

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

**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 M^a SANTIAGO OROZCO
MIGUEL ÁNGEL GÓMEZ MARTÍN

Edita:



© De los textos: sus autores

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

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

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	-----

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 conceptualizaciones 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 mundial¹

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. Como 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 Europol²: *“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 **troiano** 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 **troiano 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.

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



- Propagación de código dañino a través de los correos electrónicos.
- Uso de malware de criptojacking/cryptomining⁴.
- 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.

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

8

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	-----

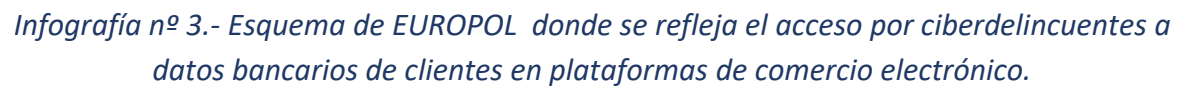
DREAM OF ELECTRIC SHEEP? HOW TECHNOLOGY SHAPES THE FUTURE OF CRIME AND LAW ENFORCEMENT”⁵, en el cual se hace un análisis detallado de este aspecto. Europol llega a afirmar que: *“El advenimiento de las llamadas tecnologías disruptivas, aquellas que alteran fundamentalmente la forma en que vivimos, trabajamos 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 2019⁶, 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



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.

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

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	-----

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

15

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.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127	128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159	160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191	192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223	224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255	256	257	258	259	260	261	262	263	264	265	266	267	268	269	270	271	272	273	274	275	276	277	278	279	280	281	282	283	284	285	286	287	288	289	290	291	292	293	294	295	296	297	298	299	300	301	302	303	304	305	306	307	308	309	310	311	312	313	314	315	316	317	318	319	320	321	322	323	324	325	326	327	328	329	330	331	332	333	334	335	336	337	338	339	340	341	342	343	344	345	346	347	348	349	350	351	352	353	354	355	356	357	358	359	360	361	362	363	364	365	366	367	368	369	370	371	372	373	374	375	376	377	378	379	380	381	382	383	384	385	386	387	388	389	390	391	392	393	394	395	396	397	398	399	400	401	402	403	404	405	406	407	408	409	410	411	412	413	414	415	416	417	418	419	420	421	422	423	424	425	426	427	428	429	430	431	432	433	434	435	436	437	438	439	440	441	442	443	444	445	446	447	448	449	450	451	452	453	454	455	456	457	458	459	460	461	462	463	464	465	466	467	468	469	470	471	472	473	474	475	476	477	478	479	480	481	482	483	484	485	486	487	488	489	490	491	492	493	494	495	496	497	498	499	500	501	502	503	504	505	506	507	508	509	510	511	512	513	514	515	516	517	518	519	520	521	522	523	524	525	526	527	528	529	530	531	532	533	534	535	536	537	538	539	540	541	542	543	544	545	546	547	548	549	550	551	552	553	554	555	556	557	558	559	560	561	562	563	564	565	566	567	568	569	570	571	572	573	574	575	576	577	578	579	580	581	582	583	584	585	586	587	588	589	590	591	592	593	594	595	596	597	598	599	600	601	602	603	604	605	606	607	608	609	610	611	612	613	614	615	616	617	618	619	620	621	622	623	624	625	626	627	628	629	630	631	632	633	634	635	636	637	638	639	640	641	642	643	644	645	646	647	648	649	650	651	652	653	654	655	656	657	658	659	660	661	662	663	664	665	666	667	668	669	670	671	672	673	674	675	676	677	678	679	680	681	682	683	684	685	686	687	688	689	690	691	692	693	694	695	696	697	698	699	700	701	702	703	704	705	706	707	708	709	710	711	712	713	714	715	716	717	718	719	720	721	722	723	724	725	726	727	728	729	730	731	732	733	734	735	736	737	738	739	740	741	742	743	744	745	746	747	748	749	750	751	752	753	754	755	756	757	758	759	760	761	762	763	764	765	766	767	768	769	770	771	772	773	774	775	776	777	778	779	780	781	782	783	784	785	786	787	788	789	790	791	792	793	794	795	796	797	798	799	800	801	802	803	804	805	806	807	808	809	810	811	812	813	814	815	816	817	818	819	820	821	822	823	824	825	826	827	828	829	830	831	832	833	834	835	836	837	838	839	840	841	842	843	844	845	846	847	848	849	850	851	852	853	854	855	856	857	858	859	860	861	862	863	864	865	866	867	868	869	870	871	872	873	874	875	876	877	878	879	880	881	882	883	884	885	886	887	888	889	890	891	892	893	894	895	896	897	898	899	900	901	902	903	904	905	906	907	908	909	910	911	912	913	914	915	916	917	918	919	920	921	922	923	924	925	926	927	928	929	930	931	932	933	934	935	936	937	938	939	940	941	942	943	944	945	946	947	948	949	950	951	952	953	954	955	956	957	958	959	960	961	962	963	964	965	966	967	968	969	970	971	972	973	974	975	976	977	978	979	980	981	982	983	984	985	986	987	988	989	990	991	992	993	994	995	996	997	998	999	1000
---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	------

En 2019, las victimizaciones que han sido registradas por las Fuerzas y Cuerpos de seguridad suman un total de 166.152¹⁰, 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 puede 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.

