2019

ESTUDIO SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

MINISTERIO DEL INTERIOR
SECRETARÍA DE ESTADO DE SEGURIDAD
GABINETE DE COORDINACIÓN Y ESTUDIOS
SEC Sistema Estadístico de Criminalidad

AUTORES

GABINETE DE COORDINACIÓN Y ESTUDIOS.
SECRETARIA DE ESTADO DE SEGURIDAD

JAIME CERECEDA FERNÁNDEZ-ORUÑA

FRANCISCO SÁNCHEZ JIMÉNEZ

DAVID HERRERA SÁNCHEZ

FRANCISCO MARTÍNEZ MORENO

MARCOS RUBIO GARCÍA

VICTORIA GIL PÉREZ

ANA Mª SANTIAGO OROZCO

MIGUEL ÁNGEL GÓMEZ MARTÍN

NIPO 126-19-018-9

Edita: MINISTERIO DEL INTERIOR — SECRETARÍA GENERAL TÉCNICA

ÍNDICE

1 INTRODUCCIÓN

21 RADIOGRAFÍA DE LA SOCIEDAD DE LA INFORMACIÓN

30 INFRAESTRUCTURAS CRÍTICAS Y CIBERSEGURIDAD

35 DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD

48 METADATA

1 INTRODUCCIÓN

MINISTERIO DEL INTERIOR
SECRETARÍA DE ESTADO DE SEGURIDAD
GABINETE DE COORDINACIÓN Y ESTUDIOS
seC Sistema Estadístico de Criminalidad

1 INTRODUCCIÓN

La Ciberdelincuencia 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 ***VII Informe sobre Cibercriminalidad***, correspondiente a la delincuencia informática registrada en el año 2019.

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. Por primera vez se aúnan en este tipo de informe los **datos de todos los cuerpos policiales del territorio nacional** (Cuerpo Nacional de Policía, Guardia Civil, Policía Foral de Navarra, Ertzaintza, Mossos d' Esquadra y distintos Cuerpos de Policía Local), tanto en la vertiente de los hechos conocidos como de las detenciones e investigados. Por dicha razón, se han reconstruido y actualizado en el presente Informe los datos de las series históricas.

Para el capítulo de victimizaciones, con la excepción de la Ertzaintza, se detallan igualmente datos de todas las Fuerzas y Cuerpos de Seguridad. Es por ello, que las series históricas publicadas hasta la fecha, se han visto modificadas, como consecuencia del nuevo suministro de datos por estos cuerpos policiales referenciados anteriormente.

Los datos proceden del Sistema Estadístico de Criminalidad (SEC), y de los incidentes que registra el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC), 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.

Este Informe aglutina datos del año 2019 no solo en relación a la información estadística sobre delitos informáticos en nuestro país, sino además, en un primer apartado y a modo introductorio, una serie de informaciones publicadas por otros organismos nacionales (INE, ONTSI) 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, hogares con telefonía fija y móvil, empresas que utilizan medios sociales, grado de confianza en internet, tipo de fines específicos del uso de internet, y por último, empresas que utilizan sistemas de seguridad y algún servicio de cloud computing.

En el segundo y tercer bloque del Informe se explican los datos procedentes del Centro Nacional de Protección de las Infraestructuras Críticas (CNPIC), 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 víctimas, detenciones efectuadas, incidentes por comunidad 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 conceptuaciones que emplea el Convenio de Budapest, 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.

La importancia que va adquiriendo la cibercriminalidad viene correlacionada con el aumento del número de usuarios a nivel mundial, que se exponen en el cuadro siguiente.

WORLD INTERNET USAGE AND POPULATION STATISTICS 2019 Year-End Estimates						
World Regions	Population (2020 Est.)	Population % of World	Internet Users 31 Dec 2019	Penetration Rate (% Pop.)	Growth 2000-2020	Internet World %
Africa	1,340,598,447	17.2 %	526,374,930	39.3 %	11,559 %	11.5 %
Asia	4,294,516,659	55.1 %	2,300,469,859	53.6 %	1,913 %	50.3 %
Europe	834,995,197	10.7 %	727,814,272	87.2 %	592 %	15.9 %
Latin America / Caribbean	658,345,826	8.5 %	453,702,292	68.9 %	2,411 %	10.0 %
Middle East	260,991,690	3.9 %	180,498,292	69.2 %	5,395 %	3.9 %
North America	368,869,647	4.7 %	348,908,868	94.6 %	222 %	7.6 %
Oceania / Australia	42,690,838	0.5 %	28,775,373	67.4 %	277 %	0.6 %
WORLD TOTAL	7,796,615,710	100.0 %	4,574,150,134	58.7 %	1,167 %	100.0 %

Infografía nº 1.- Usuarios de internet a nivel mundial[1]

Como se puede comprobar en la infografía nº 1, el 50% de los usuarios de internet a nivel mundial se concentran en Asia, siendo Europa la segunda región con mayor volumen de usuarios (15'9% sobre el total mundial). No obstante, si atendemos al porcentaje de población que tiene internet dentro de la misma región, las diferencias de América del Norte y Europa son netamente evidentes con el resto del mundo.

Dentro de otro orden de cosas y relacionado con el aspecto normativo, durante 2019 cabe destacar en España la importancia derivada de la redacción de cinco (5) Circulares por parte de la Fiscalía General del Estado:

1. Circular 1/2019, de 6 de marzo, de la Fiscal General del Estado, sobre disposiciones comunes y medidas de aseguramiento de las diligencias de investigación tecnológicas en la Ley de Enjuiciamiento Criminal.

2. Circular 2/2019, de 6 de marzo, de la Fiscal General del Estado, sobre interceptación de comunicaciones telefónicas y telemáticas.

3. Circular 3/2019, de 6 de marzo, de la Fiscal General del Estado, sobre captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos.

4. Circular 4/2019, de 6 de marzo, de la Fiscal General del Estado, sobre utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización.

5. Circular 5/2019, de 6 de marzo, de la Fiscal General del Estado, sobre registro de dispositivos y equipos informáticos.

[1] https://www.internetworldstats.com/stats.htm

Todas estas circulares se convierten en piezas imprescindibles y de suma utilidad para llevar a cabo las investigaciones en esta materia, sirviendo como un ejemplo de conjunción de fuerzas y sinergias entre la actuación de Juzgados y Tribunales, Fiscalías y Fuerzas y Cuerpos de Seguridad.

Sin embargo, quizás el aspecto más relevante del año 2019 ha sido la publicación en el BOE nº 103 de fecha 30 de abril de 2019, de la Orden PCI/487/2019, de 26 de abril, por la que se publica la ***Estrategia Nacional de Ciberseguridad 2019***, aprobada por el Consejo de Seguridad Nacional. *C*omo se dice en el referido texto normativo: *"La Estrategia establece un esquema novedoso, con cinco objetivos generales que resultan transversales a todos los ámbitos. La gestión de crisis, la cultura de Seguridad Nacional, los espacios comunes globales, el desarrollo tecnológico y la proyección internacional de España conforman una matriz estratégica donde la ciberseguridad está llamada a abrir nuevas vías hacia el modelo de presente y futuro de la seguridad en España".*

Otro hecho destacable es que dentro de la propia estrategia se da una definición de **cibercriminalidad**: *"El término cibercriminalidad, hace referencia al conjunto de actividades ilícitas cometidas en el ciberespacio que tienen por objeto los elementos, sistemas informáticos o cualesquiera otros bienes jurídicos, siempre que en su planificación, desarrollo y ejecución resulte determinante la utilización de herramientas tecnológicas; en función de la naturaleza del hecho punible en sí, de la autoría, de su motivación, o de los daños infligidos, se podrá hablar así de ciberterrorismo, de ciberdelito, o en su caso, de hacktivismo"*. Asimismo, se alude a que *"son tres los ámbitos en los que se desenvuelve la lucha contra la cibercriminalidad: (i) el ciberespacio como objetivo directo de los hechos delictivos, o de la amenaza; (ii) el ciberespacio como medio clave para su comisión; y (iii) el ciberespacio como medio u objeto directo de investigación de cualquier tipo de hecho ilícito".*

Por otro lado, la importancia que otorga la Estrategia Nacional de Ciberseguridad a la cibercriminalidad se ve corroborada por el establecimiento como Línea de Acción 3 el "*Reforzar las capacidades de investigación y persecución de la cibercriminalidad, para garantizar la seguridad ciudadana y la protección de los derechos y libertades en el ciberespacio*", esgrimiéndose una serie de medidas entre las cuales se incluyen las siguientes:

1. *Reforzar el marco jurídico para responder eficazmente a la cibercriminalidad, tanto en lo relativo a la definición de tipos penales como en la regulación de adecuadas medidas de investigación.*
2. *Fomentar la colaboración y participación ciudadana, articulando instrumentos de intercambio y transmisión de información de interés policial, y promoviendo el*

desarrollo de campañas de prevención de la cibercriminalidad orientadas a ciudadanos y empresas.

3. *Reforzar las acciones encaminadas a potenciar las capacidades de investigación, atribución, persecución y, en su caso, la actuación penal, frente a la cibercriminalidad.*
4. *Fomentar el traslado a los organismos competentes de la jurisdicción penal de la información relativa a incidentes de seguridad que presenten caracteres de delito, y especialmente de aquellos que afecten o puedan afectar a la provisión de los servicios esenciales y a las infraestructuras críticas.*
5. *Procurar a los operadores jurídicos el acceso a información y recursos materiales que aseguren una mejor aplicación del marco jurídico y técnico relacionado con la lucha y enjuiciamiento de los hechos ilícitos que correspondan.*
6. *Fomentar el intercambio de información, experiencia y conocimientos, entre el personal con responsabilidades en la investigación y persecución de la cibercriminalidad.*
7. *Asegurar a los profesionales del Derecho y a las Fuerzas y Cuerpos de Seguridad del Estado el acceso a los recursos humanos y materiales que les proporcionen el nivel necesario de conocimientos para la mejor aplicación del marco legal y técnico asociado.*
8. *Impulsar la coordinación de las investigaciones sobre cibercriminalidad y otros usos ilícitos del ciberespacio entre los distintos órganos y unidades con competencia en esta materia.*
9. *Fortalecer la cooperación judicial y policial internacional.*

En suma, todo ello configura un sistema que pretende articular sinergias para que tanto la labor de concienciación, prevención e investigación de estos ilícitos penales, confluyan paralelamente y coadyuven a una eficaz protección.

Todo este proceso de cambio estratégico y normativo, que redundará en las actuaciones policiales, viene condicionado porque según palabras de la propia Europol[2]: "*el delito cibernético se está volviendo más agresivo y conflictivo. Esto se puede ver a través de las diversas formas de cibercrimen, incluidos los delitos de alta tecnología, las violaciones de datos y la extorsión sexual*". Tal como se puede ver en la página web de dicha agencia, hay un amplio catálogo de códigos dañinos:

Una **botnet** (abreviatura de red de robots) está compuesta por computadoras que se comunican entre sí a través de Internet. Un centro de comando y control los utiliza

[2] https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime

para enviar spam, montar ataques de denegación de servicio distribuidos (DDoS) y cometer otros delitos.

Un **rootkit** es una colección de programas que permiten el acceso de nivel de administrador a una computadora o red informática, lo que permite al atacante obtener acceso root o privilegiado a la computadora y posiblemente a otras máquinas en la misma red.

Un **gusano** se replica a través de una red informática y realiza acciones maliciosas sin orientación.

Un **troyano** se hace pasar por un programa legítimo o está incrustado en él, pero está diseñado para fines maliciosos, como espiar, robar datos, eliminar archivos, expandir una botnet y realizar ataques DDoS.

Un **infector** de archivos infecta archivos ejecutables (como .exe) sobrescribiéndolos o insertando un código infectado que los desactiva.

Un **troyano de puerta trasera / acceso remoto (RAT)** accede a un sistema informático o dispositivo móvil de forma remota. Puede ser instalado por otra pieza de malware. Le da un control casi total al atacante, que puede realizar una amplia gama de acciones, que incluyen:

- Acciones de monitoreo
- Ejecutar comandos
- Enviando archivos y documentos al atacante
- Pulsaciones de teclas de registro
- Tomar capturas de pantalla

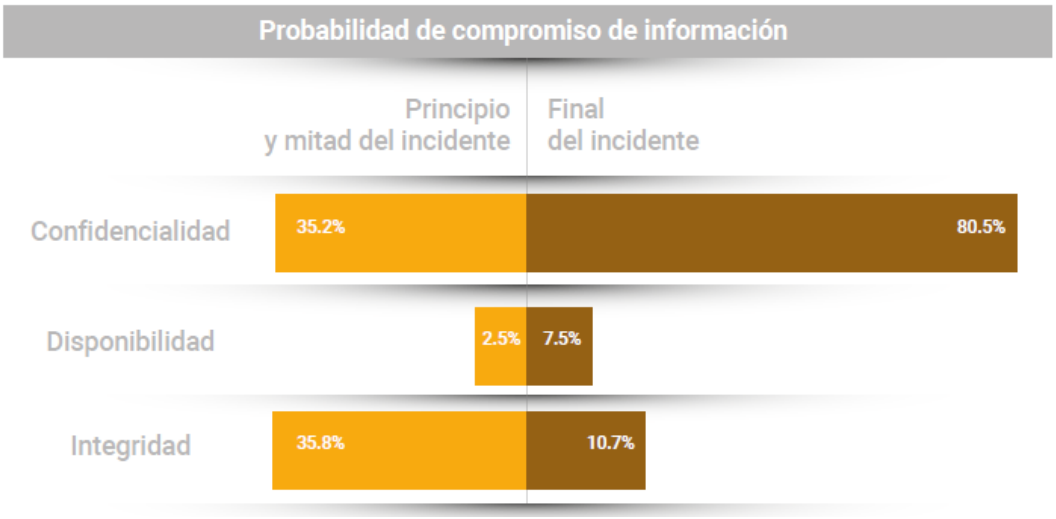
El **ransomware** impide que los usuarios accedan a sus dispositivos y exige que paguen un rescate a través de ciertos métodos de pago en línea para recuperar el acceso. Una variante, el ransomware policial, utiliza símbolos relacionados con temática policial para otorgar autoridad al mensaje de rescate.

Scareware es un software antivirus falso que pretende escanear y encontrar amenazas de malware / seguridad en el dispositivo de un usuario para que paguen por su eliminación.

El **spyware** se instala en una computadora sin el conocimiento de su propietario para monitorear su actividad y transmitir la información a un tercero.

El **adware** muestra banners publicitarios o ventanas emergentes que incluyen código para rastrear el comportamiento del usuario en Internet.

Hay que poner de relieve, que para describir la situación de la ciberseguridad en nuestro ámbito territorial, un informe de referencia es el realizado por el Centro Criptológico Nacional (CCN-CERT), relativo a las ciberamenazas y tendencias (edición del año 2019), el cual sitúa a la pérdida de la confidencialidad de los datos como el resultado más frecuente de los ataques informáticos



Infografía nº 2.-Fuente CCN-CERT[3]

Según el CCN-CERT, dentro de los métodos más usados por los ciberdelincuentes se encontrarían los siguientes:

- Propagación de código dañino a través de los correos electrónicos.
- Uso de malware de criptojacking/cryptomining[4].
- Refinamiento del phishing mediante el uso de técnicas de ingeniería social y la innovación permanente para persuadir a los usuarios de la autenticidad de las estafas.
- Innovación en las plataformas del Ciberdelito como Servicio (Crime as a Service). Además de las mejoras en los servicios ofertados, estos desarrollos permiten una mayor facilidad de uso, lo que contribuye a extender su popularidad y propiciar ataques más eficientes.

Quizás uno de los mayores problemas que se encuentran las Fuerzas y Cuerpos de Seguridad, es la diversidad de enfoques con los que tiene que afrontar la lucha contra la cibercriminalidad. En este sentido, Europol publicó un informe titulado: "DO CRIMINALS

[3] https://www.ccn-cert.cni.es/en/reports/public/3767-ccn-cert-ia-13-19-ciberamenazas-y-tendencias-resumen-ejecutivo-2019/file.html

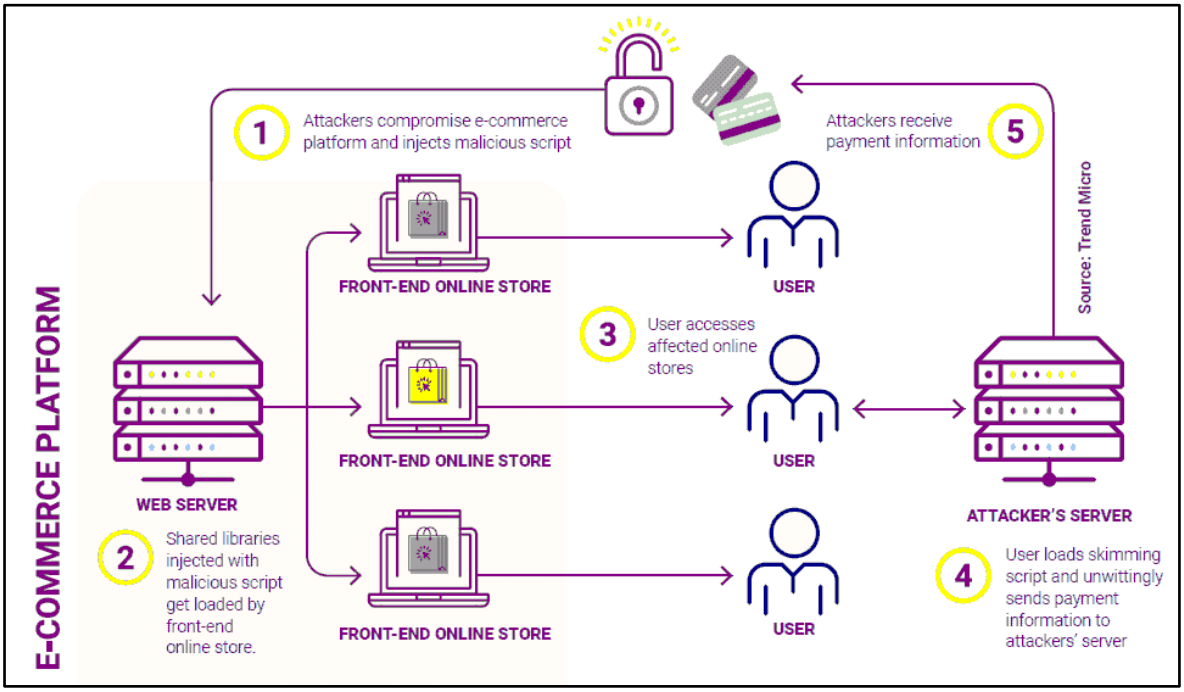
[4] Utilizar la potencia de cálculo de los sistemas informáticos de terceros para el minado de criptomonedas

DREAM OF ELECTRIC SHEEP? HOW TECHNOLOGY SHAPES THE FUTURE OF CRIME AND LAW ENFORCEMENT"[5], en el cual se hace un análisis detallado de este aspecto. Europol llega a afirmar que: "*El advenimiento de las llamadas tecnologías disruptivas, aquellas que alteran fundamentalmente la forma en que vivimos, trabajamos y nos relacionamos entre sí, proporciona a los delincuentes nuevas formas de perseguir sus objetivos ilegales, pero también equipa a las fuerzas del orden con herramientas poderosas en la lucha contra el crimen. Para seguir siendo relevante y eficaz, es necesario que las autoridades encargadas de hacer cumplir la ley inviertan en comprender y buscar activamente soluciones nuevas e innovadoras"*.

