



GOBIERNO
DE ESPAÑA

MINISTERIO
DEL INTERIOR

SECRETARÍA
DE ESTADO
DE SEGURIDAD

DIRECCIÓN GENERAL
DE COORDINACIÓN
Y ESTUDIOS



sec

Sistema Estadístico
de Criminalidad

2021

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA



Dirección General de Coordinación y Estudios
Secretaría de Estado de Seguridad

JAVIER LÓPEZ GUTIÉRREZ

FRANCISCO SÁNCHEZ JIMÉNEZ

DAVID HERRERA SÁNCHEZ

FRANCISCO MARTÍNEZ MORENO

MARCOS RUBIO GARCÍA

M^a. VICTORIA GIL PÉREZ

ANA M^a. SANTIAGO OROZCO

MIGUEL A. GÓMEZ MARTÍN

AUTORES /
AUTORAS

© De los textos: sus autores

© De la presente edición: Ministerio del Interior. Gobierno de España

NIPO: 126-20-021-2

ÍNDICE

- 4** INTRODUCCIÓN
- 27** RADIOGRAFÍA DE LA SOCIEDAD DE LA INFORMACIÓN
- 35** INFRAESTRUCTURAS CRÍTICAS Y CIBERSEGURIDAD
- 42** DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD
- 56** METADATA

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

1.- INTRODUCCIÓN

La Cibercriminalidad como fenómeno complejo y global requiere un enfoque multidisciplinar para abordar cualquier planteamiento de respuesta contra la misma. Para ello, una primera aproximación impone el conocimiento y la visualización de la realidad criminal a la que nos enfrentamos. El conocimiento de esta realidad viene obligado a describir aspectos no solamente relacionados con los datos estadísticos, sino que implica también ahondar en otras temáticas de referencia que deben ser consignadas aquí para dimensionar y comprender adecuadamente el fenómeno de la ciberdelincuencia.

Con dicho polo de actuación, la publicación periódica de informes sobre esta materia, dimensionando su realidad objetiva, trata de poner de manifiesto los aspectos más relevantes de este fenómeno criminal, alertando sobre los peligros reales y potenciales, y convirtiéndose en un elemento facilitador e imprescindible para la concienciación frente a este fenómeno.

A tales fines responde la publicación de este **IX Informe sobre Cibercriminalidad**, correspondiente a la delincuencia informática registrada en el año 2021.

Los datos de este Informe son los correspondientes a la información estadística que computa la ciberdelincuencia conocida y registrada por las Fuerzas y Cuerpos de Seguridad. Se aúnan en este tipo de informe los **datos de los cuerpos policiales del territorio nacional** (Cuerpo Nacional de Policía, Guardia Civil, Policía Foral de Navarra, Ertzaintza, Mossos d'Esquadra y Cuerpos de Policía Local que facilitan datos al Sistema Estadístico de Criminalidad), tanto en la vertiente de los hechos conocidos, victimizaciones, como de las detenciones e investigados.

Para el capítulo de victimizaciones, se añaden para el año 2021 datos de la Ertzaintza, hecho que no se produce en informes anteriores a éste.

Los datos proceden del Sistema Estadístico de Criminalidad (SEC), y de los incidentes que registra la Oficina de Coordinación de Ciberseguridad (OCC), en función de su ámbito de actuación y competencias. Reseñar, que se detallan en el apartado de Metadata, los datos que proporcionan cada Cuerpo policial en cuestión.

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

Este Informe aglutina datos del año 2021, no solo en relación a la información estadística sobre delitos informáticos en nuestro país, además, en un primer apartado y a modo introductorio, una serie de informaciones publicadas por otros organismos nacionales (INE) e internacionales (EUROSTAT, Comisión Europea), en relación a aquellas características más relevantes que permiten perfilar los rasgos distintivos de la sociedad española en relación a las tecnologías de la información y las comunicaciones (TIC).

En el segundo y tercer bloque del Informe se explican los datos procedentes de la Oficina de Coordinación de Ciberseguridad (OCC), así como los extraídos del Sistema Estadístico de Criminalidad (SEC), registrados por las Fuerzas y Cuerpos de Seguridad. Información que es desglosada en diferentes apartados (hechos conocidos, distribución territorial, perfil de las víctimas, detenciones efectuadas, incidentes por Comunidad Autónoma de referencia, por sector estratégico, etc.), lo que permite mostrar la realidad de la Cibercriminalidad en nuestro país.

Debe tenerse en cuenta que cuando dentro del presente Informe se facilitan datos de series históricas, se ven afectados por varios cambios legislativos producidos durante los últimos años. Uno de ellos fue la reforma de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, en el año 2015. La otra fue la ratificación por España del *Protocolo Adicional al Convenio sobre la Ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos*, hecho en Estrasburgo, el 28 de enero de 2003 (entró en vigor 1 de abril de 2015).

La tipificación de las conductas sigue las mismas conceptualizaciones que emplea el Convenio de Budapest¹, a los que se le ha añadido por el volumen y la importancia de la cifra registrada, las siguientes infracciones penales: a) delitos contra el honor; b) amenazas y coacciones.

Un aspecto que es necesario resaltar es el previsible aumento de la ciberdelincuencia. En palabras de las propias instituciones europeas², *“Los ciberataques y la ciberdelincuencia están aumentando en toda Europa, y cada vez son más sofisticados. Esta tendencia seguirá agravándose en el futuro, ya que se espera que 22 300 millones de dispositivos en todo el mundo estén conectados a la internet de las cosas de aquí a 2024”*.

¹ https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221
² <https://www.consilium.europa.eu/es/policies/cybersecurity/>

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

En las siguientes infografías se muestran³ datos y cifras sobre las principales ciberamenazas que ha sufrido la Unión Europea entre abril de 2020 y julio de 2021.

Principales ciberamenazas en la UE



Programas de secuestro

Tipo de ataque malintencionado en el que los ciberdelincuentes encriptan los datos de una organización y exigen un rescate para restaurar el acceso.

El precio medio de los rescates se ha duplicado.

Programas malignos

Programas informáticos malintencionados concebidos para dañar un dispositivo, perturbar su funcionamiento o acceder a él sin autorización.

Los ataques con programas malignos en la UE se han reducido en un 43 %.



Criptosequestros o criptomonera maliciosa

Uso no autorizado del ordenador, el teléfono inteligente o la tableta de un usuario para minar criptomoneda.

Las criptomonedas siguen siendo el método de pago más frecuente entre los ciberdelincuentes.

Ataques por correo electrónico

Tentativas de robo de contraseñas o datos de tarjetas de crédito a través de diversas técnicas, como el *phishing*, el *phishing* de SMS y el *spam*.

Los mensajes «gancho» relacionados con la COVID-19 siguen dominando los ataques por correo electrónico.



³ <https://www.consilium.europa.eu/es/infographics/cyber-threats-eu/>

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA



Violaciones de la seguridad de los datos y fugas de datos

Divulgación de datos sensibles, confidenciales o protegidos en un entorno no fiable.

Se ha producido un aumento de las violaciones de seguridad de datos sanitarios.