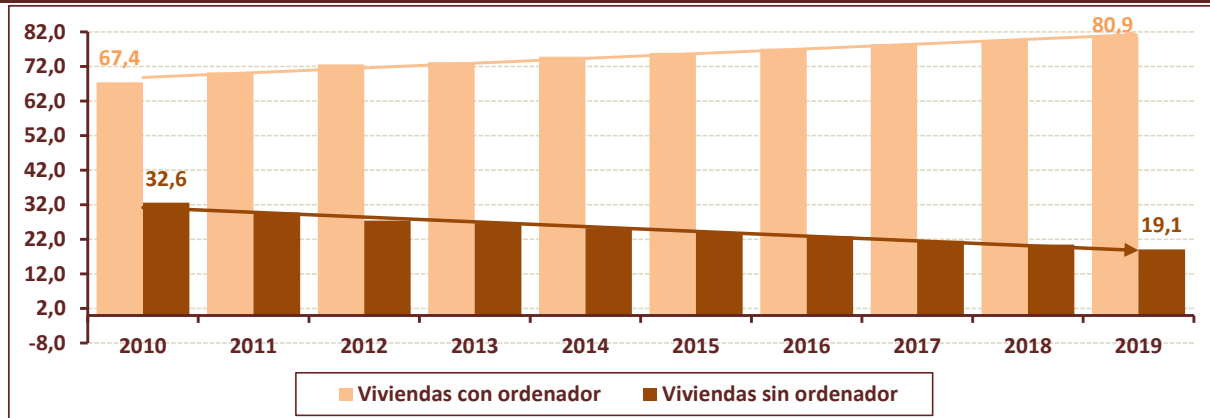
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127	128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159	160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191	192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223	224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255	256	257	258	259	260	261	262	263	264	265	266	267	268	269	270	271	272	273	274	275	276	277	278	279	280	281	282	283	284	285	286	287	288	289	290	291	292	293	294	295	296	297	298	299	300	301	302	303	304	305	306	307	308	309	310	311	312	313	314	315	316	317	318	319	320	321	322	323	324	325	326	327	328	329	330	331	332	333	334	335	336	337	338	339	340	341	342	343	344	345	346	347	348	349	350	351	352	353	354	355	356	357	358	359	360	361	362	363	364	365	366	367	368	369	370	371	372	373	374	375	376	377	378	379	380	381	382	383	384	385	386	387	388	389	390	391	392	393	394	395	396	397	398	399	400	401	402	403	404	405	406	407	408	409	410	411	412	413	414	415	416	417	418	419	420	421	422	423	424	425	426	427	428	429	430	431	432	433	434	435	436	437	438	439	440	441	442	443	444	445	446	447	448	449	450	451	452	453	454	455	456	457	458	459	460	461	462	463	464	465	466	467	468	469	470	471	472	473	474	475	476	477	478	479	480	481	482	483	484	485	486	487	488	489	490	491	492	493	494	495	496	497	498	499	500	501	502	503	504	505	506	507	508	509	510	511	512	513	514	515	516	517	518	519	520	521	522	523	524	525	526	527	528	529	530	531	532	533	534	535	536	537	538	539	540	541	542	543	544	545	546	547	548	549	550	551	552	553	554	555	556	557	558	559	560	561	562	563	564	565	566	567	568	569	570	571	572	573	574	575	576	577	578	579	580	581	582	583	584	585	586	587	588	589	590	591	592	593	594	595	596	597	598	599	600	601	602	603	604	605	606	607	608	609	610	611	612	613	614	615	616	617	618	619	620	621	622	623	624	625	626	627	628	629	630	631	632	633	634	635	636	637	638	639	640	641	642	643	644	645	646	647	648	649	650	651	652	653	654	655	656	657	658	659	660	661	662	663	664	665	666	667	668	669	670	671	672	673	674	675	676	677	678	679	680	681	682	683	684	685	686	687	688	689	690	691	692	693	694	695	696	697	698	699	700	701	702	703	704	705	706	707	708	709	710	711	712	713	714	715	716	717	718	719	720	721	722	723	724	725	726	727	728	729	730	731	732	733	734	735	736	737	738	739	740	741	742	743	744	745	746	747	748	749	750	751	752	753	754	755	756	757	758	759	760	761	762	763	764	765	766	767	768	769	770	771	772	773	774	775	776	777	778	779	780	781	782	783	784	785	786	787	788	789	790	791	792	793	794	795	796	797	798	799	800	801	802	803	804	805	806	807	808	809	810	811	812	813	814	815	816	817	818	819	820	821	822	823	824	825	826	827	828	829	830	831	832	833	834	835	836	837	838	839	840	841	842	843	844	845	846	847	848	849	850	851	852	853	854	855	856	857	858	859	860	861	862	863	864	865	866	867	868	869	870	871	872	873	874	875	876	877	878	879	880	881	882	883	884	885	886	887	888	889	890	891	892	893	894	895	896	897	898	899	900	901	902	903	904	905	906	907	908	909	910	911	912	913	914	915	916	917	918	919	920	921	922	923	924	925	926	927	928	929	930	931	932	933	934	935	936	937	938	939	940	941	942	943	944	945	946	947	948	949	950	951	952	953	954	955	956	957	958	959	960	961	962	963	964	965	966	967	968	969	970	971	972	973	974	975	976	977	978	979	980	981	982	983	984	985	986	987	988	989	990	991	992	993	994	995	996	997	998	999	1000	1001	1002	1003	1004	1005	1006	1007	1008	1009	1010	1011	1012	1013	1014	1015	1016	1017	1018	1019	1020	1021	1022	1023	1024	1025	1026	1027	1028	1029	1030	1031	1032	1033	1034	1035	1036	1037	1038	1039	1040	1041	1042	1043	1044	1045	1046	1047	1048	1049	1050	1051	1052	1053	1054	1055	1056	1057	1058	1059	1060	1061	1062	1063	1064	1065	1066	1067	1068	1069	1070	1071	1072	1073	1074	1075	1076	1077	1078	1079	1080	1081	1082	1083	1084	1085	1086	1087	1088	1089	1090	1091	1092	1093	1094	1095	1096	1097	1098	1099	1100	1101	1102	1103	1104	1105	1106	1107	1108	1109	1110	1111	1112	1113	1114	1115	1116	1117	1118	1119	1120	1121	1122	1123	1124	1125	1126	1127	1128	1129	1130	1131	1132	1133	1134	1135	1136	1137	1138	1139	1140	1141	1142	1143	1144	1145	1146	1147	1148	1149	1150	1151	1152	1153	1154	1155	1156	1157	1158	1159	1160	1161	1162	1163	1164	1165	1166	1167	1168	1169	1170	1171	1172	1173	1174	1175	1176	1177	1178	1179	1180	1181	1182	1183	1184	1185	1186	1187	1188	1189	1190	1191	1192	1193	1194	1195	1196	1197	1198	1199	1200	1201	1202	1203	1204	1205	1206	1207	1208	1209	1210	1211	1212	1213	1214	1215	1216	1217	1218	1219	1220	1221	1222	1223	1224	1225	1226	1227	1228	1229	1230	1231	1232	1233	1234	1235	1236	1237	1238	1239	1240	1241	1242	1243	1244	1245	1246	1247	1248	1249	1250	1251	1252	1253	1254	1255	1256	1257	1258	1259	1260	1261	1262	1263	1264	1265	1266	1267	1268	1269	1270	1271	1272	1273	1274	1275	1276	1277	1278	1279	1280	1281	1282	1283	1284	1285	1286	1287	1288	1289	1290	1291	1292	1293	1294	1295	1296	1297	1298	1299	1300	1301	1302	1303	1304	1305	1306	1307	1308	1309	1310	1311	1312	1313	1314	1315	1316	1317	1318	1319	1320	1321	1322	1323	1324	1325	1326	1327	1328	1329	1330	1331	1332	1333	1334	1335	1336	1337	1338	1339	1340	1341	1342	1343	1344	1345	1346	1347	1348	1349	1350	1351	1352	1353	1354	1355	1356	1357	1358	1359	1360	1361	1362	1363	1364	1365	1366	1367	1368	1369	1370	1371	1372	1373	1374	1375	1376	1377	1378	1379	1380	1381	1382	1383	1384	1385	1386	1387	1388	1389	1390	1391	1392	1393	1394	1395	1396	1397	1398	1399	1400	1401	1402	1403	1404	1405	1406	1407	1408	1409	1410	1411	1412	1413	1414	1415	1416	1417	1418	1419	1420	1421	1422	1423	1424	1425	1426	1427	1428	1429	1430	1431	1432	1433	1434	1435	1436	1437	1438	1439	1440	1441	1442	1443	1444	1445	1446	1447	1448	1449	1450	1451	1452	1453	1454	1455	1456	1457	1458	1459	1460	1461	1462	1463	1464	1465	1466	1467	1468	1469	1470	1471	1472	1473	1474	1475	1476	1477	1478	1479	1480	1481	1482	1483	1484	1485	1486	1487	1488	1489	1490	1491	1492	1493	1494	1495	149
---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	-----

