INFORME SOBRE LA CIBERDELINQÜÈNCIA A CATALUNYA

GOVERN ALTERNATIU DE CATALUNYA

Seguretat i Convivència

Ramon Espadaler, Judit Alcalá i Mario García

17 de novembre de 2023

ÍNDEX

INTRODUCCIÓ

La **ciberdelinqüència** és un fenomen que ha anat augmentat en els darrers anys, no només pel que fa al nombre d'atacs reportats, sinó també en la sofisticació dels seus procediments.

La ràpida digitalització de la societat i de l'economia crea constantment noves oportunitats per a criminals involucrats en aquests delictes. A més, el progressiu augment en el nombre d'usuaris i connexions genera noves vulnerabilitats, al temps que incrementa el número de víctimes potencials als atacs cibernètics.

Durant l'any 2020, i per l'efecte de la pandèmia COVID-19, van augmentar de forma exponencial les connexions privades a sistemes corporatius i el teletreball es va convertir en la norma en molts sectors i indústries. Davant d'això, el crim organitzat s'ha adaptat ràpidament per tal de capitalitzar els canvis en l'entorn en el que operen[1].

Les noves tipologies de frau estan, doncs, relacionades amb eines en línia i tècniques digitals. Cal tenir molt present, d'entrada, que aquest fenomen de digitalització de tot el funcionament social és imparable, i que opera cada vegada més en el dia a dia de la nostra societat, incloent també la relació dels ciutadans amb la pròpia administració pública. Aquest fet, que s'ha anat desenvolupant i consolidant en aquestes darreres dècades, és, alhora, un camp de noves oportunitats per a delinqüents implicats en delictes online: "Una conseqüència directa d'aquest procés de transformació és l'increment del risc i de les amenaces de ciberseguretat dels sistemes d'informació i dispositius connectats, ja siguin personals o corporatius, degut a dos factors: per una banda, la connectivitat extrema augmenta el nombre de superfícies d'atac a traves de les quals es poden materialitzar els ciberatacs; per altra banda, els ciberatacants disposen de manera continuada de més coneixement, recursos i capacitat per desenvolupar les eines necessàries per planificar i executar atacs cada cop més sofisticats i amb una major capacitat de de dany"[2].

Així, la ciberdelinqüència és un dels delictes transnacionals que més ràpidament creix. Si bé la ràpida evolució d'internet i de la tecnologia informàtica han permès el creixement econòmic i social, aquesta major dependència d'internet ha generat més riscos i vulnerabilitats, i ha obert noves possibilitats per les activitats delictives.

La naturalesa mateixa de la ciberdelinqüència, en tant que té un caràcter transnacional, dificulta la persecució del delicte i planteja problemes de persecució policial i d'abordatge

[1] EU serious and organised crime threat assessment 2021

[2] Agència de Ciberseguretat de Catalunya. Llibre blanc sobre la Intel·ligència Artificial aplicada a la Ciberseguretat

jurídic, donada també la diversitat dels actors que hi intervenen. El fet que els delictes puguin ser comesos arreu del món és també un handicap a nivell global, ja que trobem una àmplia diversitat de capacitats, tant tecnològiques com policials. A més, a diferència d'altres investigacions policials, en molts casos de ciberdelinqüència les proves digitals es troben principalment en el sector privat, que és qui opera i manté moltes parts de la infraestructura d'Internet. Per aquest motiu, és fonamental establir mecanismes de col·laboració ferms, amb lideratge de l'administració pública, entre les distintes parts interessades a fi d'abordar les noves amenaces cibernètiques.

El present informe incideix en la necessitat d'abordar la creixent ciberdelinqüència com a característica fonamental del "modus operandi" dels fets delictius del futur. Tot i els esforços i avenços en la ciberseguretat, els delictes online s'han multiplicat per tres el darrer any.

La ciberseguretat és un tema clau pel present i el futur de Catalunya, però és tan important com fràgil. Estem en un món completament globalitzat i connectat digitalment i, per tant, cal visualitzar la ciberseguretat des d'un prisma mundial, que va més enllà de fronteres territorials, i que tal i com hem vist recentment, es pot veure agreujat per crisis internacionals com la Covid-19 o la guerra de Rússia contra Ucraïna. Creiem fermament que cal que Catalunya acceleri en la implantació de mesures de ciberseguretat previstes, o el risc que assumirem serà massa elevat.

És evident que aquests esdeveniments internacionals recents ens han fet encara més conscients de la necessitat de garantir i ampliar la ciberseguretat tot el que sigui possible, tenint en compte que no existeix el risc zero, però constatant que la inversió en estratègies i accions de ciberseguretat poden prevenir impactes negatius tant econòmics com socials en el nostre país, especialment, si afecten a infraestructures crítiques. En l'àmbit català, hem hagut de lamentar atacs especialment greus en casos com la UAB, l'AMB i diversos Ajuntaments, així com a la Generalitat de Catalunya, on la pròpia Agència de Ciberseguretat de Catalunya xifrava en la seva memòria del 202013 en més de mil els incidents en l'àmbit de la Generalitat.

Considerem que aquesta estratègia de país ha de ser liderada sens dubte per la Generalitat de Catalunya, coordinadament amb el Govern d'Espanya i els seus organismes, a través de l'Agència de Ciberseguretat de Catalunya. Però cal també que sigui de manera coordinada amb la resta d'administracions públiques catalanes, així com amb la col·laboració públic-privada que permeti desenvolupar un sector de ciberseguretat potent en l'àmbit català

Aquest informe també posa la mirada en la protecció de la ciutadania en general, en els individus concrets, en els més vulnerables, els que no disposen de la possibilitat de protegir-se a títol individual i que han passat a fer servir el món online com a part de la seva

quotidianitat. Entenem que cal protegir-los, en la mesura del possible, des de l'administració pública.

Cal combatre la ciberdelinqüència establint mesures de protecció de la xarxa, però alhora, establir mecanismes per combatre via policial els delinqüents que vulneren la seguretat de tots els ciutadans bàsicament en tres àmbits: els delictes ciberdependents (entre ells, el blanqueig de capitals), el frau en el pagament i, amb especial atenció, els delictes relacionats amb l'explotació sexual infantil. Aquest tipus de delicte entenem que necessita d'un abordatge específic, ferm i intensiu. Cal fer-ho, però, des d'una mirada que s'adapti a la seva pròpia naturalesa, basat en dos aspectes propis: el grau de velocitat en les seves actuacions delictives i l'adaptabilitat dels delinqüents per tal de vulnerar i superar els avenços en mesures de protecció i seguretat a la xarxa.

Al respecte, cal tenir una mirada centrada no només en la protecció i persecució de possibles delictes pel que fa a infraestructures bàsiques de la nostra societat, o davant de l'activitat econòmica de la mateixa, sinó que cal avançar també, i molt, en la protecció i persecució de l'activitat delinqüencial que té per objectiu els ciutadans i ciutadanes concretes a Catalunya.

10 TIPUS DE DELICTES CIBERNÈTICS

Els 10 delictes cibernètics més comuns són: robatori d'identitat, pirateria, phishing, botnets, ciberespionatge, extorsió en la xarxa, malware, ransoware, pornografia infantil i l'assetjament cibernètic.

Robatori d'identitat: Succeeix quan algú roba informació personal i la fa servir per tal de cometre un delicte o frau. El frau amb targetes de dèbit o crèdit és un dels robatoris d'identitat més freqüents.

Pirateria: És un acte comés per un intrús a l'accedir a un sistema informàtic sense permís. Són atacs que involucren la còpia, distribució i ús il·legal de programes de software amb la intenció d'ús comercial o personal. A més, trobem les infraccions de marques registrades, les infraccions de drets d'autor i les infraccions de patents.

Phishing: És una tècnica per extraure informació confidencial, com són els números de targetes de crèdit i combinacions de contrasenya de nom d'usuari, fent-se passar per una empresa legítima. El phishing generalment es duu a terme mitjançant una suplantació d'identitat per correu electrònic, llocs web o trucades.

Botnets: Una botnet és una xarxa de computadores que els atacants infecten amb malware, les posen en perill i les connecten a un centre de comandament i control central. Els atacants

incorporen cada vegada més dispositius a la seva botnet i els utilitzen per enviar correus electrònics no desitjats, realitzar atacs i minar criptomonedes.

Ciberespionatge: És un delicte que involucra a un ciberdelinqüent que pirateja sistemes o xarxes per obtenir accés a informació confidencial en poder de un govern o altra organització.