Ataques distribuidos de denegación de servicio

Ataques que impiden a los usuarios de una red o sistema acceder a información, servicios u otros recursos pertinentes.

Se han producido más de 10 millones de ataques distribuidos de denegación de servicio debido a la COVID-19.



Desinformación

Ataque intencionado consistente en crear o divulgar información falsa o engañosa para manipular a la opinión pública.

La COVID-19 es uno de los principales temas de los ataques de desinformación.

Amenazas no malintencionadas

En su mayoría se deben a errores humanos, aunque también pueden darse como consecuencia de catástrofes naturales que causan daños en las infraestructuras informáticas.

El 50 % de estos ataques se deben a fallos de configuración.



INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA



Amenazas a la cadena de suministro

Ataques dirigidos contra una organización a través de las vulnerabilidades de su cadena de suministro, capaces de producir efectos en cascada.

El 58 % de los ataques a las cadenas de suministro tiene por objetivo obtener acceso a datos.

Fuente: Panorama de amenazas de ENISA, 2021 (cifras de abril de 2020 a julio de 2021)



Consejo de la Unión Europea
Secretaría General

© Unión Europea, 2021
Reproducción autorizada, con indicación de la fuente.

Infografía nº 1.-Principales ciberamenazas en la UE (Fuente Consejo de Europa)

Es importante destacar como aspecto referencial el hecho de que en junio de 2017 la Unión Europea estableció un marco para una respuesta diplomática conjunta de la UE a actividades cibernéticas maliciosas (la "caja de herramientas de la diplomacia cibernética"). El marco permite que la UE y sus estados miembros utilicen todas las medidas de la Política Exterior y de Seguridad Común (PESC), incluidas las medidas restrictivas si es necesario, para prevenir, desalentar, disuadir y responder a las actividades cibernéticas maliciosas que tienen como objetivo la integridad y la seguridad de la UE y sus estados miembros.⁴ El marco de la UE para medidas restrictivas contra los ciberataques que amenazan a la UE y sus estados miembros se estableció en mayo de 2019⁵.

Las propias instituciones europeas han puesto en marcha además de lo expuesto en el párrafo anterior una serie de medidas para promover una mayor resiliencia contra la ciberseguridad, entre las que destacan:

⁴ <https://www.consilium.europa.eu/es/press/press-releases/2022/05/16/cyber-attacks-council-extends-sanctions-regime-until-18-may-2025/>

⁵ <https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:02019D0797-20201124&from=EN>

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

*Identidad Digital Europea: permitirá a todos los europeos acceder a los servicios en línea sin tener que utilizar métodos de identificación privada ni compartir datos personales sin necesidad.

*Brújula Digital⁶ para la Década Digital de la UE: que persigue los siguientes objetivos para 2030.⁷

	<p>Capacidades Especialistas en TIC: 20 millones + convergencia de género Capacidades digitales básicas: mínimo el 80 % de la población</p>		<p>Transformación digital de las empresas Asimilación de la tecnología: utilización de la nube, la IA y los macrodatos por el 75 % de las empresas de la UE Innovadores: aumento de las empresas emergentes en expansión y la financiación para duplicar los unicornios en la UE Usuarios tardíos: más del 90 % de las pymes alcanzan al menos un nivel básico de intensidad digital</p>
	<p>Infraestructuras digitales seguras y sostenibles Conectividad: Gigabit para todos, 5G en todas partes Semiconductores de vanguardia: duplicar la cuota de la UE en la producción mundial Datos: borde y nube: 10 000 nodos frontera de alta seguridad y neutros desde el punto de vista climático Informática: primer ordenador con aceleración cuántica</p>		<p>Digitalización de los servicios públicos Servicios públicos clave: 100 % en línea Salud electrónica: el 100 % de los ciudadanos tienen acceso a los historiales médicos Identidad digital: utilización de la identificación digital por el 80 % de los ciudadanos</p>

Infografía nº 2: Metas digitales para 2030 de la Unión Europea.

*Ciudadanía digital: derechos y principios para los europeos. Tal como puede verse en la siguiente infografía son los siguientes:

⁶ <https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX%3A52021DC0118>

⁷ https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_es

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

Grupo de trabajo conjunto de acción contra el ciberdelito (J-CAT): Ubicado en el Centro Europeo de Ciberdelincuencia (EC3) de Europol, ayuda a combatir la ciberdelincuencia dentro y fuera de la UE.



Infografía n.º 4: Participantes del J-CAT (Fuente EC3-EUROPOL)

SPACE (Secure Platform for Accredited Cybercrime Experts): Dentro de la Plataforma de Expertos de Europol (EPE). Creada para reunir a expertos en cibercrimen de todo el mundo, SPACE se divide en dos partes: un área común visible y disponible para todos los usuarios de SPACE acreditados y una serie de subcomunidades cerradas, restringidas solo a miembros.¹⁰

Otro aspecto que va a tener un alto impacto en los niveles futuros de ciberseguridad, ha sido la aprobación de la Directiva NIS 2. Recientemente, el Centro Criptológico Nacional (CCN) publicó una nota de prensa en la que se decía lo siguiente sobre el particular¹¹:

“El Consejo y el Parlamento Europeo han llegado recientemente a un acuerdo sobre las medidas para garantizar un nivel común elevado de ciberseguridad en toda la Unión Europea, con el fin de mejorar la resiliencia y las capacidades de respuesta a incidentes tanto del sector público como del sector privado, así como del conjunto de la UE.

Esta nueva Directiva NIS 2 sustituirá a la Directiva actual sobre la seguridad de las redes y sistemas de información y sentará las bases para las medidas de gestión de riesgos

¹⁰ https://www.europol.europa.eu/cms/sites/default/files/documents/space_flyer-2019.pdf

¹¹ <https://www.ccn-cert.cni.es/seguridad-al-dia/actualidad-ccn/11799-la-union-europea-refuerza-su-ciberseguridad-y-resiliencia-con-la-aprobacion-de-la-directiva-nis-2.html>

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

de ciberseguridad y la obligación de notificación en los sectores que cubre (energía, transporte, sanidad e infraestructura digital).

El objetivo primordial es eliminar las diferencias entre los requisitos de ciberseguridad y de aplicación de las medidas entre los distintos Estados miembros. Para ello, se establecen normas mínimas para un marco regulador y mecanismos para una cooperación eficaz entre las autoridades de cada Estado miembro. Así, se establecerá la Red Europea de Organización de Enlace de Crisis Cibernéticas (EU-CYCLONe) para mejorar la coordinación en la gestión de incidentes de ciberseguridad a gran escala.”

Por último, es de destacar que la Comisión Europea¹² propuso dos iniciativas legislativas para actualizar las normas que rigen los servicios digitales en la UE: la Ley de Servicios Digitales (DSA) y la Ley de Mercados Digitales (DMA). La Comisión hizo las propuestas en diciembre de 2020 y el 25 de marzo de 2022 se alcanzó un acuerdo político sobre la Ley de Mercados Digitales, y el 23 de abril de 2022 sobre la Ley de Servicios Digitales.

Juntos forman un conjunto único de nuevas reglas que serán aplicables en toda la UE para crear un espacio digital más seguro y abierto.

