Universitat Oberta de Catalunya

La Ciberseguretat a les pimes espanyoles: realitat o repte?

Joan Ruiz Rodríguez
Grau d'Enginyeria Informàtica
05.625 TFG Seguretat Informàtica

Tutor: Gerard Farràs Ballabriga
Professora responsable de l'assignatura:
Helena Rifà Pous

Data Lliurament: 01-2023

Agraïments

A la meva estimada Montse, la meva parella que m'ha acompanyat i recolzat en aquesta dura travessia. Sense ella hauria estat impossible. Als meus tres fills, l'Èrik, l'Arlet i l'Emma per tots els moments que m'he perdut amb ells i que penso compensar quan finalitzi aquest projecte. Als meus pares per donar-me una educació i uns valors exemplars. A tots aquells familiars i amics que m'han recolzat i creuen en mi. De tot cor.


Aquesta obra està subjecta a una llicència de Reconeixement-NoComercial-SenseObraDerivada 3.0 Espanya de Creative Commons

C) Copyright

© (el autor/a)
Reservats tots els drets. Està prohibit la reproducció total o parcial d'aquesta obra per qualsevol mitjà o procediment, compresos la impressió, la reprografia, el microfilm, el tractament informàtic o qualsevol altre sistema, així com la distribució d'exemplars mitjançant lloguer i préstec, sense l'autorització escrita de l'autor o dels límits que autoritzi la Llei de Propietat Intel·lectual.

FITXA DEL TREBALL FINAL

Títol del treball:	*La Ciberseguretat a les pimes espanyoles: realitat o repte?*
Nom de l'autor:	*Joan Ruiz Rodríguez*
Nom del consultor/a:	*Gerard Farràs Ballabriga*
Nom del PRA:	*Helena Rifà Pous*
Data de lliurament (mm/aaaa):	*01/2023*
Titulació o programa:	*Grau d'Enginyeria Informàtica*
Àrea del Treball Final:	*Seguretat Informàtica*
Idioma del treball:	*Català*
Paraules clau	*Cibermaduresa,Ciberresiliencia, Ciberseguretat com a Servei (CSaaS), vector d'atac, superfície de risc.*

Resum del Treball (màxim 250 paraules):

En el món global en què vivim, qualsevol organització que vulgui ser protagonista d'una història empresarial d'èxit no només contempla la ciberseguretat com una opció de present necessària i una realitat de futur, sinó como un requisit indispensable actual per poder afrontar i garantir la seva supervivència i viabilitat.

Aquest projecte es centra en les entitats que conformen la major part del teixit industrial del país, és a dir, les pimes i els autònoms. Mitjançant (una eina que engloba) un seguit de formularis es plantegen una sèrie de qüestions sobre els diferents enfocaments de la seguretat informàtica i ens proporcionen una informació útil del punt de partida, respecte la seva maduresa, resistència i protecció davant ciberincidents.

Sovint, raons econòmiques, de manca de temps o per absència parcial o total de formació dels empleats d'aquestes empreses fan que sigui indispensable trobar les causes i els catalitzadors imprescindibles per mesurar, classificar i orientar aquestes entitats cap a una veritable possibilitat de millora de la seva *Cibermaduresa* i *CiberResiliència*.

Finalment, si en acabar l'anàlisi es detecta que hi ha un desig real de millora per part d'aquestes empreses *auditades*, però alhora també factors que impedeixen la correcció de la seva ciberseguretat, serà quan es formularà un dels principals objectius d'aquest treball: convèncer-les que adoptin la Cib*erseguretat com a Servei* (*CSaaS*) com una estratègia vàlida i complementària per assolir aquest repte.

Abstract (in English, 250 words or less):

In our present global world, any organitzation attempting to succeed in business does not only need to consider cybersecurity as a necessary present option and future reality, but also an essencial current requirement to face and ensure their survival and viability.

This project aims at the companyies that make up most of the industrial network of our country, that is, the SMEs and the *self-employed*. By using a set of forms, a number of questions are asked about the diferent approaches to their computer security provide us with useful information about the starting point regarding their maturity, resistance and protecction against cyberincidents.

Quite often financial reasons, lack ot time, or due to the parcial or total absence of training of the employees in these companyies make it essential to find out causes and catalysts and, therefore, be able to measure, classify and guide these companyies towards a genuine possibility of improving their Cibermaturity and CyberResilience.

Finally, if at the end of the analysis, it is clear that there's a real intention of improvement by these *audited* companyies, but at the same time there are also that prevent the enhancement of their cibersecurity, it will be the right moment tot present them one of the main objectives of the present paper: to convince them of the importance and need of adopting *Cibersecurity as a Service (CSaaS)* as a vàlid and complementary strategy to fulfill this challenge.

Índex

Taula d'Il·lustracions

1 Introducció

1.1 Context i Justificació de TFG

Finals de l'any 2022, el món segueix immers en un continu dinamisme global. La guerra a Ucraïna i les seves conseqüències globals, les pandèmies, els efectes del canvi climàtic i els incidents mundials en forma de ciberatacs són 4 de les principals preocupacions dels seus habitants. En aquest document, es farà un petit i modest anàlisi sobre la quarta amenaça i com afecta a les PIMES espanyoles.

Segons dades Incibe, en el que portem d'any, un 51% de les empreses estatals, sense distingir encara la seva mida, han patit durant l'any un atac informàtic, amb un cost mig d'11.000 euros. Com a exemple, els atacs ransomware han crescut un 8% i les empreses víctimes que el van pagar va ser del 64%. El percentatge de TI destinat a ciberseguretat ja es del 24%. Un 66% de les entitats disposen d'alguna mena d'assegurança ciber.

Les principals conseqüències de rebre un ciberatac són diverses i ocasionen a les entitats impactes econòmics (alguns signifiquen la seva desaparició), danys en les marques i la seva reputació, pèrdues de clients amb una major dificultat per captar-los, multes elevades, solvències amenaçades, rescissió d'acords amb socis comercials, etc.

No obstant, no totes les noticies són negatives, a les empreses amb mides reduïdes cada cop hi ha més percepció de la transcendència de estar protegit. Les principals motivacions són la preocupació per la seguretat de les dades, enfrontar les amenaces i vulnerabilitats existents, assolir i complir el compliment normatiu, implantar sistemes per detectar personal, connexions o dispositius no autoritzats, etc.

L'objectiu principal d'aquest projecte es proporcionar una petita eina que sensibilitzi i convenci a les empreses catalogades com a cibernovates que considerar e incrementar la inversió en ciberseguretat és una estratègia d'èxit i futur. Aplicar la eina no es garantia de no patir atacs, però si que ajudarà a augmentar la seva ciberresiliència davant d'escenaris no previstos. En molts casos s'hi juguen la seva viabilitat.

1.2 Objectius del Treball

Els objectius que es pretenen aconseguir amb la realització d'aquest TFG són:

- L'anàlisi i definició de paràmetres de ciberseguretat realistes que mostrin l'estat de protecció actual de la majoria de les Microempreses, Startups i PIMES ubicades en territori Espanyol.

- Comprovació que l'ús d'alguns dels principals indicadors tecnològics contemplats en l'actualitat ens ajuden a valorar a qualsevol entitat en aspectes relatius a la seguretat.

- Estudi d'indicadors basats en la confiança digital per establir un termòmetre en les percepcions de ciberseguretat a les empreses espanyoles.

- Intentar comprovar la hipòtesi de que una major inversió en matèria de seguretat redueix l'impacte econòmic i operatiu en cas d'incidents informàtics a les PIMES.

- Per últim, i conseqüència de l'estudi i anàlisi dels altres quatre objectius, construir una eina d'auto diagnòstic que ajudi en la conscienciació i establiment de les primeres decisions en la protecció i millora dels nivells de ciberseguretat de les organitzacions empresarials espanyoles de reduïda dimensió.

1.3 Metodologia aplicada

El plantejament i la resolució d'aquest TFG es caracteritza per distingir tres etapes molt marcades on es treballarà de forma diferent a cada una d'elles:

- Una primera etapa que es materialitzarà en la confecció de la proposta inicial del TFG. Es caracteritzarà per ser molt concreta, introductòria i lògicament subjecte a canvis que forçosament l'han d'anar perfilant a mesura que es vagi aprofundint en la elaboració de les dos etapes següents. Es pretendrà que el lector conegui aquí la temàtica a analitzar, els objectius del treball i la planificació per a poder resoldre el TFG amb èxit.

- La implementació de la segona etapa comportarà un enfocament molt teòric e introspectiu que tractarà de recopilar i sintetitzar les cerques a la vasta informació existent en diversos àmbits. Es prioritzarà una exposició de les problemàtiques i objectius a assolir cercant les fonts que es caracteritzin per ser el més fidedignes, recents i objectives possibles. Dades d'estudis sectorials, d'INCIBE, de CCAA, de l'INE, de l'ONTSI seran consultades amb tota seguretat.

  Conceptes com Ciberseguretat, incidents informàtics, indicadors tecnològics, confiança digital, mesures de protecció en l'àmbit de les PIMES aniran donant forma a aquest etapa proporcionant dades e informació tractable per poder elaborar la següent fase. És possible que es produeixi treball de camp en forma d'entrevista amb personal d'empreses d'auditoria o personal directiu que lideri alguna PIME molt relacionada amb el sector informàtic.

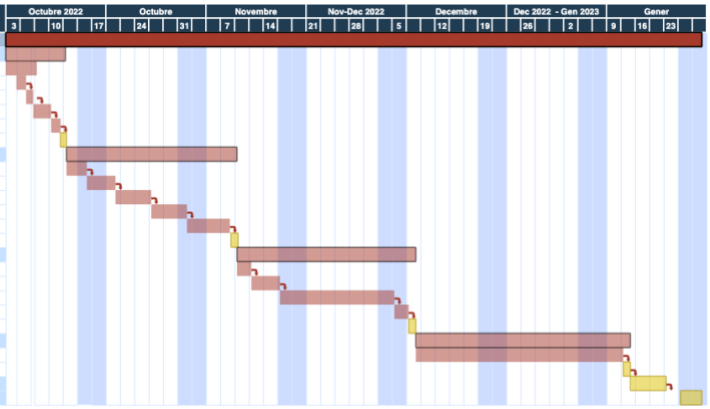
- La última fase, tindrà un enfocament pràctic i es mirarà d'escollir un programari informàtic que sigui molt visual i que ens permetrà la construcció d'una eina d'auto diagnòstic que aglutinarà en forma de qüestionari algunes de les conclusions e idees valorades com a recomanacions i quasi "obligacions" en matèria de ciberseguretat que haurien de tindre presents els directius de les PIMES per conscienciar-se de l'estat actual de les seves situacions.

  Aquesta fase també haurà de presentar finalment el document final en forma de Memòria Final del TFG, així com una presentació en vídeo que permeti defensar amb garanties el projecte davant del Tribunal que el valorarà en la prova final asíncrona.

1.4 Abast i Planificació del TFG

Per definir, abordar i preparar el llistat de tasques que s'aniran implementant s'ha confeccionat un *Diagrama de Gantt*. Aquest mostra en un esquema cronològic l'ordre i periodificació aproximada de les diferents tasques que s'esperen resoldre, esperant incrementar així les possibilitats d'èxit en les diverses entregues que es produiran en el transcurs del projecte.

	Nom Tasca	Duració	Comença	Acaba
	Execució Completa del TFG	121 dies	29.09.22	27.1.23
	Entrega del Pla de Treball	13 dies	29.09.22	11.10.22
	Revisió material docent i supervisions prèvies Tutor	7 dies	29.09.22	6.10.22
1	Introducció, Context i Justificació del Treball	2 dies	2.10.22	4.10.22
2	Objectius del Treball	2 dies	4.10.22	6.10.22
3	Metodologia aplicada i Planificació	4 dies	6.10.22	10.10.22
5	Breu descripció memòria	2 dies	8.10.22	10.10.22
	Lliurament Pla Treball (PAC 1)	1 dia	11.10.22	11.10.22
	Seguiment del TFG. 1ª Fase.	28 dies	12.10.22	08.11.22
	Preparació i Distribució Blocs Informació	2 dies	12.10.22	14.10.22
6	Ciberseguretat: Estat actual Pymes	5 dies	15.10.22	19.10.22
7	Descripció Incidències Seguretat	6 dies	20.10.22	25.10.22
8	Ús habitual Mesures Defensives	6 dies	26.10.22	31.10.22
9	Avaluació amb Indicadors Tecnològics i Confiança Digital	7 dies	01.11.22	7.11.22
10	**Lliurament 2ª Entrega (PAC 2)**	1 dia	8.11.22	8.11.22
	Seguiment del TFG. 2ª Fase	28 dies	9.11.22	06.12.22
11	Selecció eina construcció Auto-Auditoria	2 dies	9.11.22	11.11.22
12	Treball de Camp	5 dies	12.11.22	16.11.22
13	Construcció e Implementació eina avaluativa	18 dies	17.11.22	3.12.22
14	Síntesi i Proves de Camp	2 dies	4.12.22	6.12.22
15	**Lliurament 3ª Entrega (PAC 3)**	1 dia	6.12.22	6.12.22
	Presentació Memòria final del TFG. 3ª Fase	35 dies	07.12.22	10.1.23
16	Síntesi, conclusions, reserves Tutor i aspectes formals.	34 dies	07.12.22	09.1.23
17	**Lliurament definitiu Memòria Final (PAC 4)**	1 dia	10.1.23	10.1.23
18	**Lliurament Presentació vídeo TFG (PAC 5)**	7 dies	11.1.23	17.1.23
19	**Defensa Asíncrona del TFG (PAC 6)**	5 dies	23.1.23	27.1.23



Il·lustració 1: Diagrama Gantt Projecte

Com s'observa al diagrama la construcció de la eina d'auto-diagnòstic i la elaboració de la memòria final requeriran de gran part dels dies destinats a elaborar el TFG. Com aclariment els colors grocs marquen les entregues reals de documentació parcial d'aquest TFG. Per millorar la seva visualització s'inclourà a l'apartat d'annexes el diagrama en versió ampliada.

1.5 Breu descripció Memòria i Producte obtingut esperat

En acabar aquest projecte s'espera la presentació dels següents documents:

- Una memòria que recopilarà un petit estudi sobre les PIMES, Startups o empreses de petita dimensió espanyoles. Analitzarem entre d'altres els següents factors:

  Principals motivacions per invertir en ciberseguretat.
  Incidents més usuals.
  Principals mesures de seguretat adoptades.
  Indicadors tecnològics.

- Aplicació (encara pendent decidir programari) que funcionarà com un formulari de preguntes tècniques que acabaran puntuant en el aspecte que es decideixi a observar el nivell de ciberseguretat assolit per l'empresa del entrevistat/da. L'objectiu de la eina serà reflexiu, tècnic i per conscienciar

1.6 Competència de Compromís Ètic i Global (CCEG).

Aquest projecte espera contribuir de la següent forma amb els 3 principals dimensionaments:

- Sostenibilitat: es preveu que sigui inapreciable, però val a dir, que si una empresa, un cop assessorada, decideix (com veurem més endavant) l'ús de *CSaaS* com estratègia de Ciberseguretat suposarà un petitíssim estalvi energètic i contribuirà a reduir la petjada de carbó que les empreses deixem.

- Diversitat: Voluntàriament, la idea inicial que es pretén, es la de no deixar marge en cap dels continguts d'aquest treball, a què cap expressió i aportació suposi un greuge de cap estil respecte a qüestions de sexe, raça, religió. L'enfoc del treball és eminentment tècnic i es pensa que serà complicat no complir amb aquest dimensionament.

- Ètica: És en aquest dimensionament on pensem que aquest treball tindrà més transcendència. Primerament, perquè es cerca una ajuda de cara a totes aquelles empreses "cibernovates" que no es poden permetre la gestió pròpia de la seva ciberseguretat, ja sigui per una qüestió de recursos o de temps. Es creu que es una idea noble perseguir aquest objectiu.

  Per la resta no podem preveure cap implicació directa en la contribució amb els ODS.

2 La Ciberseguretat: Situació i context a l'ecosistema de Pimes Espanyoles.

2.1 Definició i context PYME.

El títol d'aquest projecte ja ens avança que el públic objectiu d'aquest estudi es refereix a les Petites i Mitjanes Empreses (d'ara endavant PIMES) espanyoles. És indispensable que el lector conegui abans una breu descripció sobre les principals característiques que defineixen a aquest tipus d'organitzacions i la seva situació actual a Espanya i a la UE.

Segons la Comissió Europea, una SMEs[1] (PIME a Espanya) en un informe[2] elaborat per la pròpia institució els tres paràmetres que les identifiquen i permeten la seva classificació i definició són els següents: El nombre d'efectius laborals, el volum de negocis anual i les dades del seu Balanç General. En la taula inferior es visualitza:

Categoría de empresa	Efectivos: Unidades de trabajo anual (UTA)	Volumen de negocios anual	o	Balance general anual
Medianas	< 250	≤ 50 millones EUR	o	≤ 43 millones EUR
Pequeñas	< 50	≤ 10 millones EUR	o	≤ 10 millones EUR
Microempresas	< 10	≤ 2 millones EUR	o	≤ 2 millones EUR

Il·lustració 2: Classificació Pimes

La rellevància d'aquestes organitzacions transcendeix l'àmbit econòmic, social i laboral i per fer-nos una idea mostrem unes classificacions en forma de taules publicades el passat mes de Setembre 2022 pel Ministeri d'Indústria, Comerç i Turisme. Un 99,8% de les empreses estatals són Pimes i aquestes donen feina a més de 10.841.785 persones, o sigui, un 60,2% del total d'assalariats.

[1] Small and medium-sized enterprises

[2] http://www.ipyme.org/es-ES/DatosPublicaciones/Documents/Guia-usuario-Definicion-PYME.pdf

Tabla 4. Distribución de empresas por tamaño y por sector									
	Agrario	%	Industria	%	Construcción	%	Servicios	%	Total
PYME	277.479	100	172.057	99,4	333.680	100	2.152.325	99,8	2.935.541
PYME sin asalariados[3] (0 asalariados) 1T2022	187.333	67,5	67.281	38,9	196.227	58,8	1.169.988	54,3	1.620.829
PYME (1-249 asalariados)	90.146	32,5	104.776	60,5	137.453	41,2	982.337	45,6	1.314.712
Microempresas (1-9 asalariados)[4]	82.019	29,5	74.018	42,7	117.522	35,2	852.709	39,5	1.126.268
Pequeñas (10-49 asalariados)	7.241	2,6	25.090	14,5	18.156	5,4	111.519	5,2	162.006
Medianas (50-249 asalariados)	886	0,3	5.668	3,3	1.775	0,5	18.109	0,8	26.438
Grandes (250 o más asalariados)	105	0,0	1.109	0,6	128	0,0	3.841	0,2	5.183
Total empresas	277.584	100	173.166	100	333.808	100	2.156.166	100	2.940.724

Il·lustració 3: Distribució de Pimes per mida i sector

El col·lectiu **autònom** està reconegut en la distinció per mides dintre de la categoria de PIMES sense assalariats o amb 0 assalariats.

Tabla 6. Distribución del empleo por tamaño de empresa y por sector									
	Agrario	%	Industria	%	Construcción	%	Servicios	%	Total
PYME	632.291	88,7	1.438.701	64,7	1.070.774	92,1	7.700.019	60,2	10.841.785
PYME sin asalariados[3] (0 asalariados) 1T2022	187.333	26,3	67.281	3,0	196.227	16,9	1.169.988	9,2	1.620.829
PYME (1-249 asalariados)	444.958	62,4	1.371.420	61,7	874.547	75,2	6.530.031	51,1	9.220.956
Microempresas (1-9 asalariados)[4]	224.622	31,5	260.957	11,7	366.655	31,5	2.570.048	20,1	3.422.282
Pequeñas (10-49 asalariados)	134.410	18,9	529.620	23,8	346.424	29,8	2.171.569	17,0	3.182.023
Medianas (50-249 asalariados)	85.926	12,1	580.843	26,1	161.468,0	13,9	1.788.414,0	14,0	2.616.651
Grandes (250 o más asalariados)	80.689	11,3	783.606	35,3	92.436	7,9	5.083.577	39,8	6.040.308
Total trabajadores	712.980	100	2.222.307	100	1.163.210	100	12.783.596	100	16.882.093

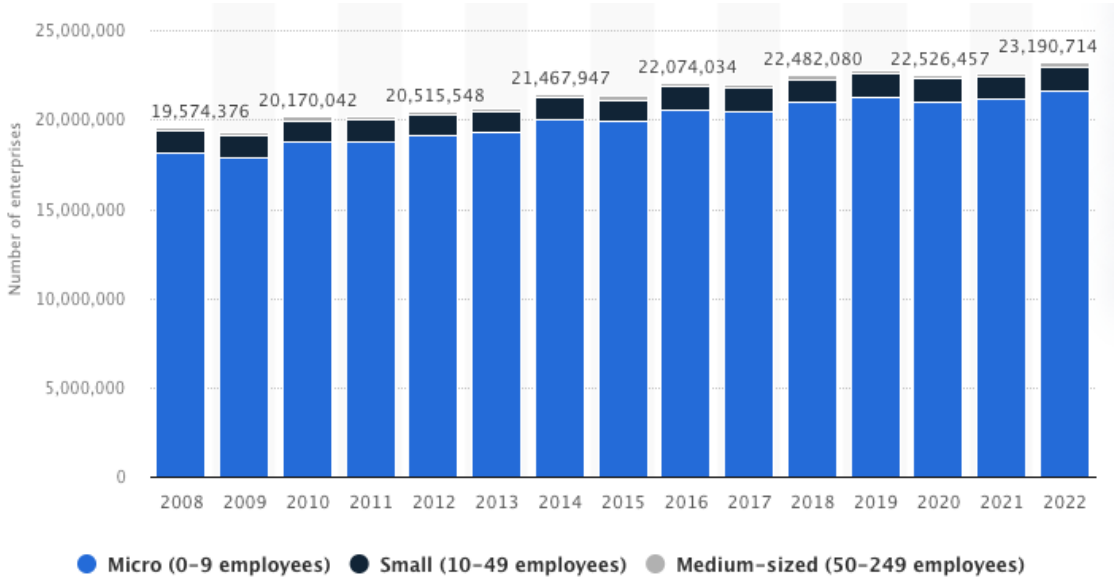
Tabla 7. Tamaño medio empresarial por sectores					
Empleados/empresa	Agrario	Industria	Construcción	Servicios	Total
septiembre 2022	2,6	12,8	3,5	5,9	5,7
septiembre 2021	2,6	12,5	3,4	5,7	5,6

Il·lustració 4: Distribució de treballs per mida i sector

A banda, observem que sectorialment el sector serveis es qui clarament té més presència en el còmput global, però són les empreses del sector industrial qui tenen una mitjana d'empleats més alta (12,8). A Espanya són responsables d'un 53,3% de les importacions i un 51,1% de les exportacions que s'efectuen.

A Europa, les SMEs segueixen un patró molt semblant. Al 2022 hi han censades 23,1 milions (un 99% del total de societats) i contracten a més de 100 milions de persones. Per mides les microempreses i autònoms també són majoria. La mitjana d'empleats contractats es superior a les d'Espanya i per últim, la suma del seu negoci global suposa més del 50% del GDP[3] d'Europa.

Number of SMEs in the European Union 2008-2022, by size. Font: Statista 2022



Il·lustració 5: Number of SMEs in UE

Ara que ja tenim definides quines són les protagonistes d'aquest estudi, i coneixem amb exactitud en termes macroeconòmics com són les PIMES podem concloure amb el lector que són unes dades aclaparadores que potser justifiquen el nostre interès en engegar aquest projecte on haurem de demostrar i convèncer que la ciberseguretat ha de ser un factor clau per protegir els seus interessos en forma de negoci.

[3] (GDP) *Gros domestic product* es el valor total monetari o valor de mercat dels béns i serveis produïts dintre de les fronteres d'un país en un determinat període de temps.

2.2 Estat Actual de la Ciberseguretat a les Pimes Espanyoles

Segons Kaspersky[4] ara que contextualitzem la situació inicial, definiríem Ciberseguretat com la pràctica de defensar equips informàtics, servidors, dispositius mòbils, xarxes, sistemes electrònics i dades de qualsevol atac maliciós.

És un concepte global que no només abasta aspectes de seguretat de les xarxes, de les aplicacions, aspectes operatius i de seguretat de la informació; també prepara per la recuperació de desastres i estudia la capacitació del usuari final. Aquests objectius nosaltres els traslladarem al món de les PIMES espanyoles, i d'ara endavant proporcionarem moltes dades extretes d'estudis.

A Espanya, si es pogués resumir sobre com aborden aquestes organitzacions la seguretat informàtica, es diria que adopten una posició ***reactiva***, és a dir, en general les empreses implementen alguna acció per assegurar els seus negocis, però el marge de millora encara és molt ampli.

En un estudi encarregat per Google al 2020[5] alerta que del 99,8% del teixit industrial d'empreses espanyoles la gran majoria no es considera objecte atractiu de ciberatacs la qual cosa les fa ser encara més vulnerables i estar poc o gens protegides contra atacs malintencionats.

L'aparició del Covid19 ha incrementat encara més aquest exposició als riscos donat que les empreses s'han vist obligades a apostar pel teletreball i el treball amb al núvol. També la explosió de tecnologies com el 5G, l'IoT augmenten la possibilitat de bretxes no autoritzades als sistemes de moltes companyes.

Com ja anticipàvem a la introducció ja sigui per manca de recursos econòmics, o bé, per una errònia mentalitat consistent en auto-excloure's i no identificar-se com a potencials objectius dels cibercriminals per ser empreses petites, això està tenint conseqüències devastadores per a moltes d'elles.

De fet ja es recull en alguns informes[6] publicats al 2019 on ja s'alerta què el 43% dels ciberatacs ja anaven dirigits contra aquest segment d'empreses ocasionant-los un impacte mig negatiu de 35000 euros i com a conseqüència provocant la desaparició del 60% de les afectades al cap de 6 mesos.

Això és degut, a que la seva capacitat de resiliència (recuperació després d'un atac) és molt menor que el de les grans empreses, degut a la seva menor potència econòmica, i la seva menor capacitat de resposta en termes de ciberseguretat. La previsió en la gestió de riscos acostuma a ser deficient.

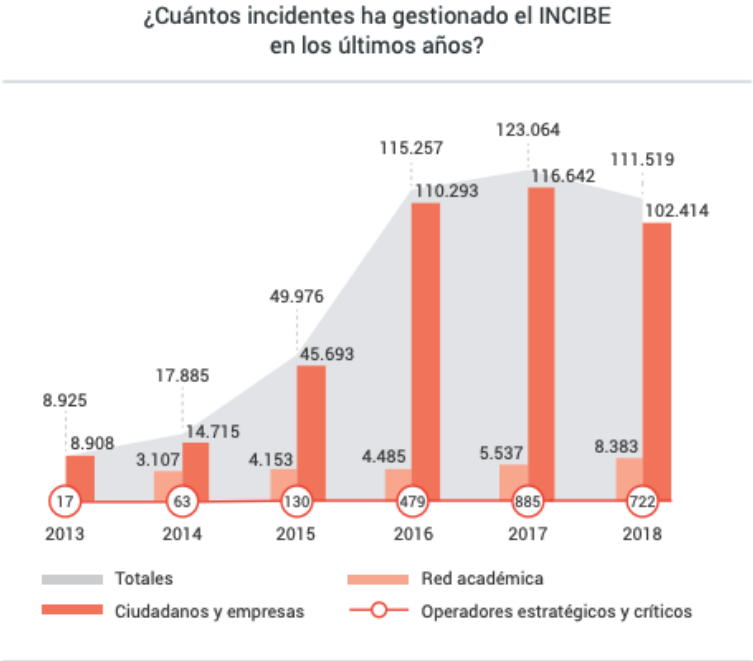
[4] © 2022 AO Kaspersky Lab: empresa multinacional de ciberseguretat fundada al 1997 a Moscou (Rússia).

[5] Panorama Actual de la Ciberseguridad en España. Retos y oportunidades para el sector público y privado. the cocktail© analysis (2020) Estudi realitzat per Google.

[6] Karspersky Lab & Ponemon Institute: "No hay víctimas pequeñas para los cibercriminales". https://www.kaspersky.es/about/press-releases/2017_no-small-victims-for-cybercriminals

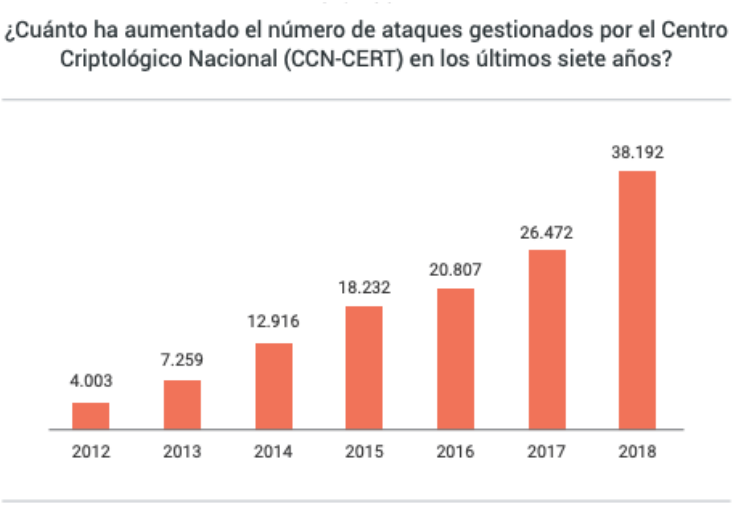
Altres motius que penalitzen i condicionen són: el baix compromís de la direcció al prioritzar altres aspectes vers la seguretat i la manca de capacitats en ciberseguretat al no haver suficients empleats ni la formació suficient per desenvolupar els rols necessaris en seguretat.

Si volen reflectir la incidència real observarem com a exemple en les següents gràfiques una tendència marcada en els últims anys en l'alça del nombre d'incidents.



Fuente: Instituto Nacional de Ciberseguridad (INCIBE).

Il·lustració 6: nombre incidents gestionats per Incibe



Fuente: Centro Nacional de Inteligencia.

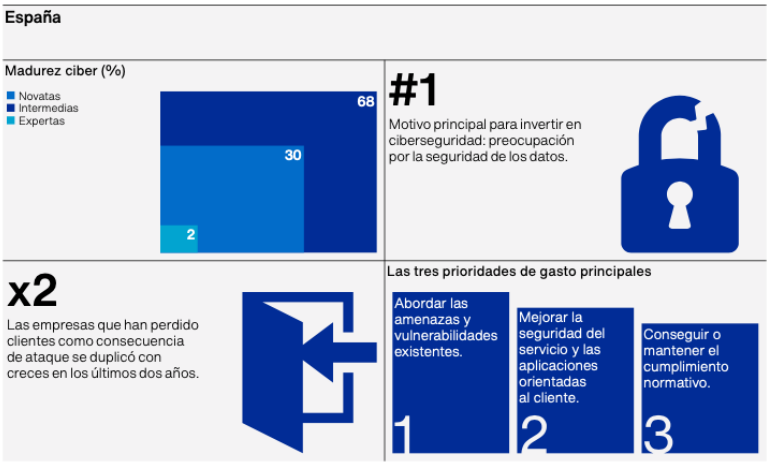
Il·lustració 7: augment atacs gestionats per CCN-CERT

La tendència com es mostra a continuació és imparable. Com es veu a continuació en l'última estadística recollida, l'any 2020 ha sigut molt disruptiu en molts aspectes i ha catalitzat el nombre d'incidents a causa del nou ordre post pandèmic, amb més mobilitat, teletreball, ús del núvol, etc.

Il·lustració 8: incidents gestionats al 2020 per Incibe

Font: https://www.incibe.es/sites/default/files/paginas/que-hacemos/balance_ciberseguridad_2020_incibe.pdf

Un informe del 2022 de la ciberasseguradora Hiscox fet a vuit països europeus (exposem dades a Espanya) mostra quines són les principals preocupacions per invertir en ciberseguretat i les conseqüències (no financeres) que es presenten quan les empreses no ho han fet com caldria i han patit un ciberatac.



Il·lustració 9: nivell cibermaduresa Espanya

Il·lustració 10: principals impactes d'un ciberatac

Font: https://www.hiscox.es/informe-de-ciberpreparacion-de-hiscox-2021

2.3 Principals Agents de l'Amenaça per les Pimes

Però qui són els principals atacants? Quins perfils tenen interessos en causar perjudicis a les organitzacions empresarials més habituals de la nostra geografia? Organismes com CCN-CERT[7] ja fa anys que els estudien i els identifica com els agents següents:

Il·lustració 11: Delictes dels Estats i grups patrocinats per estats

Il·lustració 12: principals delictes dels ciberdelinqüents

Il·lustració 13: delictes d'Hacktivistes

Il·lustració 14: incidents protagonitzats per insiders

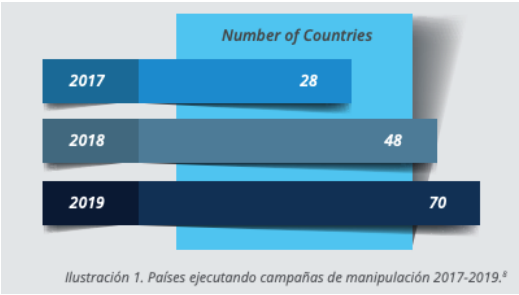
[7] CCN-CERT: Centro Respuesta Centro Criptológico Nacional del Centro Nacional de Inteligencia:

Il·lustració 15: Principals agents de l'amenaça

Com es veu a la pàgina anterior s'identifiquen algun dels 6 actors principals:

2.3.1 Actors Estat o Grups Patrocinats per Estats:

Molts estats ja inverteixen en la generació de capacitats de ciberespionatge, ciberguerra (guerra hibrida) que es destinen al sabotatge de processos crítics pel funcionament d'un país. També desenvolupen operacions d'informació encaminades a influir en les societats. Les empreses es veuen afectades sobretot per accions de manipulacions de sistemes i ciberespionatge. Els nombrosos grups APT són un exemple.



Il·lustració 16: Nombre de països protagonistes d'APT
Font: The Global Disinformation Order. Oxford University.

2.3.2 Ciberdelinqüents

Els seus objectius d'atac són institucions, bancs, escoles, hospitals i per descomptat les empreses, on les perjudiquen amb accions que tenen a veure amb el robatori i manipulació d'informació, interrupcions dels seus serveis i manipulació dels sistemes provocant greus afectacions a les empreses. Al 2019 van utilitzar bàsicament estratègies d'atac ransomware, phishing corporatiu i malware a mida.

2.3.3 Hacktivistes

Són grups reivindicatius que actuen per raons ideològiques. Afecten a les empreses sobretot en el robatori i manipulació d'informació, com també en la interrupció dels seus serveis principals. Utilitzen atacs DDoS, injeccions SQL, doxxing, *defacements*, etc. Sovint, utilitzen Twitter com a canal de comunicació per publicar els seus actes.

2.3.4 Cibervàndals

són grups amateurs i poc qualificats que només responen a l'afany d'agitar i cridar l'atenció de les societats. Afectacions lleus a les empreses.

2.3.5 Ciberterroristes i Ciberyihaidistes

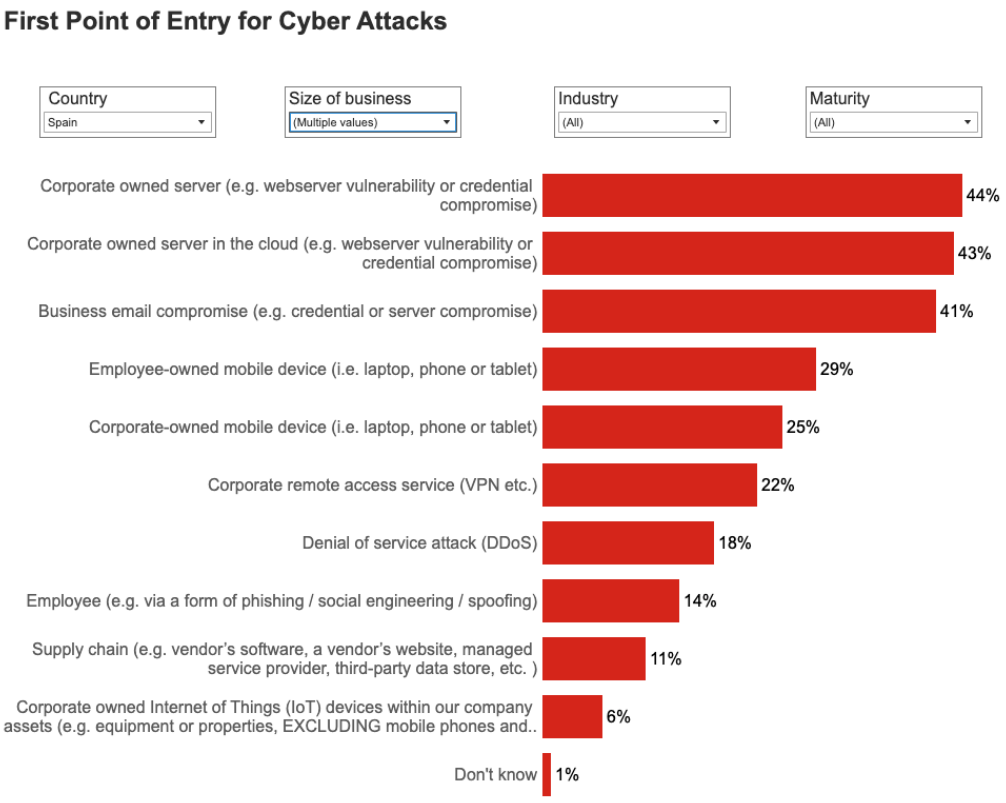
Organitzacions terroristes que han desenvolupat les seves pròpies divisions informàtiques. Els seus atacs no acostumen a ser sofisticats i tenen poca incidència en les empreses, però poden suposar una greu amenaça en determinades situacions sobretot pel sector públic.

