US$5 trillion

Pugen els casos de ciberassetjam[illegible] i extorsió a adolescents a la xarxa pe[illegible]finament

Una denuncia al mes per sextor[illegible] o acoso a menores en [illegible] Lleida

Over 1 Billion Consumers* Have Ever Been the Victim of a Cyber Crime; More Than 800 Million in the Last Year Alone

Fonts: Crowe, Premsa, Symantec



El Govern regula amb un decret el teletreball per a 40.000 dels seus empleats

Font: Gencat

Fonts: ACCIÓ, ISC2

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

ALGUNES DADES DE CONTEXT

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

Xifres dels ciberatacs amb impacte a Catalunya el 2022

+30%

Augmenten els ciberatacs

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

+38%

Campanyes de *phishing* en augment

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

20%

Protagonisme dels atacs de BEC

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

74%

Ciberatacs amb enginyeria social

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

+150%

El sector públic, objectiu dels ciberatacs

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

35%

***Ransomware* contra entitats públiques**

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

11%

El troià RootSTV lidera les infeccions

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

48%

Predomini de *botnets* en les infeccions

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

ALGUNS RISCOS QUE SON TENDÈNCIA

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

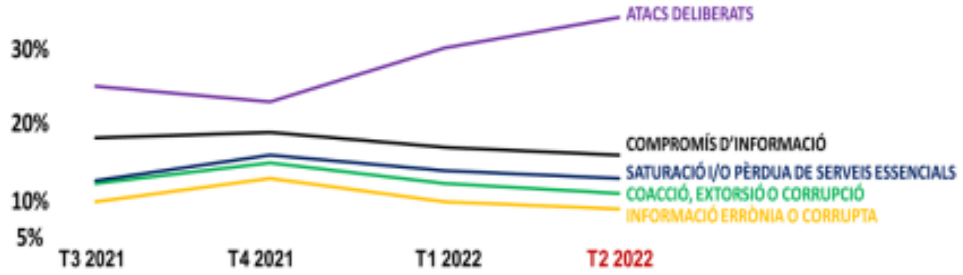
Un incident cibernètic pot afectar l'opinió que els clients o la ciutadania tenen d'una organització, d'una marca, o bé d'un producte o servei, i això pot acabar impactant en el balanç econòmic. Recuperar la reputació després d'un incident pot representar un sobreesforç en termes econòmics i de temps.

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

Baròmetre d'amenaces

S1 2022	vs	S2 2021	Ciberamenaces
1	=	1	Atacs deliberats
2	=	2	Compromis i/o pèrdua d'informació
3	=	3	Saturació i/o pèrdua de serveis essencials
4	=	4	Coacció, extorsió o corrupció
5	=	5	Informació errònia o corrupta



Atacs deliberats

La primera meitat de 2022 ha estat marcada per les campanyes de difusió de programaris maliciosos per al robatori de credencials, comptes bancaris, criptomoneders,...

Compromís i/o pèrdua d'informació

S'han detectat diverses fuites massives de dades personals que han afectat milions d'usuaris, tot i que menys que al primer semestre de 2021.

Saturació i/o pèrdua de serveis essencials

Ransomware i DDoS han buscat interrompre l'activitat de les seves víctimes. El *ransomware* dirigit a serveis essencials i els DDoS s'han vist esperonats pel conflicte entre Rússia i Ucraïna.

Coacció, extorsió o corrupció

El *ransomware* és la principal causa d'extorsió, tot i que creixen altres tècniques, com ara el robatori de dades sensibles amb l'amenaça de publicar-les o la *sextorsió*.

Informació errònia o corrupta

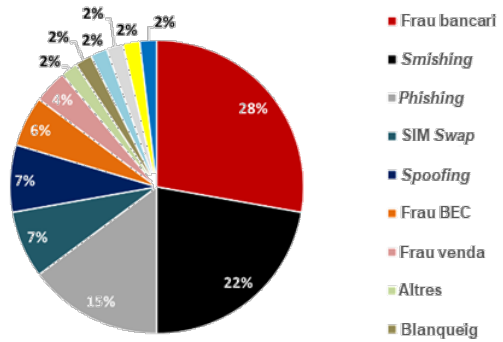
Els *wipers* han agafat un gran protagonisme gràcies al conflicte entre Rússia i Ucraïna. També han destacat les desfiguracions de pàgines web, tècnica molt utilitzada pel *hacktivisme*.