La DSA y la DMA tienen dos objetivos principales:

- Crear un espacio digital más seguro en el que se protejan los derechos fundamentales de todos los usuarios de servicios digitales;
- Establecer condiciones equitativas para fomentar la innovación, el crecimiento y la competitividad, tanto en el Mercado Único Europeo como a nivel mundial.

Otro hecho sometido a controversia es la realización de un análisis del coste de lo que suponen las amenazas cibernéticas, pues en muchos casos son datos que no son de acceso público. No obstante, existen algunos entes privados que han realizado estudios tentativos sobre esta materia. Un ejemplo de ello es el “2022 Ponemon Cost of Insider Threats Global Report.”¹³ En dicho informe se encuestó a más de 1000 profesionales de las TIC en América del Norte, Europa, Medio Oriente, África y Asia-Pacífico. El informe revelaba que, en los últimos dos años, la frecuencia y los costos asociados con las amenazas internas han aumentado drásticamente en las tres categorías de amenazas internas, que incluyen: empleados/contratistas descuidados o negligentes, información privilegiada

¹² <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>

¹³ <https://www.proofpoint.com/us/resources/threat-reports/cost-of-insider-threats>

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

malintencionada o criminal y robo de credenciales. Asimismo, aporta otro dato a tener en cuenta: “el 56% de los incidentes de amenazas internas conocidos fueron el resultado de un empleado o contratista descuidado.”¹⁴

Las amenazas a la ciberseguridad son por lo tanto objeto de una atención preferencial de las políticas públicas, prueba de ello es la nueva Estrategia de Seguridad Nacional (ESN 2021), aprobada el pasado 28 de diciembre de 2021, mediante Real Decreto 1150/2021¹⁵. En la misma, se definen los dos tipos de amenazas existentes en el ciberespacio:

Por un lado, los ciberataques, entendidos como acciones disruptivas que actúan contra sistemas y elementos tecnológicos. Ejemplos de ello son los ataques de ransomware (secuestro de datos) o la denegación de servicios, entre otros. Y, por otro lado, el uso del ciberespacio para realizar actividades ilícitas, como el cibercrimen, el ciberespionaje, la financiación del terrorismo o el fomento de la radicalización.

La importancia que se le otorga dentro de la nueva ESN 2021 a la ciberseguridad, es patente, ya que en la misma se cita textualmente que: *“En términos de ciberseguridad, se requiere garantizar el uso seguro y fiable del ciberespacio, para proteger los derechos y las libertades de los ciudadanos y promover el progreso socio económico. Para ello es importante incrementar las capacidades (tecnológicas, humanas y económicas) de la ciberseguridad nacional dirigidas a la prevención, detección, respuesta, recuperación, investigación y defensa activa”*. Para ello y dentro de la Línea de Acción 17, el ciberespacio que es considerado como uno de los espacios comunes globales junto al marítimo, aéreo y ultraterrestre, se promueve el avance en la integración del modelo de gobernanza de la ciberseguridad en el marco del Sistema de Seguridad Nacional.

Otro aspecto que se destaca en la ESN 2021 es el relacionado con la desinformación. Esta actividad tiene fuertes implicaciones para la ciberseguridad, como ha reconocido la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), en su informe “THREAT LANDSCAPE 2021”¹⁶. La citada agencia, establece cuatro tipos de objetivos que persigue la desinformación, catalogando los medios con los que se lleva cada uno de ellos.

¹⁴ <https://www.globenewswire.com/news-release/2022/01/25/2372208/35374/en/Global-Cybersecurity-Study-Insider-Threats-Cost-Organizations-15-4-Million-Annually-up-34-Percent-from-2020.html#:~:text=Organizations%20impacted%20by%20insider%20threats,percent%20in%20just%20two%20years.>

¹⁵ https://www.boe.es/diario_boe/txt.php?id=BOE-A-2021-21884

¹⁶ <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021/@/download/fullReport>

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

Target	Means	Goal
People	Disinformation, misinformation, fake news	Reduce perceived honesty and trustworthiness of individuals
Enterprises	Market distortion, misinformation, disinformation, smear campaigns, fake news, propaganda	Affect brand reputation, financial solidity of the company, and the trustworthiness of the management.
Society	Disinformation, fake news	Inability to distinguish real and fake news, apathy, exhaustion in trying to find the truth, manipulating and misleading public-opinion
Any	Sharing of inaccurate information	Make money based on advertisement

Tabla nº 1.- Objetivos y medios con los que se lleva a cabo la desinformación (Fuente: Informe THREAT LANDSCAPE 2021-ENISA)

En relación con las principales tendencias de las amenazas relacionadas con la Cibercriminalidad, un organismo de referencia es EUROPOL. Dicho organismo a través de sus informes anuales (Internet Organised Crime Threat Assessment - IOCTA)¹⁷, analiza cuales son. En su informe del año 2021¹⁸, se extraen una serie de conclusiones:

- El ransomware se ha aprovechado de las vulnerabilidades del teletrabajo.
- El aumento de mercado online lleva aparejado un incremento de las actividades intrusivas informáticas, como phishing, robos de identidad, banca online, etc.
- Creciente venta de productos médicos falsificados, como consecuencia de la pandemia generada por la Covid-19.
- La Covid-19 ha provocado un mayor acceso de la población infantil a contenidos en línea, con los riesgos que ello conlleva.
- El comercio y la venta de datos privados, al amparo de accesos ilegales informáticos, es un mercado floreciente.

Por otro lado, una prueba de que la Cibercriminalidad, es un hecho que afecta de manera global a todas las personas y entidades, jurídicas y públicas, está relacionada con la actitud que las grandes empresas relacionadas con las nuevas tecnologías vienen adoptando en los tiempos actuales. A continuación, se ofrece un ejemplo de dos titulares de prensa aparecidos recientemente:

¹⁷https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf

¹⁸ <https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021>

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

- *Google desmonta una red de bots que infectó a un millón de ordenadores Windows*¹⁹
- *Microsoft desarticula al grupo de cibercriminales chino Nickel, que había atacado a EE.UU. y otros 28 países.*²⁰

En línea con lo apuntado en párrafos anteriores y dentro del ámbito de las Fuerzas y Cuerpos de Seguridad, durante el año 2021 se realizó una intensa labor de lucha contra los ciberdelincuentes. Como botón de muestra caben citar dos operaciones:

-La primera de ellas realizada por Policía Nacional, donde se desarticuló una organización que habría defraudado más de 12.000.000 de euros²¹. En esta operación denominada “SECRETO”, fueron detenidas 105 personas, e imputadas otras 14, en una macrooperación en la que se llevaron a cabo 88 registros simultáneos en cuatro países europeos.

La red desmantelada creaba empresas fantasmas en Estados Unidos y, tras dotarlas de una falsa solvencia económica, solicitaban la expedición de tarjetas de débito con el máximo importe disponible con el pretexto de utilizarlas en sus viajes a Europa.

Una vez en España, las tarjetas americanas eran utilizadas en establecimientos conniventes por elevados importes mediante el sistema de preautorización, aprovechando la diferencia de aceptación del pago existente entre los bancos americanos y españoles.