2.3.6 Insiders (Personal Intern)

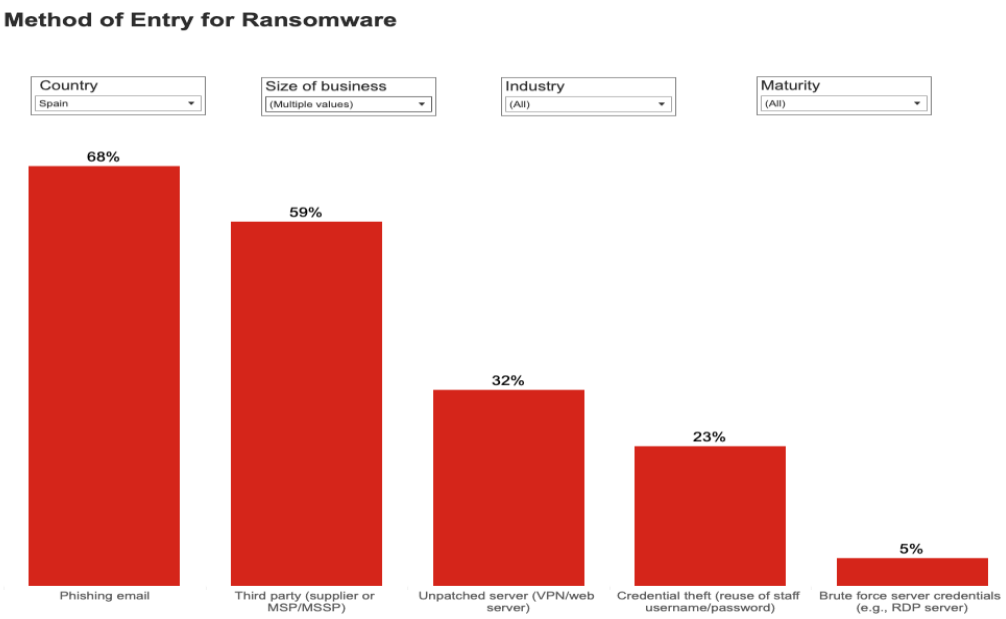
Deixant de banda un petit % d'empleats malintencionats, en general, la gran preocupació de les empreses recau en treballadors de les organitzacions que involuntàriament i per manca de conscienciació, entrenament, formació o altres errors poden ocasionen greus perjudicis econòmics i reputacionals a les empreses que els contracten. Les seves negligències permeten entre d'altres accions com el robatori d'informació o la interrupció de serveis principals. El phishing és un dels principals vectors d'atac.

2.4 Principals punts d'entrada dels ciberatacs

I com ho fan els agents d'amenaça per atacar a les pimes espanyoles? Quines són les vies principals d'entrada per aconseguir que tinguin èxit els seus atacs? En aquest quadre publicat al 2022, (filtrat per mida Pimes) l'asseguradora de ciberriscos Hiscox ens detalla quins són els principals punts crítics d'entrada.



Il·lustració 17: primer punts d'entrada ciberatacs



Il·lustració 18: mètode entrada ransomware

font: https://www.hiscox.es/informe-de-ciberpreparacion-de-hiscox-2022

Com observem als gràfics de barra la gran majoria dels atacs es centren en l'accés a servidors corporatius, ja siguin físics o al núvol. Les intrusions a través de correus electrònics corporatius també copen la majoria de casos. És preocupant observar com els mètodes d'enginyeria social, *spoofing*, *phishing* i l'accés a través d'IoT estan a l'alça.

En ell segon quadre de la pàgina anterior s'exposa, com a cas concret, un atac especialment greu, el ransomware. El primer que observem es que els ciberdelinqüents a Espanya escullen com a principals vectors d'atac l´ús de *phishing* i la suplantació de programari de tercers per perpetrar-ho.

2.5 Principals tipus d'Incidents

Tot i que existeixen molts tipus de classificacions, ens centrarem en les nostres protagonistes (les Pimes) i ens basarem en un estudi del CNT-CERT per fer més entenedor aquest apartat i el següent, de forma què a continuació es farà una primera classificació en funció del tipus de delicte o vulnerabilitat que permet l'acció d'aquests vectors d'atac. (Els veurem a l'apartat 2.6).

2.5.1 Ciberespionatge. Operacions d'adquisició d'informació:

És una amenaça que està dirigida contra el sector públic i el privat. La situació geopolítica actual i sobretot el Covid19 han marcat una nova tendència marcada per nous focus d'interès delictius que s'afegeixen a les tradicionals estratègies d'espionatge militar, polític, industrial i empresarial.

Les noves vulnerabilitats dels accessos remots del teletreball, el gran nombre de dispositius IoT i altres factors han incentivat cada cop més que hi hagi més de 100 països amb capacitat per recopilar intel·ligència del ciberespai. Aquestes capacitats les composen els denominats grups APT[8], grups molt preparats tècnicament i recolzats econòmicament que miren d'existir ocults el màxim temps a les xarxes per mirar d'extreure la màxima informació.

Existeixen molts exemples d'aquests grups: Per exemple APT29[9], va actuar contra la empresa SolarWinds[10] a l'any 2020. *APT27/EmissaryPanda* que actuen utilitzant tècniques de ransomware per robar propietat intel·lectual a empreses, APT41 que miren d'actuar contra empreses privades per motivacions econòmiques. Altres són Grupo Snake, Winnti, APT28, etc.

2.5.2 Operacions d'Influència, notícies Falses (Fakes News) i desinformació

Algunes d'aquestes accions provenen d'altres estats, que tenen entre les seves motivacions afeblir la capacitat política, tecnològica, econòmica nacional però també intenten influenciar i alterar la opinió pública. Existeixen moltes estratègies delictives però enfocant-nos en les empreses una molt coneguda és l'ús d'*Enginyeria Social*, que explicarem al apartat vectors d'atac.

Les *Fake news* han suposat una gran finestra oberta per les notícies falses, que es van propagar ràpidament entre ciutadans i empreses, en alguns casos amb greus conseqüències per la seva salut i seguretat. Són coneguts els exemples de publicacions que es van produir en les setmanes de confinament durant la pandèmia.

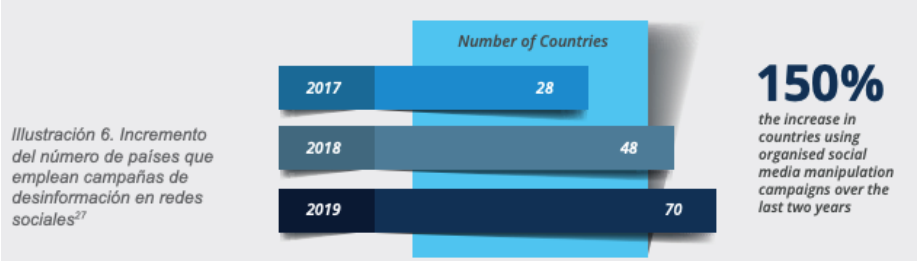
Les tècniques de desinformació i propaganda al ciberespai s'han anat perfeccionant i avui la informació no contrastada, les advertències mal interpretades i les teories de la conspiració generen confusió entre la població i les empreses facilitant en molts casos patir ciberatacs.

---

[8] APT (Advanced Persistent Threat).

[9] APT29: El 15 de abril de 2021 el gobierno de los Estados Unidos de América atribuyó este ataque al grupo conocido como APT29, del Servicio de Inteligencia Exterior (SVR) ruso: https://www.whitehouse.gov/briefing-room/statementsreleases/2021/04/15/fact-sheet-imposingcosts-for-harmful-foreign-activities-bythe-russian-government/

[10] SolarWinds: va patir una intrusió en la que els atacants van aconseguir modificar el codi d'una de les seves aplicacions de gestió de xarxa per introduir una backdoor. Aquesta modificació va ser transmesa a tots els clients, el que va desplegar la backdoor a milers d'organitzacions afectant a quasi 18000 entitats del servei públic i privat.



Il·lustració 19: increment països utilitzen Fakes News en xarxes socials

Font: Universidad de Oxford, COMPROP (The Computational Propaganda Project).

Són coneguts els casos habituals de desinformació a les xarxes socials com Facebook, Instagram i sobretot Twitter. Aquesta última degut als intents de manipulació de la seva plataforma al 2020 va haver d'actualitzar les seves polítiques contra la desinformació incloent etiquetes d'advertència sobre els continguts dels tuïts. Ara i després de la seva recent adquisició pel multimilionari *Elon Musk* torna a ser el centre d'atenció per veure quina serà la seva política de continguts.

Number of accounts challenged monthly Jan 1 - Jun 30, 2019

Month	Challenges
January	19,522,273
February	17,036,751
March	16,552,753
April	13,787,154
May	14,848,125
June	15,376,611
TOTAL	**97,123,667**

Ilustración 7. Cuentas canceladas por Twitter por intentos de manipulación[30]

Il·lustració 20: comptes cancel·lats per Twitter per intent manipulació

2.5.3 Atacs Disruptius i de control

Normalment són causats per ciberdelinqüents i actors patrocinats per governs. Consisteixen en utilitzar malware (del tipus ransomware, minat de criptomònades o atacs DDoS) que recolzant-se amb dispositius de control remot són capaços d'inutilitzar sistemes i processos productius.

Una tècnica que està en augment és la doble extorsió, que combina la disrupció de processos productius amb la publicació d'informació confidencial. Un dels primers casos coneguts és el que va patir l'empresa alemanya de programari AG al 2019 o en l'àmbit educatiu la Universitat Autònoma de Barcelona (UAB). Les dos es van negar a pagar el rescat milionari i van patir les conseqüències, en forma d'inutilització dels serveis i la exposició pública de dades.

A vegades, enlloc d'utilitzar programari maligne, s'utilitzen atacs d'esgotament (DoS o DDos) que miren de dirigir quantitats ingent de tràfic generat de vàries

formes amb l'objectiu de saturar i atacar els sistemes (webs, servidors, etc.) de les organitzacions que estan exposats a Internet. Són coneguts les afectacions per aquest tipus d'atac que van patir l'empresa de videojocs Blizzard i Xbox.

És una tècnica que té molts adeptes entre els delinqüents i contínuament cerquen la forma d'incrementar els caudals de tràfic i que aquest sigui sostingut en el temps per causar el major dany possible a les víctimes escollides.

2.5.4 Bretxes de Dades

Continuen sent habituals i la gran majoria tenen a veure amb el espionatge. Segons DBIR[11] al 2019 el 34% de les bretxes van ser causades per insiders, un 39% per ciberdelinqüents i un 23% per actors Estat. De fet són incidents que es produeixen a diari i comprometen dades personals però no acostumen a fer-se públics. Són coneguts al 2020 els casos que van patir empreses com *Microsoft, Decathlon, Twitter, Aptoide, Nintendo*, etc.

En la majoria d'atacs, la motivació és econòmica, ja què els atacants a través de malware, phishing, tècniques d'Enginyeria Social o altres tècniques aconsegueixen accedir a les *dades core* (converses, correus electrònics, telèfons, números Seguretat Social, adreces, etc.) sol·licitant un rescat a canvi què aquestes no siguin publicades.

2.5.5 Altres ciberdelictes

En aquest apartat intentarem incloure la resta d'incidents habituals. Hi ha dos estratègies molt importants HOR (Human Operated Ransomware) on es concreten atacs ransomware i BEC (Business Email Compromise), que es concreten a través d'atacs de phishing corporatius, com el conegut frau del CEO[12].

La estratègia HOR engloba una sèrie d'atacs de la modalitat ransomware. Són molt temuts i considerats com els més perjudicials de la última dècada. Es caracteritzen cada cop més per ser sofisticats amb variants com la doble extorsió, però també molt ràpids i destructius. Es van desenvolupant variants contínuament com el ransomware Exprés (*Ryuk* que busca el màxim dany possible en el mínim temps), *Ransomware as a Service*, però existeixen molts altres (*RobinHook, Avaddon, NetWalker, Maze, Snake Locker, Vcript,* etc.).

Sorprèn la facilitat dels seus atacs a entitats que se suposen són ciberexpertes amb sistemes de defensa i una maduresa en TIC[13]. No obstant, degut a que els seus mètodes cada cop són més selectius i exitosos, les petites empreses i administracions locals ja no escapen als seus efectes. Tant les quantitats

[11] Verizon Data Breach Investigation Report: https://www.verizon.com/business/resources/reports/2019/2019-data-breach-investigations-report.pdf

[12] CEO: Sigles en anglès *Chief Executive Officer* o Director, o màxim responsable d'una organització.

[13] TIC: Tecnologíes de la Informació i Comunicació

exigides com les probabilitats de que les víctimes paguin cada cop són més elevades i és per això que és un dels atacs preferits pels delinqüents.

Basant-se també en la manca de conscienciació (reutilització de credencials, phishing), també hi ha una altre estratègia molt efectiva: BEC. El phishing corporatiu s'aprofita moltes vegades de la situació del teletreball i es preparen minuciosament enganys de baix component tecnològic però on el factor humà és clau per aconseguir el seu èxit.

Es dissenyen situacions de necessitat, d'urgència que es plantegen a les víctimes normalment a través d'un correu electrònic que aconsegueix que aquestes realitzin gestions, facin transferències urgents o altres decisions que normalment les acaben perjudicant econòmicament.

El frau del CEO, on s'acostuma a suplantar la identitat d'un propietari o director d'una empresa per defraudar a la pròpia empresa, els seus empleats, client o proveïdors. La majoria de vegades el focus es contra el personal especialitzat en finances i comptabilitat, perquè són ells els que executen els pagaments. Existeixen també altres modalitats com *l'spear phishing*, *vishing*, etc.

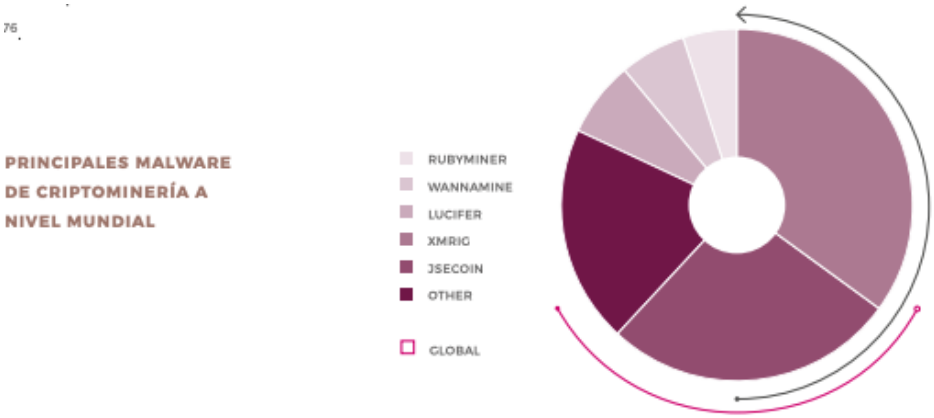
Il·lustració 21: Frau del CEO

Font: https://www.europol.europa.eu/sites/default/files/documents/es_1.pdf

La implantació de la firma digital del correu electrònic (ara poc implantat) seria una pràctica efectiva contra aquests tipus d'atacs. En l'any de la COVID i aprofitant la pandèmia com a reclam, vam sorgir iniciatives de *malware a mida* amb dispositius troians que fins i tot es comercialitzen a la *Dark Web*, com si fos un Maas (*Malware as a Service*).

Una altra ciberdelicte es el *Cryptojacking* (criptomineria) que no sembla un fet delictiu però si que ho és, perquè consisteix en l'ús no autoritzat dels recursos (potència, electricitat) d'un dispositiu sense el consentiment del propietari per minar criptomonedes mitjançant la execució de codi maliciós que passa desapercebut i és difícil de detectar.

La revalorització de les criptomònades des de el 2020 ha incentivat aquest atac, i tot i que no té conseqüències negatives en les organitzacions respecte a pèrdua de dades i segrest d'informació si que pot augmentar els costos de les TI, consum d'electricitat i la degradació dels sistemes informàtics que a mig termini pot afectar a les Pimes.



Il·lustració 22: principals malwares de criptomineria mundials

Font: https://www.checkpoint. com/downloads/resources/cyber-securityreport-2021.pdf

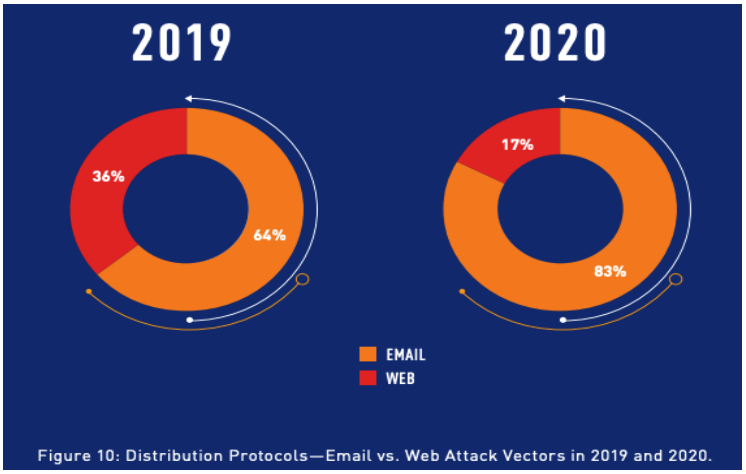
Es coneguda la existència d'autèntics supermercats a Internet que es consideren plataformes enormes de venda de tot tipus d'elements il·legals: armes, drogues, serveis de *hacking as a service*, documents falsificats, *malware*, bases de dades d'usuaris o targetes de crèdit robades, etc. Les empreses són susceptibles de ser víctimes dels productes que busquin compradors malintencionats.

No s'ha d'oblidar mai, el gran negoci que mou els e-Sports. Ja se sap que on hi ha possibilitats de lucrar-se hi ha delinqüència. A través del gran mercat dels videojocs online ja es denuncien incidents que afecten al robatori de targetes bancàries, adreces, dades biomètriques, accessos a *webcams*, micros, ubicació en temps real dels jugadors, *ciberbullying, grooming, sexting*, sextorsió, etc.

2.6 Principals Vectors d'Atac.

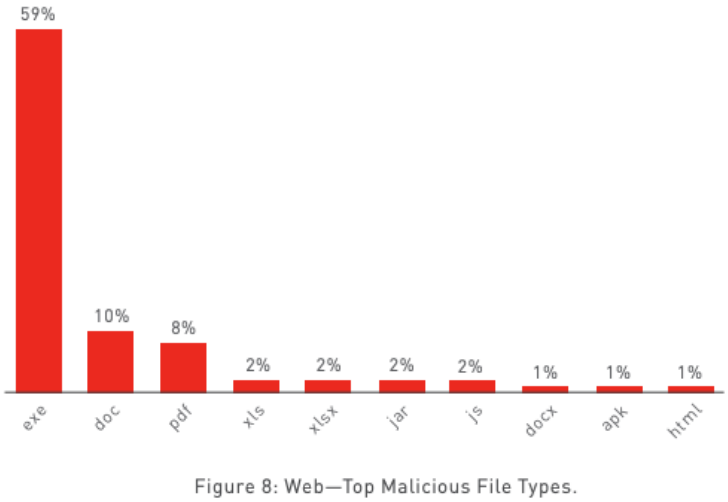
Quins són els principals mètodes d'atac utilitzats pels agents de l'amenaça? La investigació en línia malauradament ens informa d'un nombre inabastable que creix en número, en varietat i en originalitat dia rere dia. La tasca de recopilar i sintetitzar-los tots és complexa i no està a l'abast d'aquest projecte, però si descriurem els grups més importants:

Ja començant a descriure la problemàtica el que està clar és que hi ha una eina (el correu electrònic) què any rere any agafa més protagonisme com a vector d'entrada enfront d'altres accessos tradicionals com les pàgines web.



Il·lustració 23: vector atacs correu electrònic vs Web
Font: checkpoint cybersecurity report 2021

I a sota podem observar una comparativa dels tipus d'arxiu maliciós més utilitzats per infectar a les víctimes. Mentre que els habituals *.exe* executables continuen utilitzant-se en accessos web s'ha d'alertar de com els fitxers *.doc* són una autèntica mina pels dissenyadors de codi maliciós:



Il·lustració 24: Principals web Top arxius maliciosos

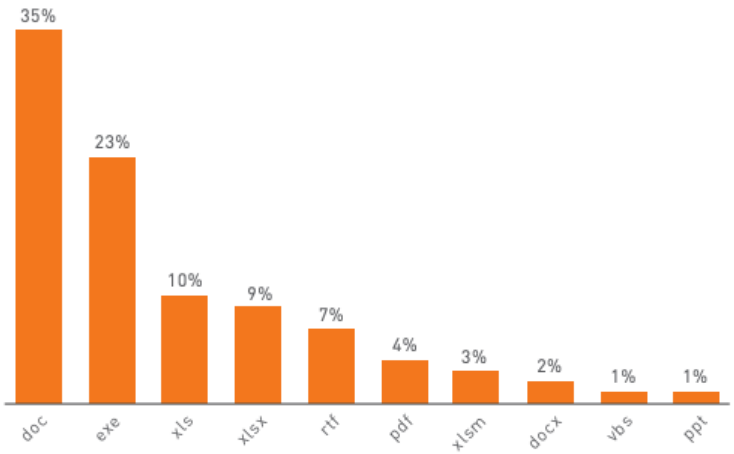


Figure 9: Email—Top Malicious File Types.

Il·lustració 25: principals correu Top arxius maliciosos

font: https://www.checkpoint.com/downloads/resources/cyber-security-report-2021.pdf

2.6.1 Ransomware

Ja hem descrit abans els models HOR (Human Operated Ransomware) on els atacants gestionen codi maliciós combinat amb altres eines ofensives per comprometre a la víctima explotant vulnerabilitats o aprofitant contrasenyes febles en sistemes exposats a Internet. El que tracten es tindre persistència en la seva infraestructura i, finalment, ex filtrar i xifrar la informació.

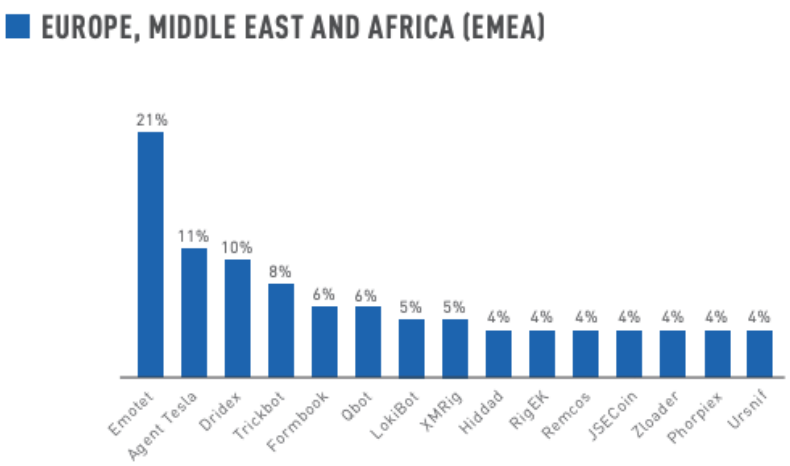
Aquests atacs són molt temuts. La raó es perquè un cop s'accedeix a la *organització víctima* els delinqüents es dediquen dies explorant la xarxa compromesa mirant de localitzar els actius més valuosos (p.e. els controladors de domini, les còpies de seguretat, etc.) i distribuir així el ransomware de forma que l'impacte ocasionat sigui màxim.

Utilitzen com a vectors inicials d'entrada el lloguer de "Botnets" (Ex. *Emotet/Trickbot* ó *Dridex/Bitpaymer*), l'ús de *spear-phising*, servidors RDP[14] exposats i mal configurats i fins i tot l'abús de proveïdors de serveis gestionats de les companyes (*MSP*[15]) per arribar als seus clients finals.

Els sectors afectats són molt diversos: logística, educació, energia, administració pública, telecomunicació, sanitari, ferroviari, industrial, automobilístic i com no a les Pimes, cada cop més atractives pels atacants. Podríem destacar atacs molt coneguts com el que al 2018 va protagonitzar *WannaCry* ocasionant més de 4000 milions de dòlars en pèrdues a molts països i empreses (*Renault, FedEx, Nissan...).*

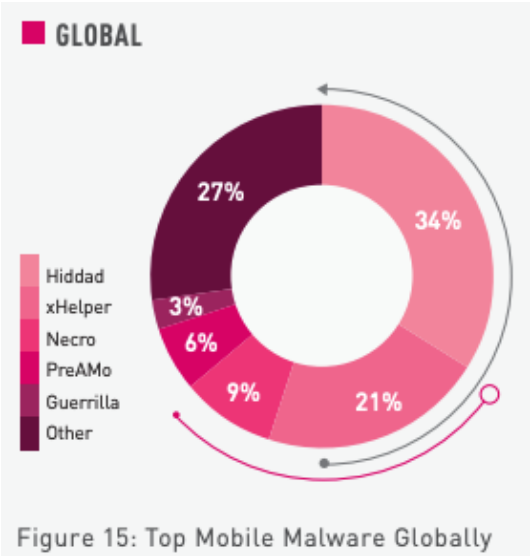
[14] Remote Desktop Protocol: permet que l'escriptori d'un equip informàtic sigui controlat a distància per un usuari remot.

[15] Managed Service Providers: a third-party company that remotely manages a customer's information technology (IT) infrastructure and end-user Systems.



Il·lustració 26: malware principals a països EMEA
Font: Check Point Research Cyber Security Report 2021

Al 2019 van destacar entre d'altres els codis maliciosos de *Bad Rabbit, Cerber, Dharma/CrySiS, Phobos, GrandCrab, Jigsaw, Katyusha, LockerGoga, PewCrypt, SamSam, STOP Ransomware, Revil/Sodinoki, Globelmposter, Buran o MegaCortex. I al 2020, Ragnarok, NetWalker, Nemty, Tycoon, SNAKE, Avaddon, Thanos, BlackKingdom, REvil, TinyCryptor, Ryuk, RansomExx, Conti, Pay2Key o Zeppelin,* entre d'altres.



Il·lustració 27: Top malware mòbils món

Font: Check Point Research Cyber Security Report 2021

Ja hem parlat de la Doble Extorsió (xifrat més sostracció de dades i publicació de dades a la *DarkWeb*). Aquest fet provoca una augment significatiu dels preus que es demanen pels rescats, incentivant a vegades la unió d'aquests grups

especialitzats per compartir coneixement, tàctiques i "*bones pràctiques*" a les seves plataformes *Dataleaks* per aconseguir millorar els èxits i beneficis dels seus atacs.

De fet, existeixen grups independents que competeixen entre ells, per veure qui guanya més. Exemples de fusions entre organitzacions criminals les trobem en varis exemples: Al 2020, sota l'amenaça *Maze*, *LockBit – RagnarLocker*. O dos casos que ampliarem detalls, *Dridex – BitPaymer* i *Emotet-Trickboot-Riuk*.

Emotet era inicialment un troià per robar credencials bancàries que ara s'utilitza mitjançant macros ocultes en correus electrònics per distribuir altres codis maliciosos com el troià bancari *Trickboot* que és el que té capacitat de moviment lateral i propagació a través d'exploits. Un cop dintre, instal.la una aplicació de control remot i si l'estudi de la víctima satisfà al atacant, instal.la el codi *Riuk* que és el que acaba finalment executant un ransomware al client.

Dridex, és un malware que infecta equips a través d'un correu electrònic que incorpora arxius adjunts maliciosos que suposadament enganyen a la víctima instal·lant actualitzacions dels navegadors. Un cop ha fet la feina d'investigació de la víctima els atacants utilitzen *BitPaymer* per executar el codi ramsonware comprometent els controladors de domini i estenent-lo per tota la xarxa. A vegades es fa en caps de setmana per tindre més temps i evitar respostes.

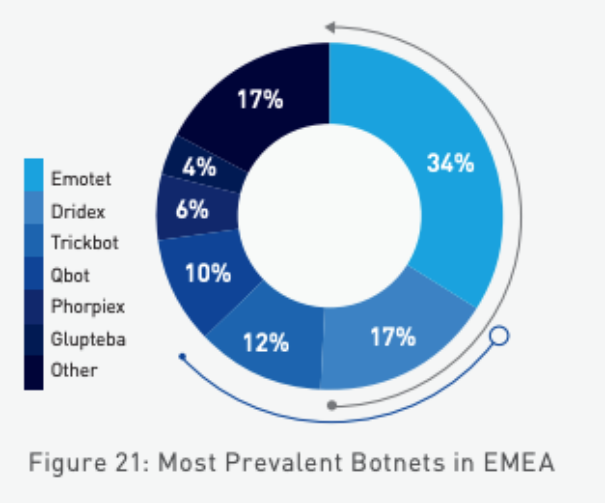
2.6.2 Botnets

Segons *Incibe*, *Botnet* és un conjunt d'ordinadors (bots) infectats amb un tipus de malware que són controlats remotament per un atacant (*botmaster)* i que poden ser utilitzats de manera conjunta per realitzar activitats malicioses (atacs DDoS, phishing, minar criptomonedes, enviament d'spam, etc.) Podem fer una petita classificació conceptual per entendre'ls:

Botnets de IoT nous i modificats: Al 2025 s'estima que hi hauran més de 30000 milions de connexions IoT, unes 4 connexions per persona. Són superfícies d'atac enormes i és molt urgent protegir-les. Sense dubte, és un pastís molt llaminer pels delinqüents i de fet al 2020 ja hi han codis maliciosos com *Dark Nexus, Mukashi, LeetHozer, Hoaxcalls*, etc.

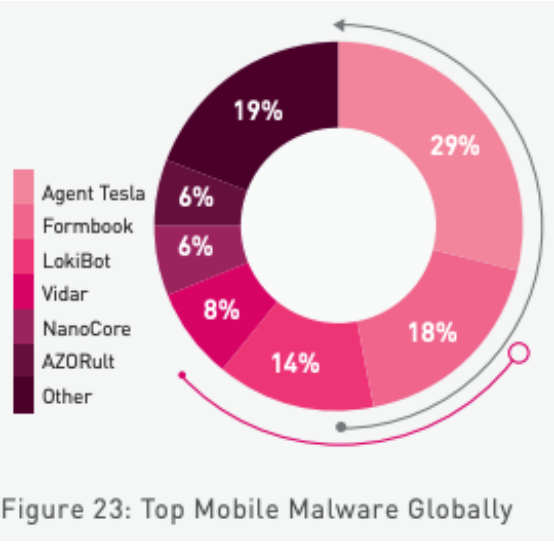
El seu creixement exponencial, les implementacions insegures, la manca d'actualitzacions de seguretat, l'ús de contrasenyes de fàbrica i la poca sensació de perill que inspiren als seus propietaris suposen una greu amenaça. Són utilitzats per dissenyar atacs DDoS o enviaments d'spam massius.

Botnets per Android: Especialistes en atacar aquest sistema operatiu tan desitjat. Operativament són molt semblants als dissenyats per atacar IoT. *IPStorm* i *Matriosh* al 2019 miraven d'aprofitar *exploits* en el port 5555 de les interfícies de depuració de dispositius com SmartTVs. També com amb IoT, s'utilitzen bàsicament per programar atacs DDoS i enviaments massius d'arxius maliciosos i de spam.



Il·lustració 28: Botnets més rellevants a EMEA
Font: Check Point Research Cyber Security Report 2021

Botnets amb Malware: Impacte molt rellevant amb l'objectiu d'iniciar campanyes d'infecció amb diferents tipus de malware *troians* com Emotet (del que ja hem parlat), *Trickboot, Raccoon* i *stealer agents* com *AZOrul, Lokibot i Tesla*, especialistes en el robatori de credencials. Al 2020 s'incorpora una família *QNodeService*.



Il·lustració 29: Top malware globals

Font: Check Point Research Cyber Security Report 2021

Rank	Malware	Note
1	Lokibot	Credential Stealer
2	AZORult	Credential Stealer
3	NanoCore	Remote Access Tool (RAT)
4	Pony	Dropper/Credential Stealer
5	TrickBot	e-banking trojan
6	Gozi	e-banking trojan
7	Emotet	Dropper/Backdoor
8	RemocsRAT	Remote Access Tool (RAT)
9	Predator Stealer	Credential Stealer
10	Adwind/JBifrost	Remote Access Tool (RAT)
11	NetWire	Remote Access Tool (RAT)
12	KPOTStealer	Credential Stealer
13	ArkeiStealer	Credential Stealer
14	NjRAT	Remote Access Tool (RAT)
15	AgentTesla	KeyLogger/Credential Stealer
16	QuasarRAT	Remote Access Tool (RAT)
17	Dridex	e-banking trojan
18	HawkEye	Credential Stealer
19	IcedID	e-banking trojan
20	CoinMiner	Various crypto currency miners
–	Others	Other malware families

Il·lustració 30: Amenaces Botnet Informe 2019
Font: The Spamhaus Project. Botnet Threat Report 2019

2.6.3 Codi Maliciós Avançat

En general aquest vector d'atac es refereix a la màxima sofisticació i elaboració de noves tècniques i amenaces (com si fos quasi un procés d'I+D[16]) per part dels ciberdelinqüents. Aquests aprofiten cada any que apareixen nous esdeveniments que succeeixen en un país, regió o continent per enfocar campanyes dirigides cap a ells. Al 2020 per exemple a la pandèmia i les vacunes.

Nosaltres reportarem alguns exemples d'aparicions en:

<u>2019</u>

- *Living off the Land* (LotL): Petyal al 2017 utilitza aquesta eina que aprofita les portes d'entrada existents als sistemes informàtics sense crear codi nou explotant la presència als sistemes d'eines legítimes com PowerShell, WMI o PsExec.
- *Fileless malware*: carrega i executa malware a la memòria de l'equip sense que existeixi cap fitxer resident al disc dur de l'equip. Indetectables per antivirus.
- *Turla*: utilitza malware basat en .NET
- *TajMahal*: framework sofisticat orientat al ciberespionatge.

[16] Investigació i Desenvolupament, en anglès Research & Development (R+D).

2020

- Aprofitar *exploits* (vulnerabilitats) crítics en dispositius exposats on existeix una demora de temps entre la publicació de l'*exploit* i el patch. Els atacants si el sistema ho permet despleguen *webshells* per interactuar amb el propi equip i amb part de l'organització. Això els va passar a empreses com *Citrix NetScaler*, Microsoft SharePoint o Microsoft Exchange.
- DLL *side-loading*: un atacant pot executar el seu codi a través de la càrrega d'un fitxer de tipus DLL en un executable signat i legítim. Ex. Mustang Panda.
- Frameworks post-explotació: *CobaltStrike*, *Powershell Empire* que ofereixen versatilitat, eficiència, estalvi de costos pels ciberdelinqüents.
- DNS over HTTPs (DoH): *PowerPepper*, protegeix la navegació dels usuaris i que no es sàpiga a quins dominis està visitant, encapsulant tràfic *DNS* en peticions HTTPS.
- Ús de malware LightSpy: utilitza *exploits* per al sistema operatiu iOS.
- Implementació de noves variants del *PlugX*.
- Atacs contra les cadenes de subministrament: Malware *SunBurst*.

2.6.4 Atacs a sistemes d'accés remot

La explotació de vulnerabilitats en serveis de connectivitat remota s'està convertint en el vector d'atac més exitós d'accés inicial a una xarxa, superant fins i tot al phishing i als tradicionals robatoris de credencials. Degut al canvi forçós arrel de la pandèmia han proliferat a moltes empreses serveis de connexions remotes.