Extorsió en la xarxa: És un delicte en línia en el què els pirates informàtics retenen les dades, llocs web, sistemes informàtics o d'altre informació confidencial com a ostatges fins acomplir amb les seves demandes de pagament.

Malware: És un software maliciós destinat a fer mal o inhabilitar computadores i sistemes informàtics sense el coneixement del propietari. Existeixen diversos tipus de malware, inclosos spyware, virus, cucs, troians i d'altres tipus de codis maliciosos que poden infiltrar-se en els equips.

Ransomware: És una forma de malware que bloqueja dispositius, xarxes i documents importants fins que la víctima paga un rescat. Les persones que utilitzen ransomware solen dirigir-se a organitzacions com a hospitals i bufets d'advocats.

Pornografia infantil: És un dels delictes cibernètics més detestables. Són imatges de nens involucrats en activitats sexuals i que es comercialitzen a Internet les 24 hores del dia. Perseguir aquest tipus de delictes mereix una dedicació especial.

Assetjament cibernètic: Consisteix en l'ús de la tecnologia per tal d'assetjar, ferir, avergonyir, humiliar o intimidar a altra persona de manera repetida e intencional. La proliferació de xarxes socials ha donat una amplitud dels llocs on es produeixen aquest fets[3].

Tabla 1. Clasificación/Taxonomía de los ciberincidentes

Clasificación	Tipo de incidente	Descripción y ejemplos prácticos
Contenido abusivo.	*Spam.*	Correo electrónico masivo no solicitado. El receptor del contenido no ha otorgado autorización válida para recibir un mensaje colectivo.
	Delitos de odio, contra la libertad o el honor.	Contenido difamatorio o discriminatorio. Ej.: ciberacoso, racismo, amenazas a una persona o dirigidas contra colectivos.
	Pornografía infantil, contenido sexual o violento inadecuado.	Material que represente de manera visual contenido relacionado con pornografía infantil, apología de la violencia, etc.
Contenido dañino.	Sistema infectado.	Sistema infectado con malware. Ej.: sistema, computadora o teléfono móvil infectado con un *rootkit*.
	Servidor C&C (Mando y Control).	Conexión con servidor de Mando y Control (C&C) mediante malware o sistemas infectados.
	Distribución de malware.	Recurso usado para distribución de malware. Ej.: recurso de una organización empleado para distribuir malware.
	Configuración de malware.	Recurso que aloje ficheros de configuración de malware Ej.: ataque de *webinjects* para troyano.

[3] Seguridad Informática Hoy: Los 10 delitos cibernéticos. Disponible a: https://seguridadinformaticahoy.com/delitos-ciberneticos/

Clasificación	Tipo de incidente	Descripción y ejemplos prácticos
Obtención de información.	Escaneo de redes (*scanning*).	Envío de peticiones a un sistema para descubrir posibles debilidades. Se incluyen también procesos de comprobación o testeo para recopilar información de alojamientos, servicios y cuentas. Ej.: peticiones DNS, ICMP, SMTP, escaneo de puertos.
	Análisis de paquetes (*sniffing*).	Observación y grabación del tráfico de redes.
	Ingeniería social.	Recopilación de información personal sin el uso de la tecnología. Ej.: mentiras, trucos, sobornos, amenazas.
Intento de intrusión.	Explotación de vulnerabilidades conocidas.	Intento de compromiso de un sistema o de interrupción de un servicio mediante la explotación de vulnerabilidades con un identificador estandarizado (véase CVE). Ej.: desbordamiento de *buffer*, puertas traseras, *cross site scripting* (XSS).
	Intento de acceso con vulneración de credenciales.	Múltiples intentos de vulnerar credenciales. Ej.: intentos de ruptura de contraseñas, ataque por fuerza bruta.
	Ataque desconocido.	Ataque empleando *exploit* desconocido.
Intrusión.	Compromiso de cuenta con privilegios.	Compromiso de un sistema en el que el atacante ha adquirido privilegios.
	Compromiso de cuenta sin privilegios.	Compromiso de un sistema empleando cuentas sin privilegios.
	Compromiso de aplicaciones.	Compromiso de una aplicación mediante la explotación de vulnerabilidades de software. Ej.: inyección SQL.
	Robo.	Intrusión física. Ej.: acceso no autorizado a Centro de Proceso de Datos.
Disponibilidad.	DoS (Denegación de servicio).	Ataque de denegación de servicio. Ej.: envío de peticiones a una aplicación *web* que provoca la interrupción o ralentización en la prestación del servicio.
	DDoS (Denegación distribuida de servicio).	Ataque de denegación distribuida de servicio. Ej.: inundación de paquetes SYN, ataques de reflexión y amplificación utilizando servicios basados en UDP.
	Mala configuración.	Configuración incorrecta del software que provoca problemas de disponibilidad en el servicio. Ej.: Servidor DNS con el KSK de la zona raíz de DNSSEC obsoleto.
	Sabotaje.	Sabotaje físico. Ej.: cortes de cableados de equipos o incendios provocados.
	Interrupciones.	Interrupciones por causas ajenas. Ej.: desastre natural.
Compromiso de la información.	Acceso no autorizado a información.	Acceso no autorizado a información. Ej.: robo de credenciales de acceso mediante interceptación de tráfico o mediante el acceso a documentos físicos.
	Modificación no autorizada de información.	Modificación no autorizada de información. Ej.: modificación por un atacante empleando credenciales sustraídas de un sistema o aplicación o encriptado de datos mediante *ransomware*.
	Pérdida de datos.	Pérdida de información Ej.: pérdida por fallo de disco duro o robo físico.
Fraude.	Uso no autorizado de recursos.	Uso de recursos para propósitos inadecuados, incluyendo acciones con ánimo de lucro. Ej.: uso de correo electrónico para participar en estafas piramidales.
	Derechos de autor.	Ofrecimiento o instalación de software carente de licencia u otro material protegido por derechos de autor. Ej.: Warez.
	Suplantación.	Tipo de ataque en el que una entidad suplanta a otra para obtener beneficios ilegítimos.
	Phishing.	Suplantación de otra entidad con la finalidad de convencer al usuario para que revele sus credenciales privadas.

LEGISLACIÓ

La regulació de la ciberseguretat no passa per una norma única sinó que es sustenta en un compendi de normes. Així, davant l'augment dels ciberatacs i del desenvolupament tecnològic dels mateixos, la Unió Europea està intentant donar respostes més firmes i més de conjunt per tal de reforçar la ciberseguretat.

La Directiva (UE) 2016/1148 del Parlament Europeu i del Consell de 6 de juliol de 2016, relativa a les mesures destinades a garantir un elevat nivell comú de seguretat de les xarxes i sistemes d'informació a la Unió, estableix les mesures destinades a garantir un espai comú de seguretat en les xarxes i sistemes d'informació de la Unió. Mesures que, per la pròpia naturalesa del tema concret, han anat modificant-se amb els propis avenços tecnològics.

L'article 14 estableix que "els Estats membres vetllaran perquè els operadors de serveis essencials prenguin les mesures tècniques i d'organització adequades i proporcionades per a gestionar els riscos que es plantegen per a la seguretat de les xarxes i sistemes d'informació que utilitzen en les seves operacions. Donada la situació, aquestes mesures garantiran un

nivell de seguretat de les xarxes i sistemes d'informació adient en relació amb el risc plantejat."

És a dir, són els Estats membres els responsables de vetllar per l'acompliment amb les mesures proporcionades o adequades al risc plantejat, i de prevenir incidents que afecten a la seguretat. D'altra banda, l'article 16 estableix el deure de l'Estat per tal que els proveïdors de serveis digitals determinin i adoptin també aquestes mesures de prevenció davant els ciberatacs.

L'acceleració de la transformació digital que va originar la crisi de la COVID-19 va suposar l'arribada d'una nova Directiva (SRI2) per tal de "seguir millorant la resiliència i les capacitats de resposta davant incidents tant del sector públic como del privat i de la UE en el seu conjunt".

A més, el mes de juny de 2019 va entrar en vigor el Reglament de Ciberseguretat de la UE, que estableix per una banda, els objectius, tasques i aspectes organitzatius relatius a ENISA (Agencia de la Unión Europea para la Ciberseguridad) i, d'altra banda, un marc per a la creació d'esquemes europeus de certificació de la ciberseguretat, a l'objecte de garantir un nivell adient de ciberseguretat dels productes, serveis i processos de TIC en la UE, així com d'evitar la fragmentació del mercat interior en el terreny dels esquemes de certificació de la ciberseguretat.