2

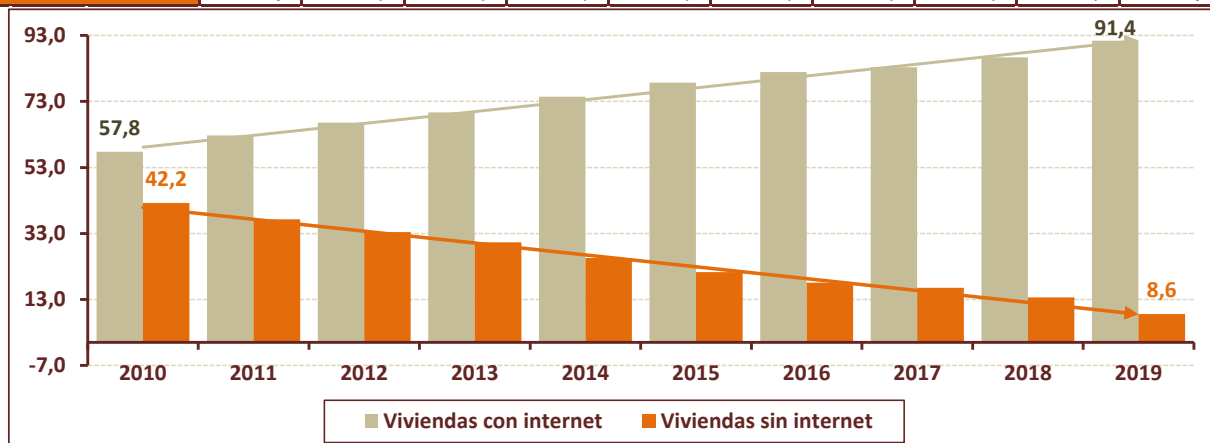
RADIOGRAFÍA DE LA SOCIEDAD DE LA INFORMACIÓN

>> 2.1. HOGARES

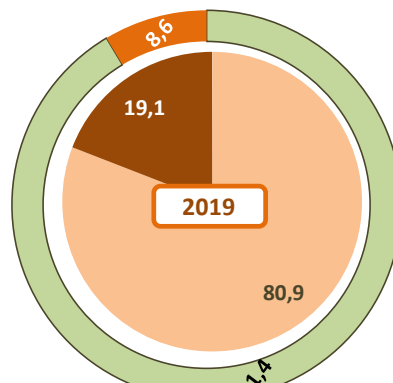
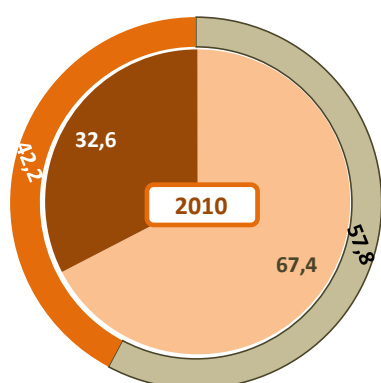
	PORCENTAJE DE VIVIENDAS CON / SIN ALGÚN TIPO DE ORDENADOR									
	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Viviendas con ordenador	67,4	70,3	72,6	73,3	74,8	75,9	77,1	78,4	79,5	80,9
Viviendas sin ordenador	32,6	29,7	27,4	26,7	25,2	24,1	22,9	21,6	20,5	19,1