REALITATS DE LES DADES PERSONALS

“Més dades personals robades avui pels ciberatacs de demà”

- Les dades personals permeten realitzar atacs d’enginyeria social personalitzats a cada víctima, incrementant la probabilitat d’èxit
- *Phishing* omnipresent: *emails*, apps de missatgeria, xarxes socials, motors de cerca, sol·licituds d’aplicacions de serveis al cloud, etc.
- El cost mitjà d’una fuita de dades ha augmentat un 42% des del 2020 i, per 12è any consecutiu, el sector sanitari és on és més elevat

Activitat dels grups cibercriminals detinguts a Catalunya el 2022 publicats als mitjans [Agència]



“*Crime as a Service* econòmic i accessible”

- Els preus dels serveis maliciosos oferts a la *dark web* han baixat, en part, gràcies a l’augment de l’oferta: el 90% d’*exploits* a la venda estan per sota dels 10 €
- Arran de les detencions d’alguns responsables de mercats negres del web fosc, els cibercriminals recorren a Telegram per ofertar la seva activitat anònimament.

Espanya no és el país que més recapta, però sí el que més multes posa per incompliments de l’RGPD

El fet que grans corporacions estiguin a Irlanda i Luxemburg fa que siguin els països que més recapten. Espanya ocupa la sisena posició, amb una mitjana de **99.486 €** per multa.

[Enforcement Tracker]

Top 10 dels països amb més quantitats econòmiques recaptades en matèria de l’RGPD

País	Suma multes (€)	Total multes
Irlanda	1.309.115.900	21
Luxemburg	746.275.100	24
França	293.419.300	33
Itàlia	142.515.996	239
Regne Unit	60.632.800	12
Espanya	57.801.930	581
Alemanya	54.750.853	116
Grècia	30.514.000	53
Àustria	24.750.150	19
Suècia	16.250.130	28

Preus de productes i serveis cibercriminals al *dark web* [Privacy Affairs]

Servei	Preu mínim	Preu màxim
Malware	41 €	5.060 €
Documentació física	138 €	3.496 €
Serveis de processament de pagaments	9 €	920 €
DDoS	9 €	782 €
Comptes Criptomonedes	83 €	368 €
Documentació	9 €	152 €
Dades de targetes de crèdit	9 €	110 €
Xarxes socials	1 €	60 €
Serveis hackejats	3 €	37 €
Bases de dades de comptes de correu	92 €	110 €

Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)

Cybersecurity threats are almost always cross-border, and a cyberattack on the critical facilities of one country can affect the EU as a whole. EU countries need to have strong government bodies that supervise cybersecurity in their country and that work together with their counterparts in other Member States by sharing information. This is particularly important for sectors that are critical for our societies.

The Directive on security of network and information systems (NIS Directive), which all countries have now implemented, ensures the creation and cooperation of such government bodies. This Directive was reviewed at the end of 2020.

As a result of the review process, the proposal for a Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) was presented by the Commission on 16 December 2020.

Cybersecurity Act

The Cybersecurity Act strengthens the role of ENISA. The agency now has a permanent mandate, and is empowered to contribute to stepping up both operational cooperation and crisis management across the EU. It also has more financial and human resources than before.