La UE ha implantat un marc únic de certificació per tal de generar confiança, augmentar el creixement del mercat de la ciberseguretat i facilitar el comerç en tota la Unió.

Pel que fa a Espanya, trobem un Código de Derecho de la Ciberseguridad, publicat en el Butlletí Oficial de l'Estat, que cita las principals normes a tenir en compte en relació amb la protecció del ciberespai. En aquest codi es fa referència a la següent normativa, entre d'altres:

Normatives de seguretat nacional:

- Llei 36/2015, de 28 de setembre, de Seguridad Nacional, que regula els principis i organismes clau així com les funcions que hauran de desenvolupar per a la defensa de la Seguridad Nacional.
- Ordre TIN/3016/2011, de 28 d'octubre, per la qual es crea el Comitè de Seguretat de les Tecnologies de la Informació i les Comunicacions del Ministeri de Treball i Immigració.

Normatives de seguretat:

- Llei Orgànica 4/2015, de 30 de març, de protecció de la seguretat ciutadana.
- Llei 5/2014, de 4 d'abril, de Seguretat Privada.

Amb relació a incidents de seguretat, existeix tot un entramat relacionat amb les Fuerzas Armadas però també es disposa d'una inclusió parcial en la Llei 34/2002, d'11 de juliol, de serveis a la societat de la informació i comerç electrònic.

Relacionades amb les telecomunicacions, existeixen les següents normes:

- Llei 34/2002, d' 11 de juliol, de serveis a la societat de la informació i comerç electrònic (esmentada abans).
- Real Decret 381/2015, de 14 de maig, pel qual s'estableixen mesures contra el tràfic no permès o irregular amb finalitats fraudulentes en comunicacions electròniques.
- Llei 9/2014, de 9 de maig, General de Telecomunicacions.
- Llei 25/2007, de 18 d'octubre, de conservació de dades relatives a les comunicacions electròniques i a les xarxes públiques de comunicacions.

Relacionat amb la ciberdelinqüència, trobem inclusions parcials en el Codi Penal, la Llei Orgànica 5/2000, de 12 de gener, reguladora de la responsabilitat penal dels menors; o en el Reial Decret d'aprovació de la Llei d'Enjudiciament Criminal.

També és d'aplicació amb allò disposat en la **Llei Orgànica 3/2018,** de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals.

CUADRO TIPOLOGÍAS PENALES

DENOMINACIÓN	CÓDIGO PENAL ESPAÑOL	TIPO HECHO SEC	VARIABLES SEC A UTILIZAR
Acceso e interceptación ilícita	Art. CP 197 A 201. Descubrimiento y revelación de secretos Art. CP 278 a 286. Delitos relativos al mercado y los consumidores (espionaje industrial)	DESCUBRIMIENTO/REVELACIÓN DE SECRETOS	Medio Empleado: Internet/informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
		ACCESO LEGAL INFORMÁTICO	Ninguna
		OTROS RELATIVOS AL MERCADO/CONSUMIDORES	Medio Empleado: Internet/informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
Interferencia en los datos y en el sistema	Arts. 183 a 267 y 625.1. Daños y daños informáticos	DAÑOS	Medio Empleado: Internet/informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
		ATAQUES INFORMÁTICOS	Ninguna
Falsificación informática	Arts CP 386 389, 399 bis, 400 y 401	FALSIFICACION DE MONEDA, SELLOS Y EFECTOS TIMBRADOS FABRICACIÓN TENENCIA DE UTILES PARA FALSIFICAR USURPACIÓN DEL ESTADO CIVIL	Medio Empleado: Internet/informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
Fraude informático	Arts. CP 248 a 251 y 623.4	ESTAFA BANCARIA	Medio Empleado: Internet/informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
		ESTAFAS CONTARJETAS DE CREDITO/CREDITO Y CHEQUES DE viaje	
		OTRAS ESTAFAS	
Delitos sexuales	Arts. CP 181, 183.1, 183 bis 184, 185, 186, 189	EXHIBICIONISMO	Medio Empleado: Internet/informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
		PROVOCACIÓN SEXUAL	
		ACOSO SEXUAL	
		ABUSO SEXUAL	
		CORRUPCIÓN DE MENORES/INCAPACITADOS	
		PORNOGRAFIA DE MENORES	
		DELITO DE CONTACTO MEDIANTE TECNOLOGÍA CON MENOR DE 13 AÑOS CON FINES SEXUALES	Ninguna
Contra la propiedad industrial/intelectual	Arts 270 a 277 y 623.5 del CP(Contra la propiedad intelectual y contra la propiedad industrial)	DELITOS CONTRA LA PROPIEDAD INTELECTUAL	Medio Empleado: Internet/informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
		DELITOS CONTRA LA PROPIEDAD INDUSTRIAL	
Contra el honor	Arts. 205 a 216 y 620.2 del Código Penal	CALUMNIAS	Medio Empleado: Internet/informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
		INJURIAS	
Amenazas y coacciones	Arts 169 a 172 y 620 del C.Penal	AMENAZAS	Medio Empleado: Internet/informática, Telefonía/comunicaciones, Intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.
		AMENAZAS A GRUPO ETNICO CULTURAL O RELIGIOSO	
		COACCIONES	

LA CIBERDELINQÜÈNCIA COM A DELICTE DE PRESENT I DE FUTUR

El terme ciberdelinqüència fa referència al conjunt d'activitats il·lícites comeses en el ciberespai que tenen per objecte els elements, sistemes informàtics o qualsevols altres béns jurídics, sempre que en la seva planificació, desenvolupament i execució resulti determinant la utilització d'eines tecnològiques; en funció de la natura del fet, de l'autoria, de la seva motivació, o dels danys infligits, es podrà parlar així de ciberterrorisme, de ciberdelicte, o en el seu cas d'haktivisme.

Així, tal com afirma l'Estratègia de Seguretat Nacional, "la cibercriminalitat és un problema de seguretat ciutadana de primer ordre, representant una de les amenaces més esteses i generalitzades, que es materialitza de forma continua i que victimitza cada vegada de manera més important a milers d'institucions, empreses i ciutadans"[4].

El terme ciberdelinqüència s'utilitza en un sentit ampli i fa referència a les normes dels mandats de l'Europol i d'Eurojust, és a dir, atacs en sistemes d'informació (atacs cibernètics), crims via cibernètica (com fraus en el no pagament efectiu i varis crims relacionats amb l'explotació sexual infantil en línia), o delictes de la criminalitat organitzada i transfronterera.

Un delicte ciberdepenent és, doncs, qualsevol activitat delictiva que pot ésser només comesa mitjançant ordinadors, xarxes informàtiques i altres formes de tecnologia de la informació i la comunicació (TIC). Aquests delictes solen restar dirigits a les computadores, xarxes i altres recursos TIC. Inclou la creació i propagació de malware, pirateria per a robar dades confidencials, dades personals o de la indústria, atacs de denegació de servei a causar danys financeres i/o de reputació i d'altres activitats criminals. Aquest tipus de delinqüència comprèn tota una sèrie de diferents tècniques d'atac i de funcionament que resten en

[4] Estrategia Nacional de Ciberseguridad 2019, pàg. 25

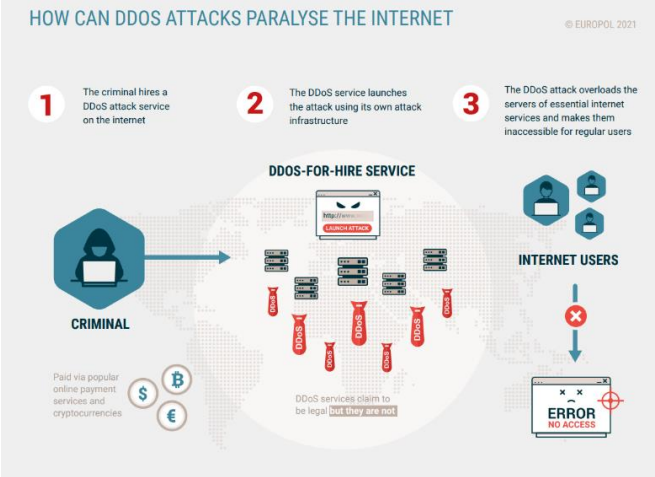
constant evolució amb la fi d'explotar prèviament totes les vulnerabilitats desconegudes. Per tant, "els ciberdelinqüents operen sota esquemes de crim organitzat i continuen explorant de manera incessant tècniques sobre les quals construir models de negoci lucratius i de baix risc, emparats sota la difícil traçabilitat de les seves actuacions[5].