Posteriormente, Europol realiza una identificación de estas amenazas entre las que incluye: *"Algunas de las tecnologías emergentes incluyen Inteligencia Artificial (IA), computación cuántica, 5G, redes descentralizadas alternativas y criptomonedas, impresión 3D y biotecnología. Se espera que tengan un profundo impacto en el panorama criminal y la capacidad de las autoridades policiales para responder a las amenazas emergentes. La interrupción proviene de la convergencia entre estas nuevas tecnologías, los casos de uso y aplicaciones nunca antes vistos, y los desafíos planteados por los marcos legales y regulatorios existente".*

Todas estas nuevas formas asociadas a la cibercriminalidad, llevan consigo que las conductas de los ciberdelincuentes sean complejas, tanto en su forma de comisión como en la prevención de las mismas. Un ejemplo de ello es cómo los ciberdelincuentes, pueden acceder a diferentes plataformas de comercio electrónico, para apoderarse de los datos bancarios de los clientes. En la infografía nº 3 se detalla un esquema de este modo de proceder, tal como figura en el informe IOCTA 2019[6], realizado por EUROPOL.

[5] https://www.europol.europa.eu/publications-documents/do-criminals-dream-of-electric-sheep-how-technology-shapes-future-of-crime-and-law-enforcement
[6] https://www.europol.europa.eu/sites/default/files/documents/iocta_2019.pdf



Infografía nº 3.- Esquema de EUROPOL donde se refleja el acceso por ciberdelincuentes a datos bancarios de clientes en plataformas de comercio electrónico.

Como se verá corroborado en el capítulo de la radiografía de la información de la sociedad española, cada vez hacemos mayor uso del comercio electrónico. Por lo tanto, muchas de las conductas de los criminales van orientadas hacia este campo de actuación. Un ejemplo de actuación policial desarrollada hacia esta modalidad criminal, fue la realizada el pasado año por el Departamento de Delitos Telemáticos de la Unidad Central Operativa (UCO) de la Guardia Civil en la denominada Operación "LUPIN", en la que se llegó a detener al considerado el mayor ciber-estafador en la historia de España, sobre el que recaían más de 25 requisitorias judiciales de detención por todo el territorio nacional, lo que lo convertía en objetivo prioritario para todas las policías de nuestro país[7].

Se trata de una serie de ciber-estafas cometidas principalmente por la venta de productos de electrónica de consumo en tiendas online fraudulentas, a través de páginas web copiadas de tiendas totalmente legales y de conocido prestigio en el mercado online, llegando a utilizar incluso sus logos y nombres de marca, todo ello con total desconocimiento del usuario estafado y con la clara intención de inducir a error al mismo.

Una característica común de estas páginas web fraudulentas, era su mínima duración en el tiempo, llegando a activarse únicamente durante un fin de semana y desapareciendo a continuación sin dejar ningún tipo de rastro. En ese breve periodo, la página era sometida a una intensa campaña de publicidad y posicionamiento web en los

[7] https://www.guardiacivil.es/es/prensa/noticias/7043.html

principales buscadores y redes sociales con llamativas ofertas, todo ello con la intención de captar el mayor número de potenciales compradores en el menor tiempo posible.

Una de las particularidades de esta organización era, aprovechando las facilidades que ofrecen las nuevas tecnologías, la continua persecución del anonimato en la red para evitar ser detectados y que se les pudiese vincular con la comisión de los delitos investigados.

Aunque esta operación se inició hace aproximadamente un año por parte de la Guardia Civil, es posible que el detenido llevase cerca de tres años cometiendo este tipo de estafas en diferentes modalidades, siendo la más utilizada la que al finalizar el usuario el procedimiento de pago del producto elegido, la web forzaba al mismo a elegir la transferencia bancaria como única forma de pago posible. Estas cuentas bancarias de destino, obligaban al estafador a manejar cientos de ellas, al igual que números de tarjetas SIM de telefonía para no dejar rastro, puestas normalmente tanto unas como otras a nombre de personas jóvenes a las que pagaba significativas cantidades de dinero por facilitar sus datos personales para este fin.

Con el tiempo estas estafas han ido perfeccionándose, con la excusa del proceso de pago, el estafador llegaba a llamar telefónicamente a la víctima, para que se instalara una App que supuestamente le informaba del seguimiento del pedido. Lo que hacía en realidad la aplicación era desviar todos los SMS de su teléfono para poder tener los códigos enviados por los bancos, lo que le permitía poder firmar transferencias y efectuar cargos a las tarjetas de crédito por altos importes, llegando a vaciar las cuentas de algunas de sus víctimas.

Una vez realizado lo anterior, sirviéndose de la tecnología "contactless", asociaba las tarjetas de crédito de las cuentas de las mulas a sus terminales móviles, para ir extrayendo el dinero en cajeros automáticos en rutas realizadas por todo Madrid en las que adoptaba fuertes medidas de seguridad. Esta práctica era repetida sucesivamente en un mismo día, llegando a acumular decenas de miles de euros en solo una jornada de actividad recaudatoria.

Continuando con los fraudes relacionados con el comercio electrónico, cabe resaltar la operación de Policía Nacional que si bien ha sido realizada en el año 2020, es fruto de una ardua labor de investigación, por la que se dio un “golpe” al mercado negro de tarjetas bancarias en Internet a nivel mundial a través de la operación “Market[8]”.

[8] https://www.policia.es/prensa/20200215_1.html

Fruto de esta operación se desarticuló una organización criminal de origen nigeriano especializada en la falsificación de tarjetas bancarias, fraude a través de Internet, falsificación de documentos y blanqueo de capitales. Sus 36 integrantes fueron detenidos por un fraude que sobrepasaba el millón y medio de euros y cuyos afectados residían en un total de 37 países.

La denominada operación Market se inició tras un exhaustivo análisis de operaciones con tarjetas bancarias vendidas en foros especializados de carding, que es como se denomina al uso ilegítimo de las tarjetas de crédito pertenecientes a otras personas con el fin de obtener bienes realizando fraude con ellas. Este mismo análisis también se llevó a cabo en los mercados clandestinos darkweb, que es como se conoce al contenido que se puede encontrar en las diferentes redes a las que sólo se puede acceder con programas específicos.

Los investigadores dieron con un punto de compromiso coincidente en la plataforma online de un conocido supermercado. De forma sistemática, el establecimiento soportaba actuaciones ilícitas al haber sido vulnerados todos sus procedimientos de solicitud, verificación y emisión de las tarjetas bancarias y, como consecuencia, se habían expedido más de 70 tarjetas bancarias fraudulentas, con las que se había llevado a cabo un fraude de más de 1.500.000 euros.

En una primera fase, se aportaba documentación con distintas identidades falsas para la emisión de las tarjetas bancarias a la financiera emisora de las tarjetas de pago. Posteriormente, una vez recibidas en los domicilios bajo el control de los investigados, se producía el uso fraudulento de las tarjetas agotando el crédito existente en ellas.

Finalmente, los delincuentes abonaban la deuda generada de forma online aportando numeraciones de tarjetas bancarias extranjeras de origen fraudulento obtenidas en foros privados de internet, así como en la deep web y la darknet. Así es como ciudadanos de 37 países tan dispares como Panamá, Malasia, China o Colombia se han visto afectados por este fraude.

Para vender en el mercado secundario estos productos disponían de perfiles en las principales redes sociales y plataformas de venta entre particulares, en los que los ofertaban a precios sensiblemente inferiores a los originales.

2 RADIOGRAFÍA DE LA SOCIEDAD DE LA INFORMACIÓN

En este *VII 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 2019 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, ONTSI) como europeos (EUROSTAT).

La Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los Hogares (año 2019), del Instituto Nacional de Estadística (INE) se trata de una investigación dirigida a las personas de 16 y más años 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 información de los menores de 10 a 15 años.

A lo largo del capítulo 2 de este Informe (Radiografía de la sociedad de la Información), en sus diferentes apartados, se trata de trazar y esquematizar 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 Instituto Nacional de Estadística (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 2019 con respecto al año 2018. Siguiendo de esta forma la tendencia general experimentada en la serie histórica que se representa (2010-2019).

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 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 2010.

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 99,1 % de los jóvenes, entre 16 a 24 años, afirman haber accedido a la Red en los últimos tres meses, porcentaje que se reduce a un 63,6% entre las personas con edades comprendidas entre los 65 y 74 años. Si bien, la mayoría de los porcentajes de los rangos de edad que comprende este análisis han experimentado un incremento con respecto a 2018, siendo el incremento más acusado en la edad de 65 a 74 años.

Por sexo, y ***por primera vez en la serie histórica se iguala el porcentaje de uso de internet de mujeres y hombres***.

Resulta llamativo, en el punto 2.3 (Perfil del menor de edad ante la sociedad de la información), 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 89,7% y 92,9, respectivamente. Por sexos, es muy pequeña la diferencia, aunque hay que reflejar que la mujer muestra mayores porcentajes en ambas categorías. En 2019, el 87,9% de los niños afirmaron haber utilizado un ordenador en los últimos tres meses, frente al 91,7% de las niñas, siendo el 92,7% cuando se hace referencia al acceso a Internet en relación al 93,1% de las niñas. Hay que significar, que el uso de ordenador ha descendido entre los menores durante el año 2019.

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 2010 el comercio electrónico se ha llegado casi a triplicar, puesto que el 46,9 % de las personas encuestadas en 2019 reconocen haber realizado alguna compra empleando esta vía, mientras que en el año 2010 solo lo hacían el 17,0%. Por sexo, los hombres muestran mayores cifras porcentuales que las mujeres (48,0% frente al 45,8%).

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 (67,2%). Por otro lado, las personas de 65 a 74 años muestran que sólo el 13’5% realiza compras por internet.

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 la cifra de viviendas con acceso a Internet en los diferentes países de la Unión Europea (28-UE) (Punto 2.5 Comparativa internacional), en la serie histórica 2010-2018. Un hecho destacable es que ***España por primera vez, se encuentra por encima de la media de la UE-28***, con un 91% frente al 90% 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 (DG CNECT) para evaluar los avances de los países de la UE hacia una economía y una sociedad digitales. Este índice agrega una serie de indicadores pertinentes, estructurados en torno a cinco dimensiones: conectividad, capital humano, uso de internet, integración de la tecnología digital y servicios públicos digitales.

A nivel nacional, desde el Observatorio Nacional de las Telecomunicaciones y de la Seguridad de la Información (ONTSI), del Ministerio de Energía, Turismo y Agenda Digital se publica de manera periódica un informe que recoge los principales indicadores de la Sociedad de la Información en España (2.7). Éste señala que en 2019, el número de hogares con telefonía fija y móvil era del 74,9% y 98,5%, respectivamente. Otro hecho referenciable, relacionado con el perfil de las empresas es el mayor uso que dan nuestras empresas a las redes sociales (95,8%). Asimismo, del porcentaje de empresas que utilizan sistemas internos de seguridad, emplean como principales técnicas la actualización de software y la copia de seguridad de datos en una ubicación separada. Otro hecho que viene experimentando un crecimiento exponencial es el relacionado con la utilización de servicio de cloud computing. Según el INCIBE[9] *el cloud computing, o computación en la nube, es un modelo de computación que permite al proveedor tecnológico ofrecer servicios informáticos a través de internet. De esta forma los recursos, es decir, el hardware, el software y los datos se pueden ofrecer a los clientes bajo demanda.*

Esta prestación de servicios permite al cliente el acceso bajo demanda y a través de la red a un conjunto de recursos compartidos y configurables (redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser rápidamente asignados y liberados con una mínima gestión por parte del proveedor. En resumen, permite acceder a

[9] https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia-cloud-computing_0.pdf

los servicios y recursos contratados proporcionando flexibilidad de dimensionamiento y acceso.

El cliente, bien sea una empresa o un particular, se abstrae de la infraestructura tecnológica necesaria para poder utilizar una determinada aplicación, ya que simplemente se requiere un navegador web con conexión a la red para tener acceso a los procesos o a los datos. El cliente puede acceder a los servicios contratados desde cualquier lugar y todos los días del año, adaptándolos a sus necesidades de forma dinámica. Todo ello sin realizar inversiones en equipos y software, y sin los gastos derivados de su mantenimiento.

En cuanto al perfil del internauta situamos como aspectos principales los siguientes: el grado de confianza en internet va creciendo paulatinamente y que el envío y recepción de correos electrónicos junto con la lectura o descarga de periódicos son las dos actividades principales que se realizan con motivos particulares.

3 INFRAESTRUCTURAS CRÍTICAS Y CIBERSEGURIDAD

En la introducción al capítulo se detallan los aspectos más relevantes en esta materia.

4 DATOS ESTADÍSTICOS 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 Gabinete de Coordinación y Estudios asumió las funciones en materia de estadística de criminalidad, que continuaron tras la publicación del Real Decreto 952/2018, de 27 de julio, 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 reza en esta Instrucción, a partir del Sistema Estadístico de Criminalidad (SEC) que se compone de la Base de Datos que registra las actuaciones policiales, se llevará a cabo la explotación estadística de los datos que se anoten 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.

En este caso concreto que nos ocupa se detalla a continuación la información estadística consignada en el SEC sobre 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 2016-2019 (datos de los cuerpos que facilitan datos se detallan 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 tecnologías de la información y la comunicación (TIC). De esta forma, se añaden categorías como las siguientes:

- Delitos contra el honor.
- Amenazas y coacciones.

En el periodo comprendido entre 2016 a 2019, se constata el aumento de los delitos informáticos. De esta forma, podemos apreciar que, en 2019, se ha conocido un total de 218.302 hechos, lo que supone un 35,8% más con respecto al año anterior. De esta cifra, el 88,1 % corresponde a fraudes informáticos (estafas) y el 5,9% a amenazas y coacciones. Hay que recordar, lo expuesto al comienzo de la introducción, en el sentido de que con motivo de la incorporación de los datos de Ertzaintza y Mossos d'Esquadra, todos los datos de la serie histórica se han visto alterados

Actualmente, la importancia de la Cibercriminalidad va creciendo año tras año, como se demuestra con el aumento del número de hechos conocidos. Pero otro hecho, innegable es el peso proporcional que va adquiriendo dentro del conjunto de la criminalidad. Como se puede observar en la tabla nº 1, hemos pasado del año 2016, donde nos situábamos en el 4,6% al año 2019 con el 9,9%.

2016	4,6%
2017	5,7%
2018	7,5%
2019	9,9%

Tabla nº 1. % 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). Los gráficos del apartado evidencian de manera esquemática los datos correspondientes a los hechos conocidos, esclarecidos y la cifra de las detenciones e investigaciones resgistradas por las Fuerzas y Cuerpos de Seguridad, en el periodo 2016 a 2019.

En relación al porcentaje de hechos esclarecidos, en el año 2019, éste supone el 15,1% del total de los hechos conocidos. Por otra parte, los detenidos e investigados han alcanzado la cifra de 8.914.

La distribución de la ciberdelincuencia, desde el punto de vista geográfico (4.3. Representación territorial de hechos denunciados de cibercriminalidad), a lo largo de 2019, sitúa a Cataluña, Madrid, 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 ránking Madrid, Barcelona, Valencia, Illes Balears, Bizkaia y Sevilla.

Los datos de la sección 4.4, 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, con excepción de la Ertzaintza.

En 2019, las victimizaciones que han sido registradas por las Fuerzas y Cuerpos de seguridad suman un total de 166.152[10], es decir, un 37,0% más que en el año 2018. La mayoría de las víctimas de ciberdelincuencia pertenecen al sexo masculino (52,3%), tienen entre 26 a 40 años, y son objeto, principalmente, de los delitos de fraudes informáticos, amenazas y coacciones y acceso e interceptación ilícita. 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 el acceso e interceptación ilícita, contra el honor y los delitos sexuales.

Además, en el punto 4.5 (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 2019, el 31,8 % 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 4.6). 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 4.7), el 88,4% de ellas son españolas, y el 11,6% restante extranjeras. En el conjunto de las víctimas de nacionalidad extranjera, son las procedentes de Rumanía, Marruecos e Italia las que aúnan valores más elevados.

Al igual que en el informe pasado, en este *VII 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 4.8 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.

[10] Se pude apreciar una diferencia entre el número de hechos ilícitos conocidos (218.302) y el de victimizaciones registradas (166.152), 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.

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 4.8.

Igualmente, en este estudio, se consignan datos relativos a la edad de la víctima (Punto 4.9 Edad de la víctima). Por lo que, en el año 2019, de las 166.152 victimizaciones registradas, 52.871 se encuadran dentro del rango de edad que comprende los 26 a 40 años, y 41.206 entre los 41 y 50 años. Los menores de edad suman un total de 3.243.

La sección 4.14 presenta la información relativa a las detenciones e investigados. Información que figura desagregada según el tipo penal y sexo, de 2019.

De la cifra total de detenciones e investigaciones (8.914) efectuadas por las Fuerzas y Cuerpos de Seguridad, el 74,3% 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.

Al desglosar la información según los distintos rangos de edad predeterminados (4.15 Detenciones/investigaciones según grupo de edad y sexo.), se observa que la mayor cifra de los responsables de ciberdelincuencia se ubican en el grupo de edad 26 a 40 años.

Por lo que respecta a las diferentes infracciones penales (4.16 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 (79,6%) (4.17). Entre los detenidos/investigados de nacionalidad extranjera son los originarios de Rumanía, Marruecos, Colombia y Venezuela, los que aglutinan un mayor número de casos.

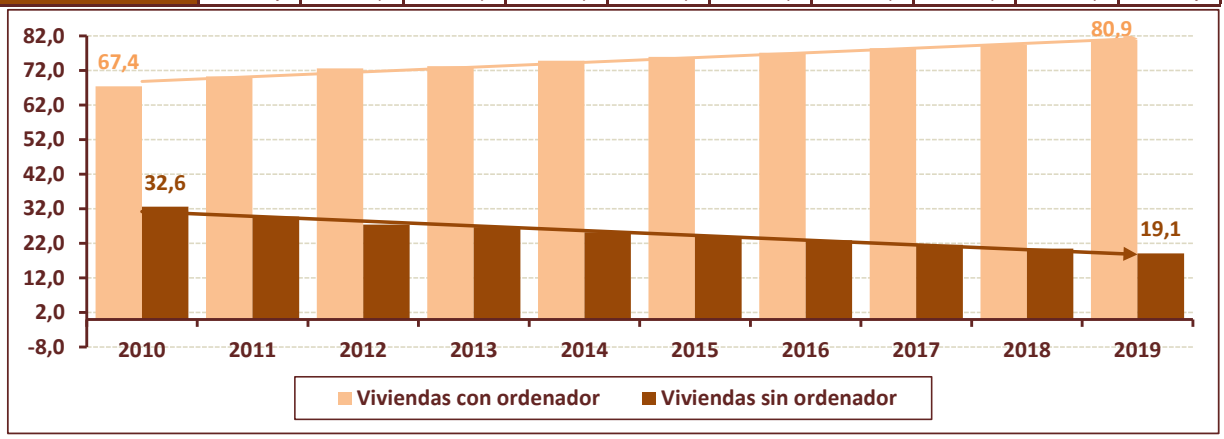
El colectivo de 26 a 40 años de los detenidos/investigados es el más numeroso de todos los rangos establecidos (4.19).