	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

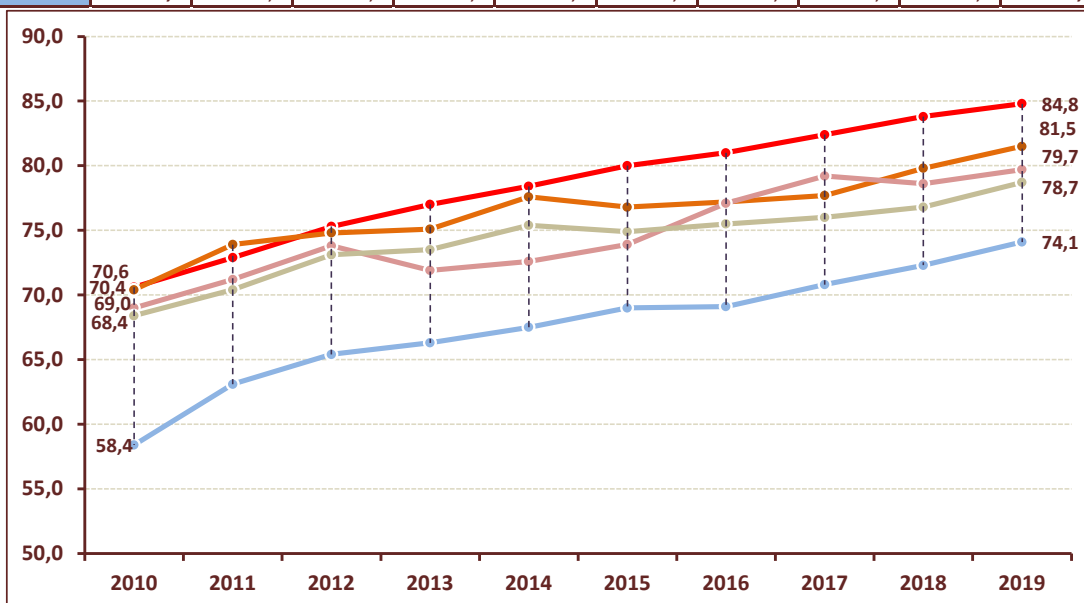


■ Viviendas con ordenador ■ Viviendas sin ordenador ²²

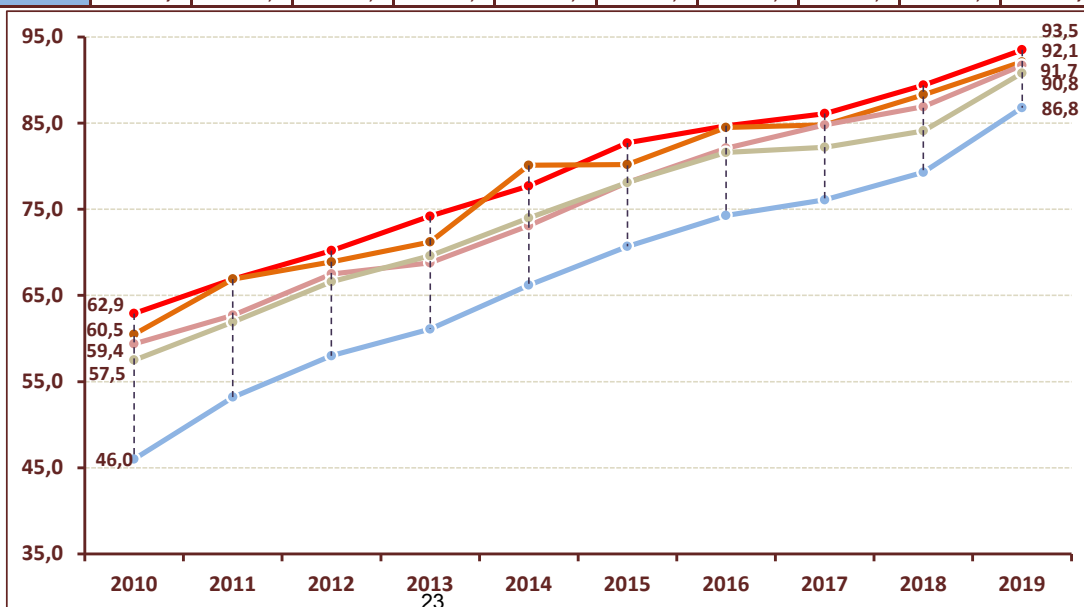
■ Viviendas con internet ■ Viviendas sin internet

>> 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

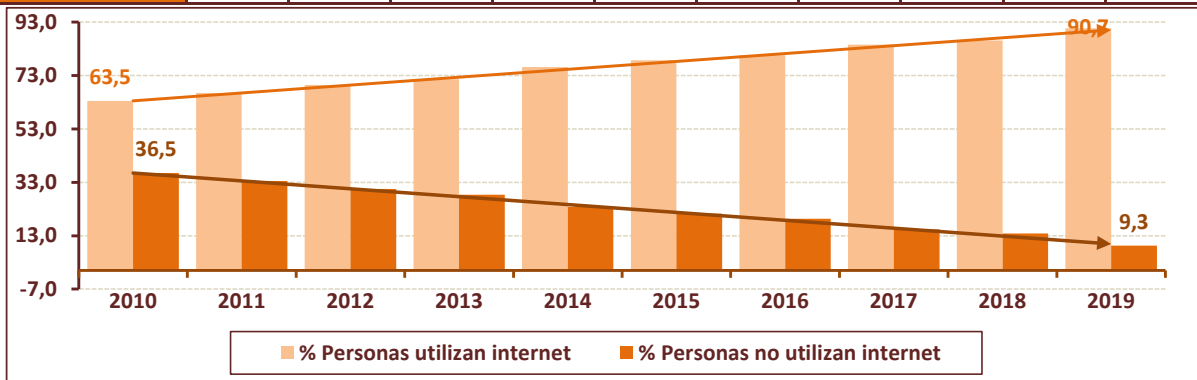


	PORCENTAJE DE VIVIENDAS CON ACCESO A INTERNET									
	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Más de 100.000 hab.	62,9	66,9	70,2	74,2	77,7	82,7	84,7	86,1	89,4	93,5
De 50.000 a 100.000 hab.	60,5	66,9	68,9	71,2	80,1	80,2	84,5	84,8	88,3	92,1
De 20.000 a 50.000 hab.	59,4	62,7	67,5	68,8	73,1	78,1	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