Així, els delinqüents aprofiten l'era digital per fer fraus en l'àmbit online tot utilitzant tècniques de phishing i pirateria, per tal d'obtenir informació personal, així com la informació de compte bancari i dades d'inici de sessió bancària de les víctimes. Els estafadors fan servir malware per tal d'interceptar les dades d'inici de sessió per a la banca en línia (que cada vegada s'utilitza més per part de la població), i ho fan fent servir plataformes d'enginyeria social en línia vinculades al procés d'autenticació dels usuaris per accedir a dades confidencials.

Aquesta capacitat de las xarxes criminals per reaccionar i adaptar-se al canvi ha estat particularment pronunciada durant la pandèmia de COVID-19, donat que la pandèmia ha fet augmentar les compres digitals i, per tant, els pagaments en línia.

Aquest moviment general cap a unes economies amb un funcionament sense diners en efectiu crea poderosos incentius pels estafadors en els pagaments online, que busquen comprometre els pagaments en línia i en la banca mòbil, mitjançant pagaments que es basen en aplicacions de telèfon falses.

Alhora, el creixent ús de dispositius mòbils per a finalitats financeres que funcionen mitjançant processos d'autenticació ha fet que es converteixin en un objectiu per als ciberdelinqüents. Segons l'avaluació d'amenaces del crim organitzat a Internet (IOCTA) més recent, el ciberdelicte és cada vegada més agressiu i enfrontat. Això es pot veure a través de les diverses formes de ciberdelinqüència, inclosos els delictes d'alta tecnologia, les violacions de dades i l'extorsió sexual.



[5] Estrategia Nacional de Ciberseguridad 2019, pàg. 26

Tot el crim cibernètic causa pèrdues financeres significatives a las empreses, als ciutadans i al sector públic. Cada any trobem despeses tant de pagaments per ransomware, amb costos de recuperació i costos també pel que fa a les mesures per millorar la seguretat cibernètica. Cal fer esment que els atacs a les infraestructures crítiques d'una societat podrien arribar a tenir un impacte significatiu i implicar greus conseqüències.

Val a dir que la disponibilitat de serveis de ciberdelinqüència en línia forma part del propi model de negoci de grups criminals organitzats, donat que ofereixen serveis que resten a l'abast de la major part de la ciutadania. Així doncs, cal tenir molt present que els serveis i eines criminals com el malware, ransomware, DDoS, i instruccions per a realitzar molts tipus d'atacs s'ofereixen en línia, sovint a la dark web. Malauradament, molts serveis i eines de ciberdelinqüència es poden comprar mitjançant el pagament d'una tarifa d'usuari, una tarifa de lloguer o inclús un percentatge dels guanys criminals.

El frau amb pagaments que no són en efectiu abasta tot tipus d'activitats fraudulentes, aquestes poden incloure:

- Frau de compromís de correu electrònic comercial, que es dirigeix a empreses i organitzacions on continua augmentant el nombre d'intents i la seva sofisticació.
- Nous modus operandi como SIM Swapping y SMishing, que representen un risc significatiu per les víctimes, identitats i finances.
- Frau d'inversions en línia, dirigit a milers de ciutadans de l'UE cada any i que depèn cada vegada més de vendre inversions noves, com les criptomonedes.
- Phishing, que segueix sent una amenaça significativa i està evolucionant encara més en la seva sofisticació.

El moviment cap a economies sense efectiu crea poderosos incentius pels estafadors de pagaments. El creixent ús de dispositius mòbils per a finalitats financeres, transaccions i processos d'autentificació ha fet convertir-los en un objectiu pels ciberdelinqüents.

L'informe d'Avaluació de l'Amenaça del Crim Organitzat en Internet (IOCTA) 2021 de l'Europol constata que, darrere de la pandèmia mundial, la nova realitat ha implicat una ràpida adaptació de la societat en el seu conjunt que, en certs aspectes, s'ha transformat de forma permanent. Aquest fet ha comportat, alhora, una continua evolució i adaptació de la ciberdelinqüència.

Segons aquest informe, la utilització de ransomware (malware que xifra els fitxers sol·licitant un rescat per recuperar-los), aprofitant cada vegada més el teletreball generalitzat, segueix sent una de les principals amenaces, juntament a d'altres com el clàssic escaneig de a la recerca de connexions insegures.

Els cibercriminals també han aprofitat l'augment de les compres en línia amb la pretensió d'enganyar a les seves víctimes perque descarreguin software maliciós, robar les seves credencials o perpetrar diferents formes de frau.

D'altra banda, els troians bancaris per a dispositius mòbils s'han convertit en una amenaça notable donada la creixent popularitat de la banca online. Els delinqüents han seguit fent servir narratives COVID-19 per a la venda en línia de productes mèdics falsificats i per tal de robar credencials d'accés a través del vishing: una pràctica fraudulenta que consisteix en l'ús de la línia telefònica convencional i de l'enginyeria social per obtenir informacions delicades, como pot ser la financera o les dades d'identitat.

Tanmateix, es considera que els atacs coneguts com a denegació de servei distribuïda (DDoS) podrien reproduir-se donada la major dependència dels serveis en la xarxa. Cal tenir present que la pròpia estructura de la xarxa facilita la consecució dels objectius dels delinqüents, que sovint no es centren només en el frau a una sola víctima, sinó que poden assolir els mateixos objectius econòmics en el atac cibernètic a milers de víctimes.

A més, és preocupant l'augment de captació de menors en la xarxa donat l'increment del temps que estan connectats, i també per l'hàbit de produir i compartir material per as guanyar reputació o diners. En aquest context general, les accions amb ransomware es centren cada vegada més en atacs contra grans organitzacions i les seves cadenes de subministrament. Els lladres d'informació produeixen un quantiós material per poder comerciar com a subproducte de l'atac principal, que és molt rentable en el mercat.

En l'àmbit de les criptomonedes, les plataformes de compravenda, moneders virtuals i altres serveis estan augmentant la seva popularitat, fet que ha incrementat les estafes a víctimes poc curoses. Els delinqüents estan convertint, cada vegada més, els guanys il·lícits en criptomonedes, inclús els beneficis obtinguts pel material de pornografia infantil ja se comercialitzen també en aquest tipus de moneda digital. Així, l'anonimat en la xarxa, agreujat

per l'adopció a gran escala de tecnologies de xifrat, pot beneficiar a la privacitat dels usuaris, però també als delinqüents.

Les projeccions a futur sobre els delictes via online plantegen que l'amenaça real dels delictes cibernètics augmentarà encara molt més i amb una major sofisticació en els propers anys, donat que el cibercrim és molt dinàmic i explota ràpidament les tecnologies avançades.

Seran les infraestructures crítiques i les administracions l'objectiu principal dels ciberdelinqüents, la qual cosa planteja riscos significatius en relació amb la nostra seguretat. Però també ho seran els individus concrets en la seva connexió diària a la xarxa per fer les seves activitats que han deixat de ser offline per passar a tenir un funcionament online.

El desenvolupament de l'Internet de les Coses, el major ús d'intel·ligència artificial (IA), i de les aplicacions per a dades biomètriques o la disponibilitat de vehicles autònoms tindran un impacte significatiu. Aquest fet determina que cal plantejar polítiques de seguretat tant a nivell de protecció de la ciberseguretat, com pel que fa a la prevenció activa dels delictes en el ciberespai i l'abordatge de la ciberdelinqüència.

Les grans tendències tecnològiques, que s'estimen que impactaran en els propers anys, estaran fortament influenciades per la crisi global que va generar la pandèmia de la COVID-19. Aquest fet ha accelerat l'arribada de dues tecnologies molt innovadores i que poden produir un gran impacte social en un futur immediat: el passaport de salut o d'immunitat, i les tecnologies de distanciament social (amb les connotacions de privacitat i control de la població, con aplicacions de rastreig de contactes i d'altres eines per indicar a on i amb qui ha estat una persona).