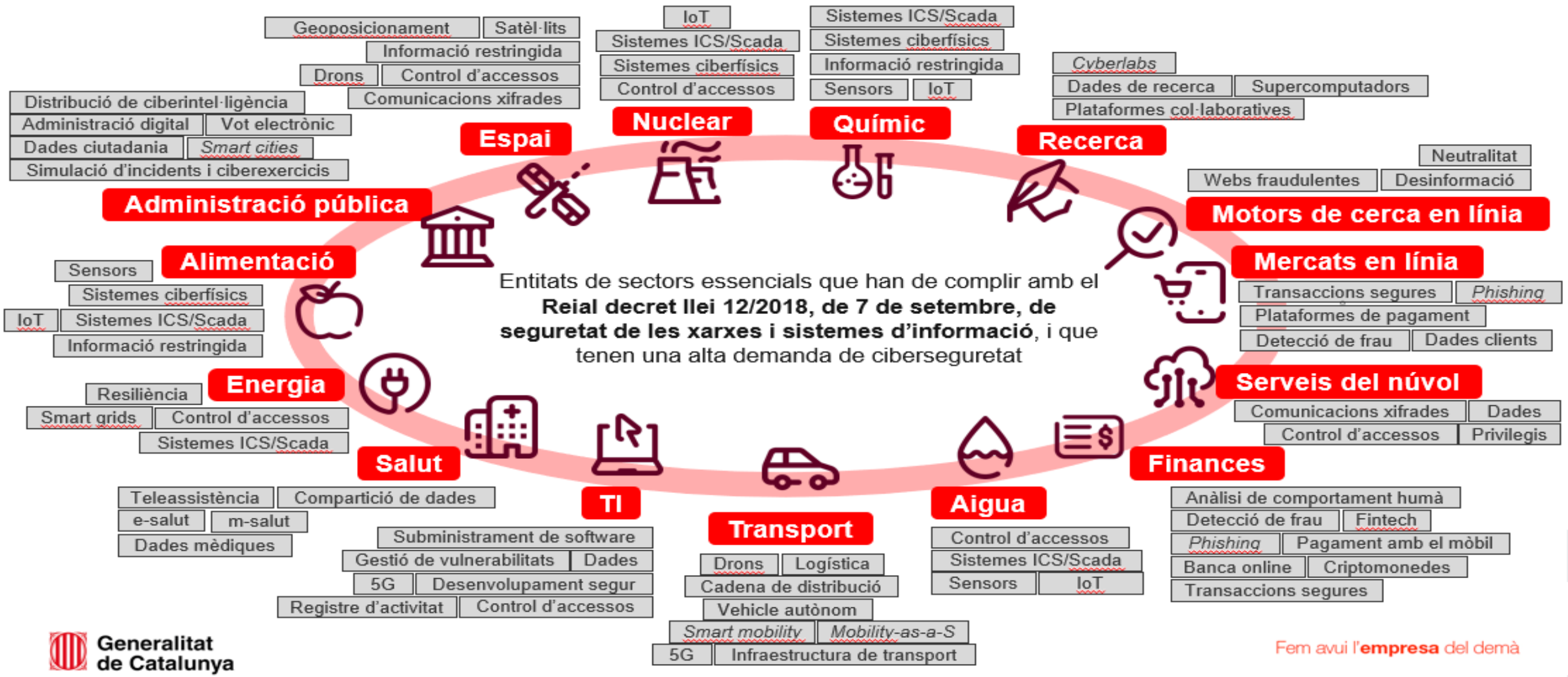
Certification

Our digital lives can only work well if there is general public trust in the cybersecurity of IT products and services. It is important that we can see that a product has been checked and certified to conform to high cybersecurity standards. There are currently various security certification schemes for IT products around the EU. Having a single common scheme for certification would be easier and clearer for everyone.

The Commission is therefore working on an EU-wide certification framework, with ENISA at its heart. The Cybersecurity Act outlines the process for achieving this framework.

PRINCIPALS SECTORS VINCULATS

Sectors de demanda



OBLIGACIONS DE SEGURETAT

NIS2

Artículo 21

Medidas para la gestión de riesgos de ciberseguridad

1. Los Estados miembros velarán por que las entidades esenciales e importantes tomen las medidas técnicas, operativas y de organización adecuadas y proporcionadas para gestionar los riesgos que se planteen para la seguridad de los sistemas de redes y de información que utilizan dichas entidades en sus operaciones o en la prestación de sus servicios y prevenir o minimizar las repercusiones de los incidentes en los destinatarios de sus servicios y en otros servicios.

GDPR

Artículo 32

Seguridad del tratamiento

1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) la seudonimización y el cifrado de datos personales;