2 RADIOGRAFÍA DE LA SOCIEDAD DE LA INFORMACIÓN

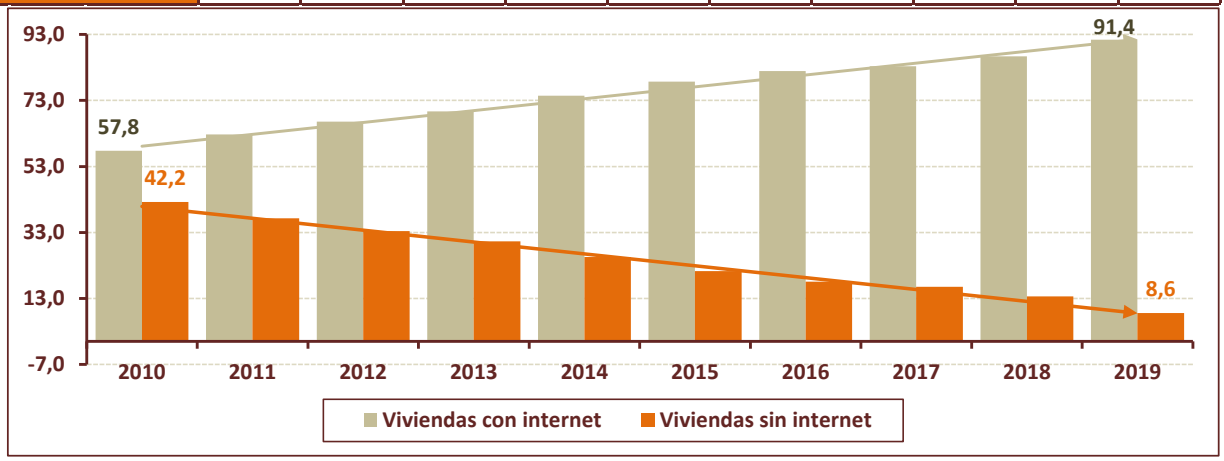
MINISTERIO DEL INTERIOR
SECRETARÍA DE ESTADO DE SEGURIDAD
GABINETE DE COORDINACIÓN Y ESTUDIOS
seC Sistema Estadístico de Criminalidad

>> 2.1. HOGARES

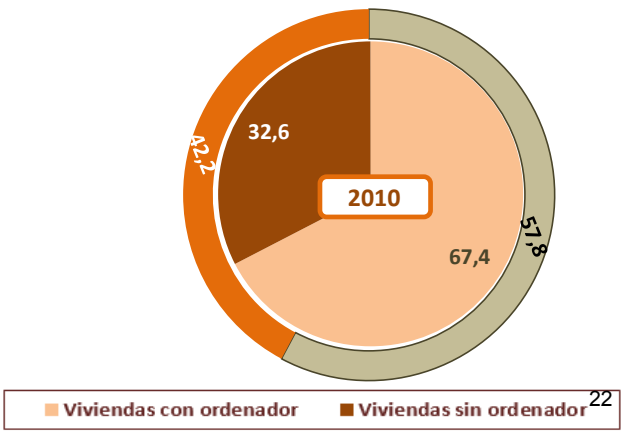
PORCENTAJE DE VIVIENDAS CON / SIN ALGÚN TIPO DE ORDENADOR	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Viviendas con ordenador	**67,4**	70,3	72,6	73,3	74,8	75,9	77,1	78,4	79,5	**80,9**
Viviendas sin ordenador	**32,6**	29,7	27,4	26,7	25,2	24,1	22,9	21,6	20,5	**19,1**

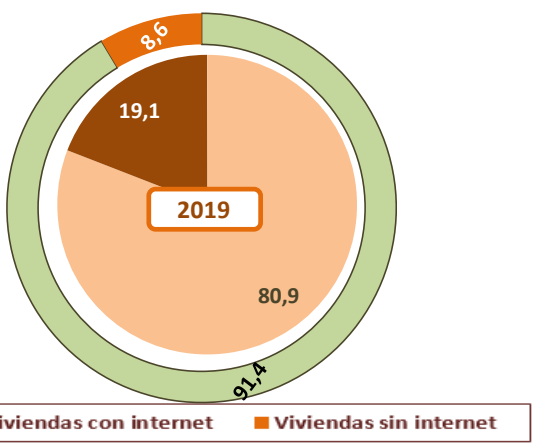


PORCENTAJE DE VIVIENDAS CON / SIN ACCESO A INTERNET	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Viviendas con internet	**57,8**	62,7	66,6	69,7	74,4	78,7	81,9	83,4	86,4	**91,4**
Viviendas sin internet	**42,2**	37,3	33,4	30,3	25,6	21,3	18,1	16,6	13,6	**8,6**



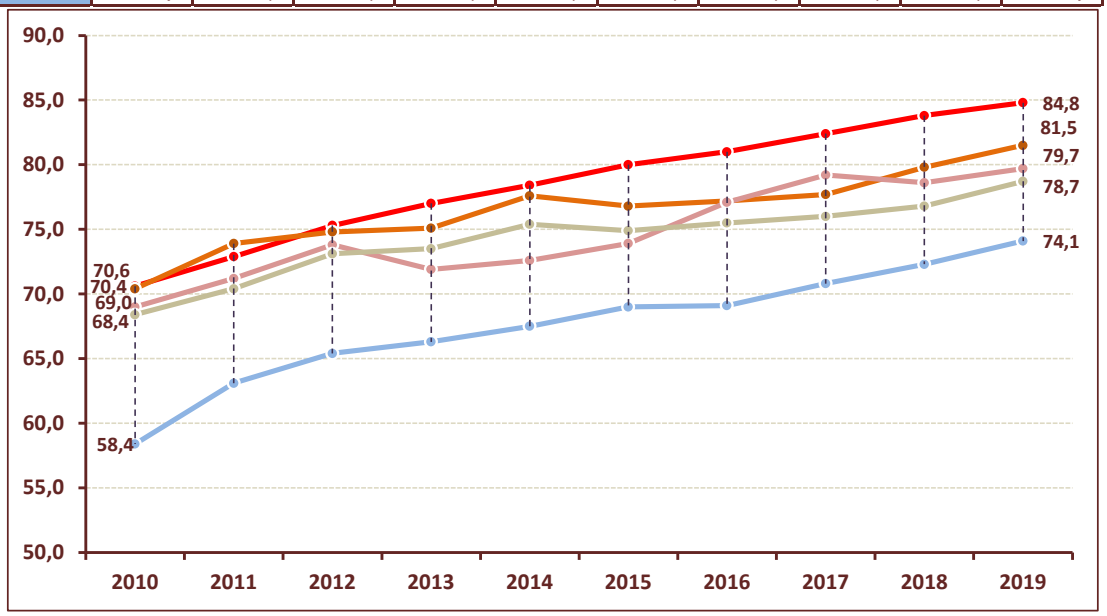
CONTRASTE EVOLUTIVO DE LAS VIVIENDAS 2009 - 2018



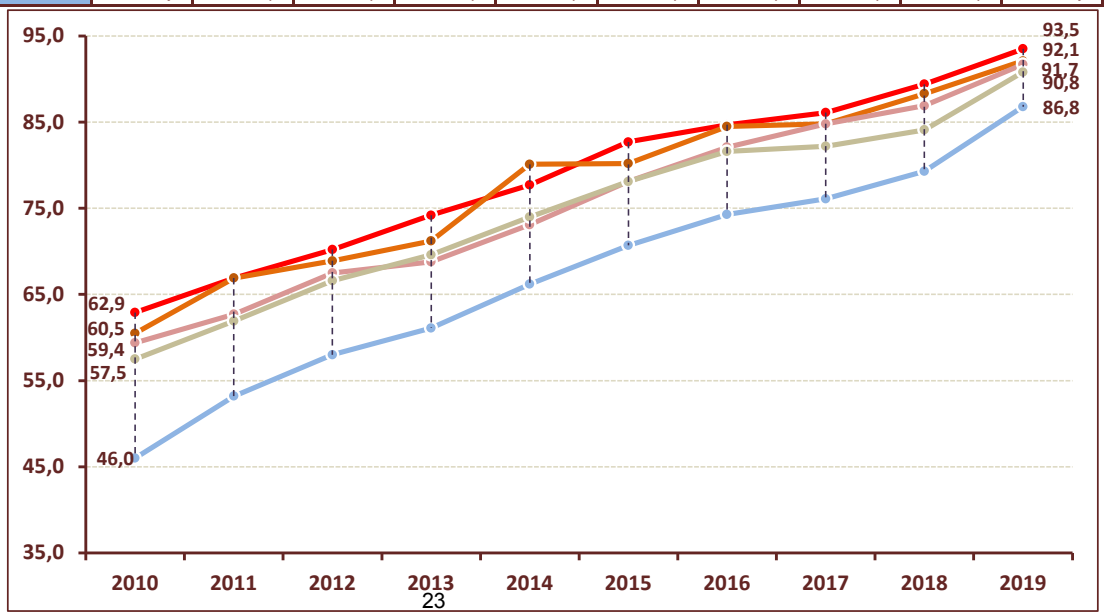


>> 2.1. HOGARES. POR TIPO DE HABITAT

	PORCENTAJE DE VIVIENDAS CON ORDENADOR									
	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Más de 100.000 hab.	**70,6**	72,9	75,3	77,0	78,4	80,0	81,0	82,4	83,8	**84,8**
De 50.000 a 100.000 hab.	**70,4**	73,9	74,8	75,1	77,6	76,8	77,2	77,7	79,8	**81,5**
De 20.000 a 50.000 hab.	**69,0**	71,2	73,8	71,9	72,6	73,9	77,1	79,2	78,6	**79,7**
De 10.000 a 20.000 hab.	**68,4**	70,4	73,1	73,5	75,4	74,9	75,5	76,0	76,8	**78,7**
Menos de 10.000 hab.	**58,4**	63,1	65,4	66,3	67,5	69,0	69,1	70,8	72,3	**74,1**

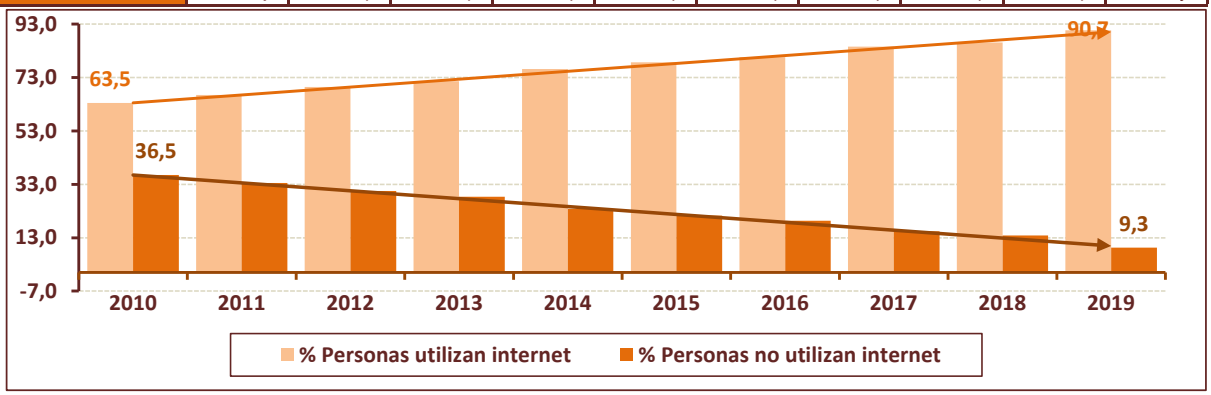


	PORCENTAJE DE VIVIENDAS CON ACCESO A INTERNET									
	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Más de 100.000 hab.	**62,9**	66,9	70,2	74,2	77,7	82,7	84,7	86,1	89,4	**93,5**
De 50.000 a 100.000 hab.	**60,5**	66,9	68,9	71,2	80,1	80,2	84,5	84,8	88,3	**92,1**
De 20.000 a 50.000 hab.	**59,4**	62,7	67,5	68,8	73,1	78,1	82,1	84,8	86,9	**91,7**
De 10.000 a 20.000 hab.	**57,5**	61,9	66,6	69,6	74,0	78,1	81,6	82,2	84,1	**90,8**
Menos de 10.000 hab.	**46,0**	53,2	58,0	61,1	66,2	70,7	74,3	76,1	79,3	**86,8**

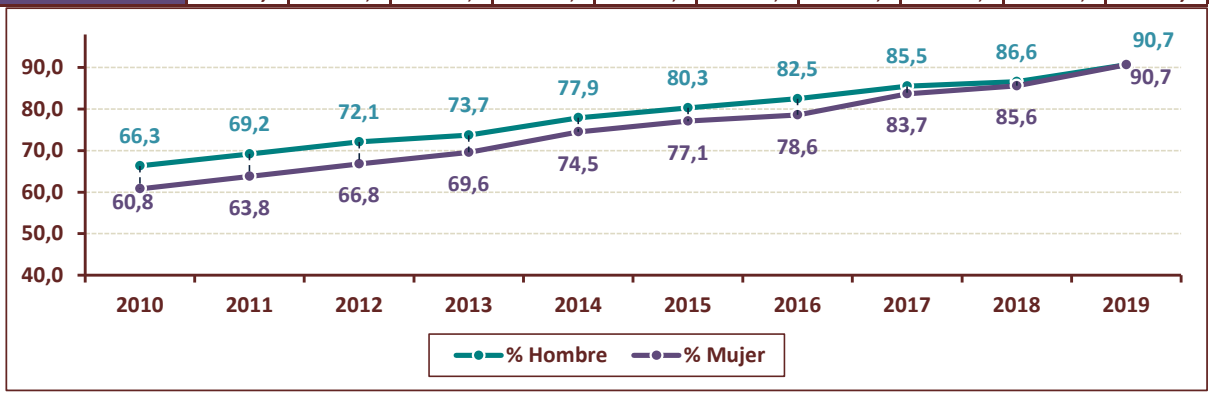


>> 2.2.PERFIL DEL CIUDADANO ANTE LA SOCIEDAD DE LA INFORMACION. USO DE INTERNET

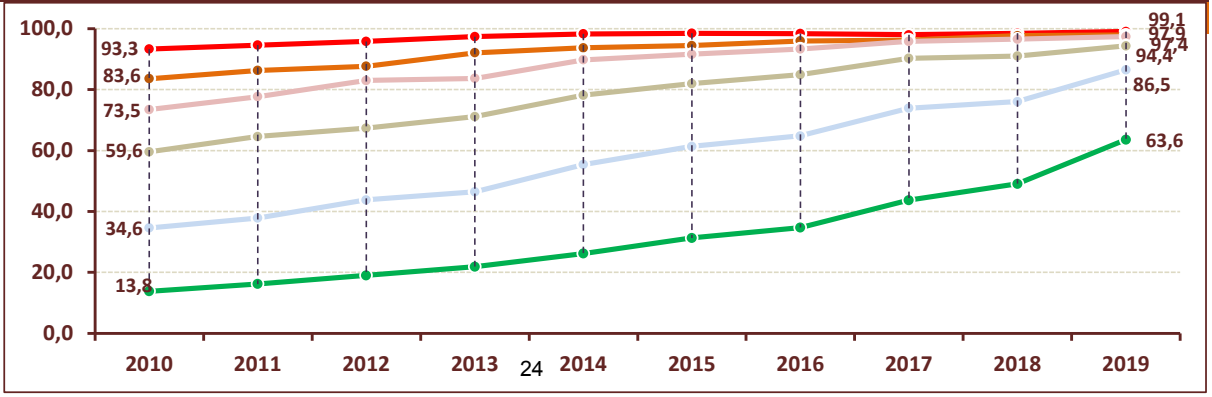
% DE PERSONAS QUE HAN UTILIZADO O NO INTERNET ÚLTIMOS 3 MESES	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Utilizado internet	**63,5**	66,5	69,5	71,6	76,2	78,7	80,6	84,6	86,1	**90,7**
No utilizado internet	**36,5**	33,5	30,5	28,4	23,8	21,3	19,4	15,4	13,9	**9,3**



% POR SEXO DE PERSONAS QUE HAN UTILIZADO INTERNET ÚLTIMOS 3 MESES	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Hombre	**66,3**	69,2	72,1	73,7	77,9	80,3	82,5	85,5	86,6	**90,7**
Mujer	**60,8**	63,8	66,8	69,6	74,5	77,1	78,6	83,7	85,6	**90,7**

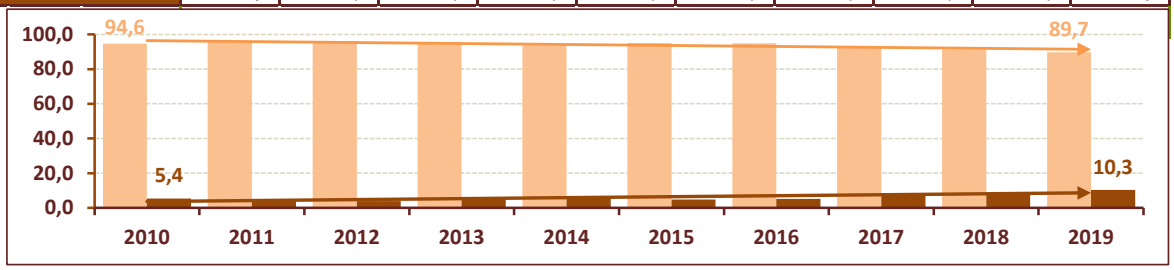


% POR GRUPO DE EDAD DE PERSONAS QUE HAN UTILIZADO INTERNET ÚLTIMOS 3 MESES	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Edad: De 16 a 24 años	**93,3**	94,6	95,8	97,4	98,3	98,5	98,4	98,0	98,5	**99,1**
Edad: De 25 a 34 años	**83,6**	86,3	87,7	92,1	93,7	94,5	96,0	96,3	97,7	**97,9**
Edad: De 35 a 44 años	**73,5**	77,7	83,0	83,7	89,8	91,6	93,3	95,8	96,6	**97,4**
Edad: De 45 a 54 años	**59,6**	64,6	67,4	71,2	78,2	82,0	84,9	90,3	91,0	**94,4**
Edad: De 55 a 64 años	**34,6**	37,9	43,8	46,5	55,4	61,4	64,8	73,9	76,1	**86,5**
Edad: De 65 a 74 años	**13,8**	16,2	19,0	21,9	26,2	31,3	34,7	43,7	49,1	**63,6**

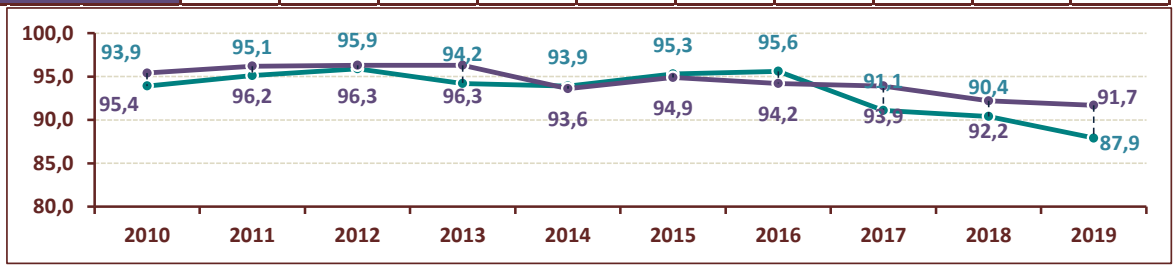


>> 2.3. PERFIL DEL MENOR DE EDAD (10 A 15 AÑOS) ANTE LA SOCIEDAD DE LA INFORMACIÓN

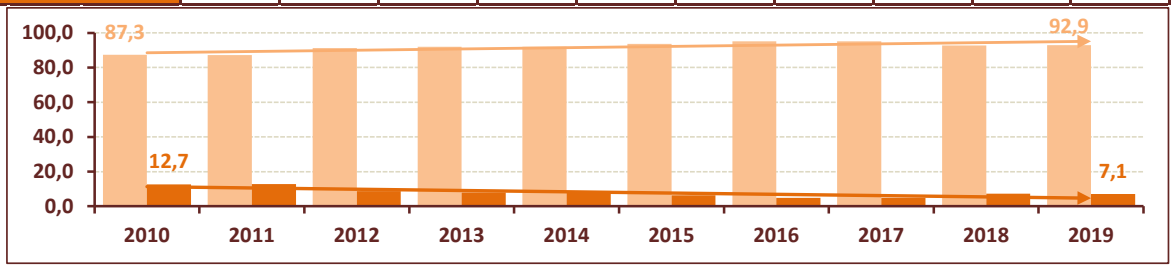
% DE MENORES QUE HAN UTILIZADO ORDENADOR ÚLTIMOS 3 MESES	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Utilizado ordenador	94,6	95,6	96,1	95,2	93,8	95,1	94,9	92,4	91,3	89,7
No utilizado ordenador	5,4	4,4	3,9	4,8	6,2	4,9	5,1	7,6	8,7	10,3