De fet, el Foro Económico Mundial considera que entre els riscos de major probabilitat dels propers deu anys estaran la concentració de poder digital, la desigualtat digital i el fracàs de la ciberseguretat; mentre que entre els de major impacte es trobaran les errades (avaries o sabotatges) en la infraestructura de les TIC. En el cas específic de la categoria tecnològica, els riscos que se estimen més probables són:

- **A curt termini (0 a 5 anys)**: Errades en la ciberseguretat; desigualtat digital i ruptura en les infraestructures per a les TIC i fracàs de la governança tecnològica, tant a nivell global, com regional, nacional i individual.
- **A mig termini (5 a 10 anys)**: Avenços tecnològics adversos o disruptius. El ciberespai està governat cada vegada més por empreses privades basades en la seva generació de beneficis, fet que concentrarà progressivament la generació de valor en l'àrea dels serveis, la qual cosa seguirà afavorint la deslocalització, tot convertint a una gran part dels Estats en consumidors necessaris i permetent un més gran poder de les grans potencies tecnològiques.

El ciberespai es continua configurant, doncs, como un àmbit ple de riscos, ciberatacs, fraus i robatoris de dades, que provenen de qualsevol punt del planeta, i que són, a més a més, de difícil atribució, especialment aquells que venen de la mà dels propis Estats.

Tal com afirma el Panorama de Tendencias Geopolíticas, "el paper de les organitzacions i administracions a l'hora de fixar estàndards, interoperabilitat i governança, serà de gran importància donat el risc del creixement i intensitat de les ciberamenaces, a cavall del desenvolupament de la IA i d'altres tecnologies. La seguretat serà cada vegada més depenent del ciberespai i la governança a nivell global i regional, conviurà amb tendències de caràcter reactiu davant les ciberamenaces (lleis i normatives que hauran de ser contínuament actualitzades), i amb altres de caràcter proactiu que intentaran dissuadir i neutralitzar tals amenaces (incloent accions preventives i ofensives)".

Estem veient com la ciberseguretat s'està convertint en un objecte de competició i confrontació geopolítica pel seu predomini, i la capacitat o no de neutralitzar les amenaces (incloses les militars) determinarà la vida i funcionament del ecosistema cibernètic. Cal tenir present que les innovacions tecnològiques, alhora, crearan oportunitats criminals i hem d'estar preparats per aquesta realitat que esdevindrà. El rendiment dels sistemes i aplicacions d'intel·ligència artificial es basen en conjunts de dades, un accés maliciós a aquestes dades implica la revelació de dades d'informació personals. Si la IA s'utilitza en els sistemes de presa de decisions, la manipulació de dades pot tenir greus conseqüències per als usuaris individuals.

A nivell europeu, la ciberdelinqüència és una de les prioritats de la UE en la lluita contra el crim greu i organitzat en el marc d'EMPACT 2022-2025. Ho és en tant que suposa un problema

creixent pels estats membres de la UE, donat que resten dotats d'una infraestructura d'internet ben desenvolupada i de sistemes de pagament en línia.

La Plataforma Multidisciplinària Europea contra les Amenaces Criminals (EMPACT) aborda les amenaces més importants que suposa la delinqüència internacional organitzada i greu que afecta la UE. EMPACT reforça la intel·ligència, la cooperació estratègica i operativa entre les autoritats nacionals, les institucions i organismes de la UE i els socis internacionals.

No es tracta només de dades financeres, sinó de dades més generals, que són un objectiu clau per als ciberdelinqüents, tot provocant més casos de frau i extorsió. El gran ventall d'oportunitats que els ciberdelinqüents han intentat explotar és impressionant. Aquests delictes inclouen:

- Utilitzar botnets (xarxes de dispositius infectats amb programari maliciós sense el coneixement dels seus usuaris) per transmetre virus que obtinguin un control remot il·lícit dels dispositius, robar contrasenyes i desactivar la protecció antivirus).
- Crear "portes del darrere" en dispositius compromesos per permetre el robatori de diners i dades, o l'accés remot als dispositius per crear botnets.
- Creació en línia d'una experiència en pirateria comercial.
- Allotjament a prova de bales i creació de serveis contra antivirus.
- Blanqueig de monedes tradicionals i virtuals.
- Cometre fraus en línia, com ara a través de sistemes de pagament en línia, targetes i enginyeria social.
- Diverses formes d'explotació sexual infantil en línia, inclosa la distribució en línia de materials d'abús sexual infantil i la transmissió en directe d'abusos sexuals infantils.
- Allotjament en línia d'operacions relacionades amb la venda d'armes, passaports falsos, targetes de crèdit falsificades i clonades i drogues i serveis de pirateria informàtica.

El mes de maig de 2021, el Consell de la Unió Europea va decidir les prioritats de la UE per a la lluita contra el crim greu i organitzat per a EMPACT 2022-2025. Entre aquestes prioritats trobem els ciberatacs que cal combatre tot:

1. Dirigint-se a combatre als delinqüents que orquestren ciberatacs, especialment aquells que ofereixen serveis delictius especialitzats en línia.
2. Dirigint-se a combatre delinqüents individuals i xarxes criminals que orquesten esquemes de frau a gran escala en línia, així com frau i falsificació de mitjans de pagament sense efectiu destinats a defraudar persones privades (incloses persones vulnerables com la gent gran), empreses i organitzacions del sector públic, especialment aquelles que generen ingressos multimilionaris cada any i que utilitzen

plataformes en línia per amplificar l'abast de les seves estafes per dirigir-se a un gran nombre de víctimes.

3. Dirigint-se a combatre l'abús infantil en línia i fora de línia, inclosa la producció i difusió de material d'abús infantil, així com l'explotació sexual infantil en línia.

El Centre Europeu de Ciberdelinqüència (EC3) va ser creat per Europol per reforçar la resposta policial a la ciberdelinqüència a la UE i ajudar així a protegir els ciutadans, les empreses i els governs europeus de la delinqüència en línia. A nivell d'operacions, l'EC3 se centra en els següents tipus de ciberdelictes:

- Delictes ciberdependents
- Explotació sexual infantil
- Frau en el pagament

EC3 ofereix suport operatiu, estratègic, analític i forense a les investigacions dels Estats membres. Per a cadascun dels tipus de ciberdelinqüència esmentats anteriorment, EC3:

- Serveix com a centre central d'informació i intel·ligència criminal.
- Dona suport a les operacions i investigacions dels Estats membres oferint anàlisi operacional, coordinació i experiència.
- Proporciona capacitats de suport forense tècnic i digital altament especialitzades a investigacions i operacions.
- Proporciona suport a les estructures de gestió de crisi de la UE, en l'àmbit del mandat de l'Europol, i facilita la col·laboració operativa, tècnica i estratègica entre les agències d'aplicació de la llei (LEAs) i altres comunitats cibernètiques rellevants i les institucions, organismes i agències de la UE (per exemple, Eurojust, EEE, ENISA, CERT-EU, Comissió, Consell, etc.).
- Proporciona suport operatiu i tècnic les 24 hores del dia, els 7 dies de la setmana, als LEAs per a la reacció immediata a incidents cibernètics urgents i/o crisis cibernètiques mitjançant el servei stand-by i el Protocol de resposta a emergències de les forces de l'ordre de la UE (EU LE ERP).
- Acull i facilita els esforços del Grup de Treball Conjunt d'Acció contra la Ciberdelinqüència (J-CAT) en la lluita contra la ciberdelinqüència.
- Dona suport a la formació i el desenvolupament de capacitats, en particular per a les autoritats pertinents dels estats membres.
- Proporciona una varietat de productes d'anàlisi estratègica que permeten la presa de decisions informades sobre la lluita i la prevenció de la ciberdelinqüència.
- Proporciona una funció de divulgació integral que connecta les autoritats policials que aborden el ciberdelicte amb el sector privat, l'acadèmia i altres socis no policials.
- Contribueix a l'elaboració i realització de campanyes i activitats normalitzades de prevenció i sensibilització en els àmbits de la ciberdelinqüència.