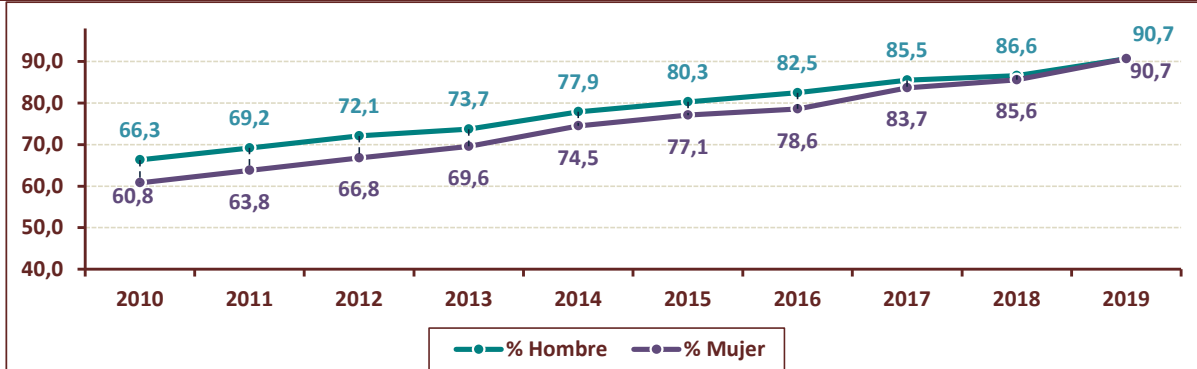


>> 2.2.PERFIL DEL CIUDADANO ANTE LA SOCIEDAD DE LA INFORMACION. USO DE INTERNET

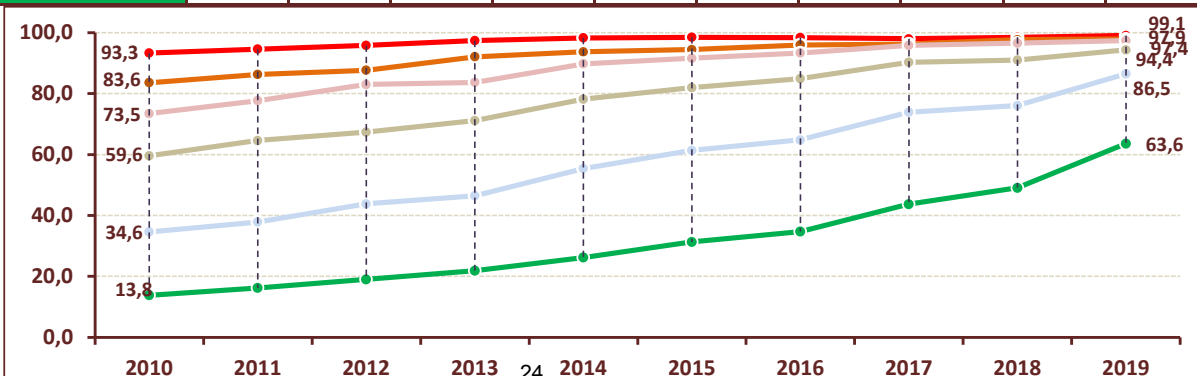
	% DE PERSONAS QUE HAN UTILIZADO O NO INTERNET ÚLTIMOS 3 MESES									
	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Utilizado internet	63,5	66,5	69,5	71,6	76,2	78,7	80,6	84,6	86,1	90,7
No utilizado internet	36,5	33,5	30,5	28,4	23,8	21,3	19,4	15,4	13,9	9,3