La investigación, que comenzó hace un año y medio, fue liderada por la Policía Nacional de manera conjunta con el Servicio Secreto Americano, contando con la participación de EUROPOL además de los cuerpos policiales de Grecia, Austria, Dinamarca, Reino Unido, Alemania, Polonia y Ucrania.

Los líderes del grupo, de origen albanés, utilizaban documentación falsa griega y contaban con personal de confianza, todos ellos españoles, que trabajaban para la organización realizando diversas funciones. Por un lado, estaban los que captaban establecimientos conniventes, empresarios o autónomos que permitieran pasar tarjetas americanas en el datafono de su comercio a cambio de una comisión del 15% del importe. Una vez se encontrase el dinero en la cuenta del connivente, éste tendría que reintegrar el 85% restante mediante transferencia bancaria a una de las muchas cuentas que manejaban

¹⁹ <https://www.europapress.es/portaltic/ciberseguridad/noticia-google-desmota-red-bots-infecto-millon-ordenadores-windows-20211208160421.html>

²⁰ <https://www.europapress.es/portaltic/ciberseguridad/noticia-microsoft-desarticula-grupo-cibercriminales-chino-nickel-atacado-eeuu-otros-28-paises-20211208114233.html>

²¹ https://www.policia.es/_es/comunicacion_prensa_detalle.php?ID=8401#

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

los principales miembros de la organización tanto en España como en diferentes países de Europa. Para justificar la supuesta transacción elaboraban facturas falsas a nombre de las mercantiles americanas que figuraban en la tarjeta, con la finalidad de simular haber comprado productos o prestado algún servicio.

-Otra operación en el ámbito de la Cibercriminalidad a destacar fue la realizada por la Guardia Civil, al disolver grupos de más de 100.000 miembros de una conocida app de mensajería dedicados al carding en una operación contra el fraude informático.

En el marco de la operación “RECOLECTOR”²² desarrollada por la Guardia Civil se consiguió la desarticulación de una organización criminal de carácter internacional dedicada a la comisión de delitos relacionados con el fraude informático en todo su espectro, procediéndose a la detención e investigación de once personas en España y Chile.

La principal actividad del entramado de ciberdelincuentes era la obtención ilícita de datos relacionados con las credenciales de pago (generalmente tarjetas de crédito), tanto para su explotación directa en plataformas de comercio online por la propia organización, como para proceder a su venta en canales de una conocida app de mensajería y en foros de la DarkWeb, este conjunto de actividades delictivas es conocida en el mundo del cibercrimen como CARDING.

El modus operandi identificado se basaba, fundamentalmente, en la suplantación de sitios web reales, método conocido como phishing, pertenecientes a entidades bancarias nacionales e internacionales, así como de conocidas empresas de servicios de contenidos en multimedia en streaming, y obtener con ello de esa manera los datos de las víctimas.

Para la consecución de sus objetivos delictivos hicieron uso de diferentes tipos de malware como el troyano bancario Zeus y TinyBanker, keyloggers, herramientas para ataques de denegación de servicio, bots, redes botnet, y diversos tipos de ransomware que se encontraban a su disposición.

A la organización se le imputaron más de 2.500 hechos delictivos con más de 300 empresas a nivel nacional afectadas, estimándose un perjuicio patrimonial que podría alcanzar el millón de euros, obteniéndose información del uso de más de 42.000 tarjetas de crédito por parte de los diferentes integrantes de la organización delictiva. Se han

22

<https://www.guardiacivil.es/es/prensa/noticias/7942.html#:~:text=Tambi%C3%A9n%20se%20ha%20conseguido%20el,pago%20de%20tarjetas%20de%20cr%C3%A9dito.>

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

localizado tarjetas de crédito utilizadas por los ciberdelincuentes de 47 países en todo el mundo, destacando especialmente las de EE.UU. y países de la Unión Europea.

2.- RADIOGRAFÍA DE LA SOCIEDAD DE LA INFORMACIÓN

En este *IX Informe sobre Cibercriminalidad*, en el que se publican los datos estadísticos de cibercriminalidad y las amenazas que han sido descubiertas a lo largo del año 2021 en nuestro país, también se hace referencia a una serie de datos relativos al uso de las TIC por parte de la sociedad española en general. Para ello, se toman como referencia estudios y encuestas de opinión realizadas por otros organismos públicos, tanto de ámbito nacional (INE) como europeos (EUROSTAT).

La Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los Hogares (año 2021), del Instituto Nacional de Estadística (INE), se trata de una investigación dirigida a las personas de 16 años en adelante, residentes en viviendas familiares, que recoge información sobre los diversos productos de tecnologías de información y comunicación de los hogares españoles, así como los usos que hacen los españoles de estos productos, de Internet y del comercio electrónico. Se dedica una atención especial al uso que los niños hacen de la tecnología, por lo que obtiene igualmente información de los menores de 10 a 15 años.

A lo largo de este Capítulo 2 del Informe, en sus diferentes apartados, se traza y esquematiza un perfil de la sociedad española enlazado al uso de las tecnologías e Internet.

Los datos del punto 2.1 (Hogares y porcentaje de vivienda con/sin acceso a Internet), procedentes de la Encuesta del INE, reflejan el porcentaje de viviendas que poseen ordenador y aquellas que no disponen de estos dispositivos, así como las que tienen contratado un servicio de acceso a Internet. En primer lugar, de un análisis genérico de los datos expuestos se aprecia que el porcentaje de viviendas que poseen ordenador y las que disponen de acceso a Internet se ha incrementado en 2021 con respecto al año 2020. Siguiendo de esta forma la tendencia general experimentada en la serie histórica que se representa (2012-2021).

Además, se puede observar que los índices sobre las viviendas que poseen o no dispositivos de esta naturaleza, así como la existencia de que éstas estén conectadas a

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

Internet, es más elevado, en ambos casos, cuanto mayor es la población de la localidad en la que se ubican los hogares.

En el apartado 2.2 (Perfil del ciudadano ante la sociedad de la información. Uso de Internet), se hace referencia a la información correspondiente, según los datos publicados por el INE, al número de personas que afirman haber accedido a Internet en los últimos tres meses. De esta forma, se puede observar que también esta variable aumenta año a año desde 2012.

Con los datos reflejados en la *Encuesta anual del INE* se pueden extraer una serie de particularidades que permiten establecer los rasgos que delimitan el perfil del usuario español ante la sociedad de la información.

Si atendemos a la edad del usuario, los grupos de edad más temprana son los que más hacen uso de las tecnologías. En este sentido, el 99,7 % de los jóvenes, entre 16 a 24 años, afirman haber accedido a la red en los últimos tres meses. Es de destacar, que todos los grupos de edad, se encuentran por encima del 90% de acceso a Internet, con excepción de los comprendidos entre los 65 a 74 años, si bien éstos aumentan de manera notable, al situarse en una franja del 73,3%, dato que casi cuadruplica los que los efectuaban en el año 2012.

Por sexos, y en línea con años recientes, se iguala el porcentaje de uso de Internet de mujeres y hombres.