EC3 allotja i dona suport al Grup de Treball Conjunt d'Acció contra la Ciberdelinqüència (J-CAT), que està format per oficials d'enllaç cibernètic de diversos estats membres de la UE, socis d'aplicació de la llei no comunitaris i EC3. Els membres del Grup de Treball proposen, seleccionen i treballen junts en casos d'alt perfil per a la investigació, donat que els cossos policials de tot el món es troben amb ciberdelictes similars i objectius criminals similars, i això demana un enfocament internacional i coordinat del problema. Els agents d'enllaç cibernètic provenen de:

- 12 Estats membres de la UE (Àustria, Bèlgica, Finlàndia, França, Alemanya, Itàlia, Països Baixos, Romania, Polònia, Suècia, Dinamarca i Espanya, que està representada per dos organismes: Policia Nacional i Guàrdia Civil).
- 7 països no socis de la UE (Austràlia, Canadà, Colòmbia, Noruega, Suïssa, el Regne Unit i els Estats Units).
- Centre Europeu de Ciberdelinqüència (EC3) de l'Europol.

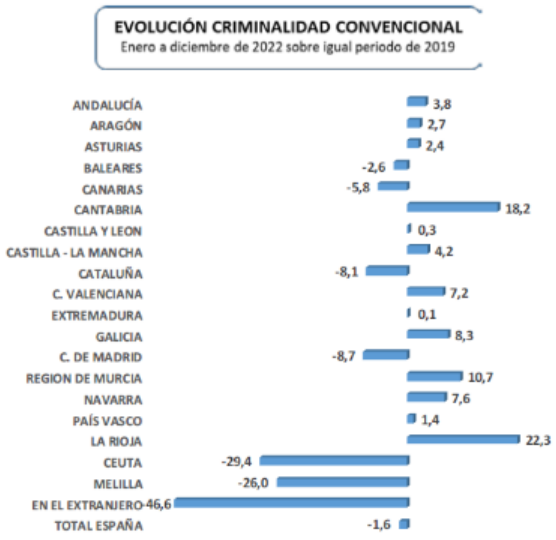
A l'any 2022 el Grupo de Trabajo Conjunto sobre Finanzas Criminales y Criptomonedas va fer una sèrie de recomanacions arrel de la 6a Conferència Global sobre Finances i Criptomonedes que pretenen destacar enfocs amplis i millores pràctiques:

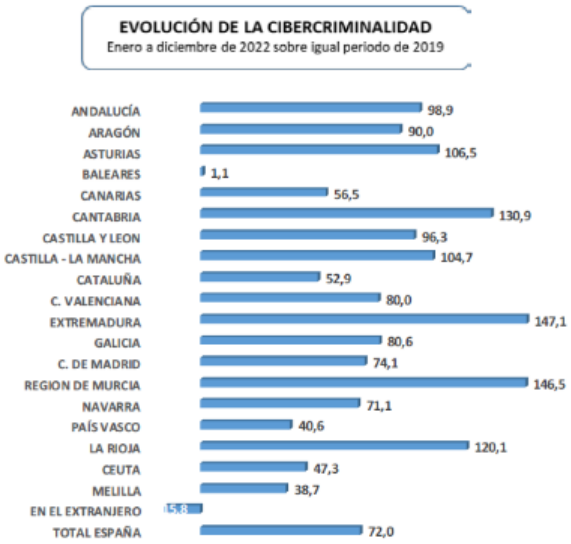
1. Trencar amb les barreres entre "tradicional" i "cripto". La separació entre el crim organitzat "tradicional" i "cripto" i el blanqueig de diner és cada vegada menys útil. L'ús de criptomonedes per a blanquejar diners mostren com els dos mons s'estan fusionant. Els estafadors fan servir el mon online per blanquejar diners procedent de les xarxes criminals tradicionals.
2. Cal harmonitzar, doncs, les actuacions policials en el món amb el món virtual en el combat contra la delinqüència. Aquí esdevé cabdal la incorporació de la formació bàsica en tecnologia blockchain i en criptomonedes i un desenvolupament professional continu, per a tots els organismes encarregats de fer acomplir la llei i per a totes les autoritats públiques pertinents, incloent les unitats d'intel·ligència financera i les autoritats judicials.
3. Generar equips multidisciplinaris especialistes en delictes financers, en el crim organitzat, i en els delictes online per tal de cooperar en casos i compartir coneixements.
4. Regular de manera més estricta el mercat de criptoactius i tipificar els delictes o fraus en aquesta matèria de manera igual als actius i delictes financers. Cal controlar de manera ferma el mercat de criptoactius per evitar un mals ús dels mateixos.
5. Desenvolupar campanyes explicatives i de sensibilització dels perills de les criptomonedes. Els usuaris comuns han comprendre els riscos d'invertir en criptoactius per tal d'evitar estafes i robatoris.
6. Els funcionaris encarregats de fer acomplir la llei han de poder identificar ràpidament els casos on hi ha risc d'un blanqueig de diner, per tant, calen cursos de formació

continuada per les forces d'ordre encarregades d'identificar actuacions que per la seva pròpia naturalesa evolucionen a molta velocitat.

7. Augmentar la col·laboració públic-privada. Cal una cooperació més estreta amb els proveïdors de serveis de criptoactius per tal de poder accelerar les sol·licituds d'aplicació de la llei per ajudar en les investigacions i congelar els fons.

Pel que a Espanya, la cibercriminalitat va en augment segons les dades del Ministeri d'Interior L'any 2022 es van produir un total de 375.506 infraccions penals catalogades com a cibercrim (16.1 % del total). Aquestes dades representen un increment del 72% respecte l'any 2019.





II. CIBERCRIMINALIDAD (infracciones penales cometidas en/por medio ciber)	**218.302**	**305.477**	**375.506**	**72,0**	**22,9**
12.-Estafas informáticas	192.375	267.011	336.778	75,1	26,1
13.-Otros ciberdelitos	25.927	38.466	38.728	49,4	0,7
III. TOTAL CRIMINALIDAD EN ESPAÑA	**2.199.475**	**1.957.719**	**2.325.358**	**5,7**	**18,8**

En base a aquest augment de la cibercriminalitat online, el Ministeri d'Interior va aprovar en 2021 el Pla Estratègic contra la Cibercriminalitat tot presentant una nova campanya de conscienciació en les xarxes socials per tal d'alertar i conscienciar a la població sobre les amenaces de la ciberdelinqüència.

Des d'aquests principis, el pla dissenya una estratègia global per assolir els següents objectius específics:

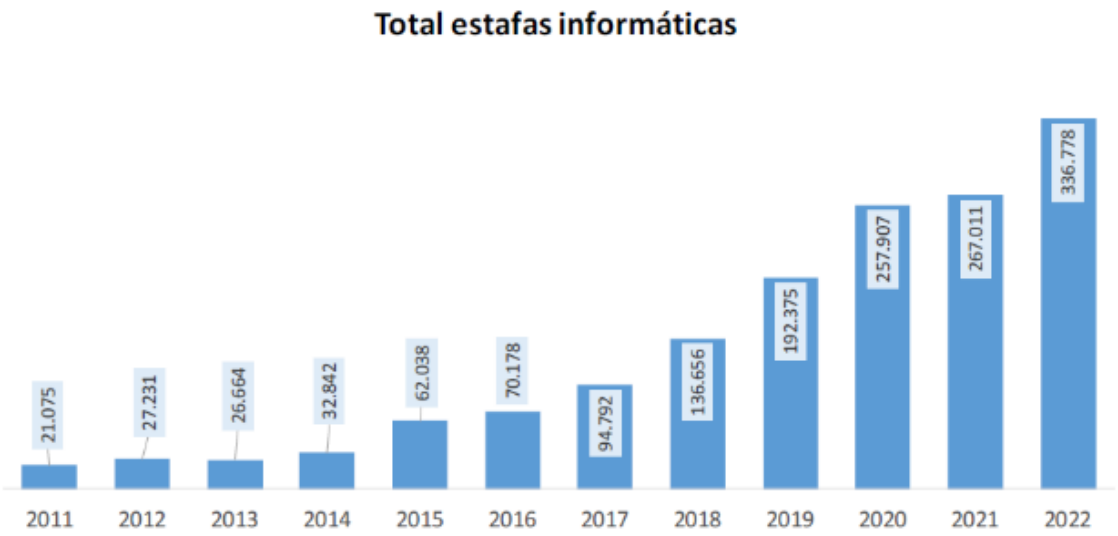
- Promoure la cultura de prevenció de la cibercriminalitat entre la ciutadania i l'empresa.
- Impulsar la formació i l'especialització dels membres de les FCSE en matèria de ciberseguretat i cibercriminalitat.
- Incrementar i millorar l'ús i disposició de les eines tecnològiques i implementar l'àmbit de la I+D+i.
- Gestionar adequadament la informació disponible en el ciberespai.