El problema rau en què aquests serveis no estan auditats ni prou assegurats augmentant així la superfície nova d'atac dels ciberdelinqüents. Existeixen 3 grans grups de vulnerabilitats: VPNs, tallafocs i entorns de treball remots.
No obstant, també estan en el punt de mira aplicacions de videoconferència com el conegut cas de *Zoom*. La gran majoria d'aquest *exploits* es solucionen amb l'aplicació d'actualitzacions pel fabricant.

2.6.5 Atacs web

Durant el 2019 es van dividir en dos blocs principals: els atacs DDoS, i els atacs a servidors web a través de l'intent de càrrega de fitxers que permetin controlar el site o amb atacs d'injecció SQL, amb l'objectiu de manipular o extreure les bases de dades del servei.

Aquests atacs i els *defacements* s'han convertit en les principals amenaces utilitzades per hacktivistes i altres atacants amb l'objectiu de perjudicar la reputació de la víctima o aprofitar-se de la caiguda dels seus serveis. Són focus

molt estesos d'atac els gestors de contingut (CMS)[17]. Els més coneguts són Drupal, Wordpress i Joomla.

Al 2020, va ser conegut un atac utilitzant com a vector un DDoS de gran capacitat detectat per Amazon de fins 2,3 terabits per segon. Al sector bancari també va patir atacs RDDoS (Ransom Distributed Denial-Of-Service Attacks) en el que es va intentar extorsionar a corporacions per pagar rescats. I a principis de 2021 també es reporten tècniques de *scraping* automatitzades a gran escala a xarxes socials com TikTok, Youtube per filtrar massivament dades personals.

2.6.6 Atacs a Sistemes Ciberfísics

La gran majoria de sistemes atacats són empreses industrials que operen els següents sectors de l'economia: fabricació, petroli, gas, metall, energia, construcció, mineria, logística e enginyeria. S'utilitzen estratègies d'atac a la cadena de subministres, explotació de vulnerabilitats i ransomware (Babuk Locker, Netwalker, etc.)

Durant el 2020 es van detectar 3 línies principals d'atac: l'abús de vulnerabilitats associades a accessos remots, la selecció com a objectiu d'infraestructures sanitàries i centres d'investigació relacionats amb la COVID19 i els atacs ransomware contra infraestructures industrials causant impacte en les operacions de producció.

2.6.7 Atacs contra la cadena de subministrament

També anomenats atacs de cadena de valor o de tercers són una amenaça creixent. Hi ha de diversos tipus, com el de la creació d'eines de creació de programari compromeses, codi robat (signatura de certificats o aplicacions malicioses signades amb la identitat de l'empresa de desenvolupament), malware preinstal·lat en dispositius, codi especialitzat corrupte que s'envia a components de maquinari o firmware, etc.

A diferència d'altres tipus d'atacs, els dirigits a les cadenes de subministres permeten evadir certs controls de prevenció i detecció al comprometre directament als proveïdors externs, socis o clients. No hi ha encara massa regulacions al respecte i això dificulta molt que les empreses controlin i validin el programari o maquinari que utilitzen.

Els atacants més avançats, aprofiten aquestes febleses per perpetrar les seves intrusions en les xarxes objectiu aprofitant que els proveïdors o entitats associades disposen d'alguna interconnexió o accés a la xarxa objectiu. S'ha d'alertar dels riscos de seguretat dels proveïdors al núvol, al traslladar a aquest des dels centres de dades fins les aplicacions, exposant a les empreses i fabricants a riscos de tercers.

[17] CMS: segons Wikipedia un sistema de gestió de continguts es un programa informàtic que permet crear un entorn de treball per la creació i administració de continguts, principalment pàgines web, per part dels administradors, editors, participants i resta d'usuaris.

El cas protagonitzat pel fabricant de programari alemany *SolarWinds* al 2020 va ser l'exemple més clar d'aquest amenaça. Mitjançant una modificació maliciosa d'un paquet d'actualització d'*Orion* (una de les eines de gestió TI del fabricant) els atacants van tindre accés potencial a milers d'organitzacions (govern americà, *Cisco, FireEye, Microsoft o Malwarebytes*).

Encara avui es desconeix l'impacte real ni l'abast real de a quantes organitzacions va afectar, ni es pot descartar que pugui afectar durant alguns anys en el futur. Tot i què, la importància de la seguretat de la cadena de subministrament està molt reconeguda, poques organitzacions tenen implantat un procés madur i eficaç de seguretat.

Les asimetries existents entre clients i proveïdors en els processos de contractació, la escassa concepció de seguretat de la informació com a procés transversal o la complexitat i volum de recursos necessaris per assegurar aquests entorns dificulten i expliquen el perquè no s'han assolit aquest processos milloradors.

2.6.8 Atacs d'Enginyeria Social

Un dels vector d'atac més utilitzats. L'objectiu dels ciberdelinqüents es enganyar a la víctima perquè, sense que se n'adoni, realitzi alguna acció perjudicial en benefici del atacant: la descàrrega de malware en el seu dispositiu, el robatori de les seves credencials o la revelació d'informació personal són alguna d'aquestes accions.

Els incidents relacionats amb aquest vector estan en expansió degut a què existeix un important mercat negre que valora comercialment aquestes dades obtingudes, ja siguin personals, financeres (targetes pagament, compte de serveis online), credencials d'accés a serveis online, adreces de correu electrònic, perfils d'usuari, identitats, tot informacions valuoses pels "Enginyers socials".

El correu electrònic és el mitjà més utilitzat a través del qual es realitzen campanyes massives de phishing, mitjançant la suplantació de serveis o persones, incitant al receptor del correu a descarregar fitxers adjunts maliciosos, clicar un enllaç, facilitar una determinada informació o realitzar fins i tot, una transferència bancària.

Hi ha altres estratègies com l'*spear-phising*, que consisteixen en un atac molt sofisticat dirigit contra persones o organitzacions específiques i que són molt complicats de detectar. Es segur que la suplantació de persones o serveis s'ha produït aprofitant que les víctimes han tingut comunicacions anteriors amb els atacants que els han donat una certa credibilitat prèvia, aconseguint que el fals correu tingui èxit.

La majoria d'aquests atacs requereixen estudis previs de les víctimes. Però no tots es fonamenten en l'ús del correu electrònic. Altres com el *smishing* es basen en aplicacions de missatgeria instantània o xarxes socials, o fins i tot, el vishing

es realitza mitjançant trucades telefòniques. El *baiting* és una altre tècnica en la que mitjançant l´ús de dispositius USB la víctima introdueix malware de forma inconscient i provocant un dany sobre el sistema.

Cal destacar que aquestes tècniques també estan agafant molt protagonisme en la propagació de campanyes de desinformació, o de *Fakes news* mitjançant la difusió en xarxes socials o aplicacions de missatgeria, explotant determinats biaixos cognitius de les persones, com són els de confirmació o pertinença a grup per aconseguir els seus objectius.

Per finalitzar aquest apartat, en aquest quadre farem una exposició dels mètodes d'atac a Espanya detectats i reportats pel CCN-CERT al 2020:

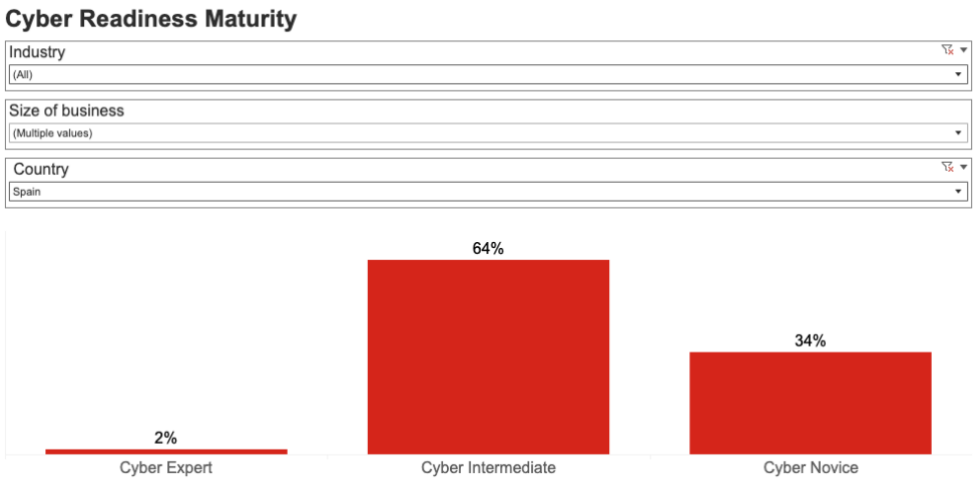
TIPOLOGÍA DE INCIDENTES DETECTADOS POR CCN-CERT	Q1 2020	Q2 2020	Q3 2020	Q4 2020
Explotación de vulnerabilidad SW	8100	7619	7780	7544
Inyección SQL	3101	2964	2649	2448
Troyano	2756	2434	1298	1561
Otros	1673	1581	1085	938
Intrusiones	1449	901	862	922
Malware	1392	1799	1294	1122
RFI	749	672	525	556
Identificación de vulnerabilidades	82	71	117	322
Acceso no autorizado a red	121	238	265	290
Spyware	933	630	493	373
DoS/DDoS	1656	234	126	160
Ataque de fuerza bruta	383	278	202	150
RAT	5645	391	147	137
Recopilación de información	1	0	70	125
Acceso a servicios no autorizados	3	14	57	48
Sistema no actualizado	1	0	0	13
Phishing	593	9	8	68
Ransomware	86	46	11	32
Política de seguridad	12	2	3	4
Exfiltración de información	5	7	7	5
Gusano	11	1	2	3
Fraude	1	0	0	0
Rootkit	1	0	0	0

Il·lustració 31: principals ciberamenaces i tendències al 2021
Font: CCN-CERT IA-23/21 Ciber Amenazas y Tendencias 2021

2.7 Avaluació de la cibermaduresa de les Pimes:

És un factor que tindrem molt en compte de cara al disseny de l'aplicació d'aquest projecte. Aquest concepte i Ciberresiliència són fonamentals en aquest estudi, es per això, que es dedica un apartat a situar al lector sobre el concepte de cibermaduresa i sota quins aspectes és classifica a les entitats espanyoles.

Com es mostra al gràfic d'aquesta pàgina, el grau de maduresa en general és decebedor. En termes de preparació contra ciberatacs, un 34% de les entitats es consideren cibernovates, i la resta tenen una preparació mitjana. Només un 2% de les pimes es consideren ciberexpertes, això es un factor preocupant, encara què aquest fet tampoc implica no ser víctima d'un ciberatac però sí que et prepara millor a superar-ho (a tindre millor ciberresiliència) com ara veurem:



Il·lustració 32: Tipus de Cibermaduresa

font: https://www.hiscox.es/informe-de-ciberpreparacion-de-hiscox-2022

Com a punt de partida escollim un model d'avaluació de la maduresa proposat per la empresa asseguradora Hiscox. El model compta amb un marc de mesura basat en sistema COBIT2019®[18] i una arquitectura de seguretat basada en SABSA®[19]. El sistema les classifica en funció de 6 àrees operacionals (dominis) que constitueixen justament els elements necessaris per instal·lar, dirigir, gestionar i governar un sistema de seguretat eficaç.

Cada domini es mesura contra cada un de tres àmbits (persones, processos i tecnologia) i es puntua en una escala de 5 punts. Puntuacions per sobre de 4 qualifica a les empreses com **ciberexpertes** i per sota de 2,5 **cibernovates**, a la resta les qualifica com **cibermitjanes**. Ens interessa d'aquest sistema la senzillesa inicial. A continuació exposem un quadre de com funciona aquest model:

[18] COBIT 2019®: https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2021/volume-6/building-a-maturity-model-for-cobit-2019-based-on-cmmi-joa-spa-1221.pdf?la=es-es

[19] SABSA®: https://sabsa.org/sabsa-executive-summary/

Cibernovatas	Personas	Procesos	Tecnología	Promedio total
Gestión de la resiliencia empresarial	1.83	1.86	1.75	1.81
Gestión de contraseñas y criptografía	1.58	1.54	1.52	1.55
Gestión de identidades y accesos	1.80	1.71	1.63	1.69
Gestión de eventos e información de seguridad	1.57	1.90	1.61	1.65
Gestión de amenazas y vulnerabilidades	1.65	1.85	2.24	1.91
Gestión de la confianza	1.76	1.71	1.72	1.73
Promedio total	1.70	1.76	1.74	1.72

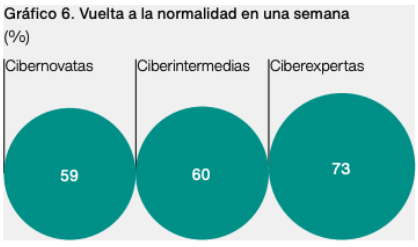
Ciberexpertas	Personas	Procesos	Tecnología	Promedio total
Gestión de la resiliencia empresarial	4.44	4.43	4.43	4.43
Gestión de contraseñas y criptografía	4.29	4.25	4.34	4.29
Gestión de identidades y accesos	4.37	4.29	4.38	4.34
Gestión de eventos e información de seguridad	4.32	4.34	4.38	4.35
Gestión de amenazas y vulnerabilidades	4.34	4.36	4.29	4.33
Gestión de la confianza	4.37	4.37	4.46	4.41
Promedio total	4.35	4.34	4.38	4.36

Il·lustració 33: criteris classificació cibernovates i ciberexpertes
font: https://www.hiscox.es/informe-de-ciberpreparacion-de-hiscox-2021

Aquesta és una primera forma de classificació senzilla, però ja apunta unes diferències marcades entre les pròpies pimes. Les empreses que es consideren ciberexpertes, comparteixen una sèrie de bones pràctiques que les distingeix, com són:

- Gestionar d'una forma activa el risc: si cal recorren a experiència externa o fins i tot algunes contracten pòlisses de ciberseguretat per augmentar la ciberresiliència davant atacs.
- Nomenar a un responsable ciberseguretat: a vegades la mida d'una pime no justifica la existència d'una persona però si sempre hauria d'existir algú amb aquest missió a l'empresa per molt petita que fos la organització.
- Fer front a les principals amenaces i vulnerabilitats: per exemple quan es va imposar el model de teletreball van comprendre que s'incrementarien els riscos d'atacs i van cercar noves solucions com establir mesures noves protecció (tallafocs, antivirus), etc.
- Fan les còpies de seguretat preferiblement fora de les instal·lacions.
- Ús mesures criptogràfiques en proteccions de contrasenyes. Pràcticament absència d´ús en les empreses cibernovates.

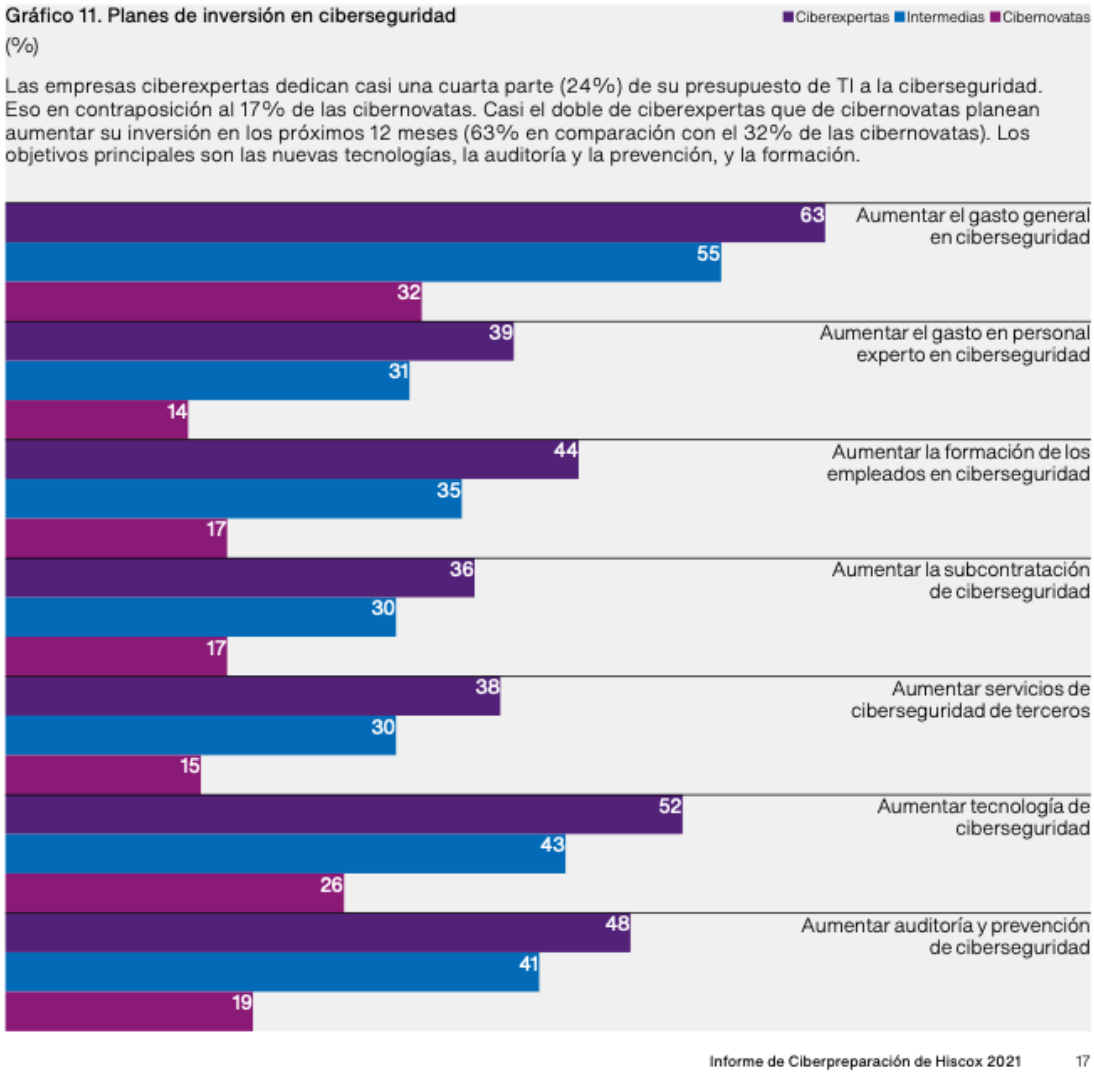
En base a atacs (alguns tan destructius com ransomware) un altre índex de la seva maduresa és la capacitat de recuperar la seva normalitat:



Il·lustració 34: quin % recupera normalitat amb ransomware
font: https://www.hiscox.es/informe-de-ciberpreparacion-de-hiscox-2021

S'ha demostrat que existeix una correlació elevada entre la exposició al risc que es percep i la probabilitat real de patir un ciberatac. De fet les empreses que reben la catalogació de ciberexpertes és notòria la seva capacitat de detectar i valorar l'alt risc d'amenaça que suposen aquestes atacs. Malauradament, algunes vegades això és conseqüència d'haver patit amb anterioritat un ciberatac.

Per exemple un paràmetre en el que pot condicionar aquest fet de la percepció dels riscos és quin pressupost es destinarà a ciberseguretat. Es torna a fer palès les grans diferències depenent la seva maduresa:



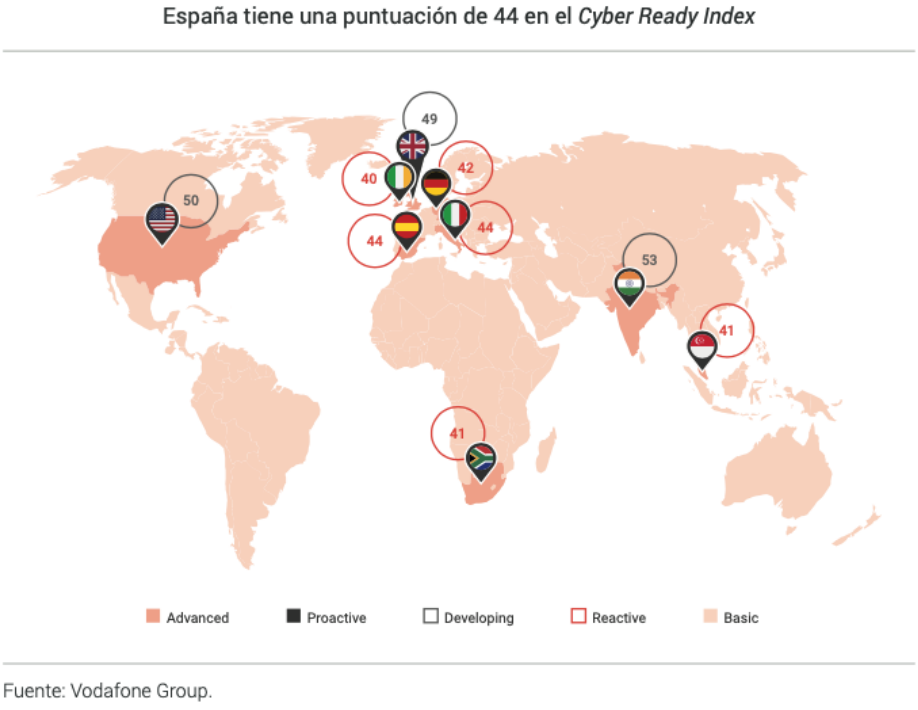
Il·lustració 35: Plans d'inversió ciberseguretat per tipus empresa

font: https://www.hiscox.es/informe-de-ciberpreparacion-de-hiscox-2021

Aquesta classificació en funció de la maduresa de la entitat ens serà molt interessant més endavant per dissenyar la nostra aplicació. La utilitzarem en la classificació i filtratge que haurem de fer per conèixer l'estat de l'organització que analitzem.

3 Estat de la l'Art

Ja s'havia indicat anteriorment que la posició en general de les empreses espanyoles respecte a la Ciberseguretat era una posició "reactiva", és a dir gestionen i procuren certes accions per assegurar els seus negocis, però tenen com es veu un marge de millora considerable comparat amb altres països. No obstant és un dels millors estats al món:



Il·lustració 36: puntuacions Cyber Ready Index països món
Font: Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf

Per valorar la situació actual de les Pimes espanyoles anem a valorar varis ítems per saber en quin estat es troben actualment. Un dels primers és saber quin percentatge del pressupost destinat a Tecnologies Informació (TI) es destina a Ciberseguretat? I al quadre següent observarem la comparativa amb altres països de la UE/Occident?

Il·lustració 37: % de la despesa en TI destinat a Ciberseguretat
Font: Informe Hiscox

Com es veu la preocupació de les empreses va en augment i cada any es destina un major percentatge. A Espanya l'any passat va créixer un 7% respecte al 2020, i previsiblement al 2022 encara s'incrementarà més. Les empreses han reorientat clarament la seva despesa en Ciberseguretat, tot i què la partida global en TI continua sent semblant.

L'efecte pandèmia, teletreball i núvol han influït molt. Però quins són els principals motius que han canviat la percepció de les empreses? Perquè es comenta que la pandèmia ha catalitzat l'increment dels pressupostos?

Gráfico 16. Cambios debido a Covid-19
(%)

Mayor número de personal que trabaja en remoto	41
Contratación pausada	33
Mayor uso de tecnologías de colaboración	32
Costes operativos reducidos	31
Mayor uso de tecnologías basadas en la nube	29
Pagos en línea ampliados	27
Planes de transformación digital acelerados	27
Canales de comercio electrónico existentes ampliados	20
Volumen reducido de cambios de TI	18
Nuevos canales de comercio electrónico añadidos	18
Número consolidado o reducido de proveedores	15

Il·lustració 38: canvis deguts a Covid 19
Font: Hiscox estudi 2021

Si hem d'analitzar les dades quantitatives i per mida d'organització a nivell de Pimes Europees també observarem una clara evolució al increment de despesa. Sobretot en els extrems de mida, les empreses més petites i les més grans.

Gráfico 12. El gasto medio por empresa en ciberseguridad o en dos años
(m€)

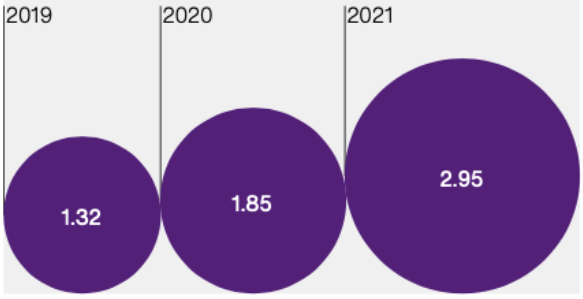
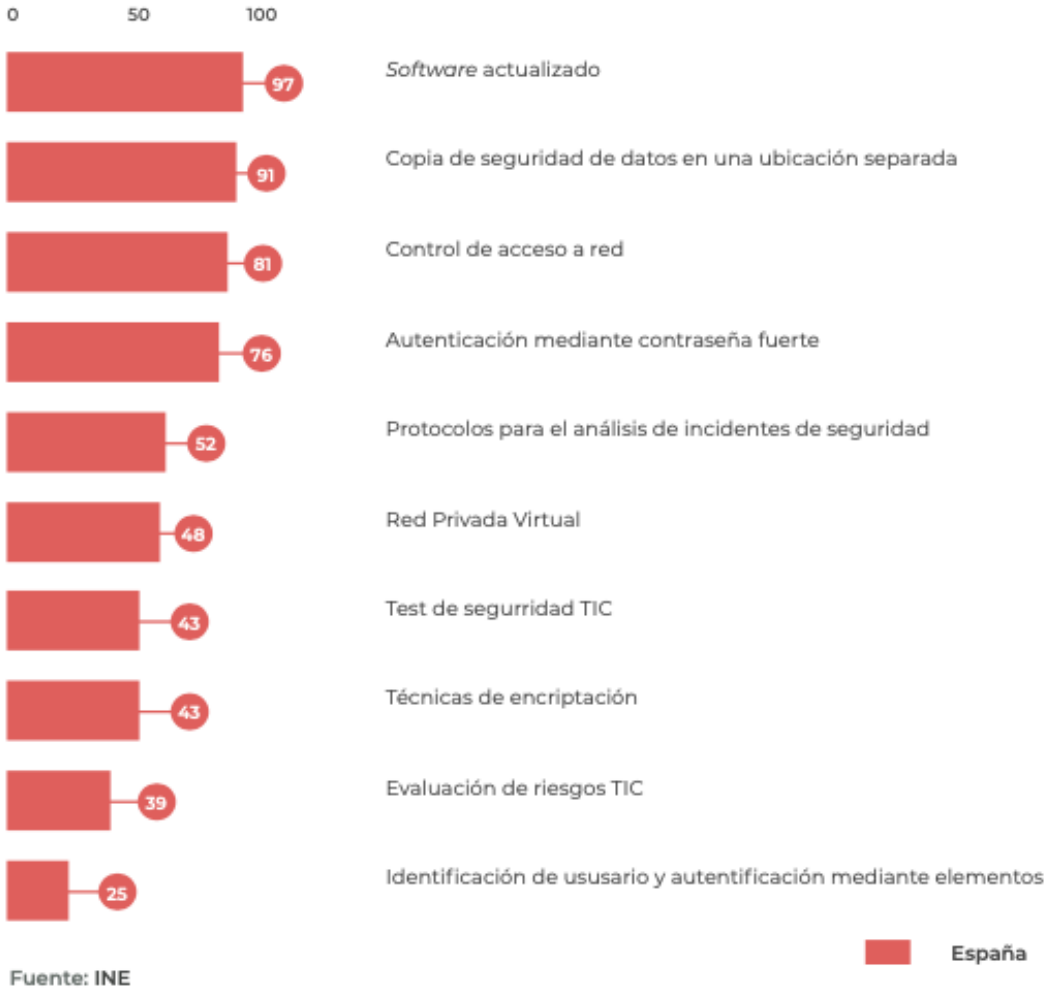


Gráfico 13. Gasto en ciberseguridad Por número de empleados
(€)

	2021	2020
1–9	112.455	12.090
10–49	359.159	72.202
50–249	289.399	255.884
250–999	1,751.905	784.380
1.000+	11,876.082	7,299.115

Il·lustració 39: despesa mitja 2 anys en ciberseguretat
font: https://www.hiscox.es/informe-de-ciberpreparacion-de-hiscox-2021

Respecte al enfoc qualitatiu de quines mesures de ciberseguretat ja és habitual que prenguin les Pimes espanyoles, al 2020 l'INE[20] va publicar aquesta estadística on es mostra en % quantes empreses utilitzen algun sistema intern de seguretat com els exposats a la llista:

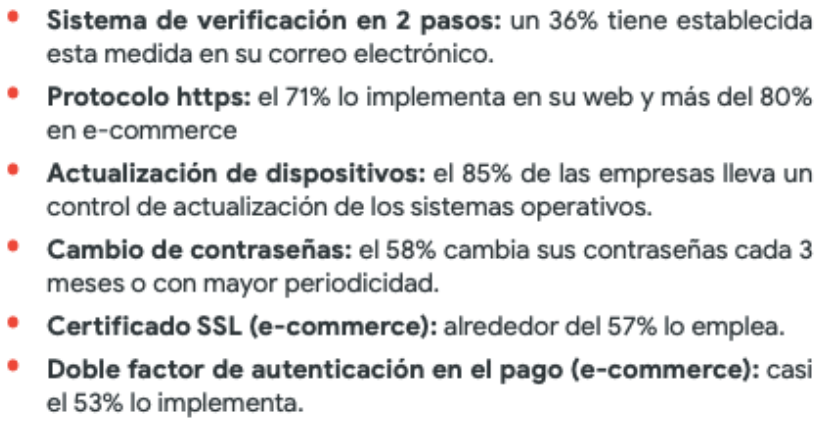


Il·lustració 40: indicadors confiança digital

Font: Carpeta. Indicadores de confiança digital observaciber octubre 2021

Altres classificacions també fetes per l'estudi de Google, també revela un estudi molt concret sobre les principals mesures i accions per part de les Pimes en matèria de Ciberseguretat. Un 40% d'aquestes ja comencen a donar-li una importància rellevant, així les principals conclusions que aporten les empreses enquestades són:

[20] INE: Institut Nacional Estadística



Il·lustració 41: principals mesures i accions portades a terme

Font: https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de- la-ciberseguridad-en-Espana.pdf

3.1 Principals Organismes Espanyols en Ciberseguretat

Com es comentava al principi de l'apartat, Espanya com a país està desenvolupant una gran tasca en la conscienciació i treball sobre Ciberseguretat. Actualment el sistema públic estatal de ciberseguretat es fonamenta sobre quatre organismes, dels que ja hem parlat en algun cas, i que mantenen una coordinació entre ells comportant-se així com un primer escut contra els problemes més greus de seguretat:

- CCN-CERT, es tracta del Centre Criptològic Nacional del Centre Nacional d'Intel·ligència dedicat al Sector Públic.
- CNPIC, és el Centre Nacional de Protecció d'Infraestructures i Ciberseguretat, que s'ocupa d'infraestructures crítiques com són els proveïdors de llum, aigua, gas, etc.
- ESPDEF-CERT, al comandament conjunt de ciberdefensa. Treballa amb les xarxes i els sistemes d'informació i telecomunicacions de les forces armades.
- INCIBE, es tracta de l'Institut Nacional de Ciberseguretat d'Espanya amb un enfoc en els ciutadans, les empreses i els operadors de serveis essencials. Està en contínua expansió.

3.2 Marc legal

Però el desenvolupament d'unes institucions centrades en l'actuació no seria complerta si no van acompanyades d'un marc legal de progrés, i aquí l'estat és un dels països més avançats al món al respecte.

No hem d'oblidar que la creació d'una bona cobertura legal en matèria de ciberseguretat és molt complexa. El principal motiu es què els atacs acostumen a ser globals, no estan vinculats a un país concret. A banda d'això, l 'anonimat és inherent a Internet, i la majoria de vegades és complex identificar l'origen d'un ciberatac.

Els principals avenços legals que representen el marc espanyol són:

- Real Decret-llei 12/201826, que transposa a l'ordenament estatal la directiva NIS27 i busca reforçar la seguretat de les xarxes i sistemes d'informació utilitzats per la provisió dels serveis digitals, així com establir un sistema de notificació d'incidents. El desenvolupament reglamentari d'aquesta norma està encara en fase d'elaboració.

- LOPD (Llei de Protecció de Dades): que avala una sèrie de "drets digitals" i garanteix un mínim de protecció front a les ciberamenaces.

- Estratègia Nacional de Ciberseguretat 2019: amb la que est pretén garantir la seguretat, les infraestructures i la tecnologia que integren el ciberespai, ja què la seva vulneració es una de les principals amenaces per la Seguretat Nacional.

- Nou reglament europeu de ciberseguretat: aprovat pel Consell Europeu al març de 2019, consolida una agència permanent de ciberseguretat això com un certificat comú de ciberseguretat per tota la UE. Els experts van assenyalar aquesta fita com una oportunitat perquè Espanya lideri les bones pràctiques en el continent ja que l'ecosistema de certificació estatal es troba en un dels millors valorats d'Europa.

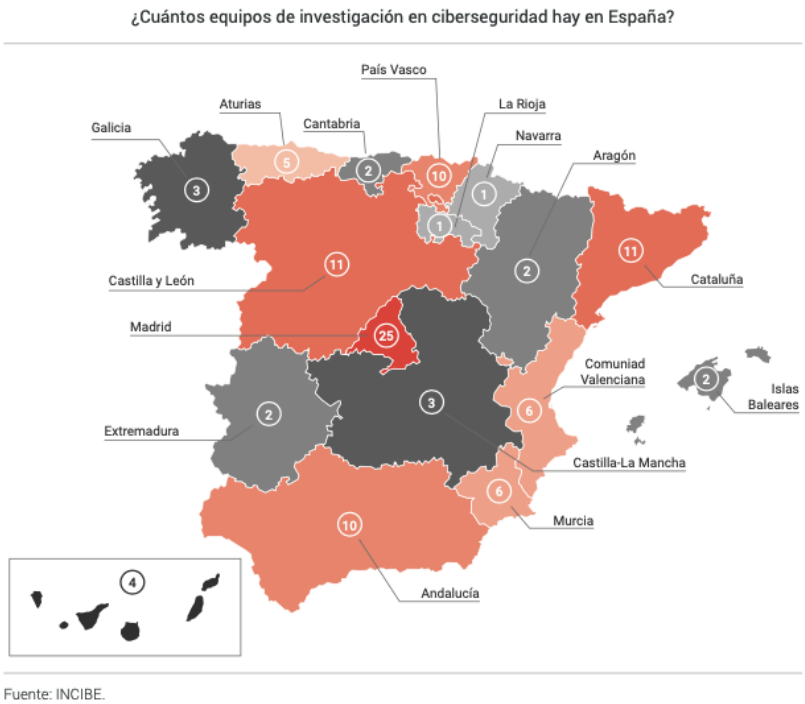
- Comissió Mixta de Seguretat Nacional Congrés-Senat: treballa en un informe en el que proposa modificar el Codi Penal per imposar penes més dures als delictes comesos per ciberdelinqüents i aconsella, a més, per una regulació de caràcter internacional.

3.3 I+D en Ciberseguretat a Espanya

Com hem avançat, el país es considera la quarta potència mundial en la matèria i afortunadament aquest punt és un dels motius pels qual la comunitat internacional ens avala. Segons dades de l'INCIBE al 2020 existeixen 104 equips d'investigació (la majoria a Universitats). Nou són centres tecnològics amb més de 1302 professionals dedicats i existeix Un centre d'investigació especialitzat.

A les següents gràfiques observarem quins són les principals temàtiques d'investigació i com estan distribuïts aquests centres per la geografia espanyola:

Il·lustració 42: Què s'investiga?



Il·lustració 43: nombre i ubicacions centres investigació estatals

Font: https://www. incibe.es/sites/default/files/paginas/red-excelencia/estudios-caracterizacion/201701_catalogo_infografia.pdf

4 Disseny de la Proposta.

4.1 Principals arguments de disseny.

Arriba el moment clau d'aquest projecte: el disseny i preparació de la "*eina digital o proposta de valoració per les pimes*". Encara no sabem quin és el nom més idoni per un "disseny" d'aquest estil; n'hi ha que els anomenen *Auto tests de Ciberseguretat*, altres *Auditories de Seguretat*, alguns també *Escàner de Vulnerabilitats*. En el propers apartats donaré resposta a aquesta qüestió.

El que sí que ja es pot entreveure són unes línies de treball clares en base a la informació introductòria i de situació del context inicial d'aquest tipus d'organitzacions a Espanya que hem obtingut en aquesta primera part del projecte. Aquestes pautes de treball les anomenarem **Indicadors Digitals o Dominis de Seguretat.**

L´ús d'ells serà la forma en la què organitzaré l'eina de treball i li donaré contingut i abast a tots els objectius d'aquest projecte, a més a més, ara sí que és el moment d'avançar sobre quins 3 conceptes clau (les meves ***keywords***) pivotarà el projecte: La **Cibermaduresa,** la **Ciberresiliència** de les Pimes i la **Ciberseguretat com a Servei.**

Aquest últim, també batejat com a **CSaaS (Cibersecurity as a Service)** he cregut que era moment d'introduir-lo perquè durant l'estudi previ s'ha observat primer que no és un concepte gaire utilitzat encara a les xarxes, però penso què podria ser clau en el futur per poder democratitzar l'adopció, ús i protecció de les pimes en matèria de ciberseguretat.