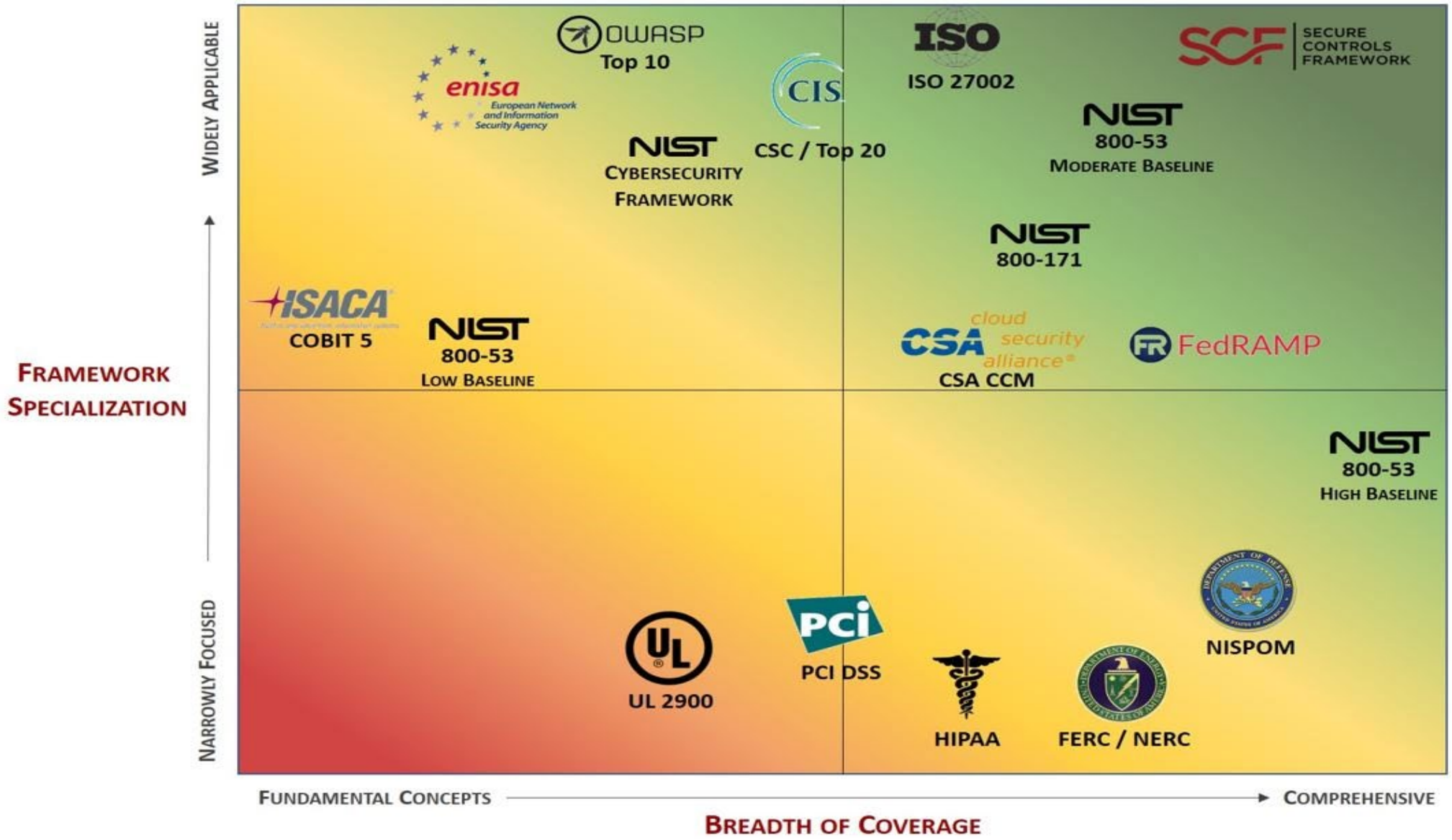
b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Programes de ciberseguretat i compliance

ESTANDARDS DE SEGURETAT



Campanya #NegoCibersegur

DIGITALITZA EL TEU NEGOCI
FES-LO CIBERSEGUR

L'Agència de Ciberseguretat de Catalunya porta la campanya NegoCibersegur, una iniciativa adreçada al teixit empresarial del país per protegir-lo i convertir-lo en capdavanter dels reptes del segle XXI.

https://internetsegura.cat/empresa

- Protegeix-te del programari maliciós
- La informació a l'empresa: un tresor a protegir
- Dispositius de feina, a punt!
- Còpies de seguretat, el pla A
- Ciberseguretat: sinònim de confiança

Recursos de #Negocibersegur

Materials de la campanya

Pòsters, bàners, una infografia, *flyers*, la guia per empreses, etc.

Avalua't

Eina que amb 12 qüestions avalua com es troba en ciberseguretat el teu negoci, en menys de 10 minuts.

Eines formatives

Aprendre conceptes bàsics de ciberseguretat pel negoci amb els micro cursos des del mòbil

Més recursos

A la pàgina web de la campanya podreu trobar-hi **un glossari, notícies, avisos, iniciatives** del món de la ciberseguretat, etc.

internetsegura.cat/empresa/recursos/

Avisos de ciberseguretat

Per estar assabentats l'Agència de Ciberseguretat de Catalunya: publica avisos de seguretat amb els nous patrons d'atac i recomanacions de protecció per evitar-los.

https://ciberseguretat.gencat.cat/ca/actualitat/avisos-i-butlletins/index.html

Eines Internet segura, aprèn, Negocibersegur

Per estar assabentats l'Agència de Ciberseguretat de Catalunya: publica avisos de seguretat amb els nous patrons d'atac.

https://internetsegura.cat/empresa/apren

Eines de ciberseguretat per a PiMEs de GCA

https://gcatoolkit.org/es/pequenas-empresas/protejase-contra-el-phishing-y-el-malware/?_tk=antivirus-es#toolkit

AGÈNCIA DE
CIBERSEGURETAT
DE CATALUNYA