- Promoure un marc legal i institucional que doni solució als desafiaments que sorgeixin relacionats amb la ciberseguretat i la cibercriminalitat.
- Impulsar la coordinació a nivell nacional i internacional i afavorir la col·laboració entre el sector públic i privat.

El Pla Estratègic contra la Cibercriminalitat dota al Ministeri de l'Interior dels recursos necessaris per a fer front a aquesta situació en cinc àrees d'actuació: detecció, prevenció, protecció, resposta i persecució, així com l'atenció adient a les víctimes.

Cal dir que els Mossos d'Esquadra han participat sobretot en els aspectes de la generació de **ciberintel·ligència i la prevenció i resolució de cibercriminalitat** a través de la seva especialitzada **Unitat Central de Delictes informàtics (UCDI) així com la d'Intel·ligència, Investigació Criminal i sobretot, la Unitat Central d'Estafes i Mitjans de Pagament (UCEMP)**.

Tot i aquests esforços, en el Balanç de Criminalitat corresponent al segon trimestre del any 2022, publicat pel Ministeri de l'Interior trobem un important augment en les dades d'estafes informàtiques, augment que accentua un increment sostingut al llarg dels darrers anys.



En els darrers 12 mesos s'han registrat un total de 236.451 delictes d'estafes informàtiques, mentre que a l'any 2019, any de referència anterior a la pandèmia, es van produir un total de 140.354 delictes, la qual cosa suposa que se ha produït un augment del 68,5 per cent en aquest tipus penal. A més a més, de forma quantitativa, les estafes informàtiques suposen ja el 13,4 per cent del total dels delictes comesos en el darrer any.

L'Estratègia de Seguretat Nacional afirma que la seguretat en les xarxes és una dimensió fonamental per l'estabilitat en preservar la defensa dels valors i principis constitucionals i democràtics, així com els drets fonamentals dels ciutadans en el ciberespai, especialment en

la protecció de les seves dades personals, la seva privacitat, la seva llibertat d'expressió i l'accés a una informació veraç i de qualitat.

Cal treballar, doncs, des d'un enfocament multidisciplinari, i de manera coordinada entre totes les administracions conjuntament amb el sector privat, per tal de preservar el bon funcionament del ciberespai i protegir la privacitat dels usuaris. Per això, és important generar estructures d'experts en ciberseguretat amb un alt nivell de formació que protegeixin els ciutadans davant possibles conductes delictives de manera preventiva.

Cal transitar cap a un enfocament preventiu i dissuasiu que permeti dotar un sistema d'alertes eficaç i alhora, d'elements que permetin investigar i perseguir els autors de les conductes delictives. A més, cal una major implicació de tota la societat mitjançant el foment d'una cultura de ciberseguretat entre tota la societat en el seu conjunt. Així, l'Estratègia Nacional de Ciberseguretat es sustenta en els principis rectors de la Seguretat Nacional: unitat d'acció, anticipació, eficiència i resiliència.

És necessari també tenir una concepció dinàmica a l'hora d'interpretar un fenomen que és de caire evolutiu en si mateix. La pròpia variabilitat i adaptabilitat dels delinqüents a les mesures de protecció establertes a la xarxa fa que la concepció pública de la protecció i seguretat online també hagi d'anar evolucionant. Tal como veiem a la figura posterior el concepte de la ciberseguretat ha anant variant amb el pas del temps, sent cada vegada més proactiu en el combat front els que volen atacar el bon funcionament del món online.

Figura 1. Evolución del concepto de ciberseguridad.

Pel que fa a Catalunya, mitjançant la Llei 15/2017, del 25 de juliol, de l'Agència de Ciberseguretat de Catalunya, es va crear l'Agència de Ciberseguretat de Catalunya, com a entitat de dret públic, amb personalitat jurídica pròpia, i sotmesa al dret privat. Té les funcions de desenvolupar i liderar el servei públic de ciberseguretat necessari per a la protecció del territori de Catalunya davant les amenaces actuals, coordinar la ciberseguretat entre els diferents actors en l'àmbit de Catalunya com a responsable d'aquesta matèria, i garantir la ciberseguretat de l'Administració de la Generalitat i del seu sector públic, i, si escau, de les altres entitats i institucions públiques de Catalunya, dels ens locals i de les persones físiques i jurídiques situades a Catalunya.

Segons **el Llibre blanc sobre la Intel·ligència Artificial** aplicada a la Ciberseguretat de l'Agència de Ciberseguretat de Catalunya, hi ha aproximadament un total de 179 empreses dedicades a l'àmbit d'Intel·ligència Artificial, amb una facturació de 1.358 milions d'euros anuals i que ocupen un total de 8.483 professionals (dades 2019). Per la seva banda, la ciberseguretat engloba aproximadament 495 empreses, amb una facturació de 1.071 milions d'euros i ocupant a 9.414 professionals (dades 2023).

L'estudi de la ciberseguretat s'aborda a partir de les cinc accions relacionades amb un ciberatac: identificar, protegir, detectar, respondre i recuperar, així com també els grans grups d'amenaces caracteritzats per ENISA (Agència de la Unió Europea per a la Ciberseguretat), des del malware fins els ciberatacs específics dirigits contra la indústria del videojoc. Al mateix temps les diferents tècniques i metodologies de la ciberseguretat hauran d'evolucionar per afrontar els reptes que sorgeixen degut a l'evolució de la tecnologia, com per exemple els que planteja la irrupció del metavers, la proliferació de la IoT o la ciberseguretat industrial en el marc de la Indústria 4.0/5.0.

El món de la ciberseguretat, tal com veiem a la imatge inferior té una forta implantació i desenvolupament a Catalunya, quelcom positiu al nostre entendre, tot i que entenem que cal una mirada de conjunt que permeti desenvolupar estratègies tant de creixement harmònic com d'abordatge de les vulnerabilitats de present i de possibles ciberatacs.

Figura 7: Agents de l'ecosistema de la Ciberseguretat a Catalunya (font: La Ciberseguretat a Catalunya, AC-CIO, març 2022)

Del total d'empreses que treballen en l'àmbit de la ciberseguretat, el 85% són petites i mitjanes, d'entre les quals un 9,5% són startups. Un altra dada interesant a destacar és que el 28.7% de les empreses són exportadores de productes, serveis o consultoria a l'exterior. En relació amb el volum, el 53.6% de les empreses facturen més d'un milió d'euros i el 21.7% més de 10 milions. Pel que fa a la paritat home-dona només un 13.8% tenen dones en posicions directives. Per últim, el 29.1% d'aquestes empreses es va crear fa menys de 10 anys, la qual cosa indica que la creixent demanda de ciberseguretat en els darrers temps ha estimulat el naixement d'un important nombre d'empreses del sector.

Però, tot i aquesta forta implantació que observem al territori de Catalunya, les dades, tant en conjunt com desgranades per província, denoten també un augment en els ciberdelictes (s'han triplicat respecte a l'any anterior). Catalunya encapçala les denúncies contra fets que tenen a veure amb la ciberdelinqüència. Les dades demostren que el recorregut de millora és molt gran, no només de present, on allò que s'ha dut a terme no ha impedit que les xifres de delictes es multipliquessin per 3. Cal assegurar també el futur donat que el creixement en l'ús de la tecnologia anirà a més per part de tota la ciutadania.