A través de l'estudi hem observat que és cert que la majoria d'empreses, sobretot després de l'impacte de la pandèmia, han "despertat" les necessitats de conscienciació, formació, adopció e inversió en matèria de Ciberseguretat. Malauradament, no és suficient. La correlació entre la mida de la organització i el seu esforç per revertir la seva vulnerabilitat davant ciberatacs és massa evident.

Només les grans corporacions, i en un nombre molt reduït, algunes pimes poden assolir aquesta tasca d'actualització i augment de la maduresa i resistència contra les ciberamenaces actuals. El realisme a Espanya és que existeixen una sèrie de barreres (veure gràfica) que de moment ho impediran a la gran majoria d' autònoms, Micropimes i altres organitzacions de petita mida i pressupost.

Il·lustració 44: barreres a la implementació de ciberseguretat

Com hem vist al següent quadre hi han molts factors, encara que no cal ser gaire llest per intuir que el principal és la greu crisi econòmica que s'imposa i fa que el factor econòmic i de cost en temps sigui primordial. D'altres ja hem parlat, veiem % elevats de motius que "*ho veuen difícil*", ò no "*ho creuen necessari*" ò "no saben", que no deixen de ser un simple poc convenciment dels directius, o d'ignorar que no són invisibles per mida a ser potencials.

Amb una elevada probabilitat, aquests arguments també serien recolzats si comptessin amb opinions i casos d´ús d'empreses especialitzades (auditors de seguretat, enginyers, investigadors, tècnics *pentesting*, etc.) en Ciberseguretat. S'han de cercar opcions per superar aquestes barreres i aconseguir que la mida i el factor econòmic ja no sigui primordial.

No m'avançaré en excés en aquest punt, doncs molts d'aquests conceptes que introduiré a continuació segur que formaran part de les conclusions d'aquest projecte; allà les desenvoluparé. Però com recomanacions que observem per afrontar la greu problemàtica existent són abordar i enfocar el futur de la ciberseguretat en les pimes de la següent forma:

- Incrementant el nombre d'organitzacions amb un grau mig de **cibermaduresa** elevat per aconseguir així millorar l'**ecosistema** de ciberseguretat de les organitzacions, societat i en definitiva del país. Òbviament, en les empreses de nova creació el repte serà reduir el temps d'stage de consideració d'empresa cibernovata a ciberexperta.

- Aconseguir el repte anterior, es fonamentarà en **incrementar la ciberresiliència** i la capacitat de resposta en general de les organitzacions contra ciberatacs. Augmentant la formació d'empleats,

clients, proveïdors i sobretot dels directius, potenciant la inversió en seguretat (amb desgravacions fiscals) i augmentar la visibilitat i comunicació a la societat de la realitat dels ciberincidents.

- Acompanyant aquestes dos mesures tan globals, un increment de **les bones pràctiques en l'adopció de la ciberseguretat** seria fonamental en aconseguir-ho. Mesures que fomentin l'augment de la **corresponsabilitat i obligacions de la societat** en la matèria i aconseguir la **conscienciació definitiva** serien elements diferencials.

  Com a exemple de bona pràctica: Les nostres empreses target d'aquest projecte són totes aquelles "*que poden demostrar que actualment no s'ho poden permetre pel motiu que sigui*". Una decisió a la que podran recórrer totes aquelles organitzacions que desitgin millorar els factors de ciberseguretat i actuar amb **corresponsabilitat i obligació amb la societat** en la matèria serà recórrer a la **Ciberseguretat com a Servei (CSaaS)**.

  Com a símil existent en l'àmbit jurídic, el dret a ser representat mitjançant un advocat d'ofici, totes les empreses haurien de tindre també el dret a ser ciberprotegides. La funció del **CSaaS,** d'alguna forma hauria d'estar promoguda, recolzada i finançada per totes les institucions per fer-la arribar de forma majoritària a la societat i **democratitzar** per fi **la** seva **ciberprotecció** pel bé general de l'ecosistema i de la societat.

Amb molta modèstia aquesta eina pretendrà de forma oberta i gratuïta mesurar l'estat de cibermaduresa i ciberresiliencia de la organització, puntuant el seu esforç actual i deixant una recomanació clara per aquelles petites organitzacions que ho desitgin i ho necessitin. Sempre serà bo comptar amb ajuda per impulsar a prendre decisions que encaminin a les Pimes a afrontar la seva pròpia Ciberseguretat o deixar-se assessorar quan .

4.2 Principals Aportacions i Objectius aspiracionals en la creació de la eina.

Sobre la cibermaduresa, ja vam introduir a l'apartat 2.7 un bon model per classificar a les empreses. Al mercat, fent una primera batuda també hem trobat diverses eines en forma de formulari per esbrinar la capacitat de resistència de les organitzacions per mitigar els principals ciberriscos, o sigui, trobar la seva ciberresiliència. Farem servir de guia un model d'*Incibe* (veure gràfica següent):

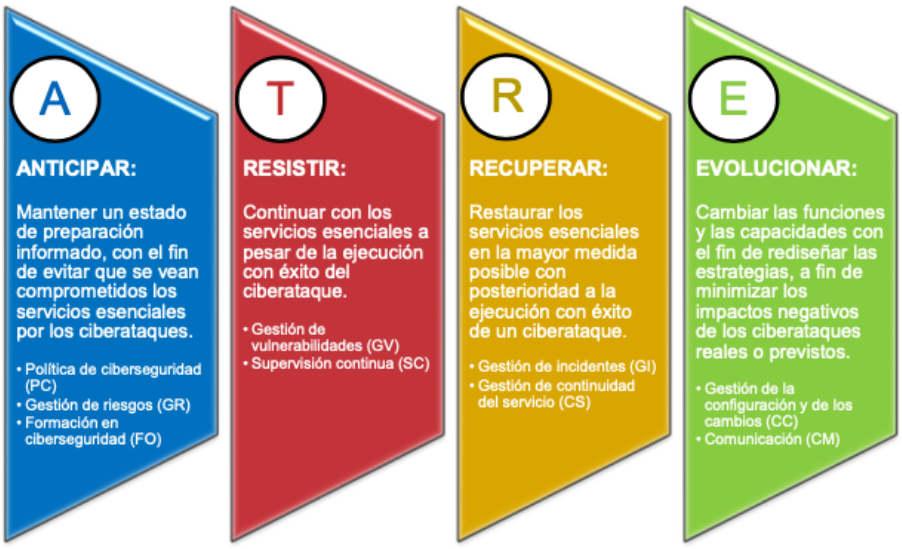


Figura 1: Marco de trabajo de ciberresiliencia

Il·lustració 45: marc de treball de ciberresiliència
Font: https://www.incibe-cert.es/guias-y-estudios/guias/imc-indicadores-mejora-ciberresiliencia

La eina, es basarà en conformar un formulari d'auto resposta avaluat i puntuat que incorpora una barreja d'aquests dos tipus d'objectius, però sobretot incorpori la gran aportació tècnica d'aquest projecte: Crear una **nova etapa tècnica en la valoració de la ciberseguretat d'una empresa** que **serveixi d'eina auto avaluativa ò adreci** (quan convingui) ràpidament **cap a una gestió** de la mateixa **mitjançant CSaaS**.

Ha de quedar molt clar d'ara endavant que **l'aportació e innovació tècnica real** d'aquest projecte es fonamentarà en dos palanques:

- Contribució a la **millora i evolució** d'arguments classificadors de millora (ja en producció i al mercat) de la ciberresiliència de les Pimes.

- Aportació de **nous indicadors digitals** que complementin i permetin avaluar la situació real de les pimes incorporant **noves tendències de mercat** en matèria de ciberseguretat que acaben d'estar publicades[21].

Un **doble objectiu** de màxims que s'aconseguiria amb aquesta eina, si superés la fase analítica i s'apliqués en fase producció seria:

- Ajudar en la formació, sensibilització i conscienciació de petites empreses que disposin de recursos i mitjans suficients per poden revisar i rectificar algunes (o totes) les conclusions de millora extretes de l'informe en forma de veritables decisions d'actuació i millora de la seva ciberseguretat, fent ús o no de CSaaS com a complement.

[21] Publicades per institucions i consultores prestigioses com Gartner i MIT (Massachussetts Institut of Technology).

- En aquelles organitzacions sense recursos de temps i diners (la gran majoria) utilitzar els resultats de l'informe com a vehicle de comunicació i presa de contacte (Pimes - empresa experta en CSaaS) actuar amb immediatesa i començar a construir i mitigar una estratègia de prevenció i millora dels seus factors de cibermaduresa i ciberresiliència.

4.3 Principals Indicadors Digitals Utilitzats.

Per donar resposta i assolir els principals objectius que exposàvem a la introducció (punt 1) d'aquest projecte serà indispensable realitzar una gran tasca en l'elecció dels principals indicadors digitals i/o **dominis de seguretat** per poder crear una aplicació usable, didàctica, realista i no excessivament complicada pel client final: la nostra empresa PIME.

La relació d'inputs o dades digitals que ens ajudaran a classificar, ordenar i entendre la organització que estem analitzant. Quan ens referim a dominis de seguretat (d'ara endavant **DS**), ens referirem a contramesures, bones pràctiques, idees, etc. que han d'ajudar a combatre un determinat apartat que s'ha englobat i determinat a pertànyer com a factor de Ciberseguretat a protegir.

L'ampliació i detall de cada un d'aquests indicadors escollits no serà motiu d'aquesta entrega parcial, doncs forma part del treball en la confecció de la eina pràctica. Sí que serà necessari introduir-los tots per poder saber quina temàtica ha de tractar el formulari auto resposta que serà el producte final de la pròxima entrega.

D'ara endavant: **En groc** senyalarem aquells Blocs on es considera que existeix Contribució neta e innovació a eines similars ja existents.

4.3.1 Determinació si entitat és Target d'estudi

BLOC 1 ID: Objectiu conèixer si es tracta d'una Pime. A banda, En cas contrari finalitza test):

- Dades econòmiques: volum negoci anual i dades balanç general anual.
- Mida: nombre empleats any anterior.

BLOC 2 ID: (Estadístic: es tracta d'ampliar informació d'empresa analitzada. Si la empresa ja disposa d'assessorament en la matèria es finalitza test. No és objectiu del projecte analitzar empreses que ja treballin amb una empresa de Ciberseguretat):

- Nom i dades fiscals.
- Sector.
- Dades geogràfiques: província.
- Xarxes socials utilitzades.
- Assessorament en Ciberseguretat: SI/NO

BLOC 3 ID: (Estudi intencions. Percepcions i experiència prèvia Ciberseguretat. En cas de detectar absència d'interès en realitzar estudi, ò pel contrari, detecció d'una empresa ciberexperta sense interès anàlisi estudi finalitza).

- Coneixement i percepció del concepte de Ciberseguretat.
- Grau d'Interès en la millora de la situació.
- Nivell confiança digital empleats i directius.
- Experiència prèvia en incidents ciberseguretat. (Ha patit algun?)

4.3.2 Determinació de la Cibermaduresa

BLOC 4 ID: (Informatiu: Comença estudi de veritat: Preguntes encaminades a esbrinar Estat de l'Art de la Pime).

- Nivell presència digital.
- Política Ciberseguretat existent.
- Pressupost anual TI. Percentatge previst destinat a Ciberseguretat.
- Qui es el principal responsable en la organització.
- Acords o intercanvis en la matèria amb tercers.

BLOC 5 ID: (Informatiu: Gestió de Riscos de l'empresa):

- Determinació de l'impacte de ciberincident en activitat essencial.
- Establiment (TMI) temps màxim d'interrupcions parcials i totals.
- Elaboració de procediments i plans de mitigació de riscos.
- Documentació e inventari dels actius que suporten activitat principal.

BLOC 6 ID: (Informatiu: Determinació i establiment de mesures bàsiques):

- Mesures potenciar conscienciació.
- Mesures corresponsabilitat i obligacions amb la societat.
- Adopció programes formatius.
- Accions conscienciació direcció empresa.
- Accions i mesures bones pràctiques en governança.

BLOC 7 ID: (Informatiu: Avaluació grau coneixements avançat organització).

- Qüestionari test noves tendències en ciberseguretat.

4.3.3 Determinació CiberResiliència Organització

A diferència dels Blocs anteriors, tots els següents apartats ja s'ocupen dels Dominis de Seguretat (**DS**) que s'ocupen d'entrar en detall amb la protecció real en diversos aspectes que engloben el concepte Ciberseguretat:

BLOC 8 **DS**: (Informatiu: Seguretat de la Infraestructura Essencial. Descripció breu instal·lacions a nivell nacional, local i com a societat)

- Adopció estàndards NIST aplicables a Espanya.
- Accessos físics a sistema. Altres proteccions.

BLOC 9 **DS**: (Operatiu: Seguretat de la xarxa).

- Mesures xarxa, WI-FI, cable i altres.
- Cas ús: *Atac Man-In-the-Middle*.

BLOC 10 **DS**: (Operatiu: Seguretat del núvol).

- Aspectes migració Segura.
- Perills *Dark web Market*: venda *cloud* accés.
- Principals vulnerabilitats núvol.
- Amenaces malware, ransomware, Botnet i criptomineria.
- Preparació i resposta a bretxes al núvol.
- Xifrat en repòs, en moviment i en procés.
- Confiança empleats en serveis al núvol.

BLOC 11 **DS**: (Operatiu: Seguretat de les Aplicacions).

- Xifrat Dades.
- Nivell actualitzacions seguretat.
- Ús de programari legal. Vigilància legacy.
- SuperApps.
- Aplicacions antimalware. Tallafocs.
- APT. Ransomware.
- Ofimàtica. Desactivació automàtica Macros.
- Navegació segura *https*.
- Esborrament segur.
- Control accessos remot empleats Teletreball.
- Mode usuari final/Administrador.
- Missatgeria Instantània.
- Defensa e-commerce. Protocol SSL.

BLOC 12 **DS**: (Operatiu: Seguretat de la Informació).

- Planificació i compliment normatiu de la legislació en SI.

- RGPD[22]: Grau coneixement i compliment.
- Percepció SI d'empleats respecte a clients d'entitat.
- Destrucció definitiva dades confidencials.
- Noves regulacions en privacitat Dades.

BLOC 13 **DS**: (Operatiu: Seguretat de l'Emmagatzematge)

- Política realització còpies seguretat: freqüència, responsable, ubicació.
- Protecció informació més sensible (core, know-how, confidencials).
- Grau confiança emmagatzematge al núvol.

BLOC 14 **DS**: (Operatiu: Correu electrònic i Seguretat dispositius mòbils).

- Tipus correu electrònic. Freqüència canvi contrasenyes.
- Check mesures mínimes dispositius mòbils: VPN, Wifi, PIN.
- Contrasenyes robustes. *Passphrase*. Arxius adjunts. Executables.
- Coneixement estratègia Confiança zero (*Zero Trust*).
- Aplicació "*Passwordless*". Seguretat sense contrasenyes.
- Control usuaris remots.
- Ús Intel·ligència Artificial i Machine Learning com a eines defensives.
- Seguretat Virtualització i Accessos.
- Identitat Digital i Blockchain.
- Seguretat en Xarxes Inal.làmbriques.
- IoT: Edge Computing. Firmware. Desactivació micros, càmeres.
- Enginyeria Social com a vector atac. Cas d´ús: phishingCorreu electrònic com a vector atac. Cas d'ús 2: Frau del CEO.

BLOC 15 **DS**: (Operatiu: Gestió Vulnerabilitats).

- Elaboració procediment. Eines identificació.
- Categorització i priorització.
- Repositoris, elaboració de procediments *parches* i actualitzacions.
- Monitorització e investigació i causes d'origen.

BLOC 16 **DS**: (Operatiu: Supervisió Contínua).

- 24x7. Monitorització contínua servei essencial.
- Supervisió xarxes comunicacions suport base.
- Cerca i supervisió programari suport a servei principal.
- Acords avisos alarma amb proveïdors externs.

BLOC 17 **DS**: (Operatiu: Gestió Incidents).

- Detecció, notificació a responsables.

[22] RGPD: Reglament General Protecció de Dades

- Procediments classificació i valoració. Criteris i Accessibilitat.
- Anàlisi Incidents per cercar resposta més idònia.
- Estructura avís i report a entitat d'incident.
- Existència opció control a incident fins solució.
- Capacitat Estimació Resposta i recuperació davant incident.
- Investigació causes i report a forces i cossos seguretat.

BLOC 18 **DS**: (Operatiu: Gestió de la Continuïtat del Servei).

- Elaboració de Pla de Continuïtat.
- Determinació RTO (Temps Objectiu Recuperació) del servei bàsic.
- Prova funcionament.
- Avaluació resposta 1: Interrupció fins recuperació mínima acceptable.
- Avaluació resposta 2: Interrupció fins recuperació total servei.
- Identificació riscos dependències, prioritats i requisits a tercers.
- Supervisió de tercers participants en servei en compliment Pla.

BLOC 19 **DS:** (Operatiu: Recuperació tres el Desastre).

- Gestió talls subministrament, desastres naturals i ciberincidents als canals comunicació
- Establiment delegacions autoritat gestió crisi.

BLOC 20 **DS**: (Operatiu: Formació En Ciberseguretat).

- Formació i sensibilització a personal implicat en servei principal.
- Identificació necessitats formatives pels serveis principals.
- Definició i posada en marxa pla conscienciació tota plantilla.
- Incentivar cultura ciberseguretat: certificacions, jocs, premis.
- Creació codis interns de bones pràctiques en ciberseguretat.
- Programes formatius: *Bug Bounty*, *mentoring*.
- Foment eines recolzament, consulta.
- Eines visibles per conscienciar directius.
- Creacions decàlegs bàsics.

4.3.4 Suggeriment i adopció d'ús de CSasS (Ciberseguretat com a Servei)

BLOC 21 ID: (Informatiu: Alternativa a empreses vulnerables o sense recurs).

- Introducció, viabilitat i beneficis d'adopció de servei.
- Percepció avantatges e inconvenients per la Pimes.
- Contacte comercial empreses especialitzades.

4.4 Definició Característiques i Programari a Utilitzar

No volem anticipar gaires coses al respecte, doncs això pertany a la tercera entrega d'aquest projecte, però a data d'avui la combinació dels dos programaris que es contemplen per implementar el formulari que ha de servir de base per complir els nostres objectius són:

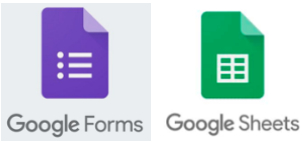
- Google Form. Totes les respostes es guardaran en:
- Google Sheets.

En falta per veure com implementaré el tipus de resposta, i sobretot la puntuació de cada pregunta i bloc per poder fer la classificació final de l'estat de l'empresa analitzada. Confio en què la corba d'aprenentatge sigui ràpida i em permeti realitzar la tercera entrega en la planificació de timing prevista.

5 Test Ciberseguretat.

5.1 Principals eines utilitzades

El disseny com hem anticipat a l'apartat anterior s'ha realitzat utilitzant l'aplicació *Google Forms* (del grup d'eines obertes de Google). El manteniment de les dades i optimització d'aquestes (que NO és objectiu d'aquest projecte) està basat en *Google Sheets*.



Els principals motius de la seva elecció han sigut:

- la facilitat de la seva corba d'aprenentatge.
- son aplicacions gratuïtes si tens compte de Google.
- Absència de limitacions respecte al espai utilitzat pels formularis i sobretot pel nombre total de preguntes que es podien plantejar e incloure al formulari (indispensable pel nostre objectiu d'aquest projecte). Es van consultar altres aplicacions de pagament que no complien aquest punt.

Per contra es va acceptar la seva excessiva senzillesa alhora de plantejar dissenys visuals (potser més atractius amb altres aplicacions) i potser ampliar les seves tipologies de resposta, però el factor temps i la seguretat que era més que suficient però poder plantejar i assolir els nostres reptes de *Cibermaduresa, CiberResiliència* i Introducció a *CiberSeguretat com a Servei* (CSaaS) ens ha fet decantar per la seva elecció.

Un cop seleccionades les aplicacions (***amb què treballar****?),* la següent dificultat ha consistit en escollir l'estratègia en com plantejar el formulari/s per poder extreure la informació justa i necessària per poder assolir els reptes. Vam necessitar uns dies molt intensos de treball de camp (previst a timing) consultant altres eines existents de pàgines com INCIBE, CCN-CERT, IBM, etc.

Aquest procés de com saber preguntar i recopilar la informació ens ha posat a prova per la quantitat ingent d'informació a valorar. Decidir què es indispensable i necessari per classificar a les entitats en base als 3 reptes anteriors ha significat pensar acuradament en cada pregunta que volíem extreure en la resposta i com plantejar les respostes per poder donar després un bon feedback.

El que sí sabíem es que havíem de subdividir el treball recopilatori en tres fases:

5.1.1 PRIMERA FASE: TEST DE CIBERSEGURAT: ETS UNA PIME?

La primera fase es importantíssima i encara que no és estrictament feina molt tècnica si que es **indispensable a nivell qualitatiu** per seleccionar quines empreses són objectius del nostre projecte. Em escollit tres criteris fonamentals per simplificar el punt de partida:

- En base al punt 2.1 d'aquest document: Què es una PIME. S'ha fet les preguntes adequades per no tindre cap dubte. S'inclouen els autònoms, i s'entén que a per molts d'ells aquest test no serà gaire realista perquè a causa de la seva definició de negoci, la gran majoria no podran valorar els ítems dels tests. No obstant els pot resultar molt útil com punt de partida.

- Empreses/autònoms que no hagin rebut en els últims 2 anys cap assessorament de cap empresa de Ciberseguretat. No té cap sentit treballar amb entitats que hagin estat *ajudades* o *influenciades* en matèria de Ciberseguretat. Aquest test ha de ser útil com a punt de partida i per cercar/fomentar relacions amb empreses de CSaaS que col·laborin amb la nostre idea.

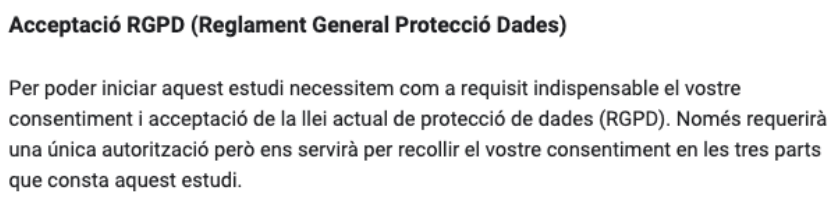
- Ha d'existir per part de les organitzacions enquestades esperit crític i de millora de les seves situacions actuals. Amb aquest tercer criteri, escollim organitzacions que **vulguin**, **s'ho puguin permetre econòmicament** i tinguin una certa estructura tècnica de negoci per poder avaluar-les. Hi ha una pregunta molt sincera i oberta on se'ls pregunta per les seves intencions.

I així s'ha dissenyat la primera de les 3 aplicacions:

Il·lustració 46: capçalera Formularis

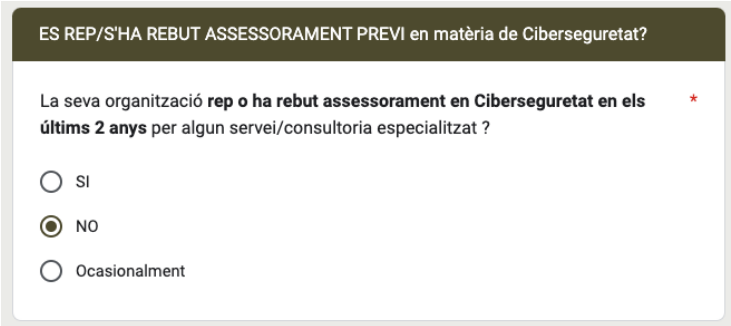
Aquest primera aplicació es caracteritza pels següents aspectes:

Es molt important d'inici complir amb la llei de protecció de dades (RGPD), i encara que l'estudi és de caire tècnic no hem d'oblidar que un dels objectius finals pot ser posar en contacte a la empresa assessorada amb una empresa de CSaaS, per això és indispensable comptar amb el consentiment de l'empresa en matèria de Llei de protecció de dades.



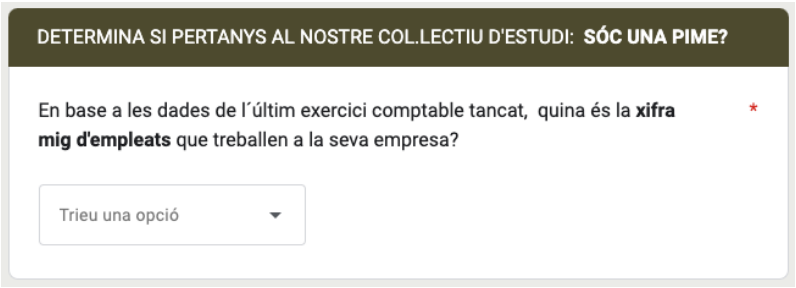
Il·lustració 47: imatge 1 formularis

Sabem les intencions reals de l'empresa assessorada. Si vol participar o no en l'estudi.



Il·lustració 48: imatge 2 formularis

Es una eina que respon als primer tres blocs definits al apartat 4.3 d'aquest projecte sobre els indicadors digitals/dominis de seguretat. Ara ja sabem si la empresa pertany o no al nostre grup d'estudi (Bloc 1):

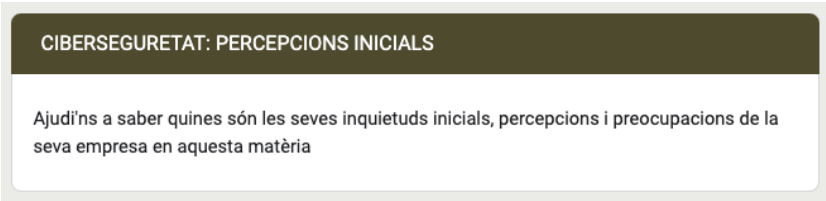


Il·lustració 49: imatge 3 formularis

Disposem també d'unes dades mínimes de contacte, classificació sectorial i quina és la seva presència digital, ús de les xarxes socials:

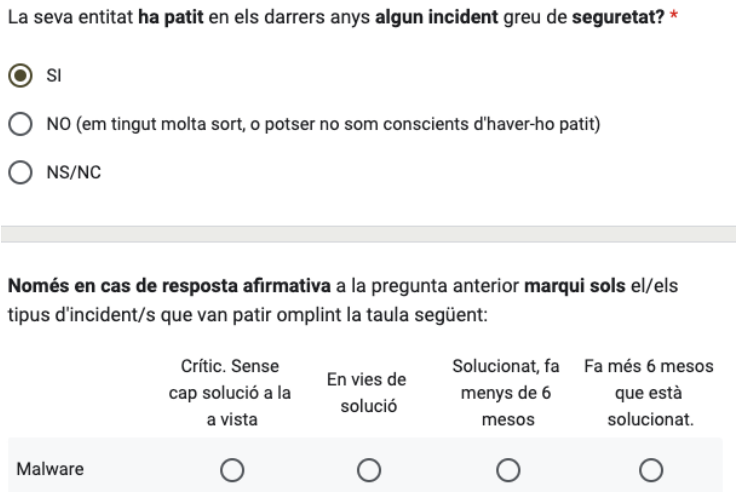
Il·lustració 50: imatge 4 xarxes socials formularis

És convenient també que existeixi un apartat definit al Bloc 3 sobre les percepcions, estat actual de la organització, nivell de confiança digital inicial dels empleats nocions en matèria de Ciberseguretat:



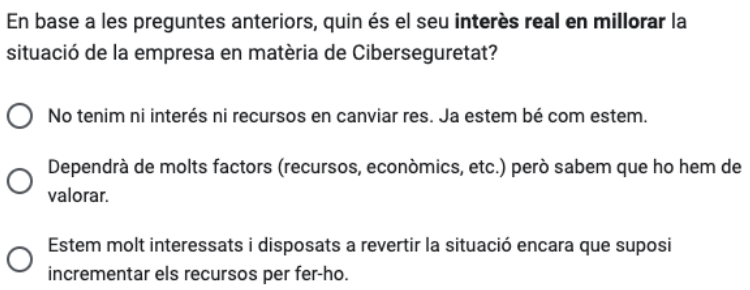
Il·lustració 51: imatge 5 formularis

També un apartat per detallar la experiència patida en ciberincidents i per les afectades el grau de solució.



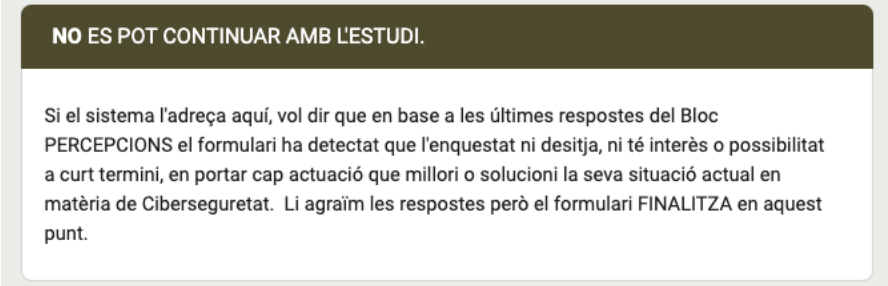
Il·lustració 52: imatge 6 formularis

Com hem anticipat abans el test ens ajudarà a descobrir les intencions reals de millora de la empresa analitzada.



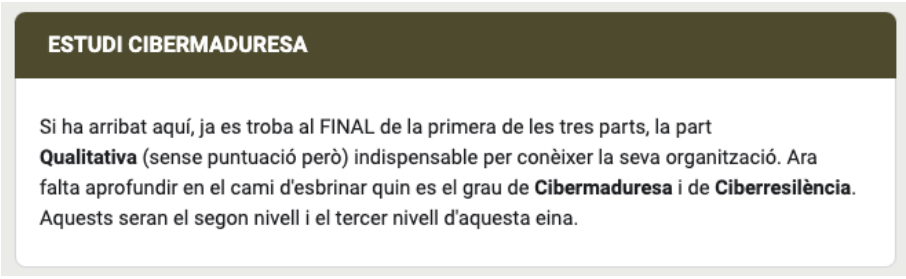
Il·lustració 53: imatge 7 formularis

Fàcil, contínua qui vol, qui no, se'l convida amablement a finalitzar-ho:



Il·lustració 54: imatge 8 formularis

En canvi, el que finalitza la primera fase se l'anima a iniciar les següents fases. És un fase com informa el formulari que es sense puntuació però valuosa per orientar i oferir una primera guia de l'entitat que emplena la nostra aplicació.



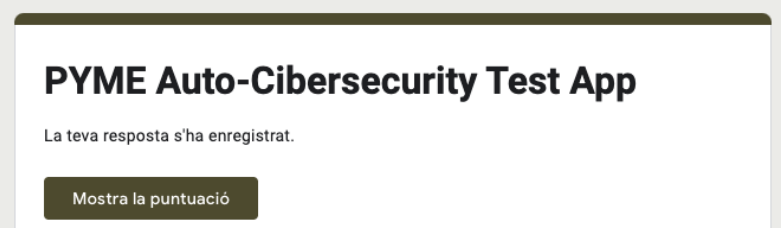
Il·lustració 55: imatge 9 formularis

Per tant aquesta primera fase, que té un temps orientatiu de resposta d'uns 10 minuts, (no volem cansar aquí als enquestats) ens permetrà de forma ordenada respondre i encaminar als nostre públic objectiu al tindre:

- Certesa en analitzar una entitat objectiu (PIME).
- Tranquil·litat en el compliment de la llei RGPD en la recopilació de dades.
- Aconseguir les dades comercials de contacte per aprofundir a posteriori en la derivació cap a una possible empresa mentora en CSaaS.

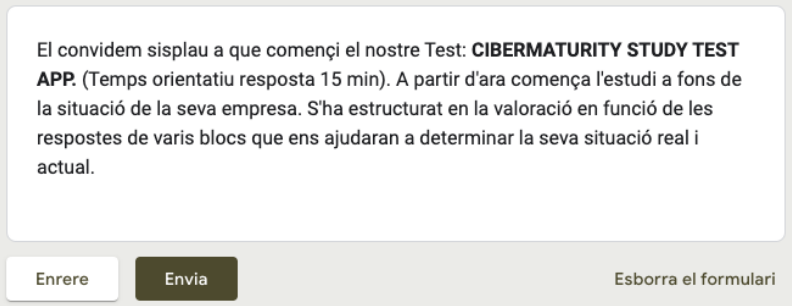
- Comptar amb la voluntat de la empresa analitzada de prosseguir i deixar-se ajudar en la millora de la seva situació actual de Ciberseguretat.
- Percebre i entendre per veu del client la seva opinió prèvia realista sobre el nivell inicial en matèria de Ciberseguretat.

I aquest és el punt de partida per iniciar (ara sí) la part densa del estudi on realment obtindrem informació detallada i àmplia que ens servirà per donar resposta al seu estat de Cibermaduresa. De fet, la primera fase es tota seqüencial i en funció de les respostes et va guiant i avançant fase o finalitzant l'estudi. Fins que s'envia el formulari. El sistema t'envia una còpia de les respostes



Il·lustració 56: imatge 10 formularis

En aquesta primera fase la persona no rep cap mena de puntuació. Recordem que la segona fase comença amb una invitació a emplenar-la com la que aquí es mostra:



Il·lustració 57: imatge 11 formularis

5.1.2 SEGONA FASE: TEST DE CIBERMADURESA

Il·lustració 58: capçalera test Cibermaduresa

Ja d'inici es detallen una sèrie d'instruccions per emplenar els formularis. En concret 3 recomanacions molt importants:

- sinceritat en les respostes.
- les preguntes es puntuaran amb la qual cosa és recomanable que es contesti tot el formulari. Ja s'avisa a autònoms o empreses que no disposin de prou estructura que responguin com si fossin qüestions teòriques.
- Recomanable que contesti el màxim responsable informàtic.

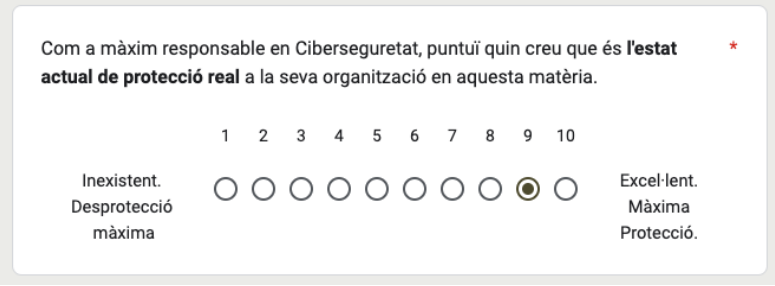
L'objectiu d'aquesta segona etapa és classificar a les empreses que segueixin l'estudi en un dels tres nivells següents:

- Empresa **CiberNovata**.
- Empresa **CiberIntermèdia**.
- Empresa **Ciberexperta**.

Un cop es finalitzi l'estudi de la segona part, la empresa rebrà a el resultat global de les seves respostes i un feedback important que les classificarà en una d'aquestes tres tipificacions. Les empreses assessorades ja tindran un primer dictamen que s'acabarà de completar amb la tercera fase del test (la Resiliència).

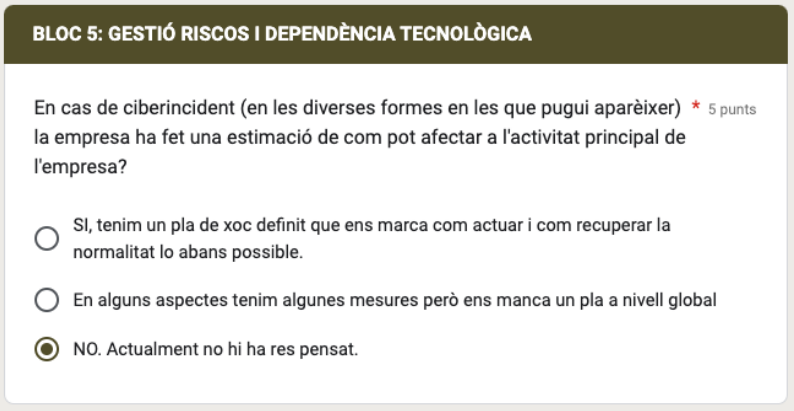
En aquesta segona part existeixen 3 tipus de preguntes:

- Preguntes d'opinió (no puntuen quasi mai però són molt útils per esbrinar les intencions de les empreses consultades en aspectes molt concrets:



Il·lustració 59: imatge 12 formularis

- Preguntes multi resposta amb una única opció correcte o amb màxima puntuació (puntuada):

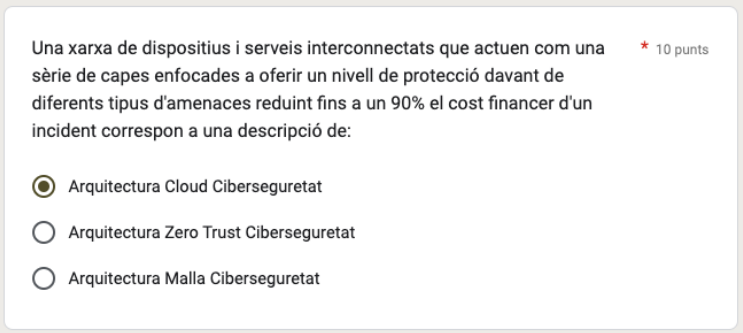


Il·lustració 60: imatge 13 formularis

- Preguntes de completar informació sobre un tema concret. La empresa simplement ha d'afirmar o negar si es realitza a la empresa la qüestió. La seva valoració oscil·la entre els 2 als 4 punts per resposta correcta.