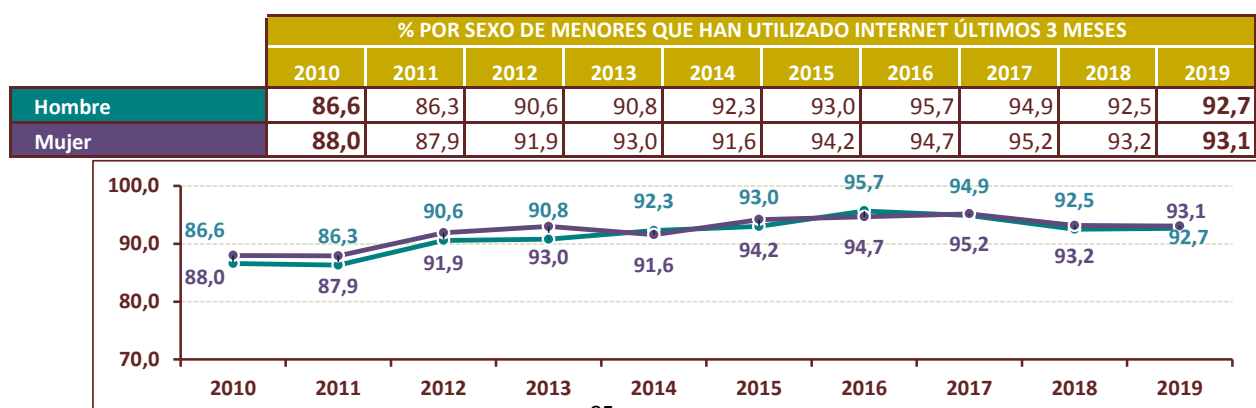
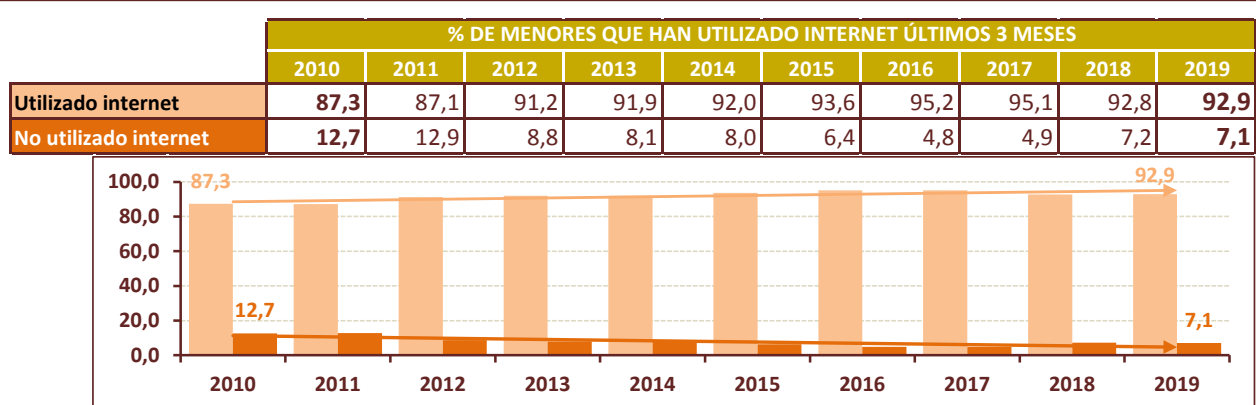
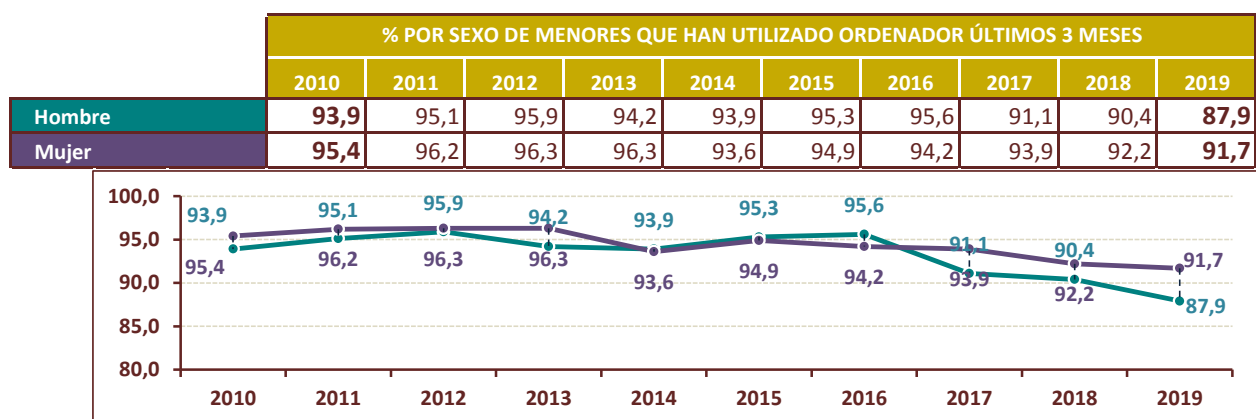
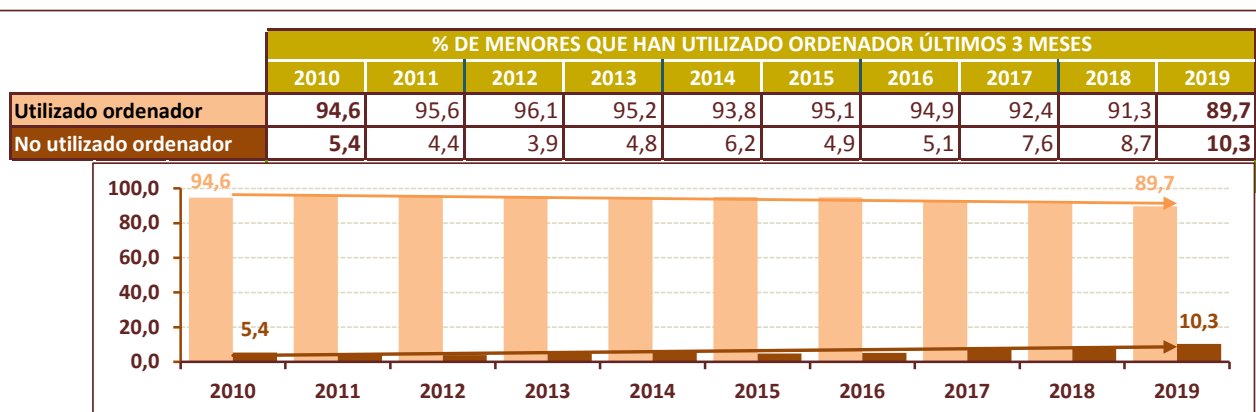
	% POR SEXO DE PERSONAS QUE HAN UTILIZADO INTERNET ÚLTIMOS 3 MESES									
	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Hombre	66,3	69,2	72,1	73,7	77,9	80,3	82,5	85,5	86,6	90,7
Mujer	60,8	63,8	66,8	69,6	74,5	77,1	78,6	83,7	85,6	90,7