Un aspecto importante se visualiza en el punto 2.3 (Perfil del menor de edad ante la sociedad de la información), donde se detalla que el porcentaje de los menores de edad (10 a 15 años) que han utilizado un ordenador y han accedido a Internet en los tres últimos meses, con el 95,1%. Por sexos, es pequeña la diferencia, aunque hay que reflejar que la mujer muestra mayores porcentajes en ambas categorías. En 2021, el 94,5% de los niños afirmaron haber utilizado un ordenador en los últimos tres meses, frente al 95,8% de las niñas, siendo el 97,4% de los chicos que se referencia su acceso a Internet en relación al 97,6% de las chicas.

El INE, asimismo, proporciona datos sobre el perfil de las personas que han comprado alguna vez por internet (2.4). Así pues, se puede apreciar que desde el año 2012 el comercio electrónico se ha llegado casi a triplicar, puesto que el 55,2 % de las personas encuestadas en 2021 reconocen haber realizado alguna compra empleando esta vía,

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

mientras que en el año 2012 solo lo hacían el 21,7%. Por sexo, los hombres muestran ligeramente mayores cifras porcentuales que las mujeres (55,7 frente al 54,8%), aunque esta diferencia con el paso de los años se viene reduciendo paulatinamente.

Por grupos o rangos de edad, son las personas con edades comprendidas entre los 25 y 34 años las que realizan más compras a través de Internet (74,3%). Por otro lado, las personas de 65 a 74 años muestran que sólo el 23,0% realiza compras por Internet, aunque es un valor al alza como se puede corroborar por el hecho de esta franja de edad en el año 2012, sólo efectuaban compras por Internet el 3,5%.

Por otra parte, en este Capítulo se incluyen datos que tratan de recrear una comparación de la sociedad española con las tecnologías de la información en relación a los demás países de la Unión Europea, en función de la información obtenida de EUROSTAT.

Así, en un primer momento, se exponen los porcentajes de viviendas con acceso a Internet en los diferentes países de la Unión Europea (27-UE) (Punto 2.5 Comparativa internacional), en la serie histórica 2012-2021. Un hecho que se viene produciendo en los últimos años es que ***España, se encuentra por encima de la media de la UE***, con un 96% frente al 92% de la Unión Europea.

En el apartado 2.6, se incluyen datos extraídos del Índice de Economía y Sociedad Digital (DESI por sus siglas en inglés). Se trata de un índice compuesto desarrollado por la Comisión Europea para evaluar los avances de los países de la UE hacia una economía y una sociedad digitales. ***España destaca en las dimensiones de “Conectividad” y “Servicios públicos digitales”***, con valores muy por encima de la media de la UE.

3.- INFRAESTRUCTURAS CRÍTICAS Y CIBERSEGURIDAD

En la introducción al Capítulo se detallan los aspectos más relevantes en esta materia, entre los que se incluyen datos sobre incidentes gestionados por el Centro de respuesta a incidentes de seguridad del Instituto Nacional de Ciberseguridad.

Dentro de dicho apartado se muestran gráficos y datos según el tipo de incidente, así como los que están relacionados con las infraestructuras críticas y el sector estratégico afectado.

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

4.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD

En enero de 2008 entraba en funcionamiento el Sistema Estadístico de Criminalidad (SEC), en sustitución del Programa Estadístico de Criminalidad (PES), que incorporaba mejoras tanto desde el punto de vista metodológico como técnico, que suponían mayores cuotas de los niveles de calidad de los procesos estadísticos que se realizan desde el Ministerio del Interior.

Como consecuencia del Real Decreto 400/2012, de 17 de febrero, por el que se desarrollaba la estructura orgánica básica del Ministerio del Interior, el entonces Gabinete de Coordinación y Estudios (actualmente Dirección General de Coordinación y Estudios) asumió las funciones en materia de estadística de criminalidad, que continuaron tras la publicación del Real Decreto 734/2020, de 4 de agosto, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior.

Fue el 31 de enero de 2013, cuando se dictó la Instrucción 1/2013, de la Secretaría de Estado de Seguridad, sobre la Estadística Nacional de Criminalidad, cuyo objeto es *“dictar las directrices básicas para el desarrollo y gestión de la Estadística Nacional de Criminalidad, determinando los elementos que la componen –especialmente el Sistema Estadístico de Criminalidad –, definiendo los actores que interactúan en la misma y fijando las responsabilidades de cada uno de ellos”*.

Así pues, y según consta en esta Instrucción, a partir del Sistema Estadístico de Criminalidad (SEC) que se compone de la Base de Datos que registra las actuaciones policiales y responsables²³, se llevará a cabo la explotación estadística de los datos que se conozcan por las por las Fuerzas y Cuerpos de Seguridad del Estado (Cuerpo Nacional de Policía y Guardia Civil), las Fuerzas y Cuerpos de Seguridad dependientes de las Comunidades Autónomas (Mossos d’ Esquadra, Ertzaintza y Policía Foral de Navarra), y también por aquellos Cuerpos de Policía Local que facilitan datos a las Fuerzas y Cuerpos de Seguridad del Estado, y en definitiva al SEC.

En este caso concreto que nos ocupa se detalla a continuación la información estadística consignada en el SEC sobre Cibercriminalidad en España.

²³ Actuaciones policiales y responsables: son dos operaciones estadísticas dadas de alta en el Inventario de Operaciones Estadísticas del INE)

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

Datos globales

El apartado 4.1 (Evolución de hechos conocidos por categorías delictivas), contabiliza el total de los hechos conocidos por las Fuerzas y Cuerpos de Seguridad durante la serie histórica 2017-2021 (la información que los Cuerpos facilitan se detalla en el apartado de metadata), siguiendo la clasificación adoptada por el Convenio sobre Cibercriminalidad o Convenio de Budapest y otras infracciones penales reguladas en nuestra legislación interna. Asimismo, junto a las categorías específicamente concretadas como ciberdelincuencia, se debe incluir dentro de este fenómeno y por lo tanto computar los registros disponibles en el SEC todos los delitos que para su comisión se hayan empleado las TIC. A los delitos contemplados en el convenio citado, se han añadido una serie de tipologías penales que por su importancia merece la pena destacar:

- Delitos contra el honor.
- Amenazas y coacciones.

En el periodo comprendido entre 2017 a 2021, se constata el aumento de los delitos informáticos. De esta forma, podemos apreciar que, en 2021, se han conocido un total de 305.477 hechos, lo que supone un 6,1% más con respecto al año anterior. De esta cifra, el 87,4 % corresponde a fraudes informáticos (estafas) y el 5,7% a amenazas y coacciones.

Actualmente, la importancia de la Cibercriminalidad va creciendo año tras año, como se demuestra con el aumento del número de hechos conocidos. No obstante, durante el año 2021 su peso proporcional ha disminuido ligeramente sobre el año 2020. A este respecto, hay que recordar que ese último año, tiene connotaciones especiales por todo lo relacionado con la pandemia generada por la Covid-19. Como se puede observar en la tabla nº 2, hemos pasado del año 2017, donde nos situábamos en el 5,7%, al año 2021 con el 15,6%.