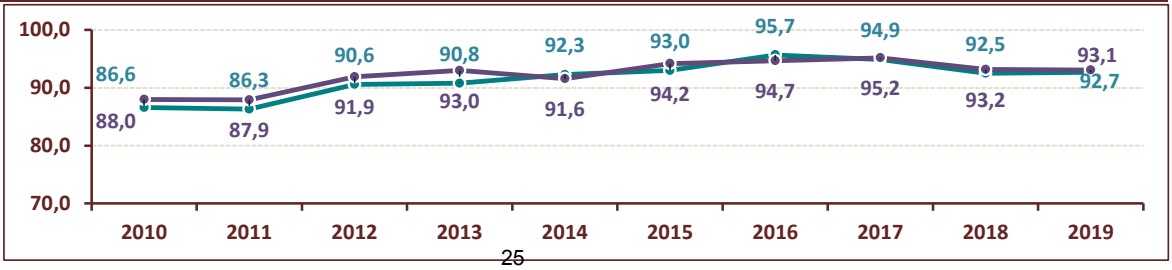
% POR SEXO DE MENORES QUE HAN UTILIZADO ORDENADOR ÚLTIMOS 3 MESES	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Hombre	93,9	95,1	95,9	94,2	93,9	95,3	95,6	91,1	90,4	87,9
Mujer	95,4	96,2	96,3	96,3	93,6	94,9	94,2	93,9	92,2	91,7



% DE MENORES QUE HAN UTILIZADO INTERNET ÚLTIMOS 3 MESES	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Utilizado internet	87,3	87,1	91,2	91,9	92,0	93,6	95,2	95,1	92,8	92,9
No utilizado internet	12,7	12,9	8,8	8,1	8,0	6,4	4,8	4,9	7,2	7,1

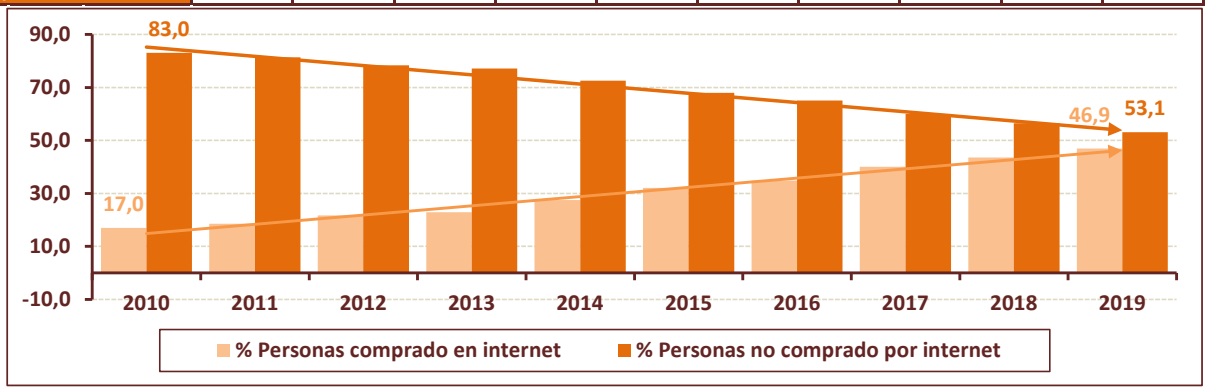


% POR SEXO DE MENORES QUE HAN UTILIZADO INTERNET ÚLTIMOS 3 MESES	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Hombre	86,6	86,3	90,6	90,8	92,3	93,0	95,7	94,9	92,5	92,7
Mujer	88,0	87,9	91,9	93,0	91,6	94,2	94,7	95,2	93,2	93,1

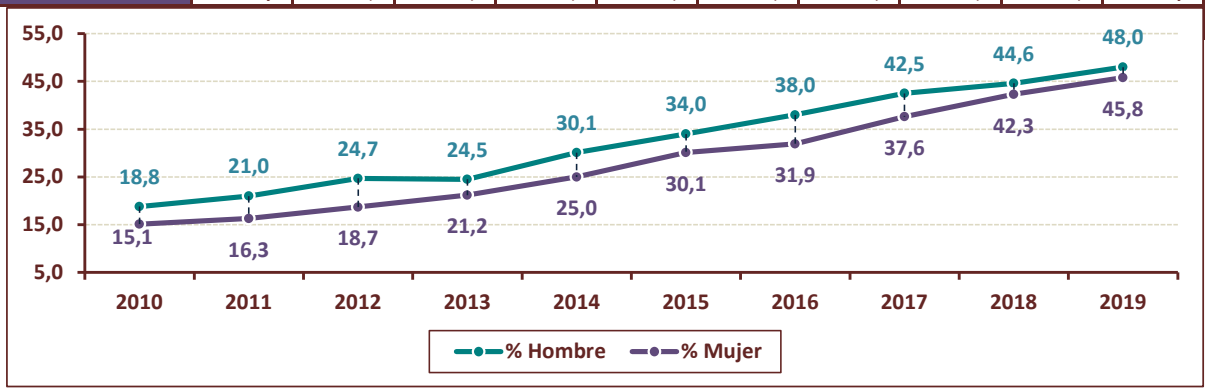


>> 2.4. PERFIL DE LAS PERSONAS QUE HAN COMPRADO ALGUNA VEZ POR INTERNET

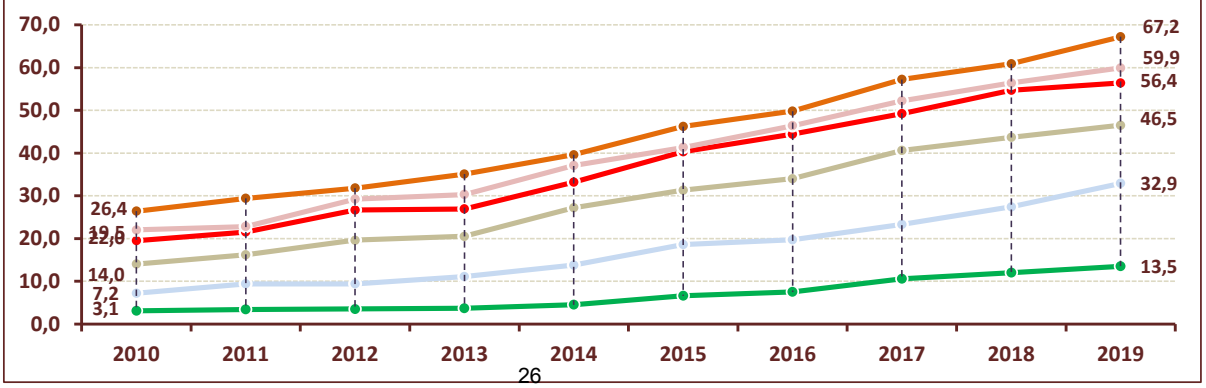
% PERSONAS QUE HAN COMPRADO ALGUNA VEZ POR INTERNET	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Comprado en internet	**17,0**	18,6	21,7	22,9	27,5	32,1	34,9	40,0	43,5	**46,9**
No comprado en internet	**83,0**	81,4	78,3	77,1	72,5	67,9	65,1	60,0	56,5	**53,1**



% POR SEXO DE PERSONAS QUE HAN COMPRADO ALGUNA VEZ POR INTERNET	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Hombre	**18,8**	21,0	24,7	24,5	30,1	34,0	38,0	42,5	44,6	**48,0**
Mujer	**15,1**	16,3	18,7	21,2	25,0	30,1	31,9	37,6	42,3	**45,8**

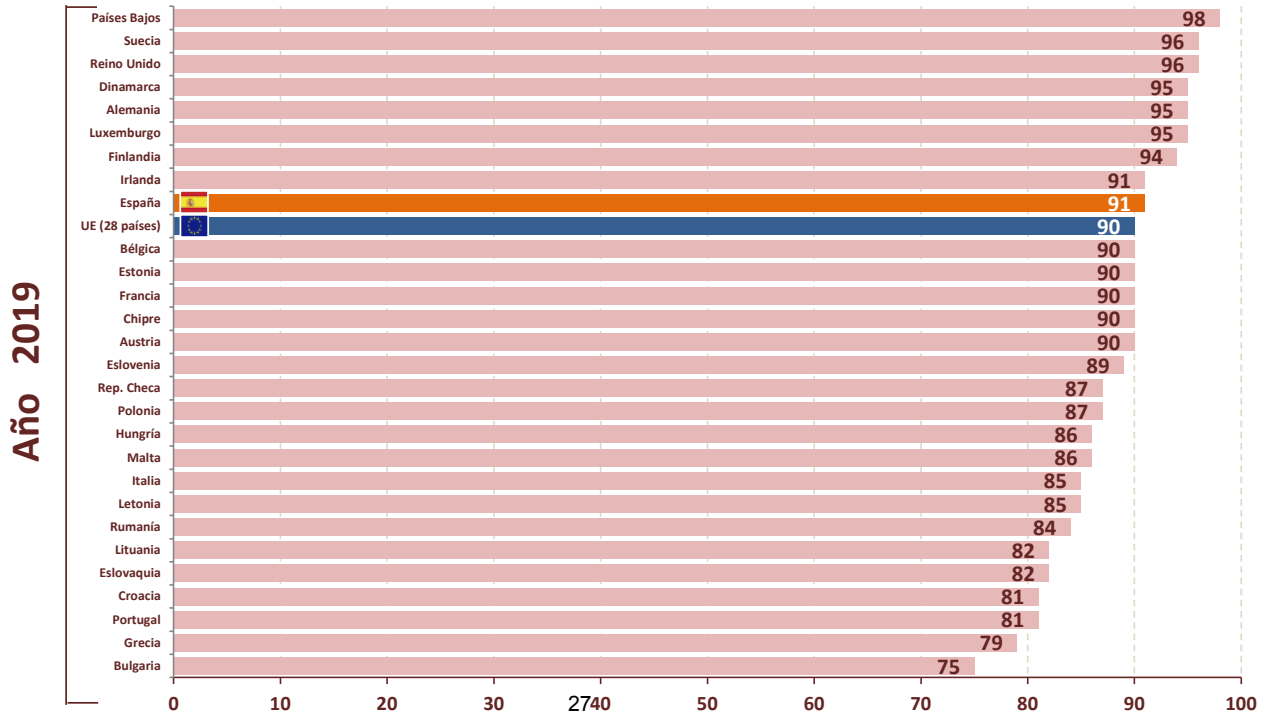


% POR GRUPO DE EDAD DE PERSONAS QUE HAN COMPRADO ALGUNA VEZ POR INTERNET	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Edad: De 16 a 24 años	**19,5**	21,5	26,7	26,9	33,2	40,3	44,4	49,2	54,7	**56,4**
Edad: De 25 a 34 años	**26,4**	29,4	31,8	35,1	39,6	46,2	49,8	57,2	60,9	**67,2**
Edad: De 35 a 44 años	**22,0**	22,8	29,2	30,3	37,1	41,3	46,4	52,2	56,4	**59,9**
Edad: De 45 a 54 años	**14,0**	16,2	19,6	20,5	27,2	31,3	34,0	40,6	43,7	**46,5**
Edad: De 55 a 64 años	**7,2**	9,4	9,4	11,1	13,8	18,6	19,7	23,3	27,4	**32,9**
Edad: De 65 a 74 años	**3,1**	3,4	3,5	3,7	4,5	6,6	7,5	10,6	12,0	**13,5**



>> 2.5. COMPARATIVA INTERNACIONAL. VIVIENDAS CON ACCESO A INTERNET

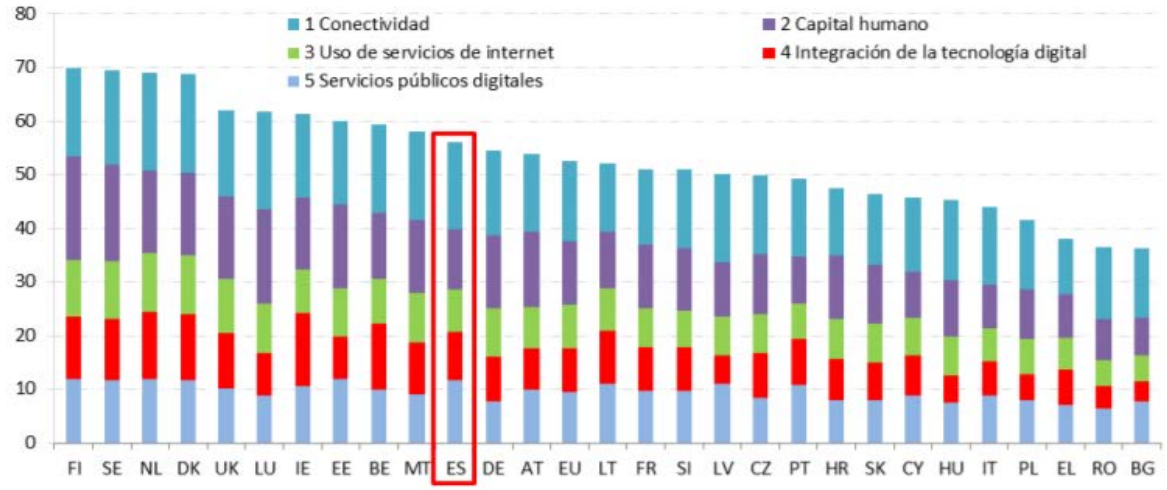
PORCENTAJE DE VIVIENDAS CON ACCESO A INTERNET	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
UE (28 países)	70	73	76	79	81	83	85	87	89	90
Bélgica	73	77	78	80	83	82	85	86	87	90
Bulgaria	33	45	51	54	57	59	64	67	72	75
Rep. Checa	61	67	73	73	78	79	82	83	86	87
Dinamarca	86	90	92	93	93	92	94	97	93	95
Alemania	82	83	85	88	89	90	92	93	94	95
Estonia	67	69	74	79	83	88	86	88	90	90
Irlanda	72	78	81	82	82	85	87	88	89	91
Grecia	46	50	54	56	66	68	69	71	76	79
España	58	63	67	70	74	79	82	83	86	91
Francia	74	76	80	82	83	83	86	86	89	90
Croacia	56	61	66	65	68	77	77	76	82	81
Italia	59	62	63	69	73	75	79	81	84	85
Chipre	54	57	62	65	69	71	74	79	82	90
Letonia	60	64	69	72	73	76	77	79	82	85
Lituania	61	60	60	65	66	68	72	75	78	82
Luxemburgo	90	91	93	94	96	97	97	97	93	95
Hungría	58	63	67	70	73	76	79	82	83	86
Malta	70	75	77	78	80	81	81	85	84	86
Países Bajos	91	94	94	95	96	96	97	98	98	98
Austria	73	75	79	81	81	82	85	89	89	90
Polonia	63	67	70	72	75	76	80	82	84	87
Portugal	54	58	61	62	65	70	74	77	79	81
Rumanía	42	47	54	58	61	68	72	76	81	84
Eslovenia	68	73	74	76	77	78	78	82	87	89
Eslovaquia	67	71	75	78	78	79	81	81	81	82
Finlandia	81	84	87	89	90	90	92	94	94	94
Suecia	88	91	92	93	90	91	94	95	92	96
Reino Unido	80	83	87	88	90	91	93	94	95	96



>> 2.6. ÍNDICE DE ECONOMÍA Y SOCIEDAD DIGITAL (DESI). COMPARATIVA ESPAÑA-UNIÓN EUROPEA

	España		UE
	puesto	puntuación	puntuación
DESI 2019	**11**	**56,1**	**52,5**
DESI 2018	11	53,2	49,8
DESI 2017	13	49,1	46,9

Índice de la Economía y la Sociedad Digitales (DESI), clasificación de 2019



	España				UE
	DESI 2017	DESI 2018	DESI 2019		DESI 2019
	valor	valor	valor	puesto	valor
1a1 Cobertura de banda ancha fija % hogares	**95 %** 2016	**96 %** 2017	**96 %** 2018	***18***	**97 %** 2018
1a2 Implantación de la banda ancha fija % hogares	**71 %** 2016	**73 %** 2017	**77 %** 2018	***10***	**77 %** 2018
1b1 Cobertura 4G % hogares (media de operadores)	**86 %** 2016	**92 %** 2017	**94 %** 2018	***21***	**94 %** 2018
1b2 Implantación de la banda ancha móvil Abonos por cada 100 personas	**86** 2016	**92** 2017	**97** 2018	***13***	**96** 2018
1b3 Preparación para la red 5G Espectro asignado como un % del total del espectro 5G armonizado	**NA**	**NA**	**30 %** 2018	***8***	**14 %** 2018
1c1 Cobertura de banda ancha de nueva generación (NGA) % hogares	**81 %** 2016	**85 %** 2017	**88 %** 2018	***13***	**83 %** 2018
1c2 Implantación de la banda ancha de nueva generación % hogares	**35 %** 2016	**43 %** 2017	**54 %** 2018	***11***	**41 %** 2018
1d1 Cobertura de la banda ancha ultrarrápida % hogares	**NA**	**84 %** 2017	**87 %** 2018	***7***	**60 %** 2018
1d2 Implantación de la banda ancha ultrarrápida % hogares	**15 %** 2016	**18 %** 2017	**30 %** 2018	***9***	**20 %** 2017
1e1 Índice de precios de la banda ancha Puntuación (0 a 100)	**70** 2016	**75** 2017	**76** 2018	***22***	**87** 2017

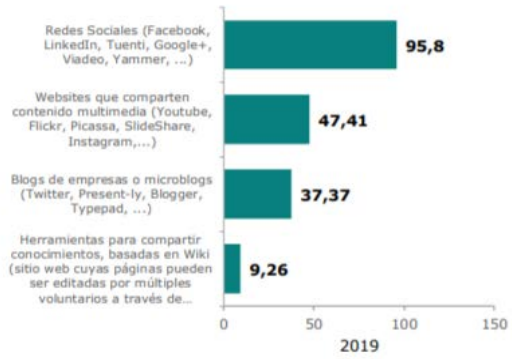
>> 2.7. INDICADORES DE LA SOCIEDAD DE LA INFORMACIÓN

(Publicación: Indicadores destacados de la sociedad de la información)

Hogares con telefonía fija y móvil (% sobre el total de hogares)

Fuente: INE

Empresas que utilizan medios sociales por tipo (% sobre las empresas que usan Medios Sociales)

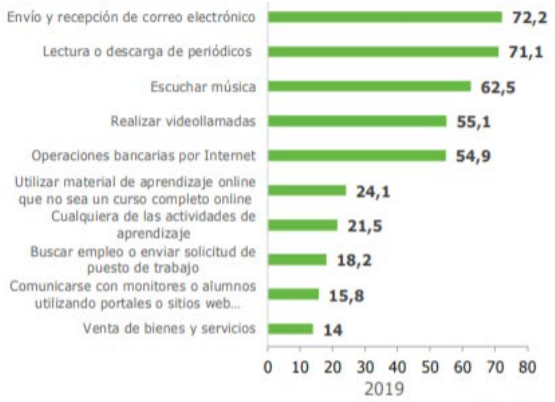


Fuente: INE

Grado de confianza en Internet (% sobre la población total)

Fuente: INE

Particulares que usan Internet con fines específicos (% sobre la población total)

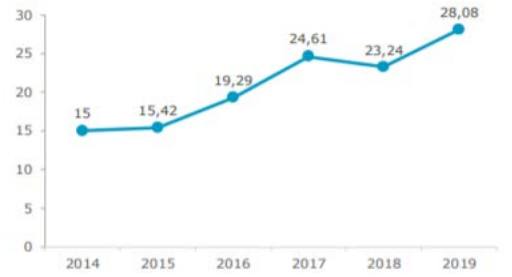


Fuente: INE

Empresas que utilizan sistemas internos de seguridad por tipo (% sobre el total de empresas que utilizan sistemas internos de seguridad)

Fuente: INE

Evolución de las empresas que compraron algún servicio de cloud computing usado a través de Internet en España (% sobre el total de empresas)



Fuente: INE

3 INFRAESTRUCTURAS CRÍTICAS Y CIBERSEGURIDAD

MINISTERIO DEL INTERIOR
SECRETARÍA DE ESTADO DE SEGURIDAD
GABINETE DE COORDINACIÓN Y ESTUDIOS
seC Sistema Estadístico de Criminalidad

3 INFRAESTRUCTURAS CRÍTICAS Y CIBERSEGURIDAD

La Oficina de Coordinación Cibernética (OCC) del Centro Nacional de Protección de Infraestructuras y Ciberseguridad, dependiente del Gabinete de Coordinación y Estudios de la Secretaría de Estado de Seguridad, es el órgano técnico de coordinación del Ministerio del Interior en materia de ciberseguridad, creado mediante Instrucción del Secretario de Estado de Seguridad 15/2014, de 19 de noviembre. Sus funciones están reguladas por el Real Decreto 952/2018, de 27 de julio, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior.