	% 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

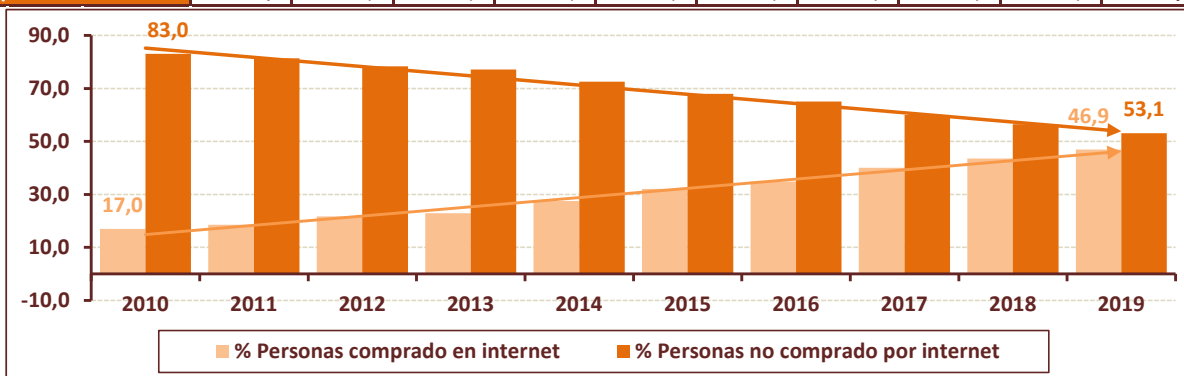


>> 2.3. PERFIL DEL MENOR DE EDAD (10 A 15 AÑOS) ANTE LA SOCIEDAD DE LA INFORMACIÓN

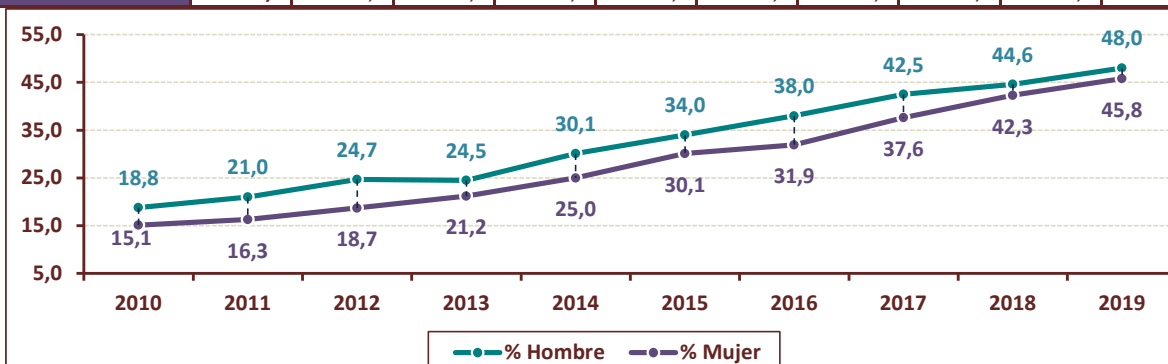


>> 2.4. PERFIL DE LAS PERSONAS QUE HAN COMPRADO ALGUNA VEZ POR INTERNET

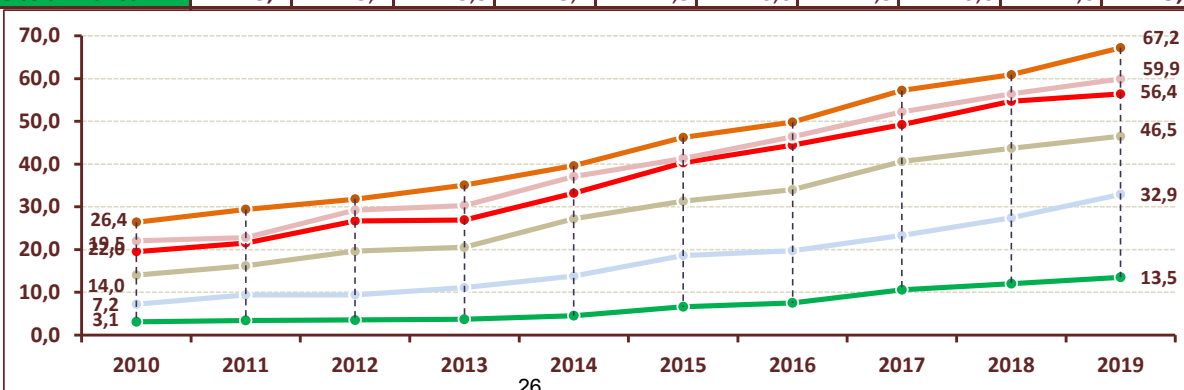
	% PERSONAS QUE HAN COMPRADO ALGUNA VEZ POR INTERNET									
	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Comprado en internet	17,0	18,6	21,7	22,9	27,5	32,1	34,9	40,0	43,5	46,9
No comprado en internet	83,0	81,4	78,3	77,1	72,5	67,9	65,1	60,0	56,5	53,1