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

3.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD

(Fuente de datos: Sistema Estadístico de Criminalidad: Datos de los cuerpos policiales)

>> 3.5. Representación territorial de hechos denunciados de cibercriminalidad. Año 2022

Hechos denunciados de CIBERCRIMINALIDAD - 2022

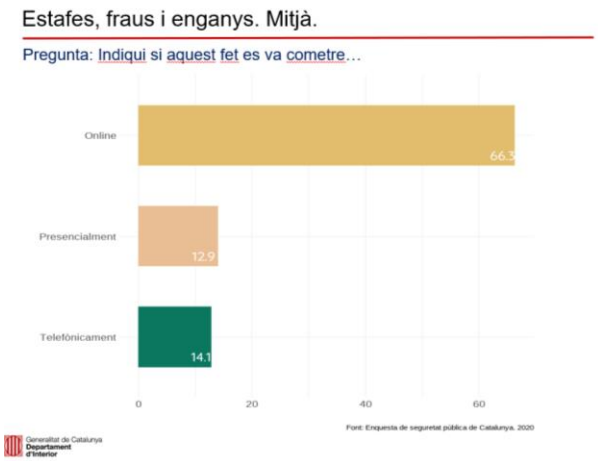
Hechos conocidos:	374.737
Esclarecimiento (*):	51.642
Detenciones/invest:	15.097

14,6%

CCAA	Hechos
CATALUÑA	63.877
MADRID (COMUNIDAD DE)	63.758
ANDALUCÍA	56.908
COMUNITAT VALENCIANA	34.005
CASTILLA Y LEÓN	21.302
GALICIA	20.914
PAÍS VASCO	20.907
CASTILLA - LA MANCHA	15.649
CANARIAS	13.684
MURCIA (REGIÓN DE)	9.971
ARAGÓN	9.620
BALEARS (ILLES)	8.701
ASTURIAS (PRINCIPADO DE)	8.560
EXTREMADURA	7.528
EN EL EXTRANJERO	5.643
NAVARRA (COMUNIDAD FORAL DE)	5.499
CANTABRIA	4.806
RIOJA (LA)	2.433
CIUDAD AUTÓNOMA DE CEUTA	567
CIUDAD AUTÓNOMA DE MELILLA	405

(*) Debido a que la Ertzaintza no facilita datos de esclarecidos el % de esclarecimiento se ha calculado sin tener en cuenta los hechos conocidos por este cuerpo policial

Aquest augment dels ciberdelictes, tot i els avenços en ciberseguretat, també resta constatat des del punt de vista de la ciutadania en la darrera Enquesta de Seguretat de Catalunya:



El Pla General de Seguretat de Catalunya 2023-2025, pel que fa enganys, estafes i fraus en l'àmbit tecnològic destaca que "en l'edició del 2020, aquella que recull les experiències de victimització de novembre del 2019 a novembre del 2020 i, per tant, registra els mesos de confinament, els resultats han estat aclaparadors. Així com tots els àmbits experimentaven un

descens o es mantenien estables, en el cas dels enganys, estafes i fraus, l'increment ha estat de més de 6 punts percentuals. D'aquesta manera, el 13.8 % de les persones enquestades manifestava haver patit com a mínim un fet relacionat amb aquest àmbit de victimització, i aquest tipus de fets va suposar el 32.5% dels fets totals registrats davant el 17.8% de l'any 2017"[6].

El Pla també alerta que la sofisticació i professionalització del cibercrim incrementa els reptes associats a la seva prevenció, detecció i persecució. La multitud de pràctiques delictives associades a l'entorn digital creix i canvia ràpidament, donant lloc a noves modalitats. La sofisticació i professionalització del cibercrim incrementa els reptes associats a la seva prevenció, detecció i persecució. D'aquesta manera, queda clar que els riscos associats a les noves tecnologies esdevenen una amenaça prioritària en el camp de la seguretat[7].

Un dels exemples més palpables són els atacs al sector sanitari, on els ciberdelinqüents pretenen fer xantatge via online mitjançant robatori de dades personals dels pacients i avenços en les assaigs clínics i en els temes d'innovació mèdica.

En el darrer informe de l'Agència de Ciberseguretat de Catalunya del més de març trobem una sèrie de dades que ens alerten per si mateixes de la necessitat de passar a l'acció de manera ferma en el combat contra la ciberdelinqüència

CONSTATACIONS I PROPOSTES

El Govern Alternatiu de Catalunya constata que:

1. La modalitat del delicte online ha crescut exponencialment en base a la utilització d'internet. Les dades i les previsions denoten que aquesta modalitat delictiva anirà a més.
2. Tot i el gran desplegament d'eines de ciberseguretat, la ciberdelinqüència s'ha triplicat el darrer any. Cal abordar la qüestió des d'una altra perspectiva més proactiva.
3. Les dades demostren que l'abordatge de la qüestió és insuficient.
4. Cal una mirada i un abordatge específic de les conclusions generals d'aquest informe pel que fa als menors d'edat en tant que subjectes especials de drets i de protecció.

[6] Pla de Seguretat de Catalunya 2025. Pàg.12

[7] Pla de Seguretat de Catalunya 2025. Pàg.12

Per aquestes raons, es proposen les següents actuacions de millora:

1. Establir mecanismes ferms de combat de la cibercriminalitat que permetin la persecució del frau i dels grups organitzats que practiquen la delinqüència online.
2. Reforçar les capacitat d'investigació i persecució de la cibercriminalitat, per garantir la seguretat ciutadana i la protecció dels drets i llibertats en el ciberespai, en consonància amb la línia d'acció 3 de l'Estratègia Nacional de Ciberseguretat.
3. Donar eines al Cos de Mossos d'esquadra i a les Policies Locals de Catalunya per poder combatre aquesta modalitat delictiva. Dotar el Cos de Mossos d'Esquadra d'una estructura amb capacitat d'adaptació a noves modalitats delictives online i amb una formació continuada.
4. Reforçar la captació de talent i l'estructura del Cos de Mossos d'Esquadra amb facultatius experts en la matèria. Val a dir que és un element que juga en contra les diferències salarials entre l'esfera pública i l'àmbit privat en aquesta qüestió.
5. Establir estructures en xarxa que permetin les alertes ràpides i actuacions de conjunt ràpides i efectives. La profusió d'empreses dedicades a la ciberseguretat pot generar oportunitats als ciberdelinqüents si no hi ha un enfocament unitari.
6. Reforçar els estudis en ciberseguretat a Catalunya.
7. Posar en marxa campanyes de sensibilització i de pedagogia per tota la població en el risc que suposa l'ús d'internet, especialment en allò que fa referència l'escletxa digital.
8. Estudiar la integració de l'Agencia de Ciberseguretat de Catalunya al si del Cos de Mossos d'Esquadra i del Departament d'Interior.
9. Establir protocols àgils de col·laboració públic-privada en l'abordatge de la ciberseguretat a Catalunya sota el lideratge de l'administració pública.
10. Obrir una convocatòria d'ajudes a les empreses i organitzacions per garantir la ciberseguretat. S'ha de garantir la formació a les universitats, instituts i a les mateixes empreses en ciberseguretat.
11. Garantir la coordinació amb l'Estat en aquesta matèria per via de:
    a. Coordinació amb el Centre d'Operacions de Ciberseguretat per adequar una resposta unitària i un treball conjunt.
    b. Coordinació amb el grup de treball liderat pel Centre Criptològic Nacional, activat per al seguiment de la guerra d'Ucraïna, per analitzar la seva vessant com a conflicte híbrid ("guerra digital").
12. Donar suport a les administracions locals, organismes públics o d'interès general. Ampliar i potenciar el model de ciberseguretat per a les administracions locals de Catalunya, iniciat al juny del 2020, perquè es converteixi en un sistema plenament complet i segur, especialment per aquelles administracions locals que per la seva mida o recursos no poden dur a terme polítiques pròpies de ciberseguretat.

13. Apostar pel desenvolupament del sector privat de la ciberseguretat garantint els següents aspectes:

a. Incrementar la competitivitat i creixement de les empreses catalanes del sector de la ciberseguretat.
b. Fomentar la internacionalització del sector empresarial de la ciberseguretat català.
c. Treball conjunt amb el teixit productiu i industrial per assegurar la seva protecció davant de ciberatacs.
d. Creació de programes de formació específica en ciberseguretat a les empreses catalanes.
e. Línia d'ajudes per a accions i estratègies de ciberseguretat a les pimes catalanes.

14. Crear una cultura de ciberseguretat a la societat i als entorns laborals que generi confiança i incrementi les capacitats de ciberseguretat en les empreses i la ciutadania, mitjançant, entre d'altres, campanyes de sensibilització, promoció i formació de ciberseguretat.
15. Garantir la generació de talent garantint els següents aspectes:
    a. Identificar, generar i desenvolupar talent en ciberseguretat.
    b. Donar resposta al creixement del sector de la ciberseguretat a Catalunya (+20% que l'any anterior), oferint els perfils i el talent necessari.
    c. Augmentar la inversió en el sistema públic universitari en els graus del sector.
    d. Ampliar el nombre de certificacions per a professionals de ciberseguretat.
16. Incorporar, a l'Estratègia 5G a Catalunya, aprovada el febrer de 2019, un apartat específic de ciberseguretat associada a la xarxa. Cal ampliar l'estratègia, fer anàlisi de vulnerabilitats (especialment de la cadena de subministres) i treballar conjuntament amb el Govern d'Espanya en la línia de la nova Llei.