La OCC ejerce como canal específico de comunicación entre los Equipos de Respuesta a Incidentes nacionales de referencia (CSIRT) y la Secretaría de Estado de Seguridad, desempeñando la coordinación técnica en materia de ciberseguridad entre dicha Secretaría de Estado y sus organismos dependientes. Además, es el punto de contacto nacional de coordinación operativa para el intercambio de información con la Comisión Europea y los Estados miembros, en el marco de lo establecido por la Directiva 2013/40/UE, de 12 de agosto, relativa a los ataques contra los sistemas de información.

El INCIBE-CERT es el CSIRT nacional de referencia competente en la prevención, mitigación y respuesta ante incidentes cibernéticos en el ámbito de las empresas, los ciudadanos y los operadores de infraestructuras críticas de titularidad privada.

Operado técnicamente por el instituto Nacional de Ciberseguridad de España (INCIBE) y el CNPIC para el ámbito competencial de Protección de Infraestructuras Críticas (PIC), el INCIBE-CERT se constituyó en 2012 a través de un Acuerdo Marco de Colaboración en materia de Ciberseguridad entre la *Secretaría de Estado de Seguridad* (SES) y la *Secretaría de Estado de Digitalización e Inteligencia Artificial.*

Los operadores de infraestructuras críticas de titularidad privada, designados en virtud de la aplicación de la *Ley 8/2011 de 28 de abril* por la que se establecen medidas para la protección de las infraestructuras críticas, tienen en el INCIBE-CERT su punto de referencia para la notificación y respuesta ante incidentes de ciberseguridad acaecidos en las infraestructuras de información y comunicación que puedan tener afectación a la prestación de servicios esenciales.

>> 3.1 INCIDENTES GESTIONADOS POR EL INCIBE-CERT (ENTIDADES PRIVADAS)

El INCIBE-CERT gestionó un total de 107.397 incidentes de ciberseguridad en España durante el año 2019.

Analizando el número de incidentes por la tipología asignada, puede observarse que, en los datos aportados, los incidentes clasificados como *Fraude* se han convertido en el año 2019 en el tipo más frecuente de incidente registrado con un porcentaje del 29,74%, seguido de *Sistema Vulnerable* con un 29,25% respecto del total de incidentes registrados. En la serie puede observarse que se ha introducido un cambio de taxonomía o clasificación para conseguir a adaptarse a la Guía Nacional de Notificación y Gestión de Ciberincidentes, lo que conlleva que categorías como *SPAM* tengan asignado un valor nulo al haber desaparecido, y que aparezcan nuevas categorías como son *Contenido Abusivo, Recolección de información y Sistema vulnerable.*

>> 3.2. INCIDENTES GESTIONADOS DE OPERADORES CRÍTICOS DEL SECTOR PRIVADO

A lo largo del año 2019 se ha comenzado a prestar servicio a CUATRO (4) Operadores Críticos nuevos, si bien el número de incidentes de ciberseguridad se ha incrementado en un 13,29% con respecto al año anterior, gestionando durante 2019 un total de OCHOCIENTOS DIECIOCHO (818) incidentes. Este valor creciente respecto al año anterior puede explicarse por el hecho de que operadores de titularidad pública de acuerdo a la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, han comenzado a reportar los incidentes que registran en sus redes y sistemas de información a su CSIRT de referencia.

El 62,84% de los incidentes relacionados con el ámbito competencial de Protección de Infraestructuras Críticas (PIC), estuvo relacionado con *Sistemas Vulnerables*, los cuales fueron detectados en su gran mayoría por los servicios proactivos que presta el INCIBE-CERT. Por otro lado, el 20,29% de los incidentes detectados en Operadores Críticos estuvo relacionado con *Malware*.

>> 3.3. INCIDENTES GESTIONADOS POR SECTOR ESTRATÉGICO

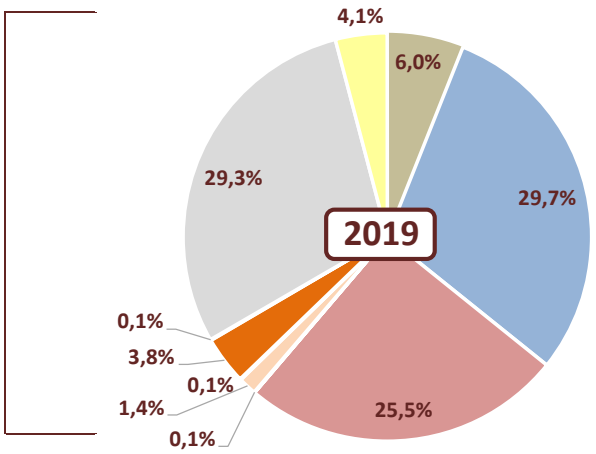
Los sectores PIC donde se detectaron mayor número de incidentes fueron el Sector Tributario y Financiero (32,52%), seguido del Sector Transporte (24,08%), y el Sector Energía (18,46%).

3 INFRAESTRUCTURAS CRÍTICAS Y CIBERSEGURIDAD

>> 3.1. INCIDENTES GESTIONADOS POR EL INCIBE-CERT

Tipo de incidente	INCIDENTES GESTIONADOS				
	2015	2016	2017	2018	2019
Intrusión	16.054	14.373	19.275	8.541	6.479
Fraude	13.410	11.843	11.959	55.932	31.938
Malware	15.177	76.811	81.090	27.016	27.358
SPAM	1.275	10.279	7.957	0	0
Disponibilidad	794	495	514	100	58
Intento de intrusión	335	381	1.435	396	1.518
Robos de información	26	37	47	63	77
Contenido Abusivo				9.353	4.064
Recolección de información				5.605	84
Sistema Vulnerable				3.731	31.414
Otros	2.905	1.038	787	782	4.407

Porcentaje del total de incidentes gestionados

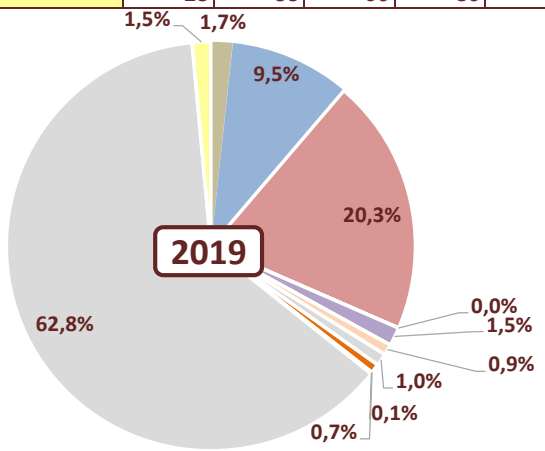


*Véase metadatos explicativos

>> 3.2. INCIDENTES GESTIONADOS EN RELACIÓN CON LAS INFRAESTRUCTURAS CRÍTICAS

Tipo de incidente	INCIDENTES GESTIONADOS				
	2015	2016	2017	2018	2019
Intrusión	15	39	97	26	14
Fraude	8	13	66	41	78
Malware	75	311	387	200	166
SPAM	0	8	21	0	0
Disponibilidad	10	28	55	54	12
Intento de intrusión	7	24	159	9	7
Robos de información	2	1	1	7	8
Contenido Abusivo				11	6
Recolección de información				111	1
Sistema Vulnerable				224	514
Otros	13	55	99	39	12

Porcentaje del total de incidentes gestionados

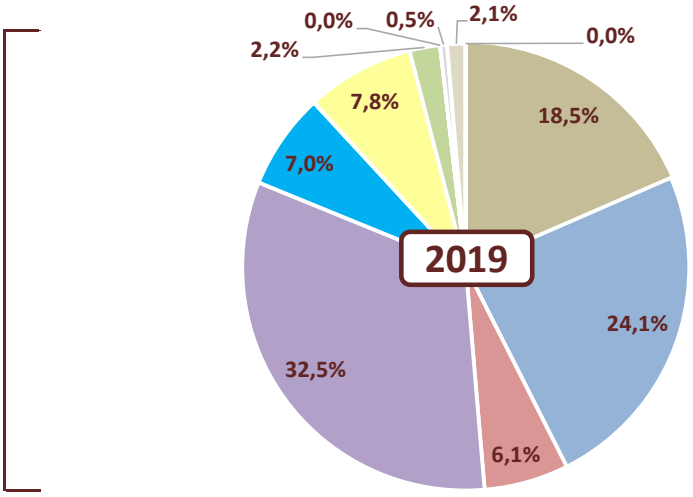


*Véase metadatos explicativos

>> 3.3. INCIDENTES GESTIONADOS POR SECTOR ESTRATÉGICO

Sector estratégico	INCIDENTES GESTIONADOS				
	2015	2016	2017	2018	2019
Energía	46	126	213	149	151
Transporte	24	90	152	192	197
Tecnologías Informac. y Comunicac. (TIC)	17	17	40	46	50
Sistema tributario y financiero	17	152	250	214	266
Alimentación	12	47	42	40	57
Agua	5	40	134	57	64
Industria nuclear	5	4	12	5	18
Administración	1	2	10	1	0
Espacio	0	0	1	3	4
Industria química	0	0	0	15	11
Instalaciones de Investigación	0	0	0	0	0
Salud	0	0	1	0	0
Todos los sectores afectados	3	1	0	0	0

Porcentaje del total de incidentes gestionados



4 DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD

MINISTERIO DEL INTERIOR
SECRETARÍA DE ESTADO DE SEGURIDAD
GABINETE DE COORDINACIÓN Y ESTUDIOS
seC Sistema Estadístico de Criminalidad

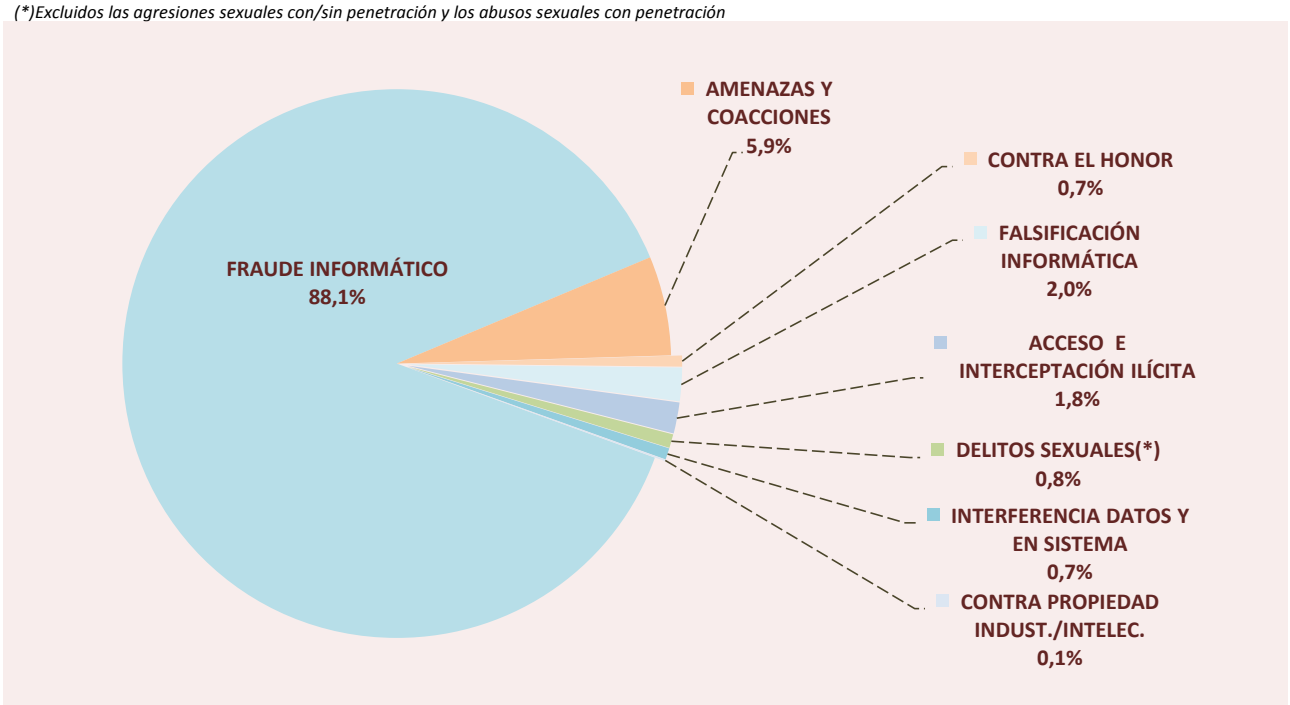
4 DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD

(Fuente de datos: Sistema Estadístico de Criminalidad)

>> 4.1. EVOLUCIÓN DE HECHOS CONOCIDOS POR CATEGORÍAS DELICTIVAS

HECHOS CONOCIDOS	2016	2017	2018	2019
ACCESO E INTERCEPTACIÓN ILÍCITA	3.243	3.150	3.384	4.004
AMENAZAS Y COACCIONES	12.036	11.812	12.800	12.782
CONTRA EL HONOR	1.546	1.561	1.448	1.422
CONTRA PROPIEDAD INDUST./INTELEC.	129	121	232	197
DELITOS SEXUALES(*)	1.231	1.392	1.581	1.774
FALSIFICACIÓN INFORMÁTICA	3.017	3.280	3.436	4.275
FRAUDE INFORMÁTICO	70.178	94.792	136.656	192.375
INTERFERENCIA DATOS Y EN SISTEMA	1.336	1.291	1.192	1.473
Total HECHOS CONOCIDOS	**92.716**	**117.399**	**160.729**	**218.302**

(*)Excluidos las agresiones sexuales con/sin penetración y los abusos sexuales con penetración



>> 4.2.EVOLUCIÓN GLOBAL DE HECHOS CONOCIDOS, ESCLARECIDOS Y DETENCIONES/INVESTIGADOS

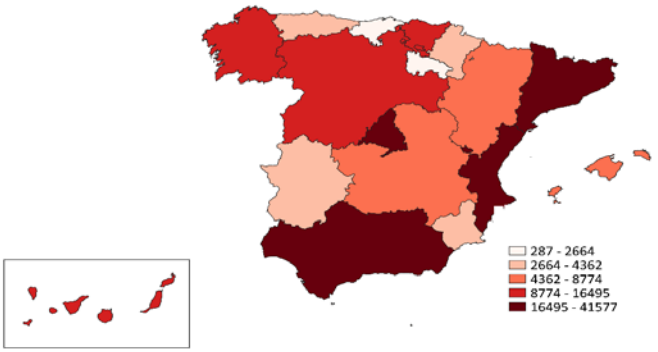
>> 4.3. REPRESENTACIÓN TERRITORIAL DE HECHOS DENUNCIADOS DE CIBERCRIMINALIDAD. AÑO 2019

Hechos denunciados de CIBERCRIMINALIDAD - 2019

Hechos conocidos:	218.302
Esclarecimiento (*):	30.841
Detenciones/invest:	8.914

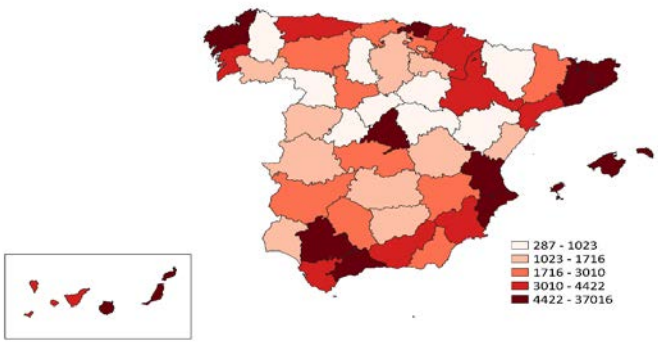
15,1%

CCAA	Hechos
CATALUÑA	41.577
MADRID (COMUNIDAD DE)	37.016
ANDALUCÍA	28.655
COMUNITAT VALENCIANA	18.983
PAÍS VASCO	14.837
GALICIA	11.631
CASTILLA Y LEÓN	10.964
CANARIAS	8.841
BALEARS (ILLES)	8.508
CASTILLA - LA MANCHA	7.687
EN EL EXTRANJERO	6.105
ARAGÓN	5.163
ASTURIAS (PRINCIPADO DE)	4.162
MURCIA (REGIÓN DE)	4.031
NAVARRA (COMUNIDAD FORAL DE)	3.211
EXTREMADURA	3.049
CANTABRIA	2.086
RIOJA (LA)	1.120
CIUDAD AUTÓNOMA DE CEUTA	389
CIUDAD AUTÓNOMA DE MELILLA	287



(*) 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

Hechos denunciados de CIBERCRIMINALIDAD - 2019



Provincias más afectadas:	Hechos
Madrid	37.016
Barcelona	30.595
Valencia/València	11.072
Balears (Illes)	8.508
Bizkaia	8.171
Sevilla	7.134
Málaga	6.550
Alicante/Alacant	6.261
EN EL EXTRANJERO	6.105
Coruña (A)	5.617
Palmas (Las)	5.125
Girona	4.442
Cádiz	4.343
Asturias	4.162
Zaragoza	4.099
Gipuzkoa	4.047
Murcia	4.031
Tarragona	3.899
Pontevedra	3.869
Santa Cruz de Tenerife	3.716