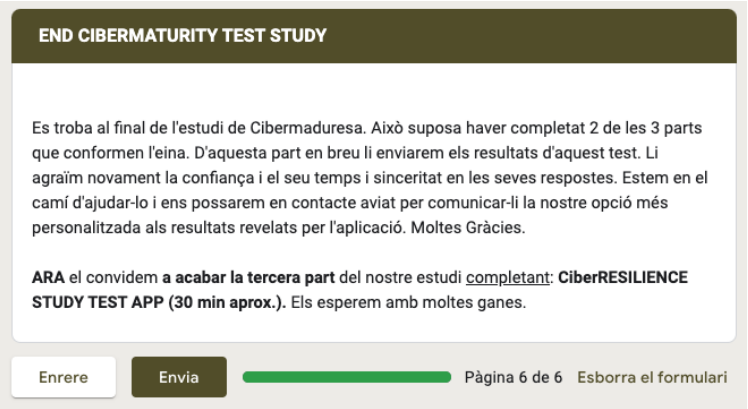
Il·lustració 61: imatge 14 formularis

- Preguntes de coneixement teòric (no acostumen a reportar més de 2 punts per cada resposta correcta). Complementen el coneixement sobre una temàtica que es té de l'organització:



Il·lustració 62: imatge 15 formularis

La major part de les preguntes que els enquestats es trobaran en els dos tests són d'aquest estil. Quan es finalitza el test, aquest ens agraeix la col·laboració i ens anima a respondre la tercera i última part: el test de CiberResiliència.



Il·lustració 63: imatge 16 formularis

5.1.3 TERCERA FASE: TEST DE CIBERRESILIÈNCIA

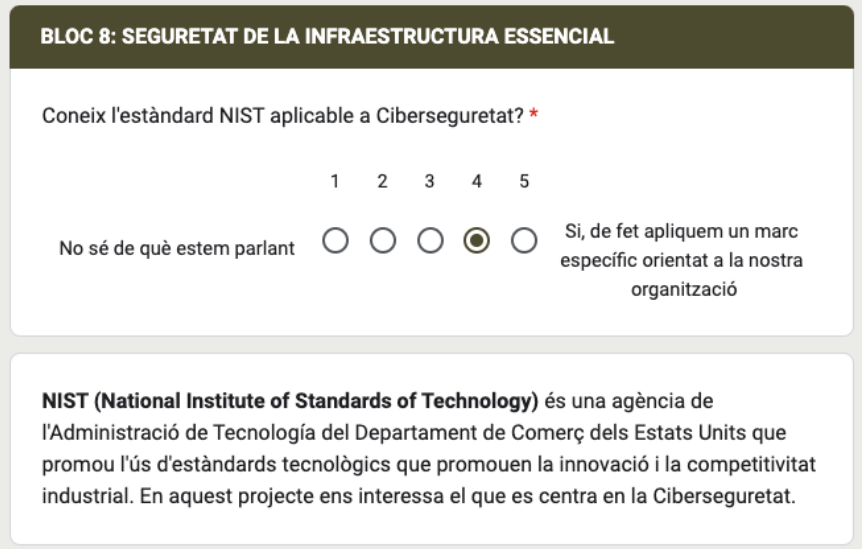
Il·lustració 64: capçalera Test Ciberresiliència

Aquesta és clarament la part més densa de tot l'estudi. Requereix un temps de resposta no inferior als 30 minuts. És força senzill e intuïtiu però incorpora un grau de coneixement elevat que requereix concentració elevat. Al inici del projecte (i encara no ho descartem) es va plantejar fer un únic formulari per complir amb el nostre objectiu.

La veritat és que per saber si és la millor solució (enviar un sol formulari als clients que englobi els 3 objectius) faltarien més proves de camps per esbrinar si un test de 50 minuts seria viable, i respectaria els temps de descans de l'enquestat. Per nosaltres és molt important que s'ompli amb la màxima predisposició i concentració per obtindré un millor feedback.

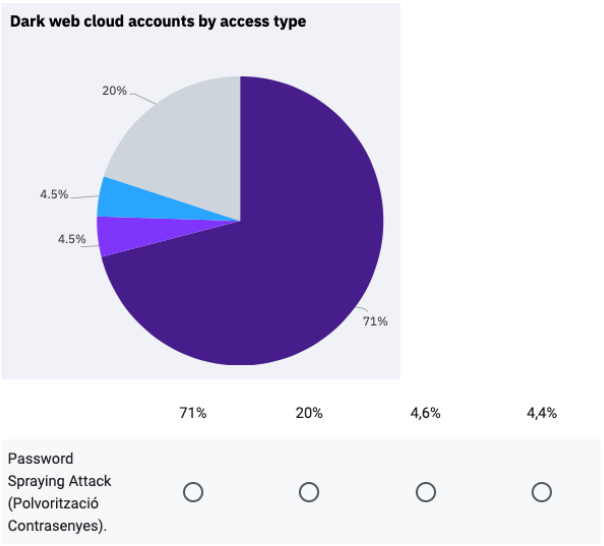
Les principals característiques de la tercera aplicació es que també es puntuada i ara si, dona resposta a tots els indicadors digitals i dominis de seguretat plantejats al punt 4. Amb aquest estudi, si que podem dir que entrem al detall, en les qüestions més importants que es considera que han d'afectar a una bona auditoria de ciberseguretat.

En aquest estudi ens podem trobar preguntes similars a les què hem introduït a la segona fase veure observarem que també apareixen algunes que requereixin explicacions addicionals per poder triar i respondre millor. Es fa una petita descripció o aportació teòrica amb l'objectiu d'aconseguir una opinió més detallada i realista



Il·lustració 65: imatge 17 formularis

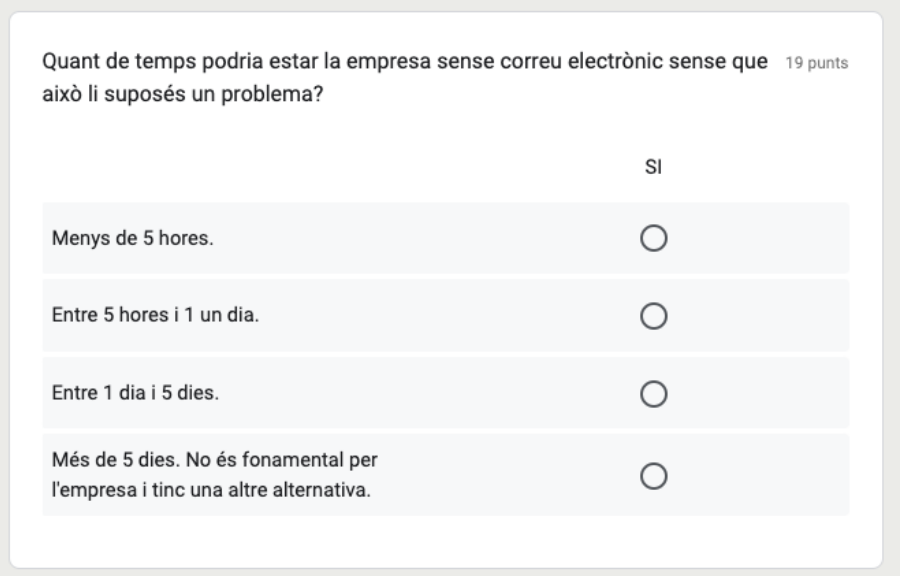
També ens podem trobar preguntes *gràfiques* d'ordenar %. No deixen de ser teòriques però analitzen factors de seguretat habituals:



Il·lustració 66: imatge 18 formularis

A mesura que s'avança en els blocs s'analitzen factors de seguretat de la infraestructura essencial, seguretat de la xarxa, seguretat del núvol, seguretat de les aplicacions, seguretat de la informació, seguretat del emmagatzematge. Són conceptes bàsics, però fonamentals. Una auditoria complerta no els pot deixar passar.

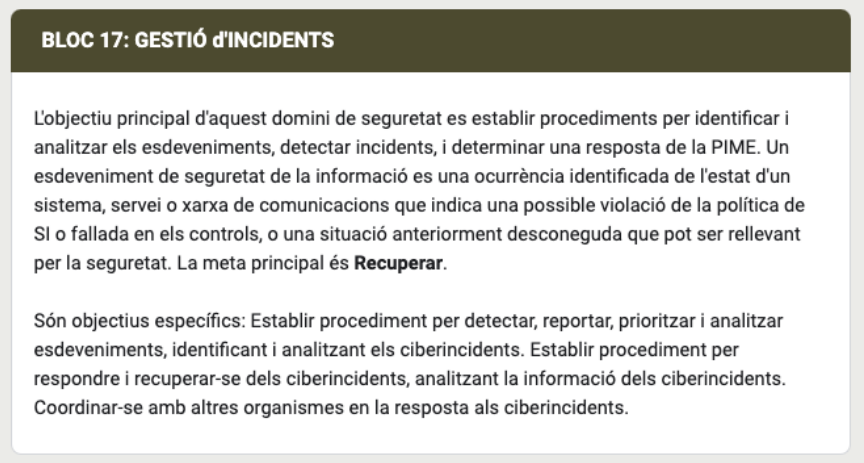
A partir del bloc 14, el test s'enfoca una mica diferent. Es tracta d'analitzar factors crítics com són les eines de correu electrònic i la virtualització. També és forçós esbrinar l'exposició i la superfície de risc de les nostres empreses en el que respecta a les xarxes socials, Internet of Things (IoT), la seguretat dels dispositius mòbils i un tema preocupant, els atacs d'Enginyeria Social.



Il·lustració 67: imatge 19 formularis

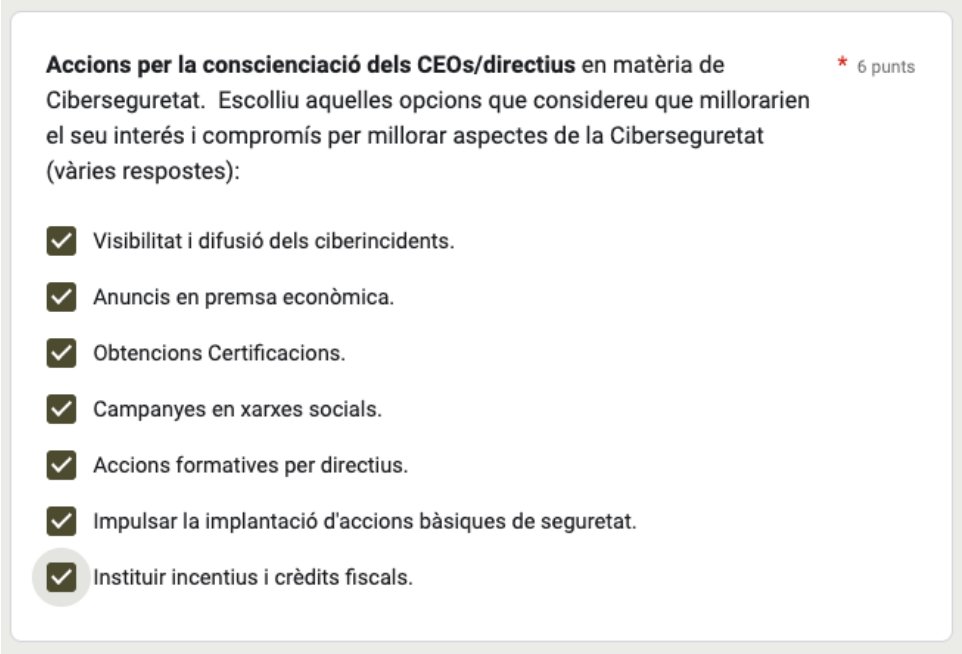
Creiem amb l'enfocament d'aquest bloc recollim de forma completa els aspectes bàsics que analitzen aquests aspectes. Val a dir que el glossari d'aquest projecte és ampli i s'han mirat d'incloure la majoria de conceptes tècnics que hi apareixen. A partir d'aquí ens centrem en el Marc de Treball de Ciberresiliència (avançat al punt 4.2), un plantejament molt encertat de l'**Incibe**.

Possiblement es la part menys *original* de l'aplicació però analitzats els punts que valida incloure-la es absolutament imprescindible. La gestió de les vulnerabilitats, la supervisió contínua, la gestió d'ncidents, la gestió de la continuïtat del servei i la recuperació tres el desastre són blocs que semblen un de sol però ens acabaran de definir l'estat real de preparació dels nostres candidats/es d'estudi.



Il·lustració 68: imatge 20 formularis

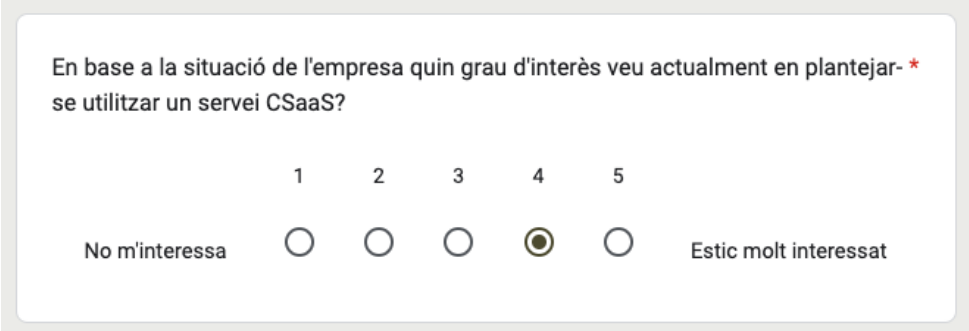
L'Aplicació acaba amb dos blocs molt importants, el Bloc 20 on es plantegen qüestions sobre la importància de la Formació i s'aborden preguntes generals però molt enfocades tant a tots als empleats però amb especial incidència als màxims responsables (CEOs, directius) de les empreses.



Il·lustració 69: imatge 21 formularis

Per últim, l'últim bloc (21) es centra en el nostre objectiu estrella del nostre projecte: CSaaS (**La Ciberseguretat com a servei**). Després a les conclusions ampliarem detalls, però donat que és el concepte que culmina, agafa el protagonisme i respon al perquè s'ha realitzat aquest estudi, era necessari, un bloc sencer per introduir-lo, presentar-lo i i posar-lo en valor.

Al bloc es visualitza, des de la seva definició com a concepte, com també es detalla un enfoc respecte a les avantatges e inconvenients d'utilitzar-lo. A banda es proporciona una bateria important de criteris per escollir un bon proveïdor de CSasS. Per última, no ens podem oblidar d'una pregunta oberta i clara requerint l'interès per adoptar o no aquesta tecnologia.



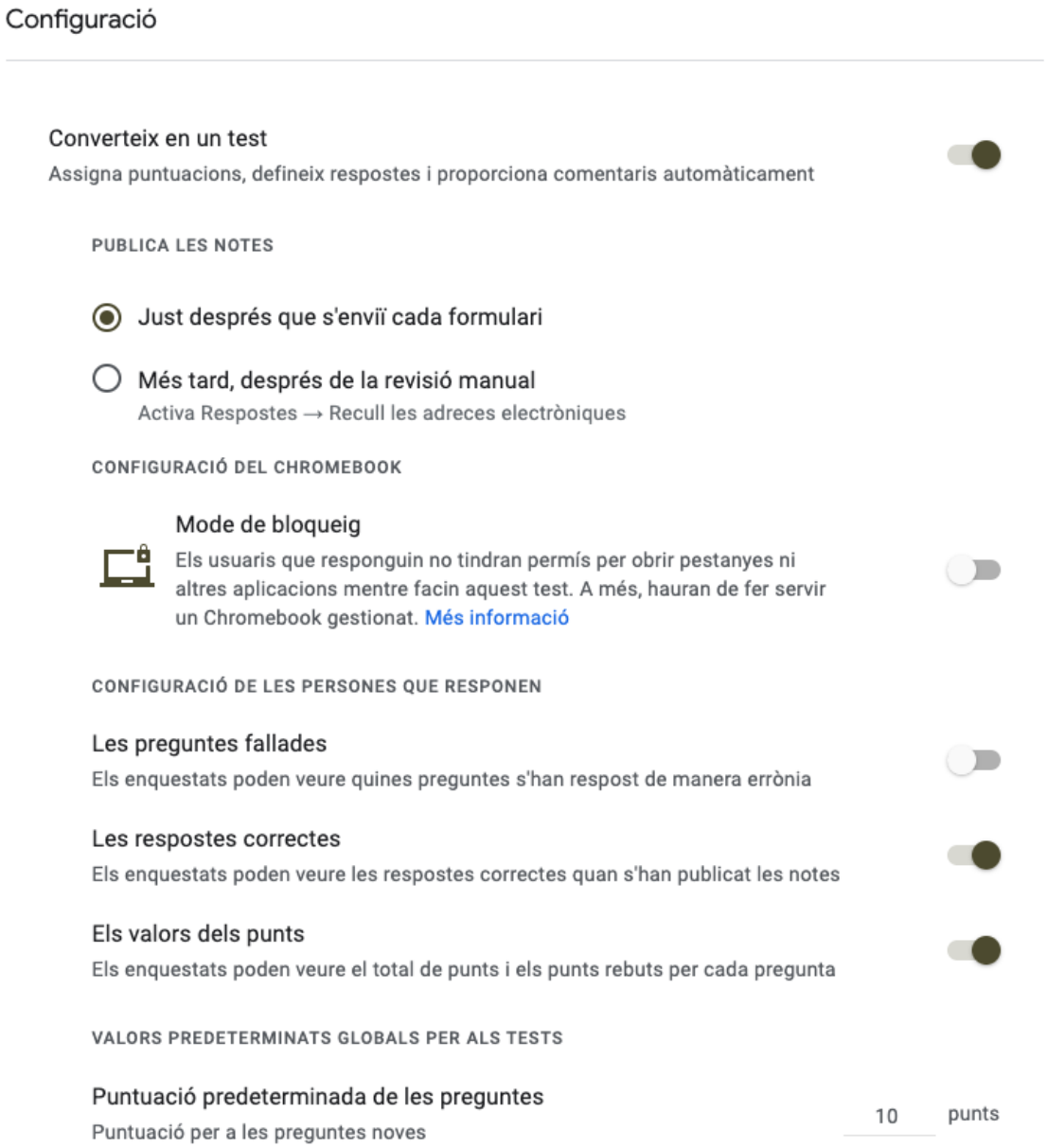
Il·lustració 70: imatge 22 formularis

5.2 Aspectes tècnics de les Aplicacions.

Com hem comentat d'inici ens hem estimat dissenyar 3 miniaplicacions amb els temps de resposta repartits (5 min + 15 min + 30 min) que no una aplicació de 50 min molt intensa. Cada formulari, en realitat presenta 3 camps importants:

Il·lustració 71: imatge 23 formularis

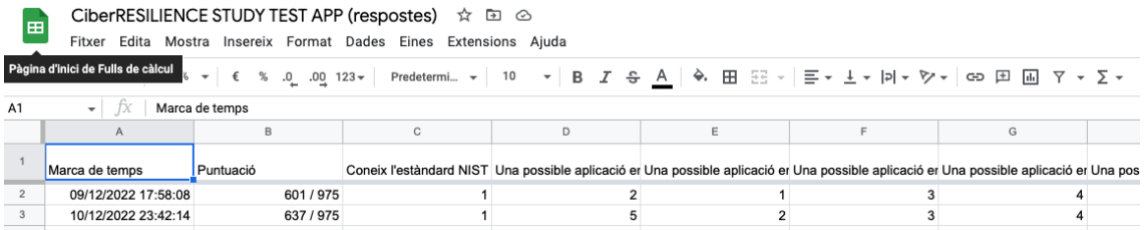
Un apartat de preguntes, on al ampliar-se ens mostra en detall les preguntes que formen les seccions. Un apartat de respostes on reben el resum i el detall de les respostes dels nostres enquestats, i finalment un apartat de configuració que és el que explicarem ara els principals criteris que utilitzarem:



Il·lustració 72: imatge 24 formularis

No hem d'oblidar que tot formulari de resposta, té com a document que el sustenta una fulla de *google sheet* on de forma una mica "vasta i poc manipulable" tots els apartats i respostes dels clients. La creació de la fulla de càlcul de suport s'aconsegueix clicant la següent icona al apartat de respostes:

L'experiència en filtrar i millorar la presentació de les dades brutes per poder després fer informes o treball de cerca de dades ha sigut poc pràctica.



Il·lustració 73: imatge Google Sheet formularis

S'ha intentat generar una aplicació que directament agafés les dades de la columna puntuació per enviar-li al feedback al client final. Però pensem que no és l'objectiu d'aquest treball. Com e veurà al proper apartat es resoldrà enviant a cada empresa un document personalitzat segons el grau de Cibermaduresa a més dels seus resultats dels 3 test.

5.3 Determinació de la CIBERMADURESA

Amb molta modèstia per poder determinar el grau de cibermaduresa d'una entitat ha sigut necessari recopilar informació definitiva sobre:

- **Aspectes Bàsics Generals**: a través d'una bateria de preguntes generals (responent als 4 primers Bloc d'Indicadors Digitals) sobre la tecnologia existent a l'empresa, la formació del personal, la ubicació física dels sistemes, la robustesa de les contrasenyes, grau inversió en noves tecnologies, política destrucció de la informació, política d'acords en ciberriscos amb tercers, pressupost destinat a TI i en concret a Ciberseguretat, presència en xarxes socials, etc.

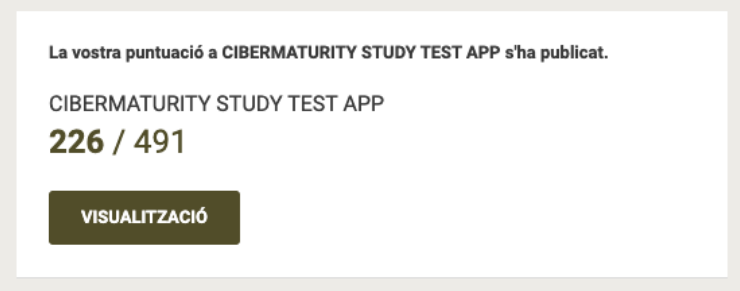
- **Gestió de Riscos i Dependència Tecnològica:** Un apartat ampli on es detallen conceptes fonamentals sobre afectacions a l'activitat principal, la web, el correu corporatiu i el teletreball en cas d'incident. Una visió sobre la política de còpies de seguretat, d'actualitzacions de sistemes, estimacions del TMI (Temps Màxim Interrupció) i una comprovació d'existència o no de pla de crisi/emergència.

- El bloc 6 es centra en un apartat molt específic sobre **mesures de conscienciació i grau de corresponsabilitat social**, és a dir, de quina forma s'involucra la societat amb el seu ecosistema de col·laboradors i actors que l'envolten.

- Les preguntes del bloc 7 sobre **noves tendències en Ciberseguretat** es centra en uns d'indicadors digitals responen a aquest punt. Està clar que un grau avançat de coneixement ajuda a millorar l'índex de cibermaduresa o a marcar la diferència en aquelles entitats amb recursos que a més estan liderades per caps/responsables informàtics amb un alt nivell d'experiència.

Amb els blocs que engloben les Aplicacions 1 i 2 (Dels primers 7 blocs) ja podem classificar mínimament a les nostres empreses que realitzen els Tests. **El tercer test** (CiberResilience Test) ens servirà per analitzar amb detall les **fortaleses i febleses** de l'empresa un cop ja ha estat classificada com a empresa cibernovata, ciberintermitja o ciberexperta.

Un cop s'envien els 3 formularis les empreses que els han realitzats reben un missatge amb la puntuació rebuda i poden visualitzar el resultat de cada apartat:



Il·lustració 74: imatge 25 formularis

5.4 Disseny Bloc i punts sobre Noves Tecnologies.

Consultant la eina de treball i els formularis, un es pot preguntar, **quin ha sigut el criteri o la inspiració** per parlar de les qüestions que s'aborden en els blocs de noves tecnologies en matèria de tendències de futur. En aquest cas, a banda d'una consulta intensa en la xarxa, si que bona part d'aquesta informació prové d'un mix proporcionat per la multinacional Gartner.[23]

S'han consultat uns informes de noves tendències de Ciberseguretat, i sobretot en previsió que moltes d'aquestes novetats puguin ser novetats, recomanacions o primícies tecnològiques arriscades i no contrastades, s'ha decidit inspirant-se en el model ***Hype Cycle*** de la multinacional *Gartner*. Al **Annex 1** ampliarem molts detalls de com funcionen, quins gràfics i quin rang de temps es contemplen.

5.4.1 **Mode Hype Cycle Gartner**.

S'escull aquest model (també denominat la *corba de Gartner*) perquè és una eina visual que intenta anticipar si les noves tecnologies que van sorgint es tracten de meres fantasies on pots invertir erròniament, o bé son tecnologies/apps que realment es convertiran en veritables apostes de futur que es consolidaran i gaudiran d'un potencial de resolució a problemes actuals prou atractiu com per invertir-hi una part o tot el pressupost destinat a TI.

[23] Gartner Inc, amb seus a molts països, es una empresa consultora i d'investigació de les TI ubicada a Stamford, Connecticut, Estats Units.

Il·lustració 75: Situacions model Hype Cycle

Encara que al gràfic superior introduïm de quina forma funciona el model, el material i els gràfics utilitzats per extreure la informació es poden consultar en annexos posteriors que s'adjunten en aquest projecte. Val a dir, que existeixen nombroses temàtiques que poden utilitzar aquest sistema però només es considera rellevant per la l'objectiu d'aquest projecte els 6 *cicles* de treball que es descriuen al següent apartat.

5.4.2 Cicles de Treball Escollits[24]

- **Midsize Enterprises**: es centra en les pimes. És un dels principals models i s'analitza un període de 5 anys (des de l'any 2017 fins el 2021). A destacar la evolució progressiva de les següents tecnologies (algunes de les quals ha aparegut en projecte): *Machine Learning*, *Disaster Recovery as a Service (DRaaS),* Firewall as a Service (FaaS), *Hybrid Cloud Computing*, *BEC Protection*, *Cloud Data Backup* i sobretot Edge Computing.

- **Blockchain Technologies:** una combinació d'*insights* i els corresponents cicles d'anàlisi (de 3 anys) ens mostra com a tendències clares (entre moltes altres) l'aplicació de validació en les *cryptocurrencies*, blockchain *wallets* i la signatura d'*Smart Contracts* i adopció de *Consensus Mechanisms* (protocols consens) i altres com el *metaverse* i els NFT.

- **Security Operations:** analitzats cicles d'un període 3 anys transcendeixen com a tecnologies destacades: Cibersecurity *Mesh* Architecture, *SOAR*, *SIEM* i *Zero Trust* Network Access.

- **Emerging Technologies:** segon model principal. Analitzat un període de 6 anys (2017-2022) es destaquen la rellevància de la IA (Intel·ligència Artificial), Edge Computing, NFT, SuperApps, Blockchain, IoT Platform, Machine Learning, 5G i Mesh Architecture (Arquitectura de Malla).

[24] es subratllen les tecnologies amb més probabilitat d'èxit

Il·lustració 76: Exemple per Emerging Technologies Hype Cicle 2022

- **Cloud Security:** Analitzats (5 anys cicles) destaquem: *ZTNA*, Cl*oud Data Backup*, *Cloud Management Platforms* i *DSaaS*.

- **IA:** Analitzats 3 anys cicles destaquem *Deep Learning*, C*hatbots*, *ML* i *Cloud IA*.

5.5 Criteris de Puntuació de les Aplicacions. Taules Guia:

	TEST STUDY APP SCORES		
	Bloc Number	**Max. Score points**	**Total Score points**
TEST 1 CYBERSECURITY			
Am I a PIME?	1	It doesn't score	
Contact Data	2		
Security Perceptions	3		
Total T1			
TEST 2 CYBERMADURITY			
Go to Basics	4	138	**69**
Risk Management	5	221	**87**
Social Stewardship	6	60	**50**
Test new Tech	7	72	**20**
Total T2		**491**	**226**
TEST 3 CYBERRESILIENCE			
Main infraestructure	8	44	**26**
Net security	9	95	**59**
Cloud security	10	92	**34**
Apps security	11	169	**91**
Data security	12	44	**14**
Storage security	13	44	**41**
Mail, IoT, smartphone...	14	209	**150**
Exploits management	15	28	**12**
Continous supervision	16	20	**5**
Incident management	17	36	**24**
Service Continuity	18	27	**15**
Disaster recovery	19	47	**29**
Training	20	36	**19**
CSaaS	21	84	**72**
Total T3		**975**	**591**

A la taula superior s'observen els teòrics de puntuació que es poden rebre emplenant els 3 qüestionaris (bàsicament el segon i el tercer test). Hem agafat com exemple un missatge. Segons les taules de classificació de la pàgina següent aquesta empresa tindria una situació molt severa amb un requisit d'actuar amb immediatesa.

Les regles que apliquem en aquesta tabla tan explícita són les **del 70% i el 90% de la puntuació màxima teòrica**. Qualsevol empresa que puntuï per sota d'un 70% (343 punts) al Test 2 se la considerarà una empresa cibernovata. Qualsevol empresa que puntuï per sobre d'un 90% (442 punts) serà considerada experta. La resta es consideraran intermitges.

Anàlogament qualsevol empresa que puntuï per sota del 70% (682 punts) al Test 3 de CiberResiliència es pot considerar que es troba en una situació de **greu exposició** a ciberatacs. Per contra, puntuacions superiors al 90% significarà una empresa amb un grau de resistència i protecció elevat[25]. La resta tindran posicions intermitges.

Evidentment no serà el mateix puntuar un 20% que un 65% però la gradació en la puntuació i la seva interpretació final correspondrà a la empresa. Aquests resultats finals el que pretenen és impactar i conscienciar de la situació real, i aconseguir un interès real i ferm en sol·licitar els serveis lo abans possible d'una empresa que es dediqui a oferir **CSaaS**.

I en base a això cada empresa rebrà un feedback determinat i unes conclusions determinades segons la següent tabla:

CyberResilience	-	**CyberMadurity**	+
-	IN DANGER	EXPOSED	DO NOT TRUST
	EXPOSED	PAY ATTENTION	PROTECTED
+	DO NOT TRUST	PROTECTED	HIGH PROTECTED

Com es veu hi han 9 situacions possibles:

IN DANGER: CyberRookie (cibernovata) + Low CyberResilience.
EXPOSED: CyberRookie + Medium CyberResilience.
EXPOSED: CyberIntermediate + Low CyberResilience.
DO NOT TRUST: CyberRookie + High CyberResilience.
DO NOT TRUST: CyberExpert + Low CyberResilience.
PAY ATTENTION: CyberIntermediate + Medium CyberResilience.
PROTECTED: CyberExpert + Medium CyberResilience.
PROTECTED: CyberIntermediate + High CyberResilience.
HIGH PROTECTED: CyberExpert + High CyberResilience.

[25] Recordem que en matèria de Ciberincidents mai no hi han un 100% de protecció segura i efectiva.

5.6 Plantilla Model Feedback.

La idea es que les empreses rebin un feedback a mode de **resum executiu d'una a dos pàgines màxim** perquè els serveixi com un full de ruta inicial per començar a treballar. Aquesta plantilla model que rebrà client ha d'incorporar els següent elements:

Il·lustració 77: capçalera Test App Cibersecurity

Adreçament Personalitzat: Al màxim responsable en Ciberseguretat de la entitat.

Classificació Organització Cibermaduresa: en base a la puntuació de la Taula Guia 1.

Determinació nivell CiberResiliència: en base a puntuació de Taula Guia 1.

Dictamen Situació: en base a classificació de Taula Guia 2 amb els 9 escenaris diferents que hem presentat.

Punts Forts: Millors puntuacions obtingudes als blocs i Dominis Seguretat.

Punts Febles: Pitjors puntuacions obtingudes als blocs d'indicadors digitals i Dominis Seguretat.

Principals Recomanacions: en base a totes les conclusions obtingudes sobre la situació personal e individual de cada PIME.

Dades Contacte: Adreçament contacte correu electrònic, proposta cita i proposta de soci tecnològic (Empresa Ciberseguretat amb model CSaaS) per iniciar primer contacte comercial i tècnic informatiu.

Al Punt 5.8 (Proves de Camp), es comentaran més detalladament en base a les respostes reals que s'han efectuat a empreses reals varis models de feedback que ajudaran a entendre més la tasca prèvia organitzada als formularis

5.7 Enllaços a Formularis i Aplicacions.

És molt important que es segueixi un estricte ordre en l'obertura:

1. **CIBERSECURITY STUDY TEST APP**:

   https://forms.gle/faDYH78d8yeTKB1N8

2. **CIBERMADURITY STUDY TEST APP**:

   https://forms.gle/DD6uDJEt3R2CwinZA

3. **CIBERRESILIENCY STUDY TEST APP**:

   https://forms.gle/pQeZMbS9noowqGzy6

5.8 Proves de Camp. Tests Reals. Enviament feedback.

Un cop dissenyat els 3 formularis inicials, era necessari provar de forma real els formularis. L'objectiu es comprovar diverses aspectes de cara a millorar l'eina i passar-la a una hipotètica propera fase de producció:

- Comprensió coherència enunciats, preguntes i explicacions.
- Comprovació durada i temps resposta dels 3 formularis.
- Estudi d'operativitat dels qüestionaris.
- Recollida d'opinions finals un cop realitzats els tests

S'han fet 3 proves de camp, una d'elles a una consultoria de RRHH que treballa per notaries i l'altre a un despatx d'advocats, la tercera tot i que no ha sigut com a PIME, ha sigut a un director tècnic d'una multinacional que ha volgut respondre els test de Cibermaduresa i CiberResiliència perquè està molt interessat en la temàtica i volia rebre nous enfocs en matèria de Ciberseguretat.

Les principals conclusions i propostes que hem recollit i que en alguns casos directament les hem aplicat i millorat als qüestionaris han sigut:

- Durada i complexitat qüestionari de Ciberresiliència. Un pel excessiva i llarga per la gran majoria de directors i caps d'empresa que no tinguin prou coneixements informàtics com per respondre exhaustivament. Ens han comentat que per la majoria de directors d'empreses podia resultar molt tècnic i difícil de contestar en 30 min.

  La solució que s'ha decidit és reduir en quantitat de preguntes el tercer test i estudiar el plantejament d'alguna de les respostes més teòriques.

- En algunes preguntes la doble negació en la pregunta i en el tipus de resposta pot comportar confusions. D'inici les preguntes als formularis s'havien plantejat així per comprovar la atenció que prestava el enquestat. En algunes preguntes per inèrcia es podria contestar a tot que SI i no volíem que fos així. No obstant es faran rectificacions en algunes preguntes.

- Les errades (o totes les que s'han detectat) que s'han trobat de tipus ortogràfic, lèxic i formal també es corregiran.

- El directiu de la multinacional ens destaca la necessitat d'ampliar detalls i recopilar més informació referent als protocols de comunicació en cas de ciberdesastre. Ens ha recomanat aclarir quins són els temps de resposta sobre els incidents. I no només als mitjans de comunicació sinó també a tots els afectats (empleats, clients, directius, inversors, etc.).

  Ha de quedar molt clar, qui, com, quan i què s'ha d'informar en tot moment. Les lleis de protecció de dades quan es tracten de dades sobre clients obliga a informar sobre quin és el grau d'afectació del incident.

- Per últim, es va detectar en algunes preguntes dels formularis que comptaven amb explicació (posterior) que aquesta havia de ser anterior a la pregunta formulada. Això s'ha corregit.

Com s'ha anticipat, un cop s'han rebut les respostes, la majoria dels principals objectius en l'obtenció de les dades s'han assolit. Es creu que amb aquesta informació obtinguda, per cada una d'aquestes empreses es pot fer una valoració força general i global del punt de partida en matèria de ciberseguretat de cara a afrontar després molts aspectes i vulnerabilitats a millorar o a tindre en compte.