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

2017	5,7%
2018	7,5%
2019	9,9%
2020	16,3%
2021	15,6%

Tabla nº 2. % que representa la Cibercriminalidad sobre el total de infracciones penales. Fuente: Sistema Estadístico de Criminalidad (SEC)

Las gráficas del punto 4.2 (Evolución global de hechos conocidos, esclarecidos y detenciones/investigados) evidencian de manera esquemática los datos correspondientes a los hechos conocidos, esclarecidos y la cifra de las detenciones e investigaciones registradas por las Fuerzas y Cuerpos de Seguridad, en el periodo 2017 a 2021.

En relación al porcentaje de hechos esclarecidos, en el año 2021, éste supone el 15,9% del total de los hechos conocidos, lo que implica un aumento con respecto al año anterior, que alcanzó el porcentaje de esclarecimiento del 14%. Por otra parte, los detenidos e investigados han alcanzado la cifra de 13.801, lo que supone un aumento de un 22,3% con respecto al año 2020, en el que se registraron 11.280 detenidos e investigados.

En el apartado 4.3 y 4.4 se detallan datos por meses, observándose que durante el 2021, el mes de mayor incidencia delictiva fue el mes de diciembre.

La distribución de la Cibercriminalidad, desde el punto de vista geográfico (4.5. Representación territorial de hechos denunciados de cibercriminalidad), a lo largo de 2021, sitúa a Madrid, Cataluña, Andalucía y Comunitat Valenciana entre las Comunidades Autónomas que concentran más infracciones penales en este ámbito. A nivel provincial, se encuentran a la cabeza del ranking estadístico, Madrid, Barcelona, Valencia, Sevilla, Alicante/Alacant, Bizkaia y Málaga.

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

Los datos de la sección 4.6, relativos a las victimizaciones registradas según grupo penal y sexo, precisan las características y el perfil de la víctima de los delitos informáticos en España. En este apartado se facilitan datos de todos los Cuerpos policiales (Ertzaintza comienza a facilitar datos de victimizaciones a partir de 2021).

En 2021, las victimizaciones que han sido registradas por las Fuerzas y Cuerpos de Seguridad suman un total de 240.100²⁴, es decir, un 11,4% más que en el año 2020. La mayoría de las víctimas de ciberdelincuencia pertenecen al sexo masculino (51,9%), tienen entre 26 a 40 años, y son objeto, principalmente, de los delitos de fraudes informáticos, amenazas y coacciones y falsificación informática. Sin embargo, si se analiza la distribución global de incidentes conocidos por ámbito y sexo, las mujeres exceden en porcentaje a las víctimas de sexo masculino cuando se trata de hechos relacionados con la falsificación informática (usurpación del estado civil), acceso e interceptación ilícita (descubrimiento y revelación de secretos), contra el honor (injurias) y los delitos sexuales [delito de contacto mediante tecnología con menor de 16 años con fines sexuales (grooming)].

Además, en el punto 4.7 (Victimizaciones según grupo de edad y sexo) tal y como figura en la información registrada en el Sistema Estadístico de Criminalidad (SEC), se aprecia que, en 2021, el 29,0 % del conjunto de las víctimas recae sobre el grupo de edad de 26 a 40 años. Siendo este grupo de edad el mayoritario tanto para las víctimas de sexo masculino como femenino.

Por otra parte, se publican datos relativos a las victimizaciones desglosadas por tipología penal y sexo (Punto 4.8). Por ello, se puede decir que entre los principales hechos conocidos cometidos contra las víctimas de ambos sexos se encuentran las estafas, las amenazas y la usurpación de estado civil.

En relación a la nacionalidad de la víctima (apartado 4.9), el 87,5% de ellas son españolas, y el 12,5% restante extranjeras. En el conjunto de las víctimas de nacionalidad extranjera, son las procedentes de Marruecos, Rumanía y Colombia las que aúnan valores más elevados.

²⁴ Se puede apreciar una diferencia entre el número de hechos ilícitos conocidos (305.477) y el de victimizaciones registradas (240.100), debido a que ambos conceptos no contabilizan la misma información. En este sentido, cuando hablamos de victimizaciones nos referimos al número de hechos denunciados por personas en los cuales manifiestan ser víctimas o perjudicados por alguna infracción penal, contabilizada dentro del ámbito de la ciberdelincuencia. En muchas ocasiones no se poseen datos de dichas víctimas. Asimismo, para el conjunto de hechos conocidos, se tienen datos de todos los cuerpos policiales, extremo que no sucede con las victimizaciones que no se poseen datos de la Ertzaintza.

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

Al igual que en el informe de 2021 (datos de 2020), en este *IX Informe sobre Cibercriminalidad*, se introducen datos que permiten realizar y establecer una relación entre los rangos de edad de las víctimas y la tipología penal de la que han sido objeto (Punto 4.10 Victimizaciones registradas según grupo penal y edad). Así pues, según los datos registrados, el fraude informático es la tipología delictiva con mayor incidencia en todos los grupos de edad establecidos (a excepción de los menores de edad), y de manera especial en los rangos de edad que va de los 26 años en adelante. Destacan sobre todo en términos porcentuales, que no cuantitativos, el grupo de mayores de 65 años.

Del análisis de la información extraída del SEC se puede observar que el comportamiento de las víctimas incluidas en el grupo menores de edad no sigue el patrón o el modelo de las víctimas mayores de edad. Las víctimas menores de edad son más vulnerables a otro tipo de hechos delictivos, en concreto a las amenazas y coacciones y delitos sexuales, tal y como refleja la tabla del apartado 4.10.

Igualmente, en este estudio se consignan datos detallados de las victimizaciones según el sexo de la misma. En las secciones 4.12 y 4.13 se aportan los del sexo masculino y las 4.14 y 4.15, las del sexo femenino. Como primera diferencia entre ambas, se aprecia que las victimizaciones de mujeres son cuantitativamente superiores en menores y en la franja de edad de 18 a 30 años, siendo la de los hombres superiores en el resto de grupos de edad. Por otro lado, comparten ambos sexos una característica común ligada al hecho de que la ciberdelincuencia sexual tiene la más amplia incidencia en los menores de edad, siendo los valores más altos en los del sexo femenino. Otra característica común está referenciada a que el grupo de edad de mayores de 65 años tiene los valores más altos en términos porcentuales en la categoría de fraude informático sobre la cifra absoluta de la Cibercriminalidad para el total de cada grupo de edad.

La sección 4.16 presenta la información relativa a las detenciones e investigados. Información que figura desagregada según el tipo penal y sexo, de 2021.

De la cifra total de detenciones e investigaciones (13.801) efectuadas por las Fuerzas y Cuerpos de Seguridad, el 71,3% corresponden a personas de sexo masculino, teniendo lugar, principalmente, por la comisión de fraudes informáticos, delitos de amenazas y coacciones y delitos sexuales. La mayoría de las detenciones/investigaciones de personas de sexo femenino se han llevado a cabo por fraudes informáticos, amenazas y coacciones, y por el delito de falsificación informática.