4 DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD

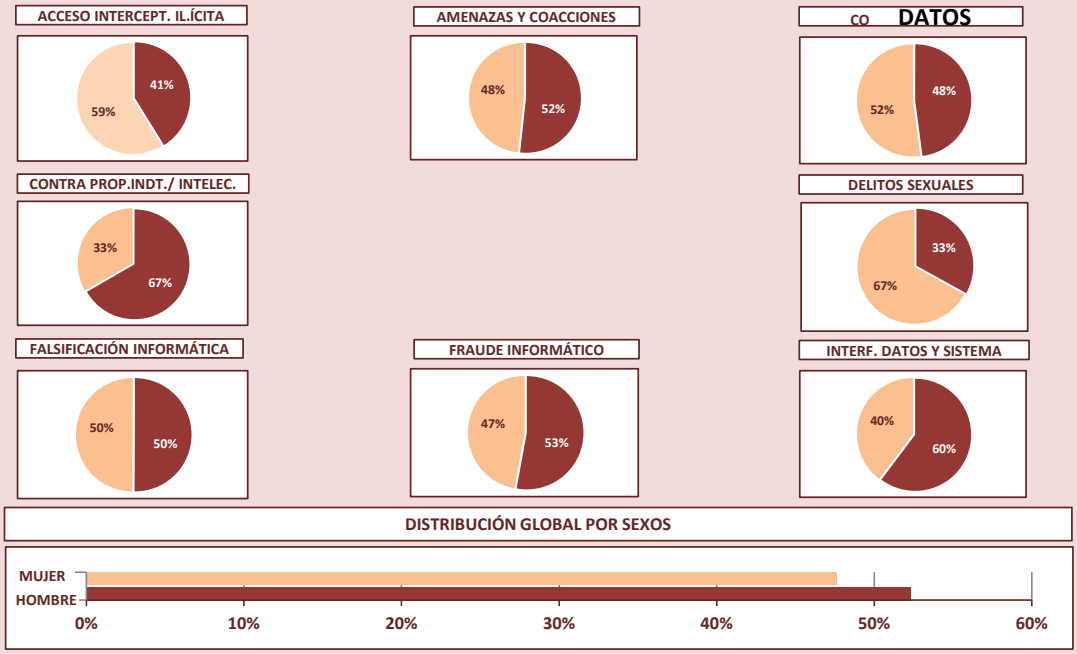
(Fuente de datos: Sistema Estadístico de Criminalidad: Datos de los cuerpos policiales, excepto Ertzaintza)

>> 4.4. VICTIMIZACIONES REGISTRADAS SEGÚN GRUPO PENAL Y SEXO. AÑO 2019

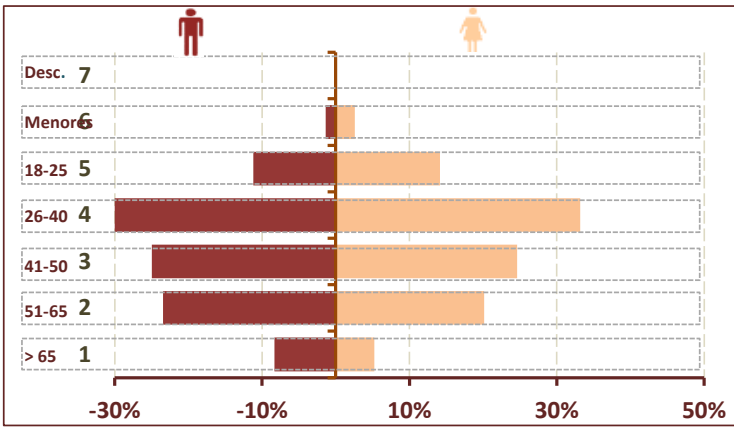
VICTIMIZACIONES	Hombre	Mujer	Desconocido	Total
ACCESO E INTERCEPTACIÓN ILÍCITA	1.455	2.078	3	3.536
AMENAZAS Y COACCIONES	6.767	6.317	32	13.116
CONTRA EL HONOR	728	791	2	1.521
CONTRA LA PROPIEDAD INDUSTRIAL/INTELECTUAL	38	19	1	58
DELITOS SEXUALES (*)	409	829	5	1.243
FALSIFICACIÓN INFORMÁTICA	1.457	1.452	4	2.913
FRAUDE INFORMÁTICO	75.398	67.185	42	142.625
INTERFERENCIA EN LOS DATOS Y EN EL SISTEMA	687	453	0	1.140
Total VICTIMIZACIONES	**86.939**	**79.124**	**89**	**166.152**

(*)Excluidos las agresiones sexuales con/sin penetración y los abusos sexuales con penetración

DISTRIBUCIÓN PORCENTUAL DE LAS VÍCTIMAS POR GRUPO PENAL SEGÚN SEXO



>> 4.5. VICTIMIZACIONES SEGÚN GRUPO DE EDAD Y SEXO. AÑO 2019



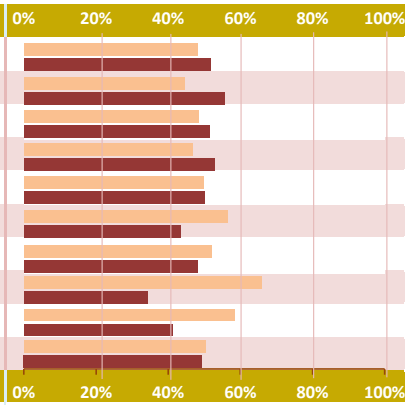
Grupo de edad	Hombre	Mujer	Descon.
Edad descon.	83	69	20
Menores de edad	1.185	2.057	1
De 18 a 25 años	9.737	11.207	2
De 26 a 40 años	26.609	26.248	14
De 41 a 50 años	21.710	19.472	24
De 51 a 65 años	20.364	15.928	18
Mayores 65 años	7.251	4.143	10
TOTAL	**86.939**	**79.124**	**89**

4 DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil de la VÍCTIMA

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

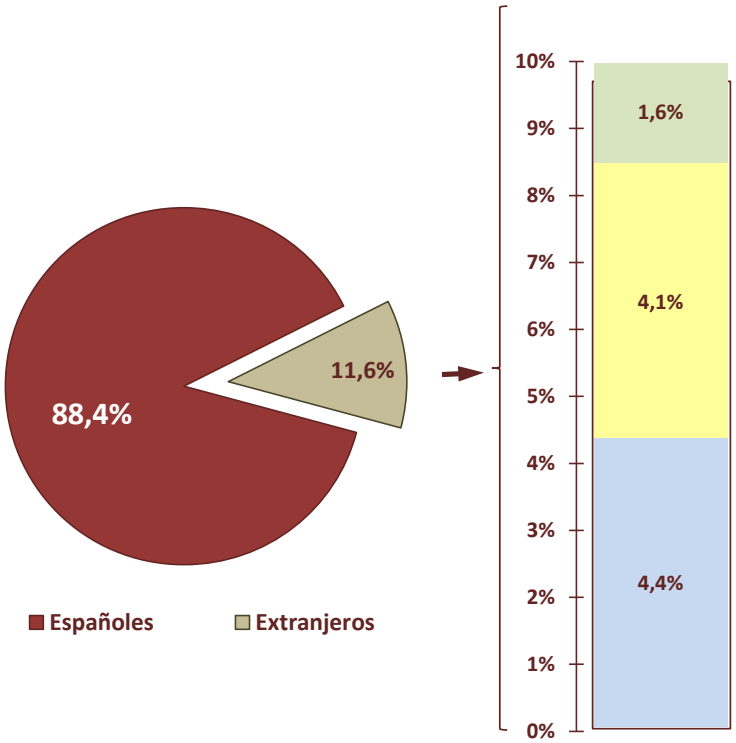
>> 4.6. VICTIMIZACIONES POR TIPOLOGÍA PENAL Y SEXO. AÑO 2019

TIPO DE HECHO	Hombres	Mujeres	Desconoc.	TOTAL
ESTAFAS CON TARJETAS DE CRÉDITO, DÉBITO Y C	36.831	34.262	14	71.107
OTRAS ESTAFAS	24.076	19.257	15	43.348
ESTAFA BANCARIA	14.491	13.666	13	28.170
AMENAZAS	5.985	5.298	30	11.313
USURPACIÓN DE ESTADO CIVIL	1.455	1.452	4	2.911
COACCIONES	781	1.017	2	1.800
ACCESO ILEGAL INFORMÁTICO	848	918	1	1.767
DESCUBRIMIENTO/REVELACIÓN DE SECRETO	602	1.159	2	1.763
INJURIAS	463	656	2	1.121
RESTO	1.407	1.439	6	2.852
Total VICTIMIZACIONES	**86.939**	**79.124**	**89**	**166.152**



>> 4.7. NACIONALIDAD DE LA VÍCTIMA. AÑO 2019

NACIONALIDAD	Víctimas	%
1.- ESPAÑOLES	**146.919**	**88,4%**
2.- EXTRANJEROS	**19.233**	**11,6%**
2.1.- UNIÓN EUROPEA	**7.229**	**4,4%**
Rumanía	1.875	1,1%
Italia	1.537	0,9%
Francia	695	0,4%
Reino Unido	582	0,4%
Alemania	483	0,3%
Resto	2.057	1,2%
2.2.- AMÉRICA	**6.889**	**4,1%**
Venezuela	1.011	0,6%
Colombia	947	0,6%
Ecuador	802	0,5%
Resto	4.129	2,5%
2.3.- ÁFRICA	**2.636**	**1,6%**
Marruecos	1579	1,0%
Senegal	240	0,1%
Resto	817	0,5%
2.4.- ÁSIA	**1.198**	**0,7%**
China Popular	449	0,3%
Paquistán	226	0,1%
Resto	523	0,3%
2.5.- RESTO PAÍSES	**1.281**	**0,8%**
Ucrania	330	0,2%
País Desconocido	273	0,2%
Otros	678	0,4%
TOTAL	**166.152**	**100%**



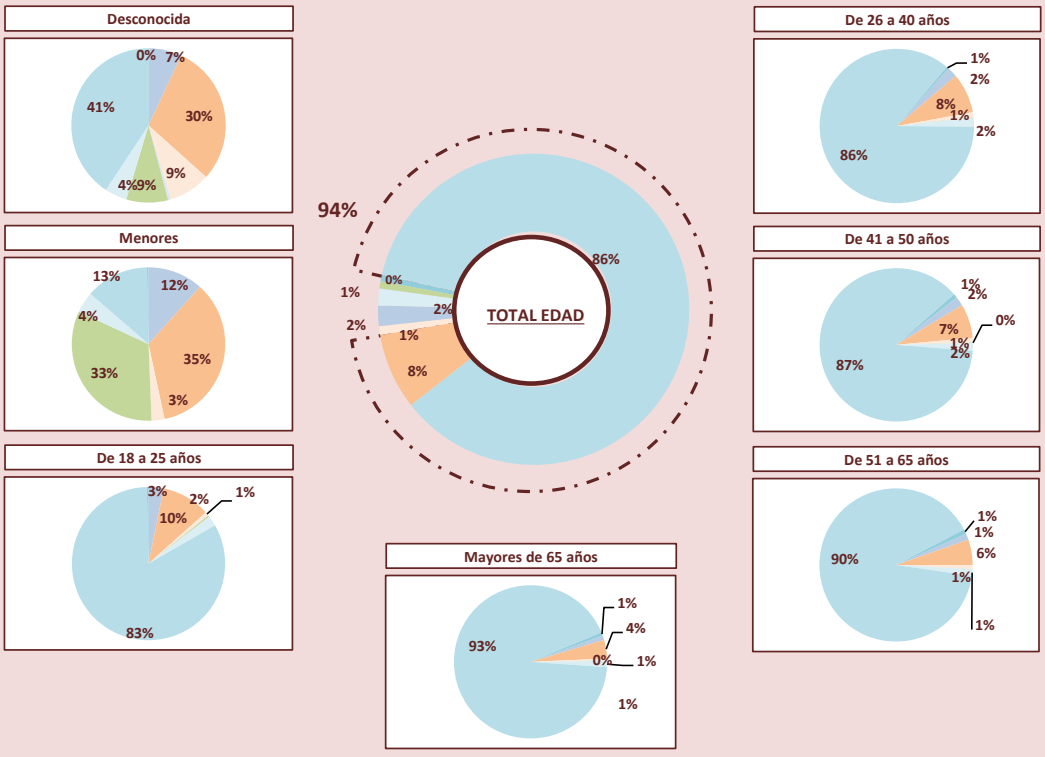
4 DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil de la VÍCTIMA

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

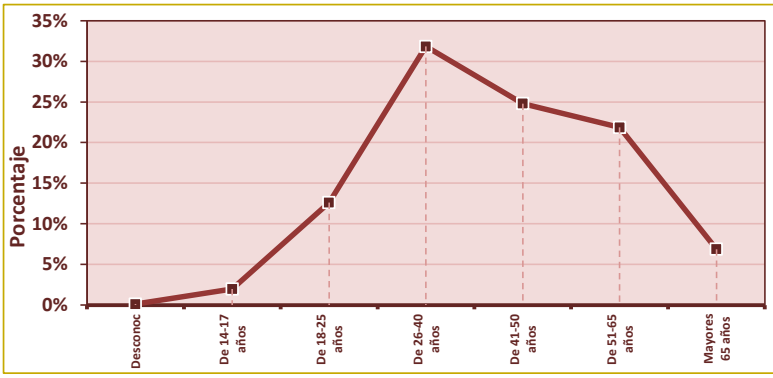
>> 4.8. VICTIMIZACIONES REGISTRADAS SEGÚN GRUPO PENAL Y EDAD. AÑO 2019

GRUPO PENAL	Rango de edad de la víctima						
	Descon.	Menores	18-25	26-40	41-50	51-65	> 65
ACCESO E INTERCEPTACIÓN ILÍCITA	12	378	663	1.108	790	478	107
AMENAZAS Y COACCIONES	51	1.135	2.140	4.425	2.954	1.961	450
CONTRA EL HONOR	15	88	172	509	402	293	42
CONTRA PROPIEDAD INDUST./INTELEC.	1	0	1	22	14	15	5
DELITOS SEXUALES(*)	15	1.056	66	56	32	14	4
FALSIFICACIÓN INFORMÁTICA	8	143	453	1.011	655	489	154
FRAUDE INFORMÁTICO	70	433	17.380	45.478	36.003	32.700	10.561
INTERFERENCIA EN DATOS Y EN SISTEMA	0	10	71	262	356	360	81
Total VICTIMIZACIONES	**172**	**3.243**	**20.946**	**52.871**	**41.206**	**36.310**	**11.404**

(*)Excluidos las agresiones sexuales con/sin penetración y los abusos sexuales con penetración



>> 4.9. EDAD DE LA VÍCTIMA. AÑO 2019



Grupo de edad	Víctimas
Edad desconocida	172
Menores de edad	3.243
De 18 a 25 años	20.946
De 26 a 40 años	52.871
De 41 a 50 años	41.206
De 51 a 65 años	36.310
Mayores 65 años	11.404
TOTAL	**166.152**

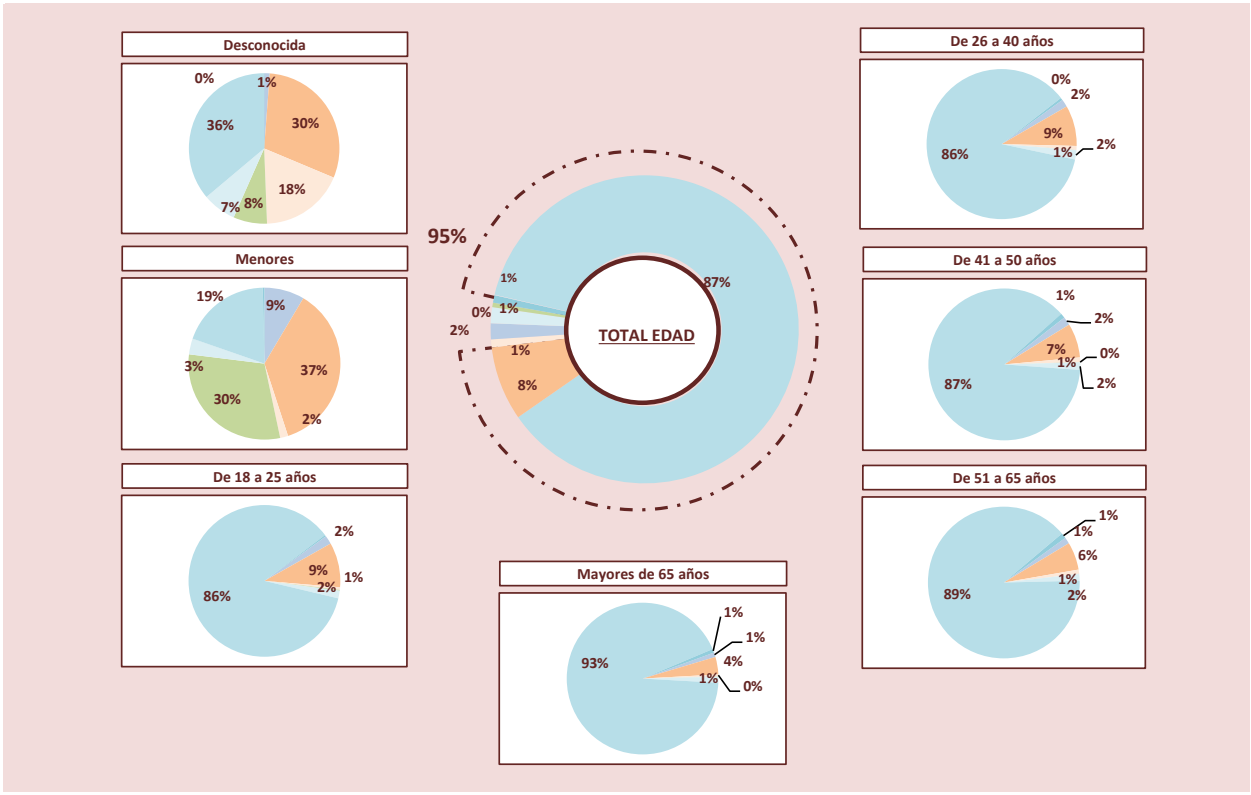
4 DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil de la VÍCTIMA (HOMBRE)