És podria reflexionar, que moltes de les preguntes teòriques de coneixement amb una petita introducció explicativa que es plantegen d'inici en els formularis puguin ser prescindibles o es puguin abordar d'una altre forma. La idea, a banda de recopilar informació, és que els formularis a mode molt introductori també servissin per proporcionar i transmetre als enquestats certes nocions bàsiques dels temes que s'han de vetllar i protegir.

En base a les respostes rebudes, i basant-nos en la plantilla (punt 5.5) s'ha volgut valorar de la forma més objectiva possible. És per això que hem incorporat com a indispensable ens resums executius:

- Dades contacte, Tecnologia que disposa l'empresa, ciberincidents previs, anàlisis model TMI (Temps màxim interrupció), anàlisi model Cibermaduresa-Ciberresiliència i per últim un anàlisi breu de fortaleses i febleses. Per últim es fa una sèrie de recomanacions principals i s'adreça un missatge per possibles contactes amb empreses de CSaaS.

Ens les pàgines següents adjuntem els tres informes que hem enviat. El primer és la resposta del director d'un bufet d'advocats. No disposen de gaire tecnologia però les respostes són bastant coherents amb la seva capacitat tecnològica.

En els altres dos informes es noten els elevats coneixements informàtics dels responsables de les respostes. Tots dos aconsegueixen un alt nivell de ciberresiliència teòrica.

INFORME EXECUTIU 1 Desembre 2022

Client: XXXXXXXXXX1

Correu client: XXXXXXXX
Responsable: XXXXXXXX
Tel.Contacte: XXXXXXXX
Població/Barcelona
Sector: Jurídic

Disposen i utilitzen:

Tecnologia: *Web Hosting*, Correu Corporatiu, Teletreball, Servidors Propis, PCs propis...
Xarxes socials: *Whatsapp.*

CiberIncidents (últims 2 anys): no reporten.
Valoració **percepció estat actual Ciberseguretat** per màxim responsable: **4** (sobre 10).
Nivell **confiança digital empleats** en organització: **5** (sobre 7)
Grau **interès millora** pròpia ciberseguretat: baix/mig (en funció d'aspectes econòmics).

Resultat Model Cibermaduresa-CiberResiliencia:

CyberRookie + Medium CyberResilience**: EXPOSED – DO NOT TRUST**

Total Score CiberMadurity Test: **171/491** points

Total score CiberResilience Test: **517**/965 points

CyberResilience \ CyberMadurity	-		+
-	IN DANGER	EXPOSED	DO NOT TRUST
	EXPOSED X	PAY ATTENTION	PROTECTED
+	DO NOT TRUST X	PROTECTED	HIGH PROTECTED

IN DANGER: CyberRookie (cibernovata) + Low CyberResilience.
EXPOSED: CyberRookie + Medium CyberResilience.
EXPOSED: CyberIntermediate + Low CyberResilience.
DO NOT TRUST: CyberRookie + High CyberResilience.
DO NOT TRUST: CyberExpert + Low CyberResilience.
PAY ATTENTION: CyberIntermediate + Medium CyberResilience.
PROTECTED: CyberExpert + Medium CyberResilience.
PROTECTED: CyberIntermediate + High CyberResilience.
HIGH PROTECTED: CyberExpert + High CyberResilience.

Comentaris: Per classificació correspondria a una entitat amb situació *EXPOSED*, però tenint en compte que molts blocs de ciberseguretat (núvol, aplicacions, etc.) no se us poden aplicar per la vostra capacitat i tecnologia instal·lada, la catalogació final de la vostra organització es:
Exposed - Do Not Trust (Entitat Exposada – No us confieu).

Anàlisi TMI (Temps Màxim Interrupció) en cas de **Ciberincident**:

	Menys 4h	De 4h a 1 dia	De 1 dia a 5	Més de 5 dies
Activitat Essencial Empresa		X		
Pàgina Web				X
Correu electrònic Corporatiu	X			
Treball en Remot	X			
Recuperació Dades		X		

Comentaris: Marge hores resposta preocupant en cas de caiguda de correu i teletreball.

Anàlisi i Valoració Principals **Blocs Aplicables**:

BLOC	NOM	Score	STRONG POINTS	WEAK POINTS
4	**Aspectes Bàsics**	**52**/138	Bones polítiques backup local i remot, de destrucció de informació. Instal·lat i actiu programari antimalware, VPN, tallafocs, actualitzacions automàtiques i xifrat de dades.	Política Ciberseguretat no definida. No formació empleats en ciberseguretat. No existeix pressupost en ciberseguretat.
5	**Gestió Riscos i Dependència Tecnològica**	**76**/221	Protecció ubicació maquinari. Ús i accés personal autoritzat. Responsable informàtic subcontractat. Béns/actius activitat essencial inventariats. Ús https connexions remotes.	TMI (Temps Màxims Interrupció) perillosos.
6	**Corresponsabilitat Social**	**25**/60		Lleu conscienciació social col·lectiva
7	**Noves Tendències**		NO APLICA	NO APLICA
8	**Seguretat Infraestructura Essencial**	**32**/44	Backup, actualitzacions automàtiques i firmware, ubicació física protegida equips	
9	**Seguretat Xarxa**	**59**/95	Bona configuració router. Protecció bona davant intercepcions	
10	**Cloud Computing**		NO APLICA	NO APLICA
11	**Seguretat Aplicacions**	**99**/169	Antivirus (malware) pagament. Bona conscienciació en navegació web i ús Whatsapp.	Xifrat informació rellevant només en disc, no en documents.
12	**Seguretat Informació**	**36**/44	Molt Bon compliment RGPD	
13	**Seguretat Emmagatzematge**	**35**/44	Bon política backup en remot i local	Replicació distància no existent.
14	**Mail, virtualització, IoT, Xarxes Socials**	**169**/209	Subcontractació gestió correu corporatiu. Bona consistència ús dispositius mòbils. Teletreball OK, coneixement mínim IoT, atacs Enginyeria Social.	TMI correu electrònic crític
15	**Exploits/Vulnerabilitats**	**12**/28	Fan anàlisi possibles situacions risc.	Pla Gestió Inexistent
16	**Supervisió Contínua**	**10**/20		Pla Inexistent
17	**Gestió Incidents**	**16**/36	Si comunicarien ciberincidents si existissin. Bona ètica.	Pla inexistent
18	**Continuïtat Servei**	**3**/27		Pla Contingència Inexistent
19	**Recuperació tras el desastre**	**18**/47	Existeix Pla a nivell funcional però no en matèria ciberseguretat	Sense Pla Contingència.
20	**Formació**	**6**/36		No existent. Preocupant
21	***CSaaS***		NO APLICA	NO interès, per desconeixement.

TOP Recomanacions:

- **Crear Pla General Contingència Ciberseguretat** (Contemplarà aspectes bàsics, gestió incidents, gestió vulnerabilitats, supervisió continua, Continuïtat del Servei i Recuperació tras desastre, etc.)
- **Augment pressupost** destinat a **TI en Ciberseguretat**, amb destinació partida CSaaS.
- Fomentar augment en **formació empleats** i conscienciació corresponsabilitat social.

Empreses CSaaS Pròxim Contacte: En breu els posarem en contacte amb alguna de les empreses reconegudes en Ciberseguretat (*inteccybersecurity.com, secureit.es, idisc.com, ipdata.es, incibe.es-llistat, etc.)* amb les que col·laborem i que desenvolupen CSaaS per iniciar la seva transformació i posada en marxa del seu projecte.

GRÀCIES per la seva Confiança

INFORME EXECUTIU 2 Desembre 2022

Client: XXXXXXXXX2

Correu client: XXXXXXXX
Responsable: XXXXXXXX
Tel. Contacte: XXXXXXXX
Població/Barcelona
Sector: Consultoria

Disposen i utilitzen:

Tecnologia: *Pàgina Web, Apps pròpies,* Correu Corporatiu, Teletreball, núvol, Plataformes de visibilitat negoci. Xarxes socials: *Whatsapp, Twitter, LinkedIn, Youtube.*

CiberIncidents (últims 2 anys): no reporten.
Valoració **percepció estat actual Ciberseguretat** per màxim responsable: **8** (sobre 10).
Nivell **confiança digital empleats** en organització: **6** (sobre 7)
Grau **interès millora** pròpia ciberseguretat: baix/mig (en funció d'aspectes econòmics).

Resultat Model Cibermaduresa-CiberResiliencia:

Low-Medium CyberMaturity + High CyberResilience**: DO NOT TRUST - PROTECTED**

Total Score CiberMadurity Test: 273**/491** points

CyberResilience \ CyberMadurity	-		+
-	IN DANGER	EXPOSED	DO NOT TRUST
	EXPOSED	PAY ATTENTION	PROTECTED
+	DO NOT TRUST X	PROTECTED X	HIGH PROTECTED

Total score CiberResilience Test: 767/965 points

IN DANGER: CyberRookie (cibernovata) + Low CyberResilience.
EXPOSED: CyberRookie + Medium CyberResilience.
EXPOSED: CyberIntermediate + Low CyberResilience.
DO NOT TRUST: CyberRookie + High CyberResilience.
DO NOT TRUST: CyberExpert + Low CyberResilience.
PAY ATTENTION: CyberIntermediate + Medium CyberResilience.
PROTECTED: CyberExpert + Medium CyberResilience.
PROTECTED: CyberIntermediate + High CyberResilience.
HIGH PROTECTED: CyberExpert + High CyberResilience.

Comentaris: Segons Model, catalogació d'entitat amb una Cibermaduresa quasi mitja però en canvi destaca per una bona Ciberresiliència. Estat actual: **Protegida**, amb algunes precaucions.

Anàlisi TMI (Temps Màxim Interrupció) en cas de **Ciberincident**:

	Menys 4h	De 4h a 1 dia	De 1 dia a 5	Més de 5 dies
Activitat Essencial Empresa	X			
Pàgina Web	X			
Correu electrònic Corporatiu	X			
Treball en Remot	X			
Recuperació Dades		X		

Comentaris: TMI preocupant. Marge resposta crític en la majoria d'aspectes principals. Només una certa flexibilitat en recuperació de dades a causa de l'excel·lent política de backup de l'empresa.

Anàlisi i Valoració Principals **Blocs Aplicables**:

BLOC	NOM	Score	STRONG POINTS	WEAK POINTS
4	**Aspectes Bàsics**	**72**/138	Bones polítiques gestió contrasenyes. Compten amb Community Manager per les xarxes. Instal·lat i actiu programari antimalware, VPN, tallafocs, actualitzacions automàtiques i xifrat de dades. Destinen entre un 5-15% pressupost a l'alça cada any.	Política Ciberseguretat moderadament definida. Poca formació empleats en ciberseguretat.
5	**Gestió Riscos i Dependència Tecnològica**	**76**/221	Protecció ubicació maquinari. Ús i accés personal autoritzat. Responsable informàtic subcontractat. Béns/actius activitat essencial inventariats. Ús https connexions remotes.	TMI (Temps Màxims Interrupció) perillosos.
6	**Corresponsabilitat Social**	**40**/60	Bona percepció, col·laboren amb ecosistema	
7	**Noves Tendències**	44/72	Bona formació del CEO	
8	**Seguretat Infraestructura Essencial**	**34**/44	Backup, actualitzacions automàtiques i firmware, ubicació física protegida equips	
9	**Seguretat Xarxa**	**84**/95	Excel·lent Protecció Xarxa	
10	**Cloud Computing**	**46**/92	Bona percepció empleats cloud.	Estudi estratègia Zero Trust, i entrenar proves penetració
11	**Seguretat Aplicacions**	**119**/169	Antivirus (malware) pagament. Bona conscienciació en navegació web i ús Whatsapp. Interacció legacy controlada.	No xifrat discos.
12	**Seguretat Informació**	**38**/44	Molt Bon compliment RGPD	
13	**Seguretat Emmagatzematge**	**44**/44	Excel·lent política Backup	
14	**Mail, virtualització, IoT, Xarxes Socials**	173/209	Subcontractació gestió correu. Bona consistència ús dispositius mòbils i virtualització. Teletreball OK, coneixement elevat IoT, atacs Enginyeria Social.	TMI < 5h (Temps Màxim Interrupció) del correu electrònic crític
15	**Exploits/Vulnerabilitats**	**20**/28	Fan anàlisi possibles situacions risc i tenen un Pla.	No s'investiguen causes vulnerabilitats
16	**Supervisió Contínua**	**15**/20	Adequada Supervisió	
17	**Gestió Incidents**	**36**/36	Excel·lent gestió. Comuniquen ciberincidents si cal. Ètica OK.	
18	**Continuïtat Servei**	**27**/27	Recullen amb 3rs seus criteris.	No quadra RTO amb realitat*
19	**Recuperació tras el desastre**	**47**/47	Excel·lent previsió desastres.	
20	**Formació**	**30**/36		Millorable formació insiders
21	***CSaaS***	**54**/74	Bon Coneixement conceptual	NO APLICA

TOP Recomanacions:

- **Millorar Pla General Contingència Ciberseguretat** (Apartat gestió vulnerabilitats, supervisió continua).
- És **crític ampliar** Temps Màxim Interrupció **TMI** de totes les activitats principals.
- Fomentar augment en **formació ciberseguretat a empleats passen a ser fixos**. Reduir superfície de risc d'eines que utilitzin per evitar Enginyeria Social. Risc d'i**nsiders, sobretot** en els empleats temporals que es contracten.

Empreses CSaaS Pròxim Contacte: En breu els posarem en contacte amb alguna de les empreses reconegudes en Ciberseguretat (*inteccybersecurity.com, secureit.es, idisc.com, ipdata.es, incibe.es-llistat, etc.)* amb les que col·laborem i que desenvolupen CSaaS per iniciar la seva transformació i posada en marxa del seu projecte.

GRÀCIES per la seva Confiança

INFORME EXECUTIU 3 Desembre 2022

Client: XXXXXXXX3

Correu: XXXXXXXX
Responsable: XXXXXXXX
Tel. Contacte: XXXXXXXX
Població/Barcelona
Sector: Altres

Disposen i utilitzen:

Tecnologia: Pàgina Web, Correu Corporatiu, E-commerce, núvol. Xarxes socials: *Instagram.*

CiberIncidents (últims 2 anys): Reporten 3 incidents, un de *malware*, un de virus i un de *ransomware*. Tots els incidents solucionats abans de 6 mesos.
Valoració **percepció estat actual Ciberseguretat** per màxim responsable: **6** (sobre 10).
Nivell **confiança digital empleats** en organització: **6** (sobre 7)
Grau **interès millora** pròpia ciberseguretat: baix/mig (en funció d'aspectes econòmics).

Resultat Model Cibermaduresa-CiberResiliencia:

Low-Medium CyberMaturity + High CyberResilience**: DO NOT TRUST - PROTECTED**

Total Score CiberMadurity Test: 232**/491** points

Total score CiberResilience Test: 765/965 points

CyberResilience \ CyberMadurity	-		+
-	IN DANGER	EXPOSED	DO NOT TRUST
	EXPOSED	PAY ATTENTION	PROTECTED
+	DO NOT TRUST X	PROTECTED X	HIGH PROTECTED

IN DANGER: CyberRookie (cibernovata) + Low CyberResilience.
EXPOSED: CyberRookie + Medium CyberResilience.
EXPOSED: CyberIntermediate + Low CyberResilience.
DO NOT TRUST: CyberRookie + High CyberResilience.
DO NOT TRUST: CyberExpert + Low CyberResilience.
PAY ATTENTION: CyberIntermediate + Medium CyberResilience.
PROTECTED: CyberExpert + Medium CyberResilience.
PROTECTED: CyberIntermediate + High CyberResilience.
HIGH PROTECTED: CyberExpert + High CyberResilience.

Comentaris: Segons Model, catalogació d'entitat amb una Cibermaduresa quasi mitja però en canvi destaca per una bona Ciberresiliència. Estat actual: **Protegida**, amb algunes precaucions.

Anàlisi TMI (Temps Màxim Interrupció) en cas de **Ciberincident**:

	Menys 4h	De 4h a 1 dia	De 1 dia a 5	Més de 5 dies
Activitat Essencial Empresa				
Pàgina Web				
Correu electrònic Corporatiu		X		
Treball en Remot				
Recuperació Dades				

Comentaris: **No estipulats**. TMI indeterminat. Aspecte negatiu que no es conegui quins són els temps límits de la organització. Aquesta informació és molt rellevant per dissenyar bons plans de contingència i resiliència.

Anàlisi i Valoració Principals **Blocs Aplicables**:

BLOC	NOM	Score	STRONG POINTS	WEAK POINTS
4	**Aspectes Bàsics**	**65**/138	Bones polítiques gestió contrasenyes i de destrucció d'informació. Instal·lat i actiu programari antimalware, tallafocs, actualitzacions automàtiques.	Política Ciberseguretat no definida. Formació quasi inexistent d'empleats en ciberseguretat. No destinen Pressupost a TI
5	**Gestió Riscos i Dependència Tecnològica**	**73**/221	Protecció ubicació maquinari. Ús i accés personal autoritzat. Responsable informàtic subcontractat. Béns/actius activitat essencial inventariats. Ús https connexions remotes.	TMI (Temps Màxims Interrupció) no definits.
6	**Corresponsabilitat Social**	**50**/60	Molt Bona percepció, col·laboren amb ecosistema	
7	**Noves Tendències**	44/72	Satisfactòria formació del CEO	
8	**Seguretat Infraestructura Essencial**	**35**/44	Backup, actualitzacions automàtiques i firmware, ubicació física protegida equips	No replicació de dades a 25 Km de distància
9	**Seguretat Xarxa**	**62**/95	Bona Protecció Xarxa	
10	**Cloud Computing**	**67**/92	Bona percepció empleats cloud,	No conserven proves forenses, manca establiment Zero Trust i entrenar proves penetració.
11	**Seguretat Aplicacions**	**142**/169	Firewall operatiu. Bona conscienciació en navegació web i ús xarxes socials. Interacció legacy controlada.	No xifrat documents i carpetes.
12	**Seguretat Informació**	**41**/44	Molt Bon compliment RGPD	
13	**Seguretat Emmagatzematge**	**41**/44	Excel·lent política Backup	
14	**Mail, virtualització, IoT, Xarxes Socials**	172/209	Subcontractació gestió correu. Bona consistència ús dispositius mòbils, xarxes socials i virtualització. Coneixement significat atac Enginyeria Social.	5h < TMI < 1d (Temps Màxim Interrupció) del correu electrònic poc flexible
15	**Exploits/Vulnerabilitats**	**28**/28	Excel·lent aplicació en Pla Contingència Vulnerabilitats.	
16	**Supervisió Contínua**	**15**/20	Adequada Supervisió	
17	**Gestió Incidents**	**20**/36	Comuniquen ciberincidents si cal. Ètica OK.	És urgent, millorar política gestió incidents
18	**Continuïtat Servei**	**15**/27		No es recull RTO. Incoherències
19	**Recuperació tras el desastre**	**36**/47	No existeix Pla, però la entitat sap com abordar-ho	Falta delegació responsabilitats en cas incident
20	**Formació**	**22**/36	Bona Formació CEO.	Millorable formació insiders
21	***CSaaS***	**69**/74	Elevat coneixement conceptual	Interès neutral en fer-ho.

TOP Recomanacions:

- **Millorar Pla General Contingència Ciberseguretat** especialment els apartats de Gestió incidents, supervisió continua, continuïtat servei).
- És **crític estipular el TMI (**Temps Màxim Interrupció) de totes les activitats principals.
- Fomentar augment en **formació ciberseguretat a empleats per** reduir risc d'insiders i disminuir la superfície de risc amb les eines que s'utilitzin per evitar atacs d'Enginyeria Social.

Empreses CSaaS Pròxim Contacte: En breu els posarem en contacte amb alguna de les empreses reconegudes en Ciberseguretat (*inteccybersecurity.com, secureit.es, idisc.com, ipdata.es, incibe.es-llistat, etc.)* amb les que col·laborem i que desenvolupen CSaaS per iniciar la seva transformació i posada en marxa del seu projecte.

GRÀCIES per la seva Confiança

6 Resultats i Conclusions

Després de varies setmanes, en las que s'ha treballat de forma molt intensa i satisfactòria (a la vegada) en la creació d'aquest projecte. Feia temps que era molt car la temàtica a escollir: la *Ciberseguretat de les Pimes*. Ara arriba el moment de plantejar els resultats i les principals conclusions. Aquestes són:

- **Factor humà**: és un component crític, i el punt de partida es clarísssim... la formació i el coneixement en Ciberseguretat és primordial. S'ha d'incidir inicialment en una tasca de convenciment del seus màxims directius o responsables per aconseguir que després arribi de forma transversal a tota la organització. Molts dels ciberincidents que es produeixen provenen d'actuacions premeditades o desafortunades d'*insiders*.

- **Factor recursos econòmics**: tenim prou dades i inputs com per demostrar una de les premisses del punt Introducció: les empreses que més pressupost destinen respecte a la seva despesa en TI tenen millor expectativa de Resistència a Ciberincidents i un potencial més elevat d'arribar a tindre un grau de cibermaduresa considerat ciberexpert.

- **Aposta pel futur**: Introduirem per analitzar i presentar als clients un model *Hype Cycle (Gartner)* per demostrar que la majoria de tecnologies que eren de futur fa (entre dos i cinc anys) son d'un present ben marcat. Per tant, les nostres propostes de futur actuals tenen una elevada probabilitat d'encert que siguin protagonistes en el futur: **CSaaS, es la principal**.

- **Factor temps**: Primordial i crític, s'han analitzat conceptes com RTO, TMI, MTMP que no deixen de ser senyals inequívoques que una bona preparació i capacitació global en altres aspectes relaciona clarament que aquests temps es redueixin o siguin superiors.

- **Factor Corresponsabilitat social**: Una col·laboració intensa amb l'ecosistema que rodeja la PIME assegura a l'empresa un bon status i una bona predisposició per la societat a revertir i correspondre aquest "altruisme i generositat". Les empreses més actives en aquest aspecte són les empreses més valuoses.

Es creu que la majoria dels criteris i objectius formulats a la introducció s'han assolit. Es partia d'una idea molt modesta però sincera dels mitjans amb els que es comptàvem però també teníem molt clar en quins tipus d'entitats podíem impactar. Les poques proves de camp efectuades ens ho han demostrat. Si es pensa que s'ha arribat a les fites marcades al principi és pels següents motius:

- S'ha efectuat amb paràmetres realistes un anàlisi exhaustiu dels principals riscos en seguretat informàtica de les pimes (1r objectiu).

- Es plantegen escenaris i el treball s'enfoca en tot moment seguint la línia marcada pels principals indicadors digitals per mesurar aspectes de la seguretat informàtica com també de la confiança digital (2n i 3r objectiu).

- Tenim una certesa superior respecte a l'inici del treball que la relació causa-efecte *més inversió en ciberseguretat implica millor protecció*.

- S'ha construït una eina en forma de formulari i feedback, amb uns models de cibermaduresa-ciberresiliència i anàlisi dels TMI, que ens han ajudat a implementar tota una sèrie de preguntes i qüestions per respondre a tots els altres objectius.

Pel que respecta a la metodologia i la planificació temporal del projecte, ha sigut bona i no hi han hagut desviacions importants. És cert, que en la tercera entrega sí que ha requerit més temps del previst perquè s'ha necessitat un temps addicional per aconseguir les respostes reals d'empreses a les Proves de camp. No era una tasca planificada d'inici, però comptar amb elles ha donat més solidesa i verificació "de mercat" al projecte.

L'anàlisi final als dimensionaments **CCGS,** conclou que no es té la percepció que amb l'elaboració d'aquest projecte s'hagin mitigat aspectes de *sostenibilitat*, no obstant, sí que contínuament, en la seva execució s'ha sigut molt respectuós amb el compliment dels criteris de *diversitat*. Per últim, es confirma, tal com a la introducció inicial es contemplava, un impacte positiu en el criteri *ètic-social*, al cercar una idea *noble* d'ajuda en entitats sense recursos.

Ha aparegut un altre criteri *ètic-social* (no previst) amb un impacte positiu. Es tracta de la capacitat per fer reflexionar i conscienciar a les empreses que han patit ciberincidents que la millor opció és informar del fets. Malauradament molts delictes detectats no s'han publicat per por a conseqüències legals i reputacionals. Fer-ho és un tema ètic, social i regulat per llei. En base al nostre model qualsevol canvi en les actituds del client vers a aquest tema és un èxit.

La veritat, és que no hi ha hagut una gran sorpresa en els resultats obtinguts. Es sabia què és el que es perseguia amb aquest projecte i la informació extreta de les xarxes i les respostes rebudes amb els formularis aplicats a empreses reals ens confirmen el que es plantejava d'inici: manca una preocupant millora i actualització en la matèria en la majoria de casos.

La principal línia de treball futur que ha quedat pendent d'explorar és justament l'acompliment del principal objectiu d'aquest projecte: convèncer a les empreses sense suficients recursos propis (econòmics i en temps) d'adoptar la estratègia de Ciberseguretat com a servei com una solució òptima per els seus interessos. Nosaltres actuem com consultaria intermediària.

Tot i què el nostre projecte ha posat la part prèvia d'estudi i conscienciació, precisament ens ha faltat comprovar l'acceptació per part d'empreses proveïdores que ja desenvolupen aquest servei i quina és la seva predisposició a treballar amb un projecte (el nostre) de captació d'empreses que vulguin estar assessorades i rebin després els seus serveis per millorar la seva resistència a ciberincidents.

7 Glossari

PIME: Petita i Mitjana Empresa
RANSOMWARE: atac molt temut consistent en el segrest de dades.
CIBERSEGURETAT: Seguretat informàtica
CIBERNOVATA: Amb molt poca experiència en Ciberseguretat.
CIBEREXPERT: Amb molta experiència en Ciberseguretat.
CIBERRESILIÈNCIA: Capacitat d'una organització per evitar ciberincidents, resistir-los i recuperar-se més tard.
CIBERMADURESA: Grau de evolució i maduresa d'una entitat en aspectes de seguretat informàtica.
STARTUP: Empresa de nova creació amb gran potencial de creixement.
INCIBE: Institut Nacional de Ciberseguretat.
INE: Institut Nacional Estadística
I+D: Investigació i Desenvolupament
ONTSI: Observatori Nacional de Tecnologia i Societat
DIAGRAMA DE GANTT: Eina gràfica de planificació temporal de projectes.
SMEs: Small and Medium-sized enterprises (PIMEs).
GDP: Gross Domestic Product, el que aquí coneixem com a PIB.
IoT: Internet of Things
CCN-CERT: Centre Criptològic Nacional Centre Resposta.
PHISHING: Tècniques que utilitzen Enginyeria Social per utilitzar engany.
MALWARE: Programari maliciós que actua sense que la víctima tingui coneixement.
DDoS: Distributed Denial of Service. Atac per causar indisponibilitat d'actius.
INJECCIONS SQL: Infiltració codi maliciós aprofitant una vulnerabilitat.
DOXXING: Obtenció informació privada per fer-la pública extorsionant víctima.
DEFACEMENT: Atac per desconfiguracions de la web.
VPN: Virtual Private Network
DBIR: Data Breach Information Report
ENGINYERIA SOCIAL: Manipulació psicològica per fer aprofitar-se amb accions delictives.
SPOOFING: Suplantació Identitat
BACKDOOR: Porta del darrera per evitar seguretat.
UAB: Universitat Autònom Barcelona
CRYPTOJACKING: Criptomineria.
SUPPLY CHAIN: Cadena Subministrament, des d'inici comanda client fins l'entrega.
TIC: Tecnologies de la Informació i Comunicació.
FAKE NEWS: Notícies falses.
INSIDER: Atac premeditat o (desgraciat) realitzat a través de personal intern de l'empresa.
HOR (Human Operated Ransonware): xifra discos víctima per demanar rescat.
BEC (Business E-mail Compromise): Atac Enginyeria Social
5G: Cinquena Generació Telefonia.
RAAS: Ransomware as a Service:
RYUK: Tipus Ransomware dirigit a entitats públiques.
ROBIN HOOK: Modalitats d'atac de tipus RaaS.
AVADDON: Modalitats d'atac de tipus RaaS.
EMEA: Europe Middle East Africa
NETWALKER: modalitat d'atac de tipus RaaS.
MAZE: modalitat atac de tipus RaaS.
SNAKE LOCKER: modalitat atac de tipus RaaS.
CRYPTOCURRENCIE: criptomoneda, es mitjà intercanvi digital que utilitza criptografia.

PHARMING: modalitat phishing amb redirecció trànsit web a lloc fraudulent.
MAAS: Malware as a Service
RUBYMINER: modalitat de crypto malware.
WANNAMINE: modalitat de crypto malware.
LUCIFER: modalitat de crypto malware.
XMRIG: modalitat de crypto malware.
JSECOIN: modalitat de crypto malware.
TROIÀ: fragment codi aparentment inofensiu però en realitat es tracta de malware.
SPEAR PHISHING: modalitat phishing (mitjançant correu) obtenen informació client.
CEO: Chief Executive Officer. Es conegut estafa frau del CEO.
HAAS: Hacking as a Service.
E-SPORT: Competicions videojocs digitals.
CYBERBULLILNG: assetjament a través de les xarxes.
GROOMING: assetjament i abús sexual online.
SEXTING: enviament missatges sexuals a través dels smartphones.
SEXTORSIÓ: xantatge mitjançant sexting.
VECTOR ATAC: mètode que utilitza una amenaça per atacar un sistema.
VISHING: ús de la telefonia per fer atacs de phishing.
DATALEAK: fugida de dades.
DARK WEB: contingut World Wide Web en zones fosques.
BOTNET: conjunt de robots o bots que s'executen de forma automàtica en forma d'atac.
EMOTET: modalitat d'atac Botnet
TRICKBOT: modalitat d'atac Botnet
DRIDEX: modalitat d'atac Botnet
BITPAYMER: modalitat d'atac Botnet.
WANNACRY: Modalitat d'atac Ransomware.
RDP: Remote Desktop Protocol
MSP: Manage Service Providers
TI: Tecnologia d'Informació.
EXPLOIT: Vulnerabilitat.
SPAM: Correu brossa
IPSTORM: modalitat d'atac Botnet.
MATRIOSH: modlaitat d'atac Ransomware
STEALER AGENTS: codi maliciós de tipus troià.
LOTL (Living off the Land): tipus de ciberatac utilitzant programari legítim.
POWERSHELL: Interfície de consola per escriure comandes e instruccions.
FILELESS MALWARE: Ciberatac que es basa en la memòria RAM víctima atac.
TURLA: malware basat en .NET
WEBSHELLS: Interfície similar a Shell per remotament atacar servidor web.
FRAMEWORK: entorn de treball.
MALWARE LIGHTSPY: vulnerabilitats per al sistema operatiu IOS.
ZOOM: Programari de videotelefonia.
CMS (Content Management System): Gestor Continguts.
SOAR: Security Orchestration, Automation and Response.
SMISHING: Atac Enginyeria Social mitjançant SMSs telefònics.
USB: Universal Serial Bus.
SPYWARE: malware específic d'espionatge d'un equip o sistema.
ATAC FORÇA BRUTA: recuperar un clau intentant totes les combinacions.
CUC: subtipus de malware que infecta replicant-se contínuament.
ROOTKIT: programari maliciós que permet accedir a privilegis en un PC.
BAITING: atac d'Enginyeria Social que consisteix en una "oportunitat" falsa.
CVE (Common Vulnerabilities and Exposoures): llista exploits coneguts.
ECOSISTEMA: comunitat de dispositius, programari i altres que envolta un dispositiu.
2FA: Sistema Verificació en 2 passes.

CERTIFICAT SSL: certificat digital d'autentificació.
E-COMMERCE: compra i béns per Internet.
PROTOCOL HTTPS (Hypertext Transfer Protocol Secure).
CSAAS: Cibersecurity as a Service.
DLL SIDE-LOADING: ciberatac que utilitza el mecanisme de Windows DLL search order.
KEYWORDS: paraules clau.
(DoH) DNS over Https: protocol seguretat per realitzar resolució remota a t. Https.
MACRO: conjunt d'instruccions que es configuren mitjançant aplicacions ofimàtiques.
LOPD: Llei Orgànica Protecció Dades.
WI-FI: tecnologia que permet la connexió sense fils de dispositius electrònics.
TARGET: objectiu
MAN-IN-THE-MIDDLE: En criptografia, atac que permet adquirir la capacitat de llegir, insertar i modificar a voluntat.
NIST : National Institute of Standards of Technology
CLOUD: Núvol
FEEKBACK: Report
LEGACY: Programari Antic que conviu amb nous sistemes.
SUPERAPP: superaplicació que permet multiples serveis.
REPOSITORI: espai centralitzat on s'enmmagatzema, organitza... informació digital.
PATCH: Parche:
KNOW-HOW: actiu intangible, que pot ser el bé més valuós d'una empresa.
PIN: Personal Identification Number
PASSPHRASE: contrasenya en forma de frase.
PASSWORDLESS: autentificació sense contrasenya.
ML: Machine Learning.
BLOCKCHAIN: cadena de blocs.
TIMING: organitzar, planificar i desenvolupar en base a temps.
PENTESTING: atacs simulats dirigits a trobar les vulnerabilitats de qui es testeja.
PASSWORD SPRAYING ATTACK: Polvorització Contrasenyes.
JAILBREAKING: procés de suprimir les limitacions imposades per Apple.
MENTORING: relacions de desenvolupament personal.
BUG BOUNTY: programa de recompenses.
EDGE COMPUTING: execució de processos o gestió de dades en lloc físic.
RTO: temps objectiu de recuperació.
GOOGLE SHEET: Fulla de càlcul grup Google.
GOOGLE FORMS: Formularis del grup Google.
TMI: Temps Màxim Interrupció.
HYPE CYCLE: model de cicle de sobre expectació del grup Gartner.
DSAAS: Disaster as a Service.
FAAS: Firewall As a Service.
ZTNA: Zero Trust Network Access. Estratègia de seguretat de xarxa.
SIEM Security Information and Event Management.
CCEG: Competència de Compromís Ètic i Global.

8 Bibliografia

[1] Annual report on European SMEs 2020/2021 : digitalisation of SMEs : background document. [en línea], (sin fecha). *Home - Publications Office of the EU*. [Consultado el 23 de octubre de 2022]. Disponible en: https://op.europa.eu/es/publication-detail/-/publication/849659ce-dadf-11eb-895a-01aa75ed71a1

[2] SMEs [en línea], (sin fecha). *Internal Market, Industry, Entrepreneurship and SMEs*. [Consultado el 23 de octubre de 2022]. Disponible en: https://single-market-economy.ec.europa.eu/smes_en#:~:text=Small%20and%20medium-sized%20enterprises%20(SMEs)%20are%20the%20backbone,every%20sector%20of%20the%20economy.