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

Por lo que respecta a las diferentes infracciones penales (4.18 Detenciones/investigaciones por tipología penal y sexo), los datos establecen que las causas por las que las personas de sexo masculino han sido objeto de la detención/investigación ha sido principalmente por estafas, amenazas, y la pornografía de menores. Asimismo, se puede observar que las estafas, amenazas e usurpación de estado civil predominan entre las razones para actuar contra los responsables de sexo femenino.

La mayoría de los detenidos/investigados por ciberdelincuencia son de nacionalidad española (79,3%) (4.19). Entre los detenidos/investigados de nacionalidad extranjera son los originarios de Marruecos, Rumanía y República Dominicana, los que aglutinan un mayor número de casos.

Al desglosar la información según los distintos rangos de edad predeterminados (4.20 Detenciones/investigaciones según grupo de edad y sexo), se observa que las mayores cifras de los responsables de ciberdelincuencia se ubican en el grupo de edad 26 a 40 años.



GOBIERNO DE ESPAÑA

MINISTERIO DEL INTERIOR

SECRETARÍA DE ESTADO DE SEGURIDAD
DIRECCIÓN GENERAL DE COORDINACIÓN Y ESTUDIOS



se Sistema Estadístico de Criminalidad



2021 SOST

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

3

INFRAESTRUCTURAS CRÍTICAS Y CIBERSEGURIDAD >>

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

los sistemas. Por esta razón, se ha estimado que su presencia únicamente genera sesgos al no permitir una comparación con lo dispuesto en el Título III del RD-I 12/2018.

>> 3.1. Incidentes gestionados por el INCIBE-CERT (entidades privadas)

El INCIBE-CERT gestionó un total de 109.126 incidentes de ciberseguridad en España durante el año 2021.

Analizando el número de incidentes en función de su tipología, se concluye que los incidentes tipo *malware* son los más frecuentes según el registro del pasado año; con un porcentaje del 29,88%, respecto del total; seguido de los *Fraudes* con un 28,60%.

Con respecto a los tipos de *malware* con mayor relevancia, y efectos, en el año 2021, significar los siguientes:

Emotet: Funciona como “*downloader*” permitiendo la descarga y ejecución de otros códigos dañinos, así como la monitorización del tráfico de red, obteniendo cualquier información contenida en los navegadores de la víctima, desde credenciales de usuario hasta información bancaria.

Las campañas de *Emotet* más habituales durante el año 2021 implicaron el envío de correos electrónicos *phishing* con archivos adjuntos maliciosos que contenían macros que funcionaban como descargadores de *malware*. La mayoría de los archivos adjuntos se identificaron como ficheros de Microsoft Office, si bien, se observaron archivos con otros formatos tales como ZIP y PDF.

Mekotio: También conocido como BestaFera, representa una amenaza grave para todos aquellos usuarios que hacen uso de servicios de banca *online* o de criptodivisas, concretamente de Bitcoins, ya que se trata de un troyano bancario que afecta a todas las versiones del sistema operativo Windows, comprendidas entre Windows XP y Windows 10.

Funciona como “*downloader*” permitiendo la descarga y ejecución de otros códigos dañinos, así como la monitorización del tráfico de red, obteniendo cualquier información contenida en los navegadores de la víctima.

Las campañas de *Mekotio* más habituales durante el año 2021 implicaron el envío de correos electrónicos *phishing* con archivos adjuntos maliciosos que contenían macros que funcionaban como descargadores de *malware*.

Flubot: *Software* malicioso de tipo troyano para dispositivos Android. Las campañas más habituales implicaron el envío de SMS fraudulentos que avisaban de la recepción de un paquete suplantando a diferentes empresas logísticas, como FedEx, DHL o Correos.

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

Estos mensajes invitan al receptor a instalar una aplicación en su dispositivo móvil con el incentivo de que éste pueda conocer el paradero del paquete. Una vez que el usuario realiza la instalación de la aplicación en su dispositivo, ésta comienza a rastrear los identificadores de todas las aplicaciones que se inicien, con la capacidad de inyectar páginas superpuestas al detectar un inicio de sesión en una de las aplicaciones objetivo, de forma que el usuario se confía en que está introduciendo las credenciales en la web original cuando, en realidad, las está enviando al servidor de mando y control controlado por los operadores del código dañino.

Anatsa: *Malware* de tipo troyano para dispositivos Android que ha sido analizado, en paralelo, por diferentes organizaciones asignándole diferentes nombres como: Anatsa, TeaBot o Toddler.

Al igual que en Flubot, una vez que el usuario realiza la instalación de la aplicación en su dispositivo, ésta comienza a rastrear los identificadores de todas las aplicaciones iniciadas, con la capacidad de inyectar páginas superpuestas al detectar un inicio de sesión en una de las aplicaciones objetivo, de forma que el usuario se confía en que está introduciendo las credenciales en la web original cuando, en realidad, las está enviando al servidor de mando y control controlado por los operadores del código dañino.

Hive: *Malware* de tipo *ransomware* que implementa las funcionalidades de cifrado de la información de un equipo infectado, imposibilitando la recuperación de los datos de forma sencilla.

Por otro lado, con respecto a los incidentes relativos al **fraude** significar que, durante el año 2021 han continuado proliferando campañas de suplantación de la identidad de clientes o proveedores, mediante vía telefónica y correo electrónico, con un total de 31.529 incidentes entre todos los ámbitos del sector privado.

Suplantación de identidad (Fraude al CEO): envío de correo electrónico personalizado, tras un análisis exhaustivo de la víctima, para que realice una transferencia, modifique la cuenta de pago de la factura de un proveedor, etc. A una cuenta contralada por los delincuentes.

Phishing: Consiste principalmente en la recepción por parte de la víctima de un correo electrónico destinado a engañarla y que comparta, normalmente a través de un enlace a una web fraudulenta, credenciales, datos personales, números de cuenta bancaria, datos de tarjetas de crédito o cualquier otro dato confidencial.

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

>> 3.2. Incidentes gestionados de Operadores Críticos del sector privado

A lo largo del año 2021, el número de incidentes de ciberseguridad disminuyó en un 21,02% con respecto al año anterior, gestionándose un total de 680 incidentes.

Con respecto a los tipos de incidentes con mayor relevancia se encuentran los relacionados con **sistemas vulnerables**, con un 49,85%, seguido por **malware** y **robo de información** con un 26,03% y un 17,21%, respectivamente.

>> 3.3. Incidentes gestionados por Sector Estratégico

Los sectores PIC donde se han detectado un mayor número de incidentes han sido el sector **Energía**, con un 30,44%, seguido del sector **Tributario y Financiero**, con un 25,29% y el sector **Agua**, con un 17,21%.