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

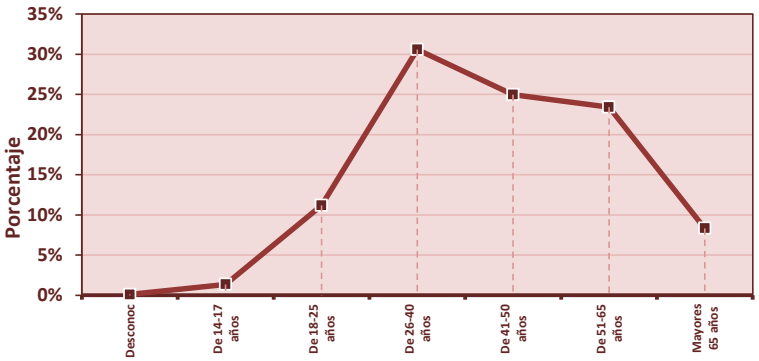
>> 4.10. VICTIMIZACIONES REGISTRADAS SEGÚN GRUPO PENAL Y EDAD. AÑO 2019

GRUPO PENAL	Rango de edad de la víctima						
	Descon.	Menores	18-25	26-40	41-50	51-65	> 65
ACCESO E INTERCEPTACIÓN ILÍCITA	1	101	178	444	387	274	70
AMENAZAS Y COACCIONES	25	432	926	2.322	1.584	1.208	270
CONTRA EL HONOR	15	20	54	225	211	175	28
CONTRA PROPIEDAD INDUST./INTELEC.	0	0	0	15	8	10	5
DELITOS SEXUALES(*)	6	359	18	9	11	2	4
FALSIFICACIÓN INFORMÁTICA	6	40	158	528	344	291	90
FRAUDE INFORMÁTICO	30	229	8.373	22.924	18.945	18.170	6.727
INTERFERENCIA EN DATOS Y EN SISTEMA	0	4	30	142	220	234	57
Total VICTIMIZACIONES	**83**	**1.185**	**9.737**	**26.609**	**21.710**	**20.364**	**7.251**

(*)Excluidos las agresiones sexuales con/sin penetración y los abusos sexuales con penetración



>> 4.11. EDAD DE LA VÍCTIMA. AÑO 2019

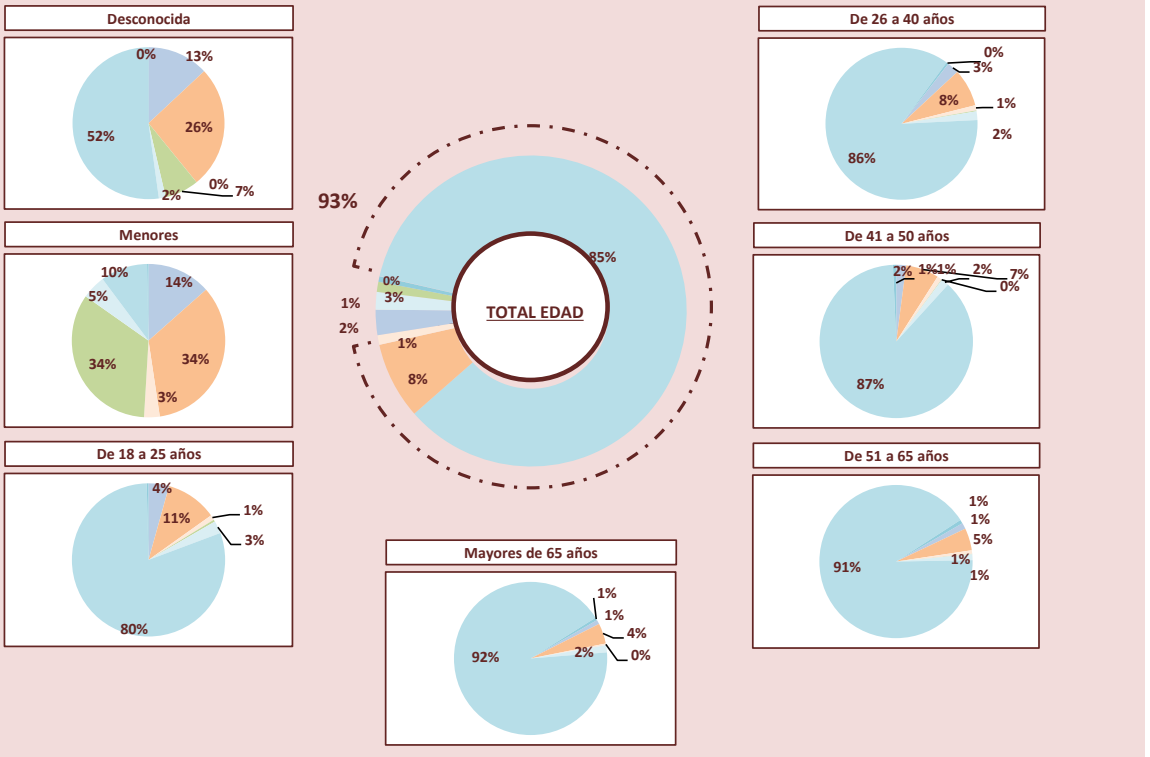


Grupo de edad	Víctimas
Edad desconocida	83
Menores de edad	1.185
De 18 a 25 años	9.737
De 26 a 40 años	26.609
De 41 a 50 años	21.710
De 51 a 65 años	20.364
Mayores 65 años	7.251
TOTAL	**86.939**

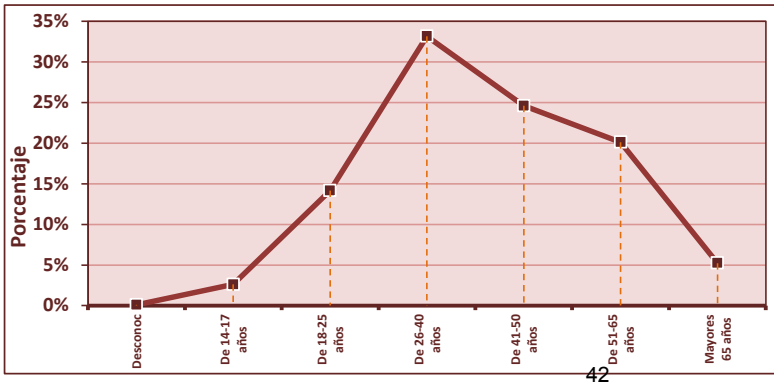
>> 4.12. VICTIMIZACIONES REGISTRADAS SEGÚN GRUPO PENAL Y EDAD. AÑO 2019

GRUPO PENAL	Rango de edad de la víctima						
	Descon.	Menores	18-25	26-40	41-50	51-65	> 65
ACCESO E INTERCEPTACIÓN ILÍCITA	9	277	485	663	403	204	37
AMENAZAS Y COACCIONES	18	703	1.214	2.099	1.358	746	179
CONTRA EL HONOR	0	68	118	284	189	118	14
CONTRA PROPIEDAD INDUST./INTELEC.	0	0	1	7	6	5	0
DELITOS SEXUALES(*)	5	696	48	47	21	12	0
FALSIFICACIÓN INFORMÁTICA	1	103	295	483	311	196	63
FRAUDE INFORMÁTICO	36	204	9.005	22.545	17.048	14.521	3.826
INTERFERENCIA EN DATOS Y EN SISTEMA	0	6	41	120	136	126	24
Total VICTIMIZACIONES	**69**	**2.057**	**11.207**	**26.248**	**19.472**	**15.928**	**4.143**

(*)Excluidos las agresiones sexuales con/sin penetración y los abusos sexuales con penetración



>> 4.13. EDAD DE LA VÍCTIMA. AÑO 2019



Grupo de edad	Víctimas
Edad desconocida	69
Menores de edad	2.057
De 18 a 25 años	11.207
De 26 a 40 años	26.248
De 41 a 50 años	19.472
De 51 a 65 años	15.928
Mayores 65 años	4.143
TOTAL	**79.124**

4 DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil del RESPONSABLE

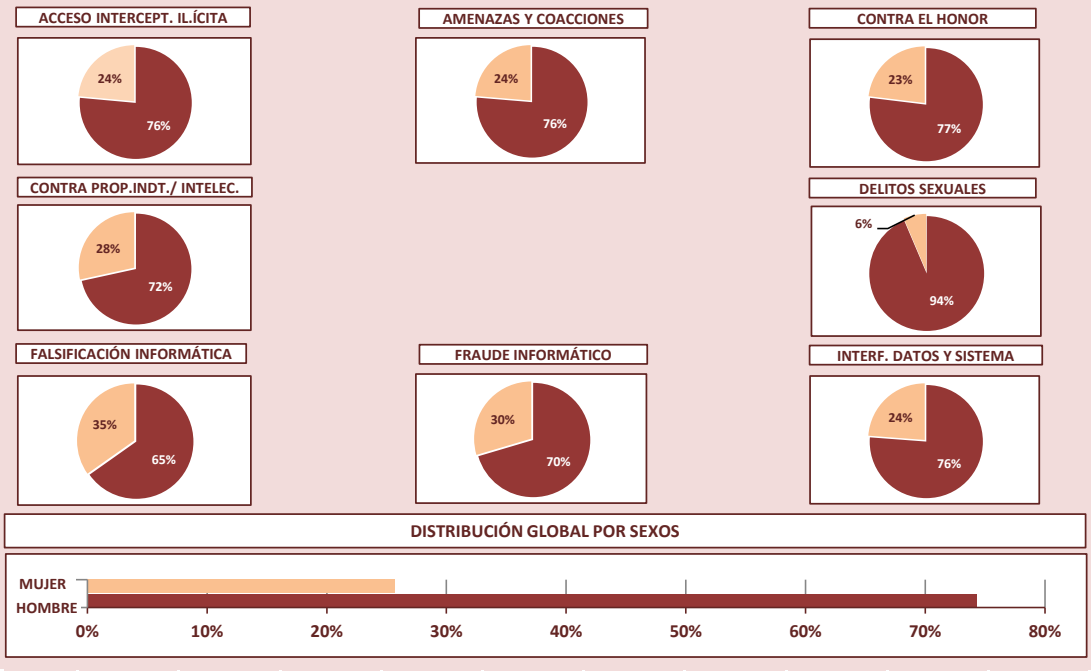
(Fuente de datos: Sistema Estadístico de Criminalidad: Datos de los cuerpos policiales)

>> 4.14. DETENCIONES/INVESTIGADOS REGISTRADOS SEGÚN GRUPO PENAL Y SEXO. AÑO 2019

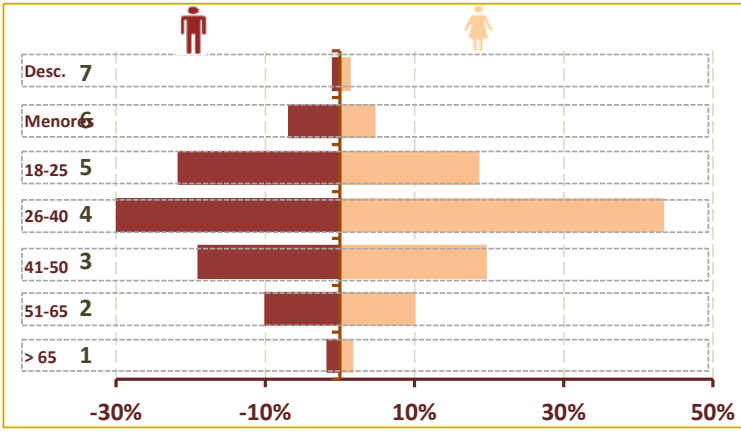
DETENCIONES/INVESTIGADOS REGISTRADOS	Hombre	Mujer	Total
ACCESO E INTERCEPTACIÓN ILÍCITA	357	110	467
AMENAZAS Y COACCIONES	1.334	414	1.748
CONTRA EL HONOR	120	36	156
CONTRA LA PROPIEDAD INDUSTRIAL/INTELECTUAL	141	56	197
DELITOS SEXUALES(*)	907	62	969
FALSIFICACIÓN INFORMÁTICA	266	142	408
FRAUDE INFORMÁTICO	3.484	1.464	4.948
INTERFERENCIA EN LOS DATOS Y EN EL SISTEMA	16	5	21
Total DETENCIONES/INVESTIGADOS REGISTRADOS	**6.625**	**2.289**	**8.914**

(*)Excluidos las agresiones sexuales con/sin penetración y los abusos sexuales con penetración

DISTRIBUCIÓN PORCENTUAL DE LAS DETENCIONES/INVESTIGADOS POR GRUPO PENAL SEGÚN SEXO



>> 4.15. DETENCIONES/INVESTIGADOS SEGÚN GRUPO DE EDAD Y SEXO. AÑO 2019



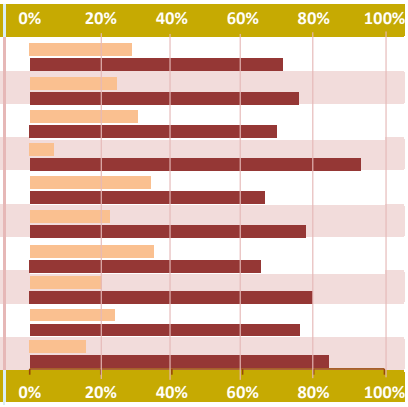
Grupo de edad	Hombre	Mujer
Edad desconocida	71	33
De 14 a 17 años	461	109
De 18 a 25 años	1.441	428
De 26 a 40 años	2.596	995
De 41 a 50 años	1.265	451
De 51 a 65 años	671	232
Mayores 65 años	120	41
TOTAL	**6.625**	**2.289**

4 DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil del RESPONSABLE

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

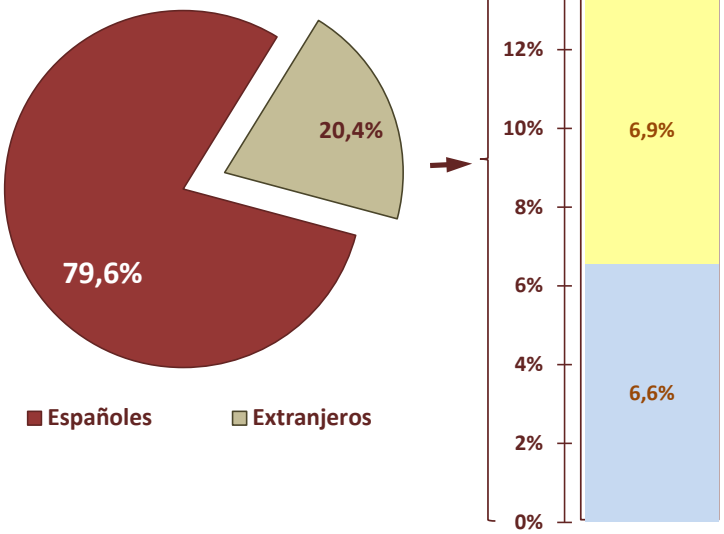
>> 4.16. DETENCIONES/INVESTIGADOS POR TIPOLOGÍA PENAL Y SEXO. AÑO 2019

TIPO DE HECHO	Hombres	Mujeres	TOTAL
OTRAS ESTAFAS	2.592	1.048	3.640
AMENAZAS	1.105	356	1.461
ESTAFAS TARJ CRÉDITO, DÉB. Y CHEQ.VIAJE	540	235	775
PORNOGRAFÍA DE MENORES	547	40	587
ESTAFA BANCARIA	352	181	533
DESCUBR./REVEL.DE SECRETOS	319	92	411
USURPACIÓN DE ESTADO CIVIL	262	140	402
COACCIONES	225	57	282
CONTRA LA PROPIEDAD INTELECTUAL	92	29	121
RESTO	591	111	702
Total VICTIMIZACIONES CIBERCRIMINALIDAD	6.625	2.289	8.914



>> 4.17. NACIONALIDAD DE LAS DETENCIONES/INVESTIGADOS. AÑO 2019

NACIONALIDAD	Detenciones	%
1.- ESPAÑOLES	7.098	79,6%
2.- EXTRANJEROS	1.816	20,4%
2.1.- UNIÓN EUROPEA	588	6,6%
Rumanía	271	3,0%
Irlanda	61	0,7%
Bulgaria	43	0,5%
Italia	35	0,4%
Francia	32	0,4%
Resto	146	1,6%
2.2.- AMÉRICA	619	6,9%
Colombia	108	1,2%
Venezuela	81	0,9%
Dominicana	78	0,9%
Resto	352	3,9%
2.3.- ÁFRICA	430	4,8%
Marruecos	271	3,0%
Nigeria	41	0,5%
Resto	118	1,3%
2.4.- ÁSIA	80	0,9%
Paquistán	29	0,3%
China Popular	23	0,3%
Resto	28	0,3%
2.5.- RESTO PAÍSES	99	1,1%
País Desconocido	44	0,5%
Ucrania	20	0,2%
Otros	35	0,4%
TOTAL	8.914	100%



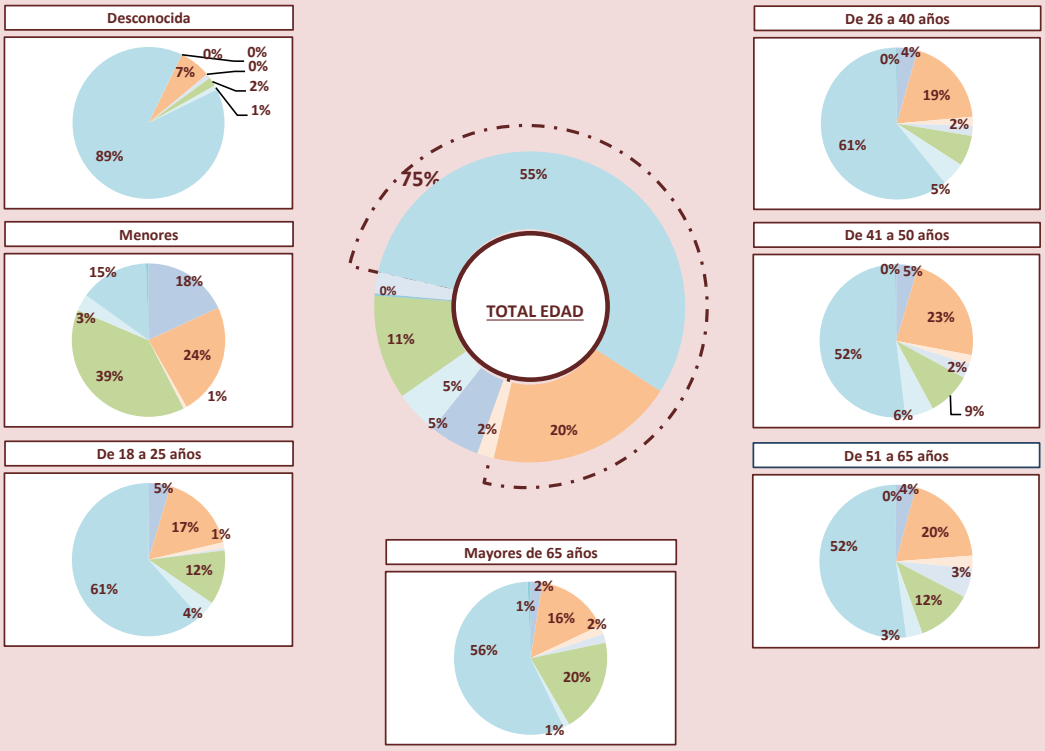
4 DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil del RESPONSABLE

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

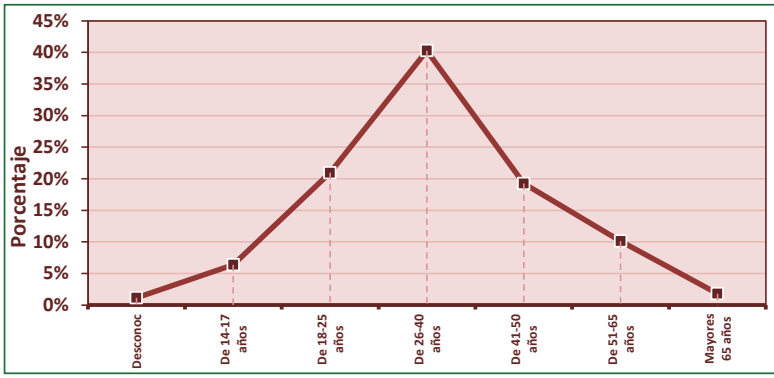
>> 4.18. DETENCIONES/INVESTIGADOS REGISTRADAS SEGUN GRUPO PENAL Y EDAD. AÑO 2019