[3] *Dirección General de Industria y de la Pequeña y Mediana Empresa*. [Consultado el 23 de octubre de 2022]. Disponible en: http://www.ipyme.org/es-ES/DatosPublicaciones/Documents/Guia-usuario-Definicion-PYME.pdf

[4] *Dirección General de Industria y de la Pequeña y Mediana Empresa*. [Consultado el 21 de octubre de 2022]. Disponible en: http://www.ipyme.org/es-ES/ApWeb/EstadisticasPYME/Documents/CifrasPYME-septiembre2022.pdf

[5] SMEs in the EU 2022, by size | Statista [en línea], (sin fecha). *Statista*. [Consultado el 23 de octubre de 2022]. Disponible en: https://www.statista.com/statistics/878412/number-of-smes-in-europe-by-size/

[6] Pymes. Motor económico de España [en línea], (sin fecha). *CEMAD*. [Consultado el 23 de octubre de 2022]. Disponible en: https://www.cemad.es/pymes-motor-economico-espana/

[7] Fernando, J., (2003). Gross Domestic Product (GDP): Formula and How to Use It [en línea]. *Investopedia*. [Consultado el 23 de octubre de 2022]. Disponible en: https://www.investopedia.com/terms/g/gdp.asp

[8] SMEs in the EU 2022, by size | Statista [en línea], (sin fecha). *Statista*. [Consultado el 23 de octubre de 2022]. Disponible en: https://www.statista.com/statistics/878412/number-of-smes-in-europe-by-size/

[9] ¿Qué es la ciberseguridad? [en línea], (sin fecha). *latam.kaspersky.com*. [Consultado el 25 de octubre de 2022]. Disponible en: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

[10] Estudio cocktail analysis 2019-2020 [Consultado el 26 de Octubre de 2022] Disponible en: https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama -actual-de-la-ciberseguridad-en-Espana.pdf

[11] No hay víctimas pequeñas para los cibercriminales [en línea], (sin fecha). *www.kaspersky.es*. [Consultado el 26 de octubre de 2022]. Disponible en: https://www.kaspersky.es/about/press-releases/2017_no-small-victims-for-cybercriminals

[12] Ciberseguridad. ¿Por qué las pymes sufren la mayor parte de los ataques informáticos? [en línea], (sin fecha). *Finanzarel*. [Consultado el 1 de noviembre de 2022]. Disponible en: https://www.finanzarel.com/blog/ciberseguridad-pymes-sufren-la-mayor-parte-de-los-ataques-informaticos/

[13] *CCN-CERT*. [Consultado el 2 de noviembre de 2022]. Disponible en: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/5377-ccn-cert-ia-13-20-ciberamenazas-y-tendencias-edicion-2020/file.html

[14] (sin fecha). *CCN-CERT*. [Consultado el 2 de noviembre de 2022]. Disponible en: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/6338-ccn-cert-ia-13-21-ciberamenazas-y-tendencias-edicion-2021-1/file.html

[15] Informe de Ciberpreparación de Hiscox 2022 | Hiscox España [en línea], (sin fecha). *Hiscox España | Seguros especializados para empresas, hogar y arte*. [Consultado el 2 de noviembre de 2022]. Disponible en: https://www.hiscox.es/informe-de-ciberpreparacion-de-hiscox-2022

[16] Informe de Oxford Internet Institute 2019 | The Global Disinformation Order [Consultado el 3 de noviembre de 2022]. Disponible en: https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1209&context=scholcom

[17] Informe Oxford Internet Institute 2020 | 2020 Global Inventory of Organized Social Media Manipulation [Consultado el 03 de noviembre de 2022]. Disponibe en: https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/127/2021/02/CyberTroop-Report20-Draft9.pdf

[18] Informe Verizon 2019 | Data Breach Investigations Report [Consultado el 4 de noviembre de 2022]. Disponible en: https://www.verizon.com/business/resources/reports/2019/2019-data-breach-investigations-report.pdf

[19] Check Point Research | Cyber Security Report 2021 [Consultado el 4 de novembre de 2022]. Disponible en: https://www.checkpoint.com/downloads/resources/cyber-security-report-2021.pdf

[20] Fraude del CEO |Europol [Consultado el 4 de novembre de 2022]. Disponible en: https://www.europol.europa.eu/sites/default/files/documents/es_1.pdf

[21] Seibt, S., (2019). La police allemande démantèle Wall Street Market, empire de la vente de drogue en ligne [en línea]. *France 24*. [Consultado el 5 de noviembre de 2022]. Disponible en: https://www.france24.com/fr/20190506-darknet-wall-street-market-arrestation-drogue-arme-internet-supermarche

[22] Top Ransomware Attacks [en línea], (sin fecha). *usa.kaspersky.com*. [Consultado el 5 de noviembre de 2022]. Disponible en: https://usa.kaspersky.com/resource-center/threats/top-ransomware-2020

[23] Botnet [en línea], *INCIBE*. [Consultado el 5 de noviembre de 2022]. Disponible en: https://www.incibe.es/aprendeciberseguridad/botnet

[24] *Leaders in IP and domain reputation data | Spamhaus Technology*. [Consultado el 5 de noviembre de 2022]. Disponible en: https://www.spamhaus.com/custom-content/uploads/2020/04/2019-Botnet-Threat-Report-2019-LR.pdf

[25] *Advancing IT, Audit, Governance, Risk, Privacy & Cybersecurity | ISACA*. [Consultado el 7 de noviembre de 2022]. Disponible en: https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2021/volume-6/building-a-maturity-model-for-cobit-2019-based-on-cmmi-joa-spa-1221.pdf?la=es-es

[26] SABSA Executive Summary - The SABSA Institute [en línea], . *The SABSA Institute*. [Consultado el 7 de noviembre de 2022]. Disponible en: https://sabsa.org/sabsa-executive-summary/

[27] *Una Unión que resiste mejor a los ciberataques:El Consejo confirma un acuerdo sobre la certificación común y sobre una agencia reforzada*. (s. f.). Home - Consilium. [Consultado el 10 de noviembre de 2022]. Disponible en: https://www.consilium.europa.eu/es/press/press-releases/2018/12/19/eu-to-become-more-cyber-proof-as-council-backs-deal-on-common-certification-and-beefed-up-agency/

[28] *BOE.es - BOE-A-2018-12257 Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.* (s. f.). BOE.es - Agencia Estatal Boletín Oficial del Estado. [Consultado el 10 de noviembre de 2022]. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2018-12257

[29] *BOE.es - BOE-A-2018-12257 Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.* (s. f.). BOE.es - Agencia Estatal Boletín Oficial del Estado. [Consultado el 10 de noviembre de 2022]. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2018-12257

[30] ¿Hacia dónde va la seguridad cibernética? [en línea], *KIO Networks : Home ES*. [Consultado el 11 de noviembre de 2022]. Disponible en: https://www.kionetworks.com/blog/ciberseguridad/hacia-donde-va-la-seguridad-cibernetica

[31] Hacia dónde va la ciberseguridad: tendencias y retos | Ciberseguridad LATAM [en línea], *Ciberseguridad LATAM*. [Consultado el 10 de noviembre de 2022]. Disponible en: https://www.ciberseguridadlatam.com/2022/07/11/hacia-donde-va-la-ciberseguridad-tendencias-y-retos/

[32] ¿Qué es la ciberseguridad? | IBM [en línea], (sin fecha). *IBM - Deutschland | IBM*. [Consultado el 10 de noviembre de 2022]. Disponible en: https://www.ibm.com/es-es/topics/cybersecurity

[33] IBM Security X-Force Threat Intelligence Index [en línea], (sin fecha). *IBM - Deutschland | IBM*. [Consultado el 10 de noviembre de 2022]. Disponible en: https://www.ibm.com/reports/threat-intelligence/es-es/#malware

[34] Cyber Resilient Organization Study 2021 | IBM [en línea], (sin fecha). *IBM*. [Consultado el 11 de noviembre de 2022]. Disponible en: https://www.ibm.com/resources/guides/cyber-resilient-organization-study/

[35] Fortalecer Cloud [en línea], (sin fecha). *IBM - Deutschland | IBM*. [Consultado el 11 de noviembre de 2022]. Disponible en: https://www.ibm.com/downloads/cas/WMDZOWK6

[36] Las 8 principales predicciones de ciberseguridad para 2021-2022 [en línea], (sin fecha). *Gartner*. [Consultado el 11 de noviembre de 2022]. Disponible en: https://www.gartner.es/es/articulos/las-8-principales-predicciones-ciberseguridad-para-2021-2022

[37] Las 10 tendencias en ciberseguridad que marcarán el 2021 [en línea], (sin fecha). *Deloitte Chile*. [Consultado el 11 de noviembre de 2022]. Disponible en: https://www2.deloitte.com/cl/es/pages/risk/articles/diez-tendencias-ciberseguridad-2021.html

[39] Image Cabecera. Banco Imágenes Gratuito [en línea], (sin fecha). [Consultado el 20 de noviembre de 2022]. Disponible en: https://cdn.pixabay.com/photo/2017/10/26/11/21/ssl-2890762_960_720.jpg

[40] Agencia Tributaria: Personal asalariado (casillas 00041 y 00042) [en línea], (sin fecha). *Agencia Tributaria: Inicio*. [Consultado el 22 de noviembre de 2022]. Disponible en: https://sede.agenciatributaria.gob.es/Sede/ayuda/manuales-videos-folletos/manuales-practicos/manual-sociedades-2021/capitulo-2-identificac-autoliq-compl-incn/personal-asalariado-casillas-00041-00042.html

[41] ▷ Cómo afecta la LOPD en tu estrategia de captación de leads | Roiting [en línea], (imatge). *Roiting*. [Consultado el 26 de noviembre de 2022]. Disponible en: https://www.roiting.com/blog/gdpr/

[42] imagenes publicas percepciones - Google Suche [en línea], (sin fecha). *https://www.google.com/*. [Consultado el 26 de noviembre de 2022]. Disponible en: https://www.google.com/search?q=imagenes+publicas+percepciones&tbm=isch&ved=2ahUKEwiX6bLby8z7AhUUw4UKHVTKAhAQ2-cCegQIABAA&oq=imagenes+publicas+percepciones&gs_lcp=CgNpbWcQAzoECCMQJzoGCAAQCBAeOggIABAIEAcQHlDyB1jFFWDZFmgAcAB4AIABZ4gB0AaSAQM5LjG

YAQCgAQGqAQtnd3Mtd2l6LWltZ8ABAQ&sclient=img&ei=XGqCY5fLCZSGlwTUlluAAQ&bih=969&biw=1920&rlz=1C5CHFA_enES819ES819#imgrc=vHcpxP1bBcZsLM

[43] ¿Qué es la confianza digital? [en línea], (sin fecha). *CSO España | Información y recursos para el responsable de seguridad*. [Consultado el 27 de noviembre de 2022]. Disponible en: https://cso.computerworld.es/tendencias/que-es-la-confianza-digital

[44] La nueva sensación: Confianza Digital para interacciones en el Entorno Digital | Cecilia Kahn - IUS 360 [en línea], (sin fecha). *IUS 360*. [Consultado el 27 de noviembre de 2022]. Disponible en: https://ius360.com/la-nueva-sensacion-confianza-digital-para-interacciones-en-el-entorno-digital/

[45] Toledo, R., (2022). Avances de la ciberseguridad en España: últimas novedades [en línea]. *Web corporativa de Grupo Cibernos. Presentación.* [Consultado el 3 de diciembre de 2022]. Disponible en: https://www.grupocibernos.com/blog/avances-de-la-ciberseguridad-en-espana-ultimas-novedades

[46] Cybersecurity [en línea], (sin fecha). *NIST*. [Consultado el 3 de diciembre de 2022]. Disponible en: https://www.nist.gov/cybersecurity

[47] Ramiro, R., (2018). Cómo implantar el Framework NIST [en línea]. *CIBERSEGURIDAD .blog*. [Consultado el 3 de diciembre de 2022]. Disponible en: https://ciberseguridad.blog/como-implantar-el-framework-nist/

[48] Ramiro, R., (2018a). Cómo implantar el Framework NIST [en línea]. *CIBERSEGURIDAD .blog*. [Consultado el 3 de diciembre de 2022]. Disponible en: https://ciberseguridad.blog/como-implantar-el-framework-nist/

[49] Contributors to Wikimedia projects, (2010). Intercepció - Viquipèdia, l'enciclopèdia lliure [en línea]. *Viquipèdia*. [Consultado el 3 de diciembre de 2022]. Disponible en: https://ca.wikipedia.org/wiki/Intercepció

[50] Els atacs Man in the Middle - Efimatica [en línea], (sin fecha). *Efimatica*. [Consultado el 3 de diciembre de 2022]. Disponible en: https://www.efimatica.com/man-in-the-middle/

[51] Cloud Computing: Que és, característicasy ventajas [en línea], (sin fecha). *OpenWebinars.net*. [Consultado el 4 de diciembre de 2022]. Disponible en: https://openwebinars.net/blog/cloud-computing-que-es-caracteristicas-y-ventajas/

[52] ¿Qué es una superapp? [en línea], (sin fecha). *Gartner*. [Consultado el 4 de diciembre de 2022]. Disponible en: https://www.gartner.es/es/articulos/que-es-una-superapp

[53] Reforzar la ciberseguridad y la resiliencia en toda la UE: acuerdo provisional entre el Consejo y el Parlamento Europeo [en línea], (sin fecha). *Home - Consilium*. [Consultado el 5 de diciembre de 2022]. Disponible

en: https://www.consilium.europa.eu/es/press/press-releases/2022/05/13/renforcer-la-cybersecurite-et-la-resilience-a-l-echelle-de-l-ue-accord-provisoire-du-conseil-et-du-parlement-europeen/

[54] Cumplimiento Legal [en línea], (sin fecha). *INCIBE*. [Consultado el 5 de diciembre de 2022]. Disponible en: https://www.incibe.es/protege-tu-empresa/que-te-interesa/cumplimiento-legal

[55] ¿Cómo puedo participar en un Bug Bounty? ¿Merecen la pena las recompensas? [en línea], (sin fecha). *RedesZone*. [Consultado el 6 de diciembre de 2022]. Disponible en: https://www.redeszone.net/tutoriales/seguridad/participar-bug-bounty-recompensas/

[56] Mentoring – Escuela de Mentoring. Gen Consulting Desarrollo de Proyectos [en línea], (sin fecha). *Escuela de Mentoring. Gen Consulting Desarrollo de Proyectos – Pioneros en la mentorización como primera empresa Española certificada en este área*. [Consultado el 6 de diciembre de 2022]. Disponible en: https://www.escueladementoring.com/mentoring/

[57] ciberseg1922, (2022). Todo lo que debes saber sobre la Ciberseguridad como servicio (CSaaS) [en línea]. *Ciberseguridad*. [Consultado el 7 de diciembre de 2022]. Disponible en: https://ciberseguridad.com/guias/recursos/ciberseguridad-como-servicio-csaas/

[58] Cybersecurity [en línea], (sin fecha). *Translation and IT Services Agency | iDISC*. [Consultado el 20 de diciembre de 2022]. Disponible en: https://www.idisc.com/en/it-services/cybersecurity

[59] Empresa de seguridad informática y de la información · Secure&IT [en línea], (sin fecha). *Secure&IT*. [Consultado el 20 de diciembre de 2022]. Disponible en: https://www.secureit.es

[60] IPDATA Solutions Cisco Partner [en línea], (sin fecha). *IPDATA*. [Consultado el 20 de diciembre de 2022]. Disponible en: https://www.ipdata.es

[61] Intec [en línea], (sin fecha). *Intec*. [Consultado el 20 de diciembre de 2022]. Disponible en: https://inteccybersecurity.com

[62] Hype Cycle | Gartner | España [en línea], (sin fecha). *Gartner*. [Consultado el 24 de diciembre de 2022]. Disponible en: https://www.gartner.es/es/metodologias/hype-cycle#:~:text=El%20Hype%20Cycle%20de%20Gartner%20es%20una%20representación%20gráfica%20en,reales%20y%20aprovechar%20nuevas%20oportunidades.

[63] Colaboradores de los proyectos Wikimedia, (2009). Gartner (empresa) - Wikipedia, la enciclopedia libre [en línea]. *Wikipedia, la enciclopedia libre*. [Consultado el 30 de diciembre de 2022]. Disponible en: https://es.wikipedia.org/wiki/Gartner_(empresa)

[64] Vivantic, (2017). Como crear una tabla de ilustraciones en Word (Paso a Paso) [en línea]. *YouTube*. [Consultado el 1 de enero de 2023]. Disponible en: https://www.youtube.com/watch?v=fNSKs6zzXko

[65] Carlos Pérez del Molino, (sin fecha-c). Gartner y el futuro de Blockchain [en línea]. *We facilitate the digital transformation of organizations - Izertis*. [Consultado el 1 de enero de 2023]. Disponible en: https://www.izertis.com/es/-/blog/gartner-y-el-futuro-de-blockchain

[66] 5 Strategic Technologies On The Gartner Hype Cycle For Midsize Enterprises 2018 [en línea], (sin fecha). *Gartner*. [Consultado el 1 de enero de 2023]. Disponible en: https://www.gartner.com/smarterwithgartner/5-strategic-technologies-on-the-gartner-hype-cycle-for-midsize-enterprises-2018

[67] 5 Strategic Technologies On The Gartner Hype Cycle For Midsize Enterprises 2018 [en línea], (sin fecha-b). *Gartner*. [Consultado el 1 de enero de 2023]. Disponible en: https://www.gartner.com/smarterwithgartner/5-strategic-technologies-on-the-gartner-hype-cycle-for-midsize-enterprises-2018

[68] 3 Major Trends Drive the Gartner Hype Cycle for Midsize Enterprises, 2019 [en línea], (sin fecha). *Gartner*. [Consultado el 1 de enero de 2023]. Disponible en: https://www.gartner.com/smarterwithgartner/3-major-trends-drive-gartner-hype-cycle-midsize-enterprises-2019

[69] 3 Themes Emerge From the Gartner Hype Cycle for Midsize Enterprise, 2020 [en línea], (sin fecha). *Gartner*. [Consultado el 1 de enero de 2023]. Disponible en: https://www.gartner.com/smarterwithgartner/3-themes-emerge-from-the-gartner-hype-cycle-for-midsize-enterprise-2020

[70] hype cycle for midsize enterprises - Buscar con Google [en línea], (sin fecha). *Google*. [Consultado el 1 de enero de 2023]. Disponible en: https://www.google.com/search?q=hype+cycle+for+midsize+enterprises&tbm=isch&ved=2ahUKEwiXgaeLo5L8AhX4RaQEHeCcA4MQ2-cCegQIABAA&oq=hype+cycle+&gs_lcp=CgNpbWcQARgAMgQIIxAnMgQIIxAnMgUIABCABDIFCAAQgAQyBQgAEIAEMgUIABCABDIFCAAQgAQyBQgAEIAEMgUIABCABDIFCAAQgAQ6BAgAEB46BggAEAUQHjoGCAAQCBAeUM4SWPIaYKU3aABwAHgAgAFKiAGRBJIBATiYAQCgAQGqAQtnd3Mtd2l6LWltZ8ABAQ&sclient=img&ei=APOmY5eBHPiLkdUP4LmOmAg&bih=969&biw=1905&rlz=1C5CHFA_enES819ES819&hl=es#imgrc=zQk668IFuL6MWM

[71] Top Trends In The Gartner Hype Cycle For Emerging Technologies 2017 [en línea], (sin fecha). *Gartner*. [Consultado el 1 de enero de 2023]. Disponible en: https://www.gartner.com/smarterwithgartner/top-trends-in-the-gartner-hype-cycle-for-emerging-technologies-2017

[72] Las 5 tendencias en el Hype Cycle de tecnologías emergentes 2018 de Gartner [en línea], (sin fecha). *smartlighting*. [Consultado el 1 de enero de 2023]. Disponible en: https://smart-lighting.es/tendencias-tecnologias-emergentes-2018-gartner/

[73] 5 Trends Appear On The Gartner Hype Cycle For Emerging Technologies 2019 [en línea], (sin fecha). *Gartner*. [Consultado el 1 de enero de 2023]. Disponible en: https://www.gartner.com/smarterwithgartner/5-trends-appear-on-the-gartner-hype-cycle-for-emerging-technologies-2019

[74] 5 tendencias impulsan el Hype Cycle de Gartner para tecnologías emergentes de 2020 [en línea], (sin fecha). *Gartner*. [Consultado el 1 de enero de 2023]. Disponible en: https://www.gartner.es/es/articulos/5-tendencias-impulsan-hype-cycle-gartner-para-tecnologias-emergentes-2020

[75] Tres tendencias por descubrir en el Hype Cycle de Gartner para las tecnologías emergentes de 2021 [en línea], (sin fecha). *Gartner*. [Consultado el 1 de enero de 2023]. Disponible en: https://www.gartner.es/es/articulos/tres-tendencias-por-descubrir-en-el-hype-cycle-para-las-tecnologias-emergentes-2021

[76] Novedades del Hype Cycle de Gartner de 2022 para las tecnologías emergentes [en línea], (sin fecha). *Gartner*. [Consultado el 1 de enero de 2023]. Disponible en: https://www.gartner.es/es/articulos/novedades-del-hype-cycle-de-gartner-para-las-tecnologias-emergentes-2022

[77] Blockchain Technology & How it Helps Business Growth | Gartner [en línea], (sin fecha). *Gartner*. [Consultado el 1 de enero de 2023]. Disponible en: https://www.gartner.com/en/information-technology/insights/blockchain

[78] Gartner blockchain hype cycle: Crypto trading only killer use case - Ledger Insights - blockchain for enterprise [en línea], (sin fecha). *Ledger Insights - blockchain for enterprise*. [Consultado el 1 de enero de 2023]. Disponible en: https://www.ledgerinsights.com/gartner-blockchain-web3-hype-cycle/

[79] Carlos Pérez del Molino, (sin fecha). Gartner y el futuro de Blockchain [en línea]. *We facilitate the digital transformation of organizations - Izertis*. [Consultado el 1 de enero de 2023]. Disponible en: https://www.izertis.com/es/-/blog/gartner-y-el-futuro-de-blockchain

[80] Gartner - hype cycle for blockchain [en línea], (sin fecha). *Fast and Reliable Blockchain Infrastructure Provider - Chainstack*. [Consultado el 1 de enero de 2023]. Disponible en: https://pages.chainstack.com/hype-cycle-for-blockchain-technologies-2020

[81] Five Biggest Takeaways from Gartner Hype Cycle for Security Operations 2022 [en línea], (sin fecha). *Cymulate*. [Consultado el 1 de enero de 2023]. Disponible en: https://cymulate.com/blog/gartner-hype-cycle-security-operations/

[82] Picus, (2021). 2021 Gartner® Hype Cycle™ for Security Operations [en línea]. *THE COMPLETE SECURITY VALIDATION PLATFORM*. [Consultado el 1 de enero de 2023]. Disponible en: https://www.picussecurity.com/resource/gartner-hype-cycle-for-security-operations-2021

[83] Columbus, L., (2020). What's New In Gartner's Hype Cycle For Endpoint Security, 2020 [en línea]. *Forbes*. [Consultado el 1 de enero de 2023]. Disponible en: https://www.forbes.com/sites/louiscolumbus/2020/08/30/whats-new-in-gartners-hype-cycle-for-endpoint-security-2020/

[84] Gartner Highlights iPaaS and Low-code Platforms in Cloud Platform Hype Cycle [en línea], (sin fecha). *Datanami*. [Consultado el 1 de enero de 2023]. Disponible en: https://www.datanami.com/2022/08/10/gartner-highlights-ipaas-and-low-code-platforms-in-cloud-platform-hype-cycle/

[85] Cómo evaluar las tecnologías de seguridad de la nube para tu estrategia de nube [en línea], (sin fecha). *Gartner*. [Consultado el 1 de enero de 2023]. Disponible en: https://www.gartner.es/es/articulos/4-tecnologias-imprescindibles-que-integraron-el-hype-cycle-de-gartner-para-la-seguridad-en-la-nube-2021

[86] Top Actions From Gartner Hype Cycle for Cloud Security, 2020 [en línea], (sin fecha). *Gartner*. [Consultado el 1 de enero de 2023]. Disponible en: https://www.gartner.com/smarterwithgartner/top-actions-from-gartner-hype-cycle-for-cloud-security-2020

[87] Novedades del Hype Cycle de Gartner para la inteligencia artificial de 2022 [en línea], (sin fecha). *Gartner*. [Consultado el 1 de enero de 2023]. Disponible en: https://www.gartner.es/es/articulos/novedades-del-hype-cycle-de-gartner-para-la-inteligencia-artificial-2022

[88] Las 4 tendencias que prevalecen en el Hype Cycle de Gartner para la IA de 2021 [en línea], (sin fecha). *Gartner*. [Consultado el 1 de enero de 2023]. Disponible en: https://www.gartner.es/es/articulos/las-4-tendencias-que-prevalecen-en-el-hype-cycle-de-gartner-para-la-ia-2021

[89] 2 megatendencias dominan el Hype Cycle de Gartner de 2020 en el campo de la inteligencia artificial [en línea], (sin fecha). *Gartner*. [Consultado el 1 de enero de 2023]. Disponible en: https://www.gartner.es/es/articulos/2-megatendencias-dominan-hype-cycle-2020-inteligencia-artificial

[90] Las tendencias principales de seguridad y riesgos de Gartner en 2021 [en línea], (sin fecha). *Gartner*. [Consultado el 1 de enero de 2023]. Disponible en: https://www.gartner.es/es/articulos/principales-tendencias-de-seguridad-y-riesgos-gartner-2021

[91] Las principales tendencias de seguridad y riesgos de Gartner para 2022 [en línea], (sin fecha). *Gartner*. [Consultado el 1 de enero de 2023]. Disponible en: https://www.gartner.es/es/articulos/las-7-principales-tendencias-en-ciberseguridad-para-2022

9 Annexos

ANNEX 1

HYPE CYCLE MODEL

CÓM INTERPRETAR-HO?

¿Qué es el Hype Cycle de Gartner?

Cuando las nuevas tecnologías hacen promesas audaces, ¿cómo podemos distinguir lo que es una exageración de lo que es comercialmente viable? ¿Y cuándo se llegarán a amortizar estas soluciones, suponiendo que lo lleguen a hacer?

El Hype Cycle de Gartner es una representación gráfica en forma de curva que representa la madurez y adopción de las tecnologías y apps y cómo son potencialmente relevantes para resolver problemas comerciales reales y aprovechar nuevas oportunidades.

La metodología del Hype Cycle (literalmente, "ciclo de sobreexpectación" en español y a menudo llamado "curva de Gartner") de Gartner te permite ver cómo una tecnología o app evolucionará con el tiempo, y te proporciona una fuente sólida de información para que puedas gestionar su implementación dentro del contexto de tus objetivos de negocio específicos.

PRINCIPALS ESCENARIS EN LES FASES DEL MODEL

UTILITAT DEL MODEL:

¿Qué utilidad tiene el Hype Cycle?

Nuestros clientes utilizan los Hype Cycles para informarse sobre las promesas que realiza una tecnología emergente dentro del contexto de su industria y el apetito individual por el riesgo.

¿Deberías anticiparte a los demás? Si estás dispuesto a asumir riesgos y eres consciente de que las inversiones arriesgadas no siempre dan resultados, podrías llegar a obtener los beneficios de optar por una adopción temprana.

¿Es mejor adoptar un enfoque moderado? Los ejecutivos más moderados comprenden el argumento a favor de hacer una inversión temprana, pero también insistirán en la realización de un análisis de coste / beneficio sólido cuando las nuevas formas de hacer las cosas aún no estén completamente consolidadas.

¿Deberías esperar a que se alcance una mayor maduración? Si hay demasiadas preguntas sin respuesta sobre la viabilidad comercial de una tecnología emergente, puede ser mejor esperar hasta que otras hayan podido ofrecer un valor tangible.

FUNCIONAMENT I ETAPES DEL MODEL

¿Cómo funciona y qué etapas tiene el Hype Cycle de Gartner?

Cada Hype Cycle profundiza en las cinco fases clave del ciclo de vida de una tecnología.

- **Lanzamiento:** un potencial avance tecnológico pone en marcha las cosas. Las primeras historias de prueba de concepto y el interés de los medios de comunicación generan una publicidad considerable. A menudo, no existen productos utilizables y la viabilidad comercial no se ha demostrado.
- **Pico de expectativas sobredimensionadas:** la publicidad temprana produce una serie de historias de éxito, a menudo acompañadas de decenas de fracasos. Algunas empresas toman medidas; muchas no lo hacen.
- **Abismo de desilusión:** el interés se desvanece a medida que los experimentos y las implementaciones no se cumplen. Los productores de la tecnología se tambalean o fracasan. Las inversiones continúan solo si los proveedores que logran sobrevivir mejoran sus productos a satisfacción de los primeros usuarios.
- **Rampa de consolidación:** más ejemplos de cómo la tecnología puede beneficiar a la empresa comienzan a materializarse y a entenderse mejor. Aparecen productos de segunda y tercera generación de la mano de los proveedores de tecnología. Más empresas financian proyectos piloto, pero las empresas conservadoras siguen siendo cautelosas.
- **Meseta de productividad:** la adopción generalizada comienza a despegar y los criterios para evaluar la viabilidad del proveedor están definidos con mayor claridad. La amplia aplicabilidad y relevancia de la tecnología en el mercado está claramente dando sus frutos.

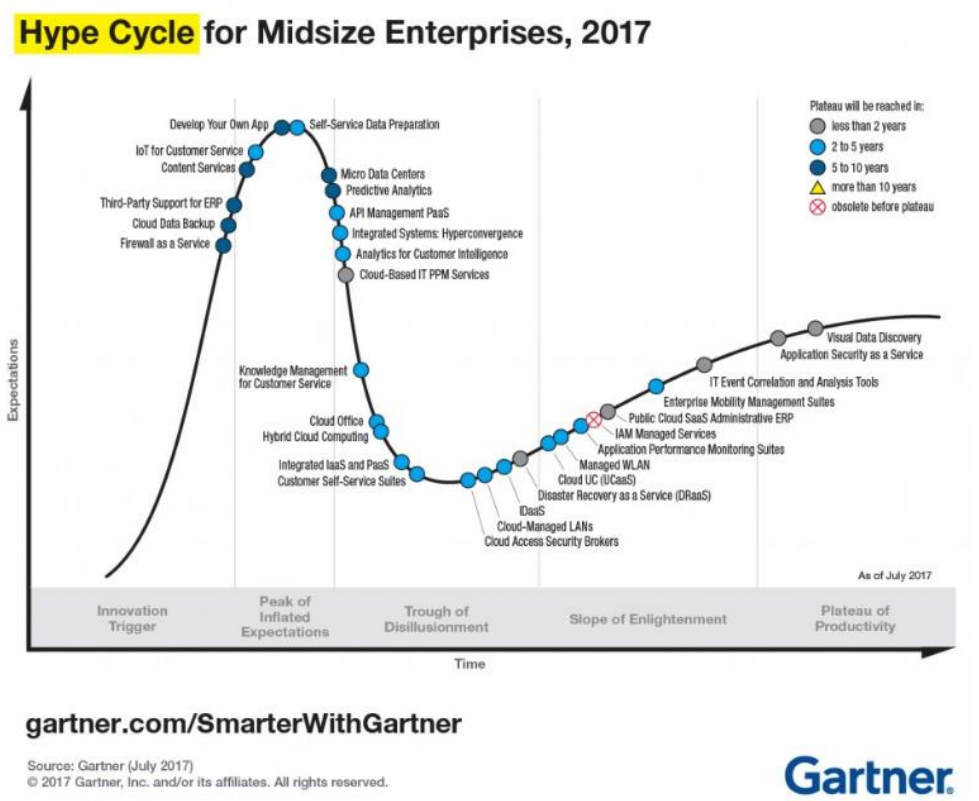
COM APROFITAR EL MODEL? DE QUINA FORMA POT AJUDAR?

¿Cómo te ayudan los Hype Cycles?

Utiliza los Hype Cycles de Gartner para:

- Separar la sobreexpectación de los verdaderos impulsores de la promesa comercial de una tecnología.
- Reducir el riesgo de tus decisiones de inversión en tecnología.
- Comparar tu comprensión del valor comercial de una tecnología con la objetividad de los analistas de Tecnología de la Información (TI) más experimentados.

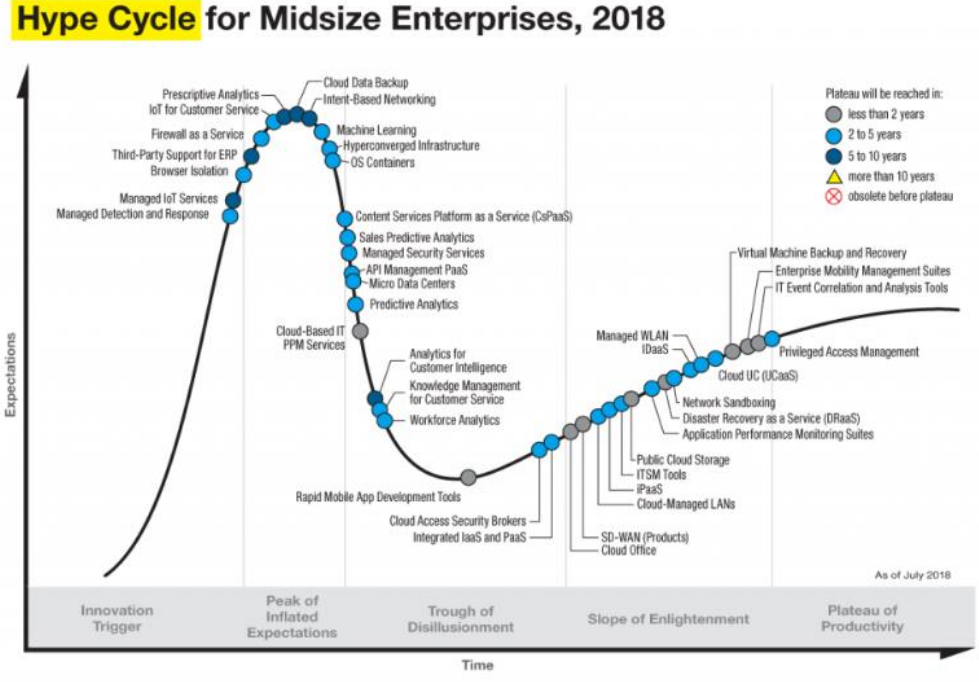
HYPE CYCLE for MIDSIZE ENTERPRISES



gartner.com/SmarterWithGartner

Source: Gartner (July 2017)
© 2017 Gartner, Inc. and/or its affiliates. All rights reserved.

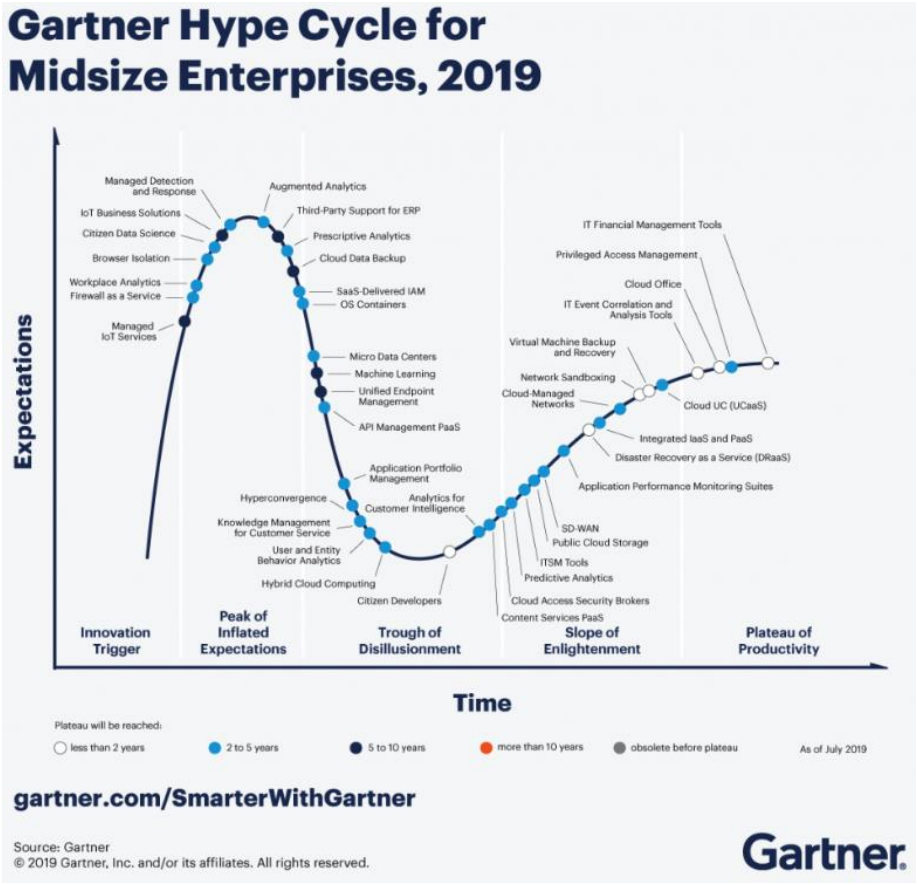
Gartner



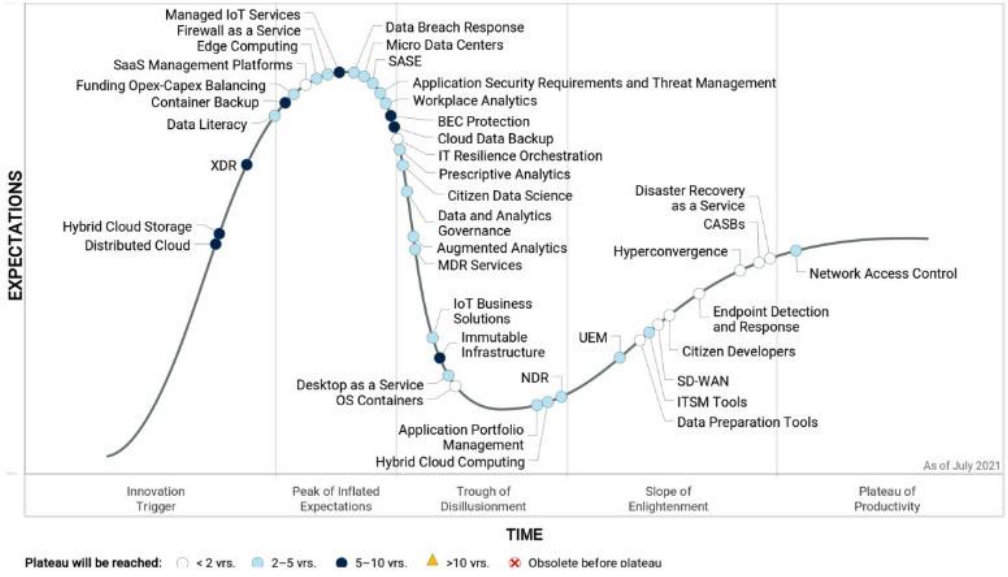
gartner.com/SmarterWithGartner

Source: Gartner (August 2018)
© 2018 Gartner, Inc. and/or its affiliates. All rights reserved.