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

2.6. Índice de Economía y Sociedad Digital (DESI). Comparativa España-Unión Europea

Digital Economy and Society Index 2021. Spain

https://administracionelectronica.gob.es/pae_Home/dam/jcr:580a4fc8-a552-448e-b89b-cd2f88ec0b5c/DESI_2021_Spain_es.pdf

>> Datos estadísticos de criminalidad

Origen de los datos

Los datos han sido obtenidos del Sistema Estadístico de Criminalidad (SEC). Para su cómputo se tienen en cuenta los hechos de los que han tenido conocimiento los siguientes Cuerpos policiales: Cuerpo Nacional de Policía, Guardia Civil, Policía Foral de Navarra, Mossos d' Esquadra y las Policías Locales que facilitan datos al Sistema Estadístico de Criminalidad (SEC). La Ertzaintza aporta datos de hechos conocidos y detenciones e investigados, no así de hechos esclarecidos. Con respecto a las victimizaciones sólo existen disponibles datos para este Cuerpo policial a partir del año 2021.

Definición y cómputo estadístico de Cibercriminalidad

Se detallan las conductas ilícitas registradas en el Sistema Estadístico de Criminalidad (SEC), siguiendo la clasificación adoptada por el Convenio sobre Cibercriminalidad o Convenio de Budapest¹. Se adjunta cuadro explicativo al final de la metadata.

No obstante, además de las conductas que introduce el Convenio de Budapest, nuestra realidad criminal denota que existen otras categorías distintas que conviene reseñar. Es pues, que cuando los medios empleados en su comisión sean las tecnologías

¹ https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

poseerse datos de la Ertzaintza, los datos de hechos esclarecidos del País Vasco están infrarrepresentados.

El porcentaje de esclarecimiento se obtiene dividiendo el total de hechos esclarecidos por el total de hechos conocidos y multiplicando el resultado por 100. Dado que la Ertzaintza no aporta datos de esclarecidos, el cálculo de este porcentaje se ha obtenido teniendo en cuenta solamente los hechos conocidos y esclarecidos de CUERPO NACIONAL DE POLICÍA, GUARDIA CIVIL, MOSSOS D' ESQUADRA, POLICÍA FORAL DE NAVARRA y CUERPOS DE POLICÍA LOCAL que facilitan datos al Sistema Estadístico de Criminalidad (SEC).

Se considera que una persona física o jurídica, está investigada a causa de la atribución de participación en un hecho penal, sin adoptar medidas restrictivas de libertad para esa persona investigada. La detención va más allá, realizando todo el proceso que lleva a la lectura de derechos de la persona física, privándole de libertad y poniéndolo a disposición judicial, por la atribución de la comisión de una infracción penal.

El concepto de victimización viene referido al número de hechos denunciados por personas en los cuales manifiestan ser víctimas o perjudicados por alguna infracción penal. Se diferencia del concepto de víctima, ya que éste se refiere a personas individuales.

En una denuncia pueden darse varios hechos conjuntamente, e incluso pueden existir varias víctimas o perjudicados, siendo las victimizaciones el término que engloba a los diferentes hechos que afectan a una determinada víctima.

Los contrastes entre victimización y víctima se pueden ejemplificar con el siguiente supuesto: una persona presenta una denuncia y manifiesta que, en un determinado período de tiempo, ha sido objeto de 3 hechos de malos tratos en el

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

ámbito familiar y un delito de amenazas. Además, en esta misma denuncia manifiesta que su hijo de tres años también ha sido objeto de malos tratos en una ocasión.

- Total denuncias: 1
- Total víctimas: 2
- Total victimizaciones: 5 (3 hechos de malos tratos al denunciante + 1 delito de amenazas al denunciante + 1 hecho de malos tratos al niño).

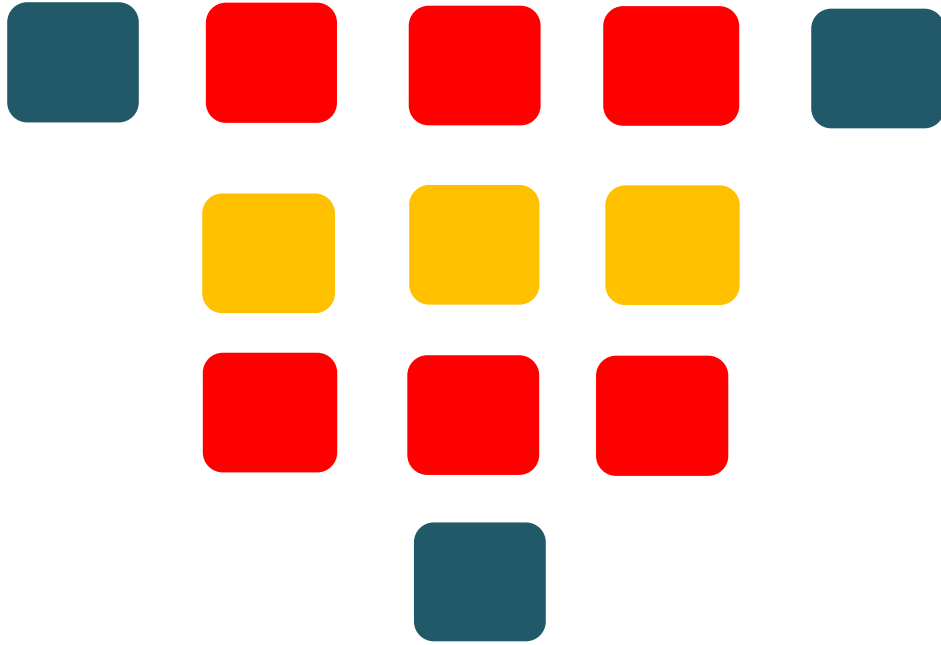
Hay que significar, que como se ha reseñado anteriormente, la Ertzaintza facilita datos de victimizaciones a partir del año 2021.

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

- **ÍNDICE DE ABREVIATURAS EMPLEADAS EN EL INFORME:**

CCN	Centro Criptológico Nacional
CEPOL	Escuela Europea de Policía
DESI	Índice de Economía y Sociedad Digital
DMA	Ley de Mercados Digitales
DSA	Ley de Servicios Digitales
EC3	Centro Europeo de Ciberdelincuencia de Europol
EE.UU.	Estados Unidos
ENISA	Agencia Europea de Seguridad de las Redes y de la Información
EPE	Plataforma de Expertos de Europol
ESN	Estrategia de Seguridad Nacional
EUCTF	Grupo de trabajo sobre ciberdelincuencia de la Unión Europea
EU-CYCLONe	Red Europea de Organización de Enlace de Crisis Cibernéticas
EUROPOL	Agencia de la Unión Europea para la Cooperación Policial
EUROSTAT	Oficina Estadística Europea
INCIBE-CERT	Centro de respuesta a incidentes de seguridad del Instituto Nacional de Ciberseguridad
INE	Instituto Nacional de Estadística
IOCTA	Internet Organised Crime Threat Assessment
J-CAT	Grupo de trabajo conjunto de acción contra el ciberdelito
OCC	Oficina de Coordinación de Ciberseguridad
PES	Programa Estadístico de Criminalidad
PESC	Política Exterior y de Seguridad Común
SEC	Sistema Estadístico de Criminalidad
SPACE	Secure Platform for Accredited Cybercrime Experts
TIC	Tecnologías de la información y las comunicaciones
UE	Unión Europea

ESPAÑA



2021

INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA



Síguenos en Twitter

@interiorgob

www.interior.gob.es

2021