GRUPO PENAL	Rango de edad de los detenidos/investigados						
	Descon.	14-17	18-25	26-40	41-50	51-65	> 65
ACCESO E INTERCEPTACIÓN ILÍCITA	0	103	86	158	78	38	4
AMENAZAS Y COACCIONES	7	135	313	689	402	177	25
CONTRA EL HONOR	0	4	24	68	33	24	3
CONTRA PROPIEDAD INDUST./INTELEC.	1	0	8	77	52	56	3
DELITOS SEXUALES(*)	2	222	215	234	158	106	32
FALSIFICACIÓN INFORMÁTICA	1	20	72	180	102	31	2
FRAUDE INFORMÁTICO	93	83	1149	2176	886	470	91
INTERFERENCIA EN DATOS Y EN SISTEMA	0	3	2	9	5	1	1
Total DETENCIONES/INVESTIGADOS	**104**	**570**	**1.869**	**3.591**	**1.716**	**903**	**161**

(*)Excluidos las agresiones sexuales con/sin penetración y los abusos sexuales con penetración



>> 4.19. EDAD DE LAS PERSONAS DETENIDAS/INVESTIGADAS. AÑO 2019



Grupo de edad	Det./Inv.
Edad desconocida	104
De 14 a 17 años	570
De 18 a 25 años	1.869
De 26 a 40 años	3.591
De 41 a 50 años	1.716
De 51 a 65 años	903
Mayores 65 años	161
TOTAL	**8.914**

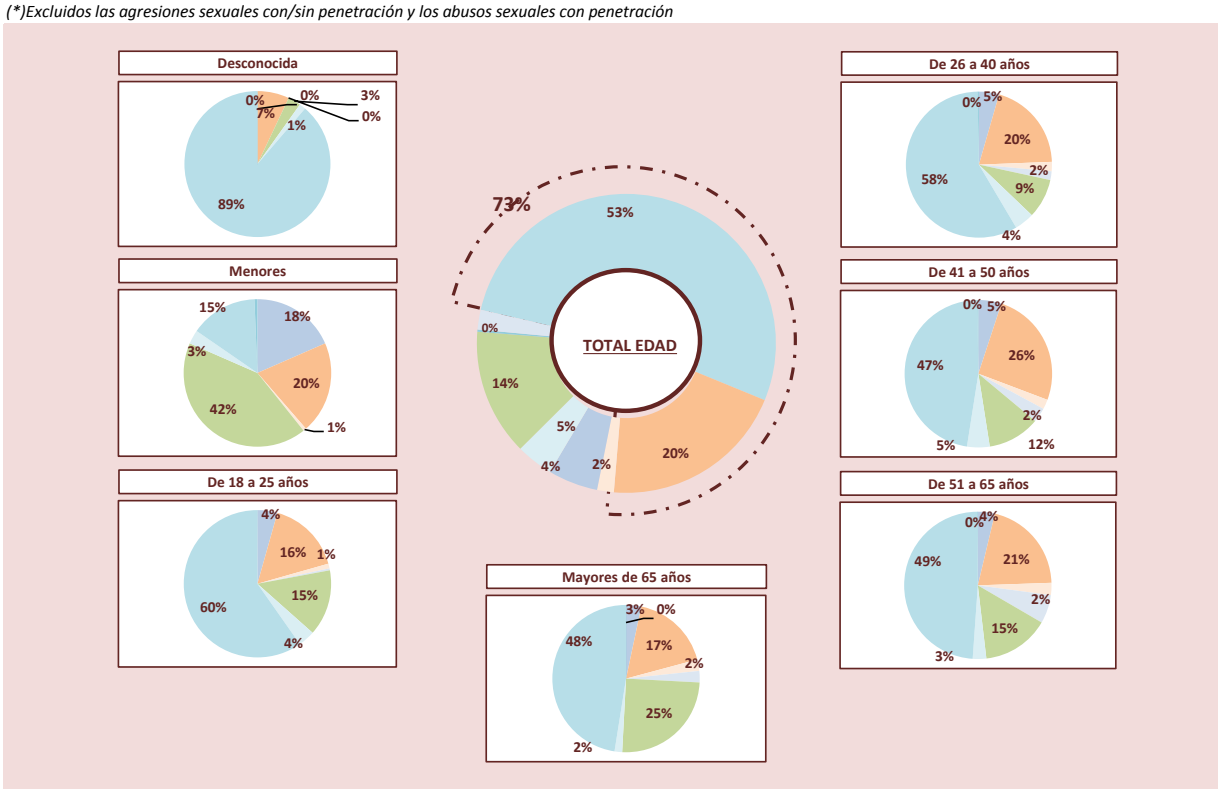
4 DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil del RESPONSABLE (HOMBRE)

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

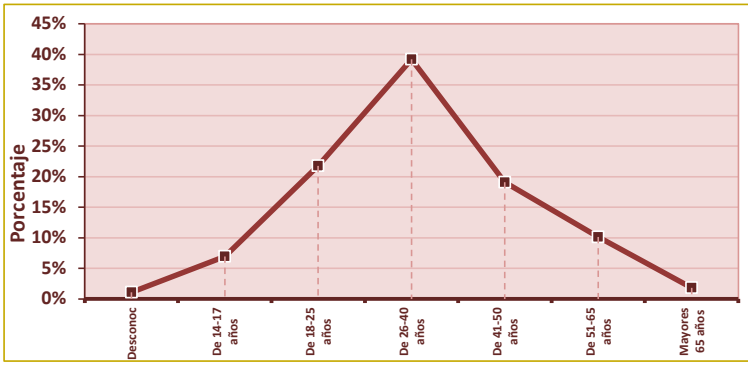
>> 4.20. DETENCIONES/INVESTIGADOS REGISTRADAS SEGÚN GRUPO PENAL Y EDAD. AÑO 2019

GRUPO PENAL	Rango de edad de los detenidos/investigados						
	Descon.	14-17	18-25	26-40	41-50	51-65	> 65
ACCESO E INTERCEPTACIÓN ILÍCITA	0	85	63	116	64	25	4
AMENAZAS Y COACCIONES	5	93	234	517	325	139	21
CONTRA EL HONOR	0	3	15	54	27	18	3
CONTRA PROPIEDAD INDUST./INTELEC.	0	0	6	50	40	42	3
DELITOS SEXUALES(*)	2	195	209	227	145	99	30
FALSIFICACIÓN INFORMÁTICA	1	14	53	113	63	20	2
FRAUDE INFORMÁTICO	63	68	860	1.511	598	327	57
INTERFERENCIA EN DATOS Y EN SISTEMA	0	3	1	8	3	1	0
Total DETENCIONES/INVESTIGADOS	**71**	**461**	**1.441**	**2.596**	**1.265**	**671**	**120**

(*)Excluidos las agresiones sexuales con/sin penetración y los abusos sexuales con penetración



>> 4.21. EDAD DE LAS PERSONAS DETENIDAS/INVESTIGADAS. AÑO 2019



Grupo de edad	Det./Inv.
Edad desconocida	71
De 14 a 17 años	461
De 18 a 25 años	1.441
De 26 a 40 años	2.596
De 41 a 50 años	1.265
De 51 a 65 años	671
Mayores 65 años	120
TOTAL	**6.625**

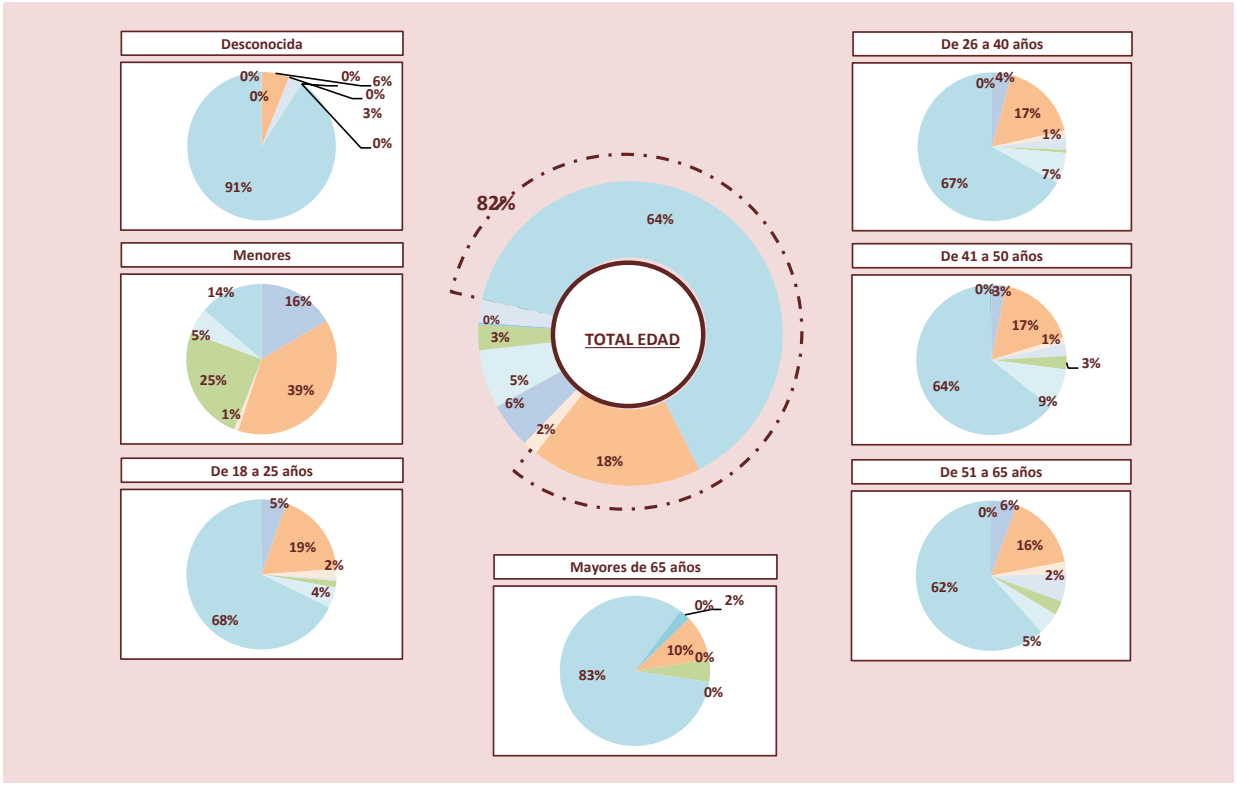
4 DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil del RESPONSABLE (MUJER)

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

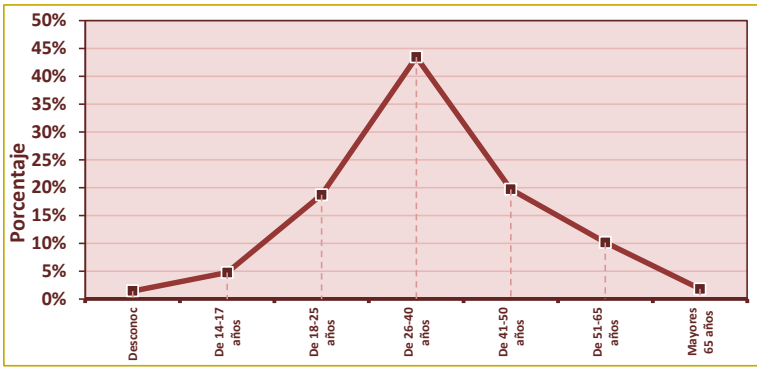
>> 4.22. DETENCIONES/INVESTIGADOS REGISTRADAS SEGÚN GRUPO PENAL Y EDAD AÑO 2019

GRUPO PENAL	Rango de edad de los detenidos/investigados						
	Descon.	14-17	18-25	26-40	41-50	51-65	> 65
ACCESO E INTERCEPTACIÓN ILÍCITA	0	18	23	42	14	13	0
AMENAZAS Y COACCIONES	2	42	79	172	77	38	4
CONTRA EL HONOR	0	1	9	14	6	6	0
CONTRA PROPIEDAD INDUST./INTELEC.	1	0	2	27	12	14	0
DELITOS SEXUALES(*)	0	27	6	7	13	7	2
FALSIFICACIÓN INFORMÁTICA	0	6	19	67	39	11	0
FRAUDE INFORMÁTICO	30	15	289	665	288	143	34
INTERFERENCIA EN DATOS Y EN SISTEMA	0	0	1	1	2	0	1
Total DETENCIONES/INVESTIGADOS	**33**	**109**	**428**	**995**	**451**	**232**	**41**

(*)Excluidos las agresiones sexuales con/sin penetración y los abusos sexuales con penetración



>> 4.23. EDAD DE LAS PERSONAS DETENIDAS/INVESTIGADAS. AÑO 2019



Grupo de edad	Det./Inv.
Edad desconocida	33
De 14 a 17 años	109
De 18 a 25 años	428
De 26 a 40 años	995
De 41 a 50 años	451
De 51 a 65 años	232
Mayores 65 años	41
TOTAL	**2.289**

5 METADATA

5 METADATA

Los datos utilizados en el presente informe han utilizado la metodología y fuentes de datos que a continuación se relacionan:

>> RADIOGRAFÍA DE LA SOCIEDAD DE LA INFORMACIÓN:

2.1. HOGARES. Fuente: INE (Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los hogares 2019).

- Porcentaje de viviendas con / sin algún tipo de ordenador
- Porcentaje de viviendas con / sin acceso a internet
- Contraste evolutivo de las viviendas 2010-2019
- Porcentaje de viviendas con ordenador por tipo hábitat
- Porcentaje de viviendas con acceso a internet por tipo hábitat

https://www.ine.es/jaxi/Tabla.htm?path=/t25/p450/base_2011/a2019/l0/&file=02001.px&L=0

2.2. PERFIL DEL CIUDADANO ANTE LA SOCIEDAD DE LA INFORMACIÓN. Fuente: INE (Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los hogares 2019)

- Porcentaje de personas que han utilizado o no internet últimos 3 meses.
- Porcentaje por sexo de personas que han utilizado internet últimos 3 meses.
- Porcentaje por grupo de edad de personas que han utilizado internet últimos 3 meses.

https://www.ine.es/jaxi/Tabla.htm?path=/t25/p450/base_2011/a2019/l0/&file=02002.px&L=0

2.3. PERFIL DEL MENOR DE EDAD (10 A 15 AÑOS DE EDAD) ANTE LA SOCIEDAD DE LA INFORMACIÓN. Fuente: INE (Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los hogares 2019)

- Porcentaje de menores que han utilizado ordenador últimos 3 meses.
- Porcentaje por sexo de menores que han utilizado ordenador últimos 3 meses.
- Porcentaje de menores que han utilizado internet últimos 3 meses.
- Porcentaje por sexo de menores que han utilizado internet últimos 3 meses.

https://www.ine.es/jaxi/Tabla.htm?path=/t25/p450/base_2011/a2019/l0/&file=02004.px&L=0

2.4. PERFIL DE LAS PERSONAS QUE HAN COMPRADO ALGUNA VEZ POR INTERNET. Fuente: INE (Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los hogares 2019)

- Porcentaje personas que han comprado alguna vez por internet
- Porcentaje por sexo de personas que han comprado alguna vez por internet
- Porcentaje por grupo de edad de personas que han comprado alguna vez por internet

https://www.ine.es/jaxi/Tabla.htm?path=/t25/p450/base_2011/a2019/l0/&file=02002.px&L=0

2.5. COMPARATIVA INTERNACIONAL. VIVIENDAS CON ACCESO A INTERNET (Fuente datos: EUROSTAT)

- Porcentaje de viviendas con acceso a internet. ICT usage in households and by individuals. Connection to the internet and computer use. Households - level of internet Access (EUROSTAT)

http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_ci_in_h&lang=en

2.6. ÍNDICE DE ECONOMÍA Y SOCIEDAD DIGITAL (DESI). COMPARATIVA ESPAÑA-UNIÓN EUROPEA

- Digital Economy and Society Index 2019. Spain (Comisión Europea)

https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60004

2.7. INDICADORES DE LA SOCIEDAD DE LA INFORMACIÓN

- Indicadores destacados de la Sociedad de la Información (noviembre 2019-ONTSI)

https://www.ontsi.red.es/sites/ontsi/files/2019-11/IndicadoresDestacadosNoviembre2019.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: Guardia Civil, Cuerpo Nacional de Policía, 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 y victimizaciones. Como consecuencia de la incorporación al presente informe de los datos de la Ertzaintza y Mossos d' Esquadra, las series históricas publicadas hasta la fecha se han visto alteradas.

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 Budapest. Se adjunta cuadro explicativo al final de la metadata.

No obstante, además de las conductas que introduce el Convenio de Budapest, nuestra realidad criminalidad denota que existen otras categorías distintas que conviene reseñar. Es pues, que cuando los medios empleados en su comisión sean las tecnologías de la información y la comunicación (TIC), se pueden encuadrar dentro de los delitos tecnológicos las siguientes tipologías delictivas:

- Delitos contra el honor.
- Amenazas y coacciones.

La explotación estadística se hace en base a la localización del hecho, es decir, el territorio donde se produce, independientemente de la unidad policial que lo conozca y de la fecha de instrucción de las diligencias policiales.

CONCEPTO DE CONOCIDOS, ESCLARECIDOS, DETENCIONES/INVESTIGADOS Y VICTIMIZACIONES:

Por hechos conocidos se entiende el conjunto de infracciones penales y administrativas, que han sido conocidas por las distintas Fuerzas y Cuerpos de Seguridad, bien por medio de denuncia interpuesta o por actuación policial realizada motu proprio (labor preventiva o de investigación).

Los hechos esclarecidos se clasifican como tales cuando en el hecho se da alguna de estas circunstancias:

- Detención del autor "in fraganti".

• Identificación plena del autor, o alguno de los autores, sin necesidad de que esté detenido, aunque se encuentre en situación de libertad provisional, huido o muerto.

• Cuando exista una confesión verificada, pruebas sólidas o cuando haya una combinación de ambos elementos.

• Cuando la investigación revele que, en realidad, no hubo infracción.

Hay que significar, que como se ha apuntado anteriormente, sólo hay datos de hechos 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). Es por ello, que al no 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.

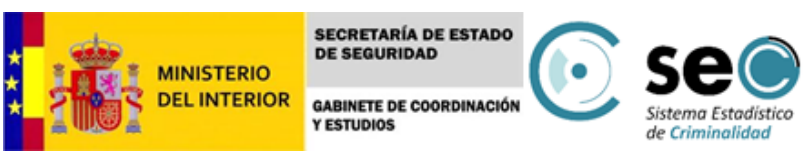
Los contrastes entre victimización y víctima se pueden ejemplificar con el siguiente supuesto: una persona presenta una denuncia y manifiesta que, en un determinado período de tiempo, ha sido objeto de 3 hechos de malos tratos en el ámbito familiar y un delito de amenazas. Además, en esta misma denuncia 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 apuntado anteriormente, sólo hay datos de victimizaciones 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). Es por ello, que al no poseerse datos de la Ertzaintza, los datos de victimizaciones del País Vasco están infrarrepresentados.

MÓDULO DE CONSULTA DE CIBERCRIMINALIDAD

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 ILEGAL 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. 263 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 388-389, 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 CON TARJETAS DE CREDITO, DEBITO 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 210 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 ÉTNICO CULTURAL O RELIGIOSO	
		COACCIONES	


MINISTERIO
DEL INTERIOR
SECRETARÍA DE ESTADO
DE SEGURIDAD
GABINETE DE COORDINACIÓN
Y ESTUDIOS
Sistema Estadístico
de Criminalidad