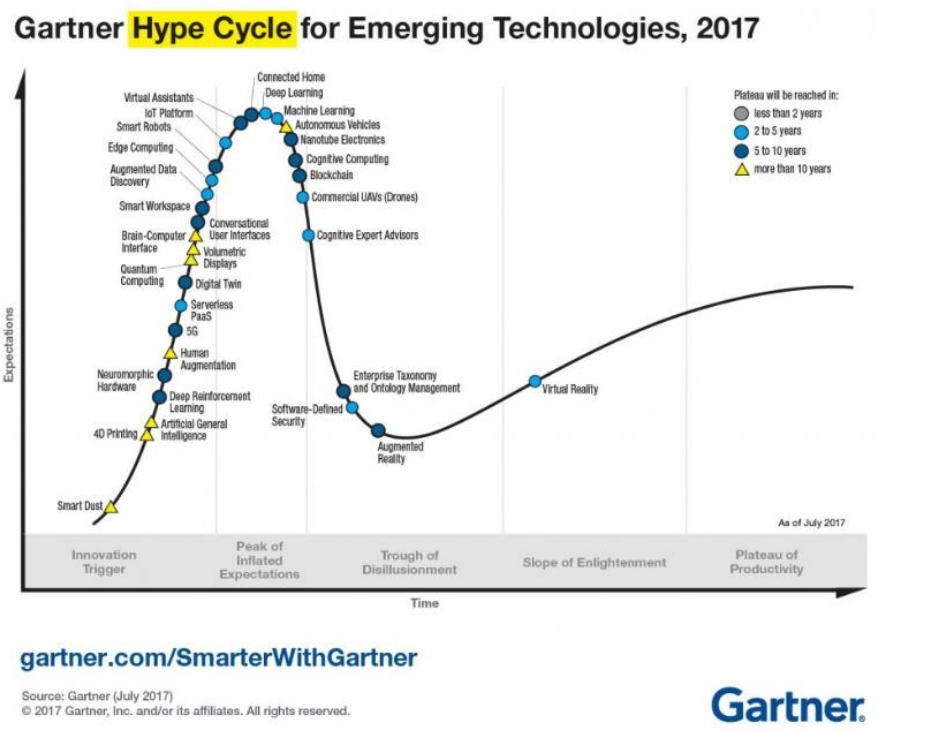
Gartner



Hype Cycle for Midsize Enterprises, 2021



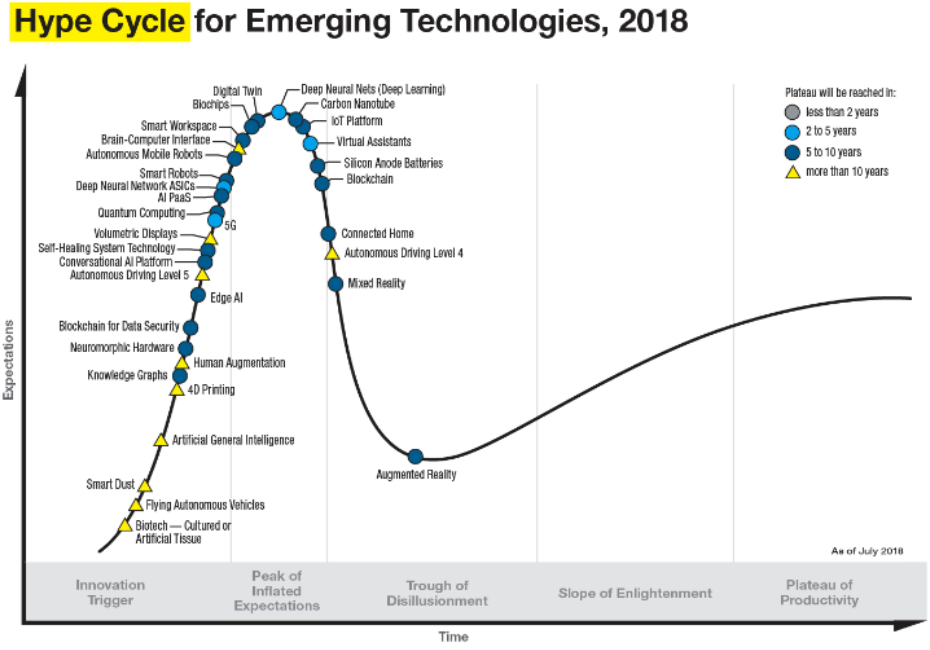
HYPE CYCLE FOR EMERGING TECHNOLOGIES



gartner.com/SmarterWithGartner

Source: Gartner (July 2017)
© 2017 Gartner, Inc. and/or its affiliates. All rights reserved.

Gartner



gartner.com/SmarterWithGartner

Source: Gartner (August 2018)
© 2018 Gartner, Inc. and/or its affiliates. All rights reserved.

Gartner

Gartner Hype Cycle for Emerging Technologies, 2019

gartner.com/SmarterWithGartner

Source: Gartner
© 2019 Gartner, Inc. and/or its affiliates. All rights reserved.

Gartner

Hype Cycle para las tecnologías emergentes, 2020

gartner.es/es/articulos

Fuente: Gartner
© 2020 Gartner, Inc. y/o sus afiliados. Todos los derechos reservados. Gartner y Hype Cycle son marcas registradas de Gartner, Inc. y sus afiliados en EE. UU.

Gartner

Hype Cycle para las tecnologías emergentes, 2021

Cuándo se alcanzará la meseta de productividad:

○ en menos de 2 años ● de 2 a 5 años ● de 5 a 10 años ▲ en más de 10 años ⊗ obsoleto antes de alcanzarla

Datos correspondientes a agosto de 2021

gartner.es

Source: Gartner
© 2021 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner and Hype Cycle are registered trademarks of Gartner, Inc. and its affiliates in the U.S. 1448000

Gartner

Hype Cycle para las tecnologías emergentes, 2022

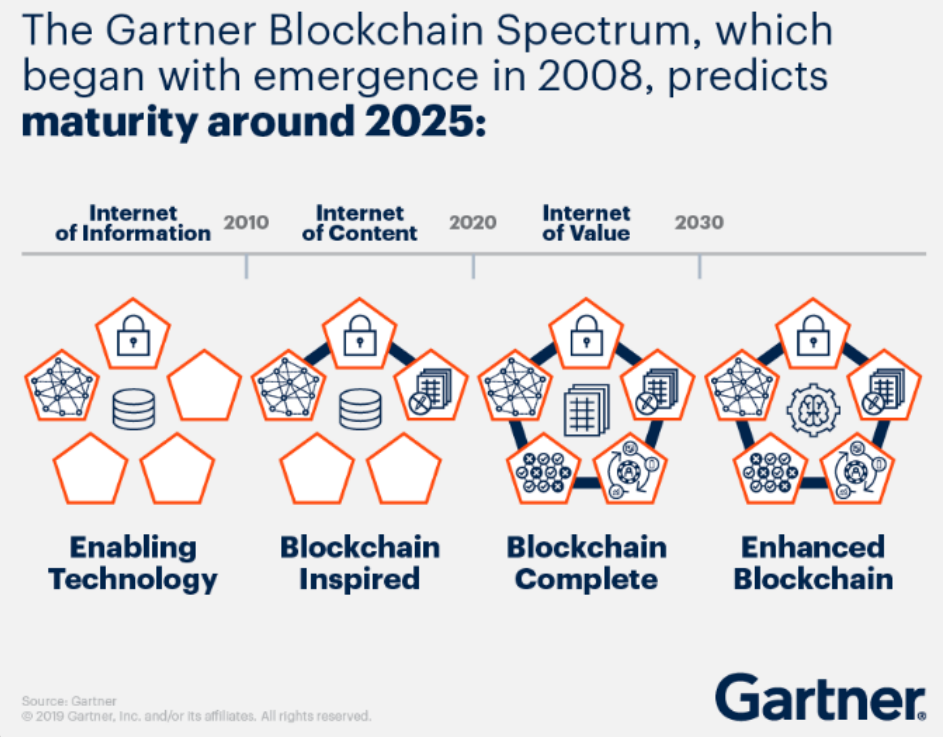
Cuándo se alcanzará la meseta de productividad:

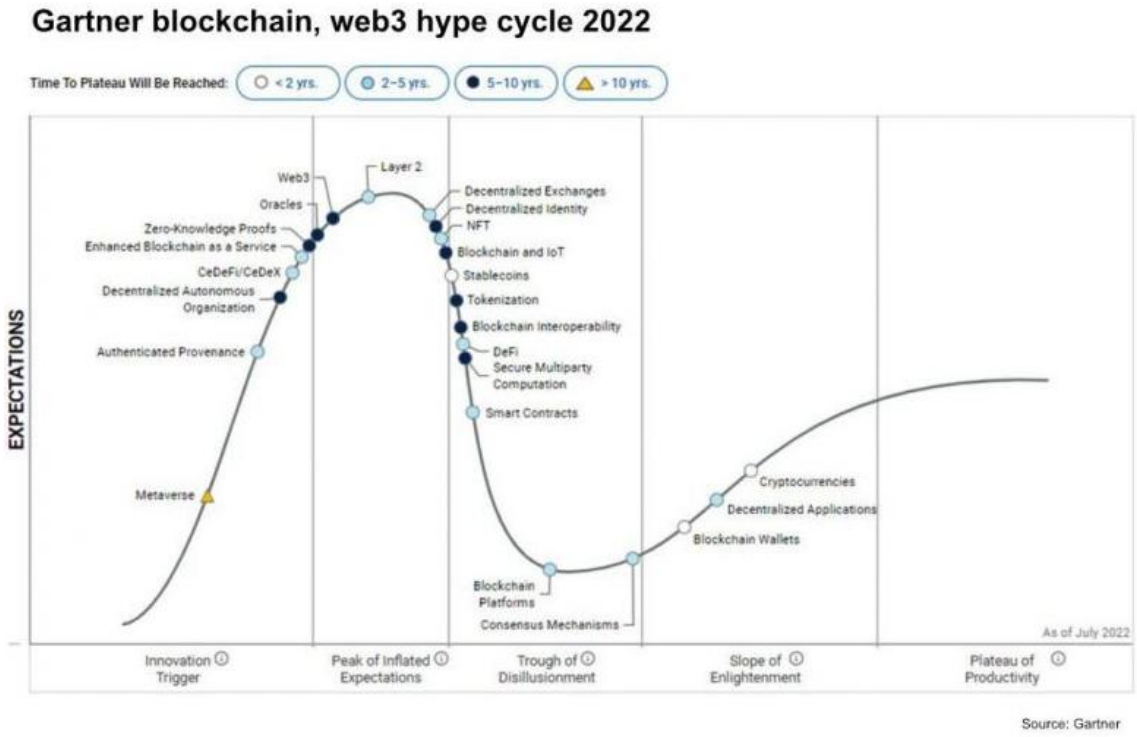
○ en menos de 2 años ● de 2 a 5 años ● de 5 a 10 años ▲ en más de 10 años ⊗ obsoleto antes de alcanzarla

Datos correspondientes a agosto de 2022

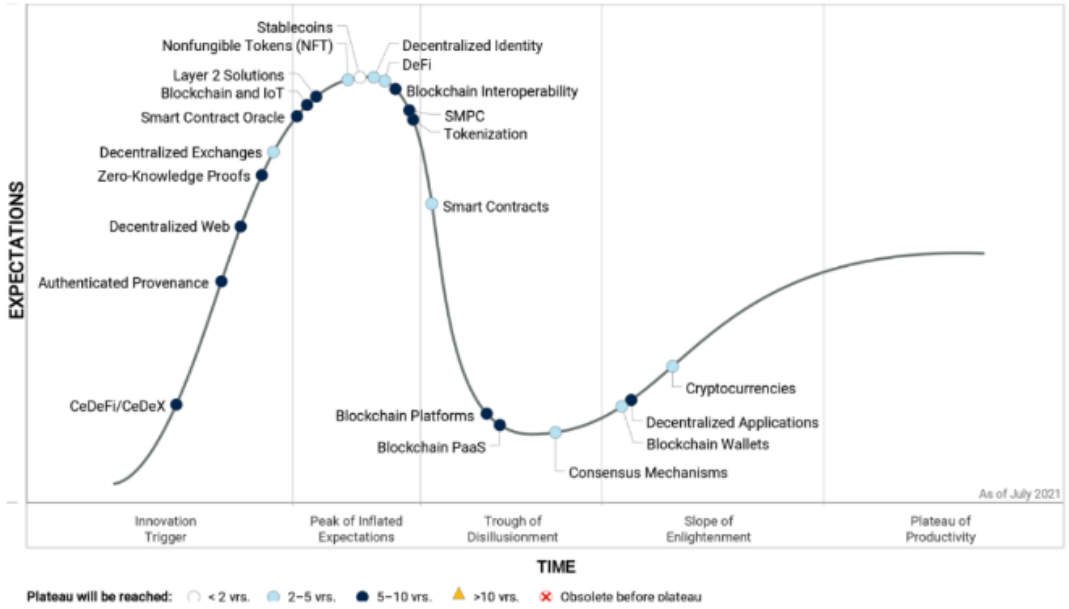
gartner.es

HYPE CYCLE for BLOCKCHAIN: Model 2008-2025



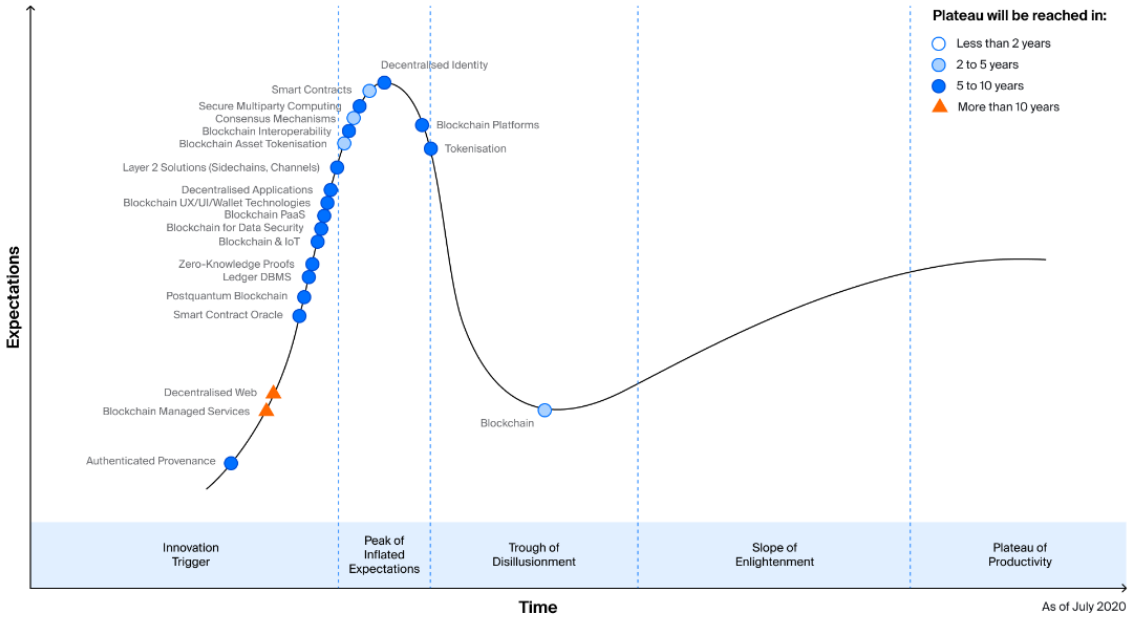


Hype Cycle for Blockchain, 2021



Source: Gartner (July 2021)

Hype Cycle for Blockchain Technologies, 2020

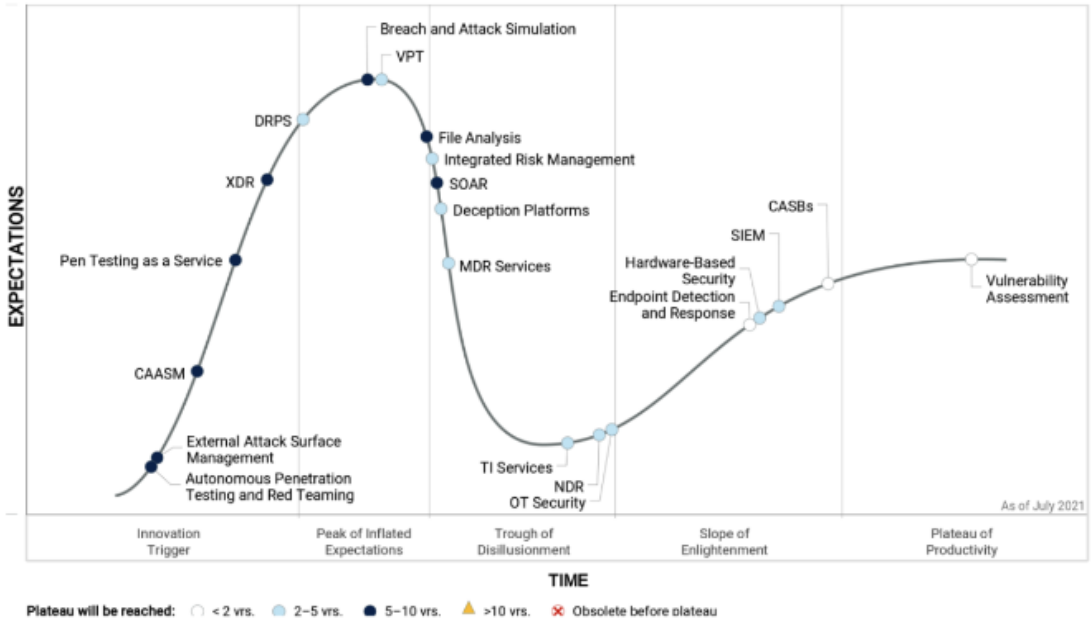


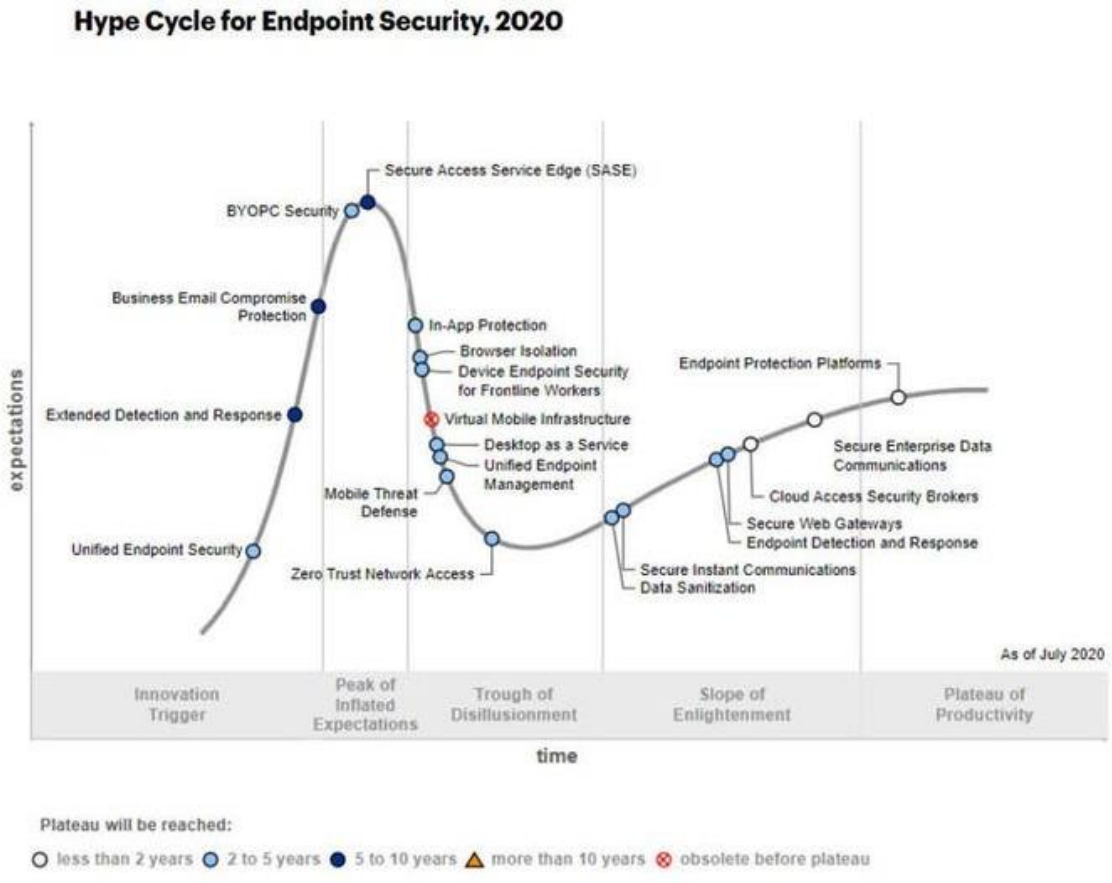
Source: Gartner (2020)

Chainstack

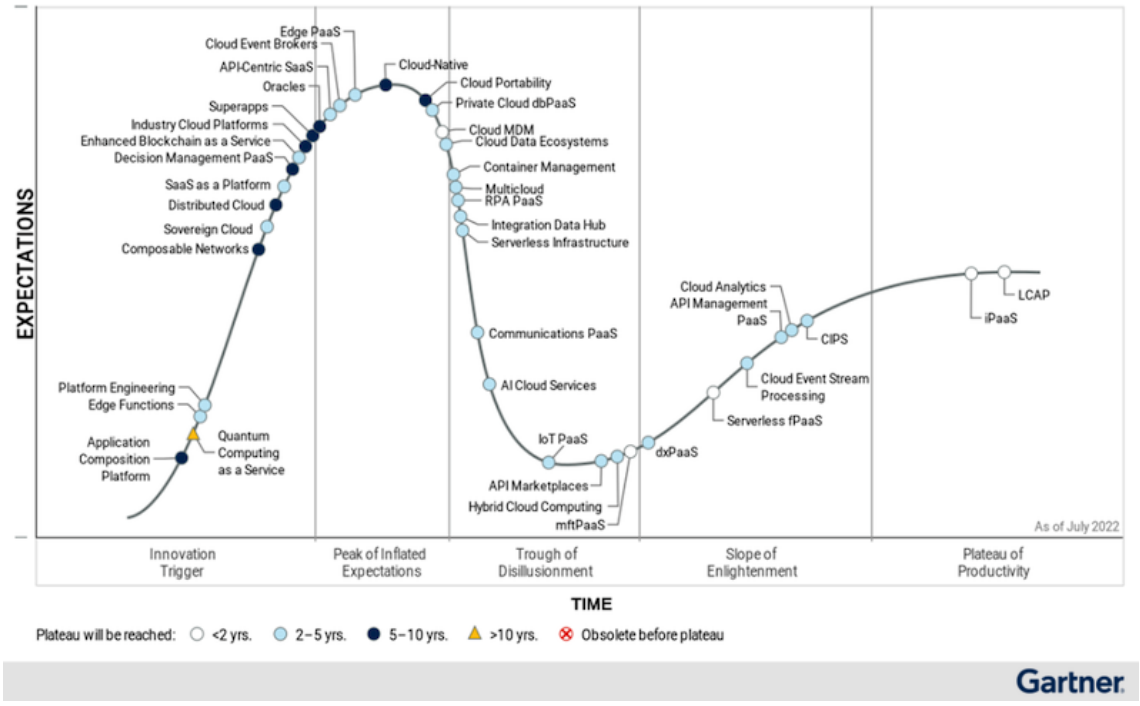
HYPE CYCLE for SECURITY OPERATIONS

Hype Cycle for Security Operations, 2021

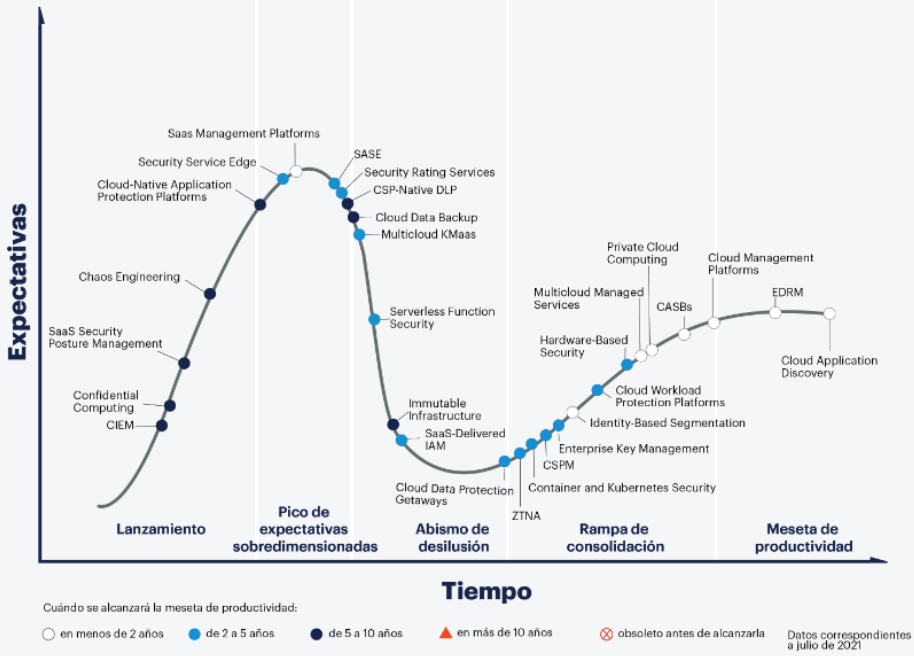




HYPE CYCLE for CLOUD SECURITY



Hype Cycle para la seguridad en la nube, 2021



Cuándo se alcanzará la meseta de productividad:

○ en menos de 2 años ● de 2 a 5 años ● de 5 a 10 años ▲ en más de 10 años ⊗ obsoleto antes de alcanzarla

Datos correspondientes a julio de 2021

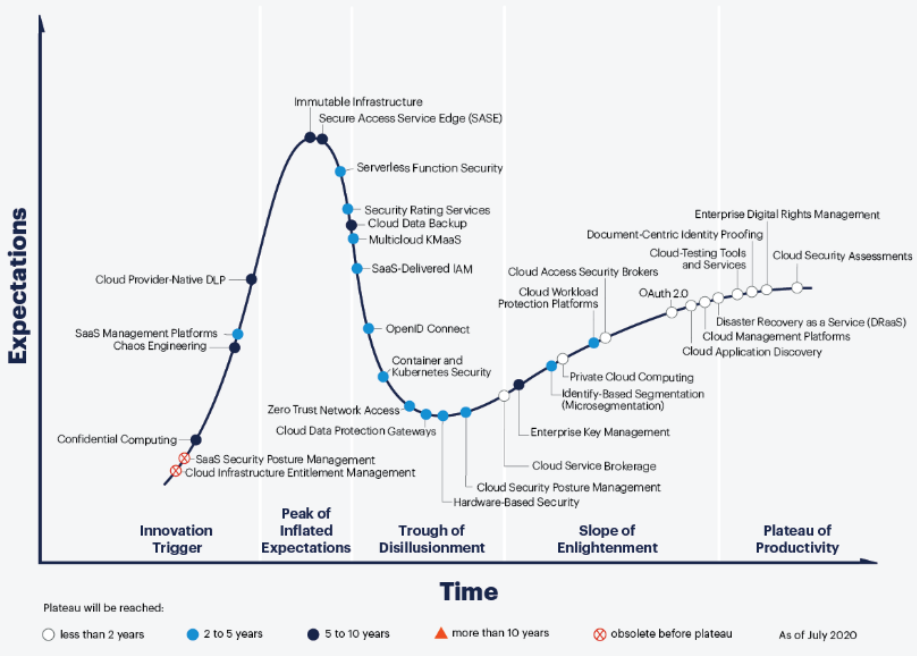
gartner.es/es/smarterwithgartner

Fuente: Gartner
© 2021 Gartner, Inc. y/o sus afiliados. Todos los derechos reservados. Gartner y Hype Cycle son marcas registradas de Gartner, Inc. y sus afiliados en EE.UU.

Gartner

Hype Cycle for Cloud Security, 2020

Gartner Hype Cycle for Cloud Security 2020



Plateau will be reached:

○ less than 2 years ● 2 to 5 years ● 5 to 10 years ▲ more than 10 years ⊗ obsolete before plateau

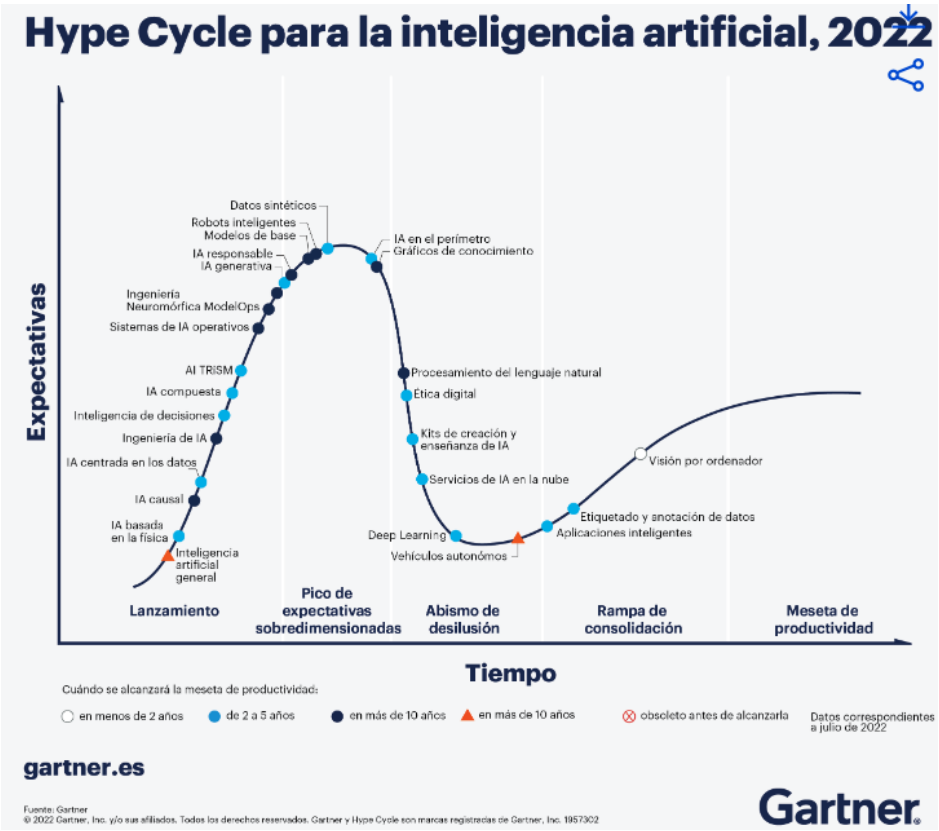
As of July 2020

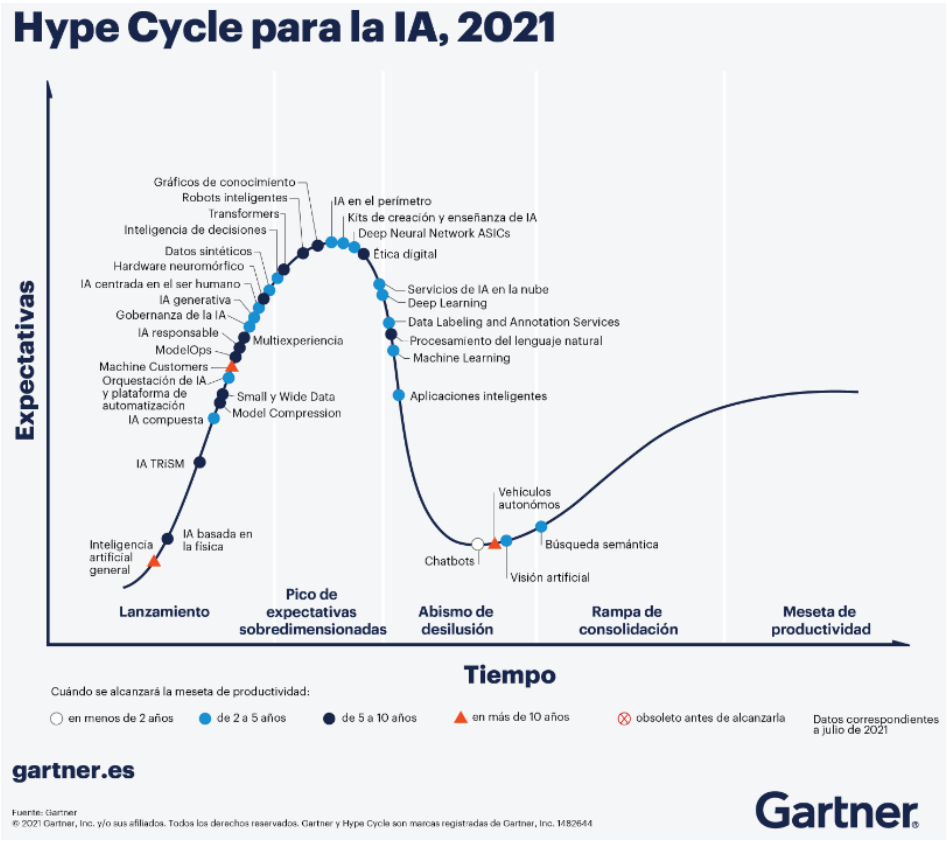
gartner.com/SmarterWithGartner

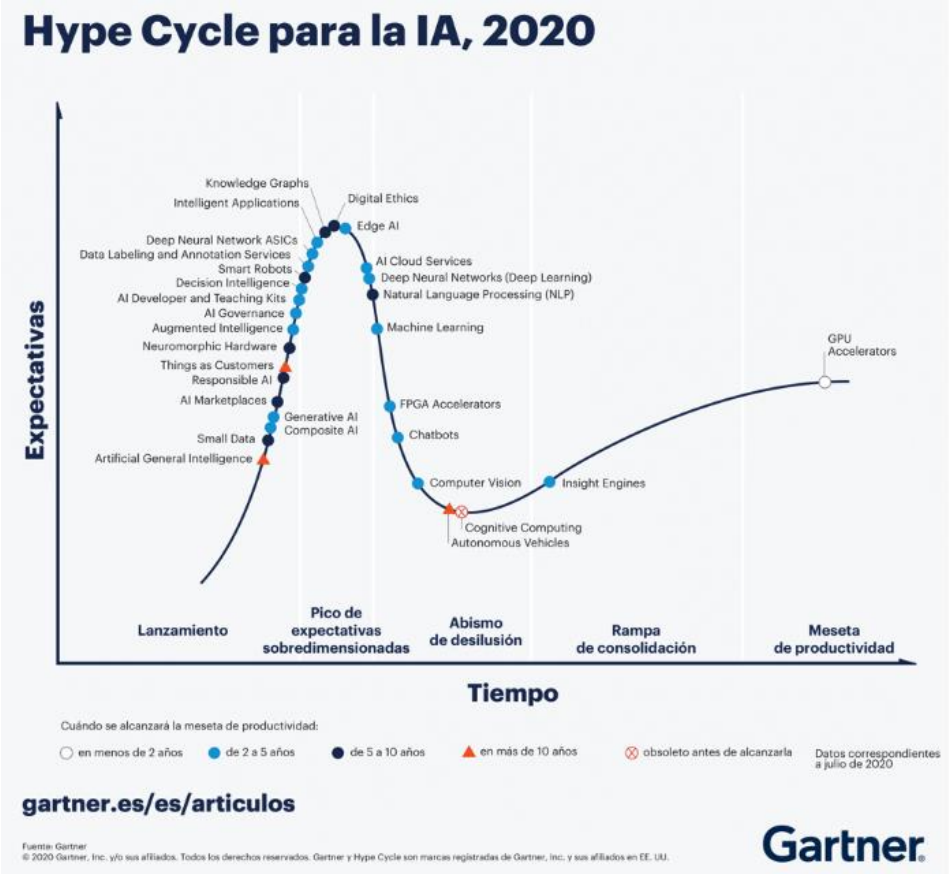
Source: Gartner
© 2020 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner and Hype Cycle are registered trademarks of Gartner, Inc. and its affiliates in the U.S.

Gartner

HYPE CYCLE per INTEL.LIGÈNCIA ARTIFICIAL







PRINCIPALS TENDÈNCIES DE SEGURETAT I RISCOS

Principales tendencias en ciberseguridad, 2022

gartner.es

Fuente: Gartner

© 2022 Gartner, Inc. Todos los derechos reservados. PR_1764850

Gartner