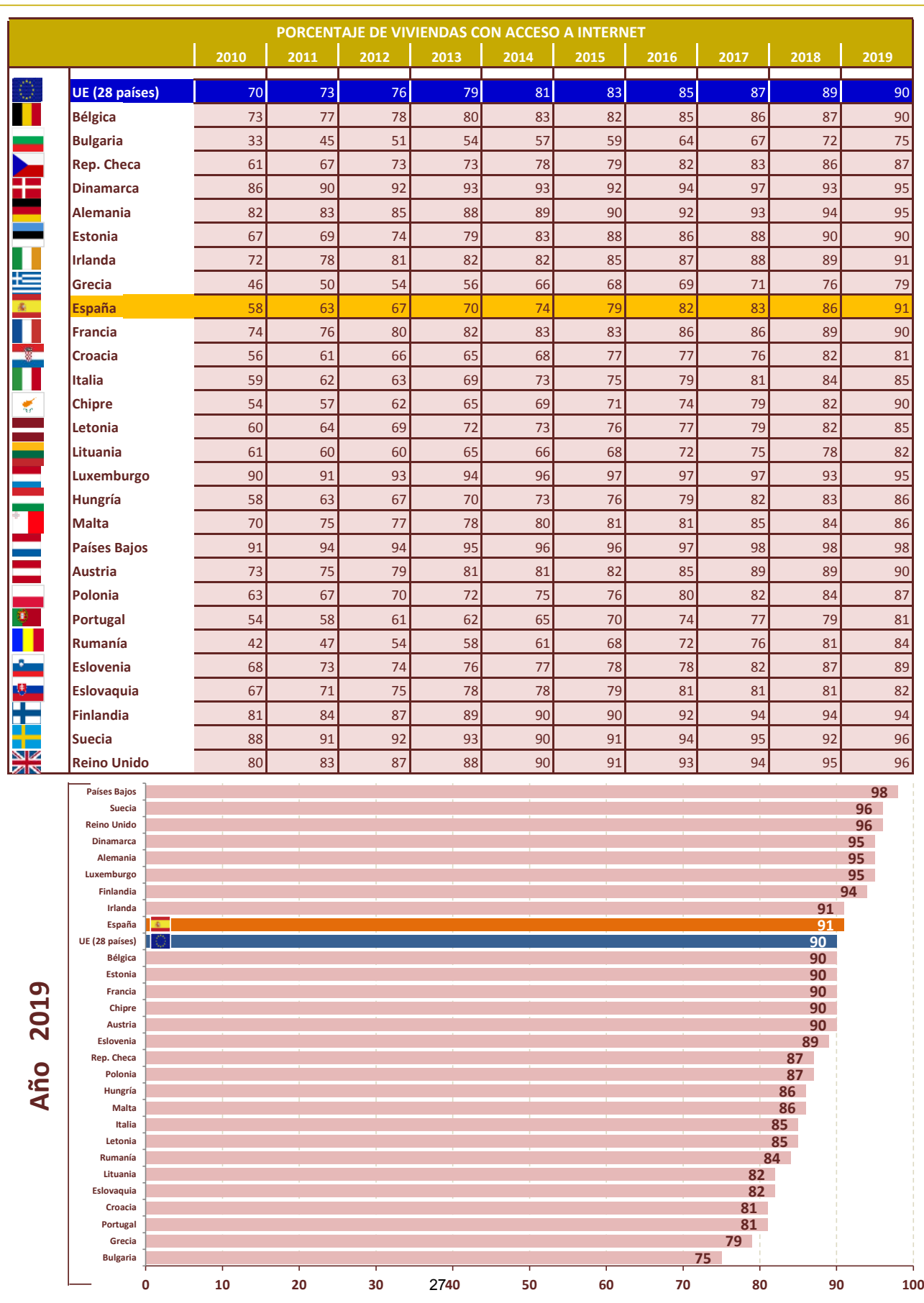
	% POR SEXO DE PERSONAS QUE HAN COMPRADO ALGUNA VEZ POR INTERNET									
	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Hombre	18,8	21,0	24,7	24,5	30,1	34,0	38,0	42,5	44,6	48,0
Mujer	15,1	16,3	18,7	21,2	25,0	30,1	31,9	37,6	42,3	45,8



	% 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



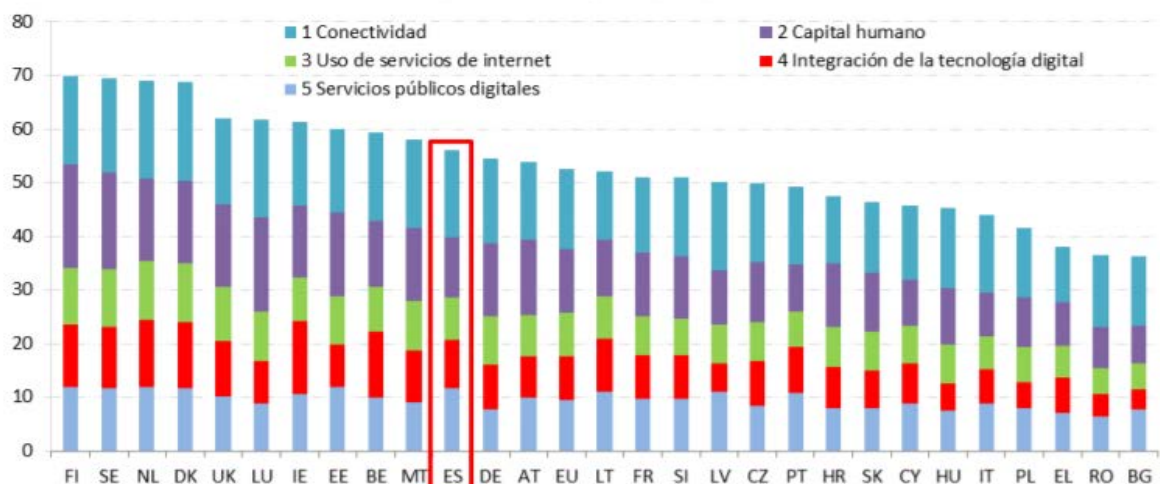
>> 2.5. COMPARATIVA INTERNACIONAL. VIVIENDAS CON ACCESO A INTERNET



>> 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



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

>> 2.7. INDICADORES DE LA SOCIEDAD DE LA INFORMACIÓN

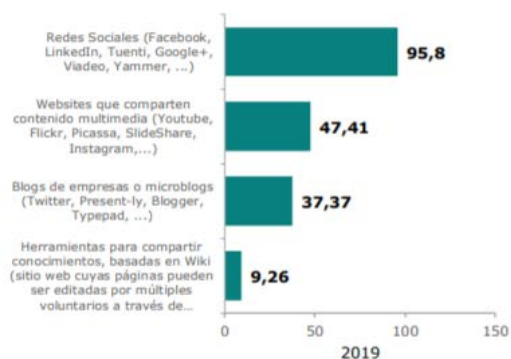
(Publicación: Indicadores destacados de la sociedad de la información)

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

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 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*.

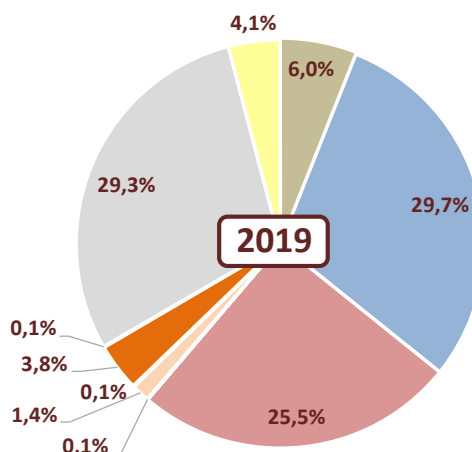
>> 3.3. INCIDENTES GESTIONADOS POR SECTOR ESTRATÉGICO

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%).

>> 3.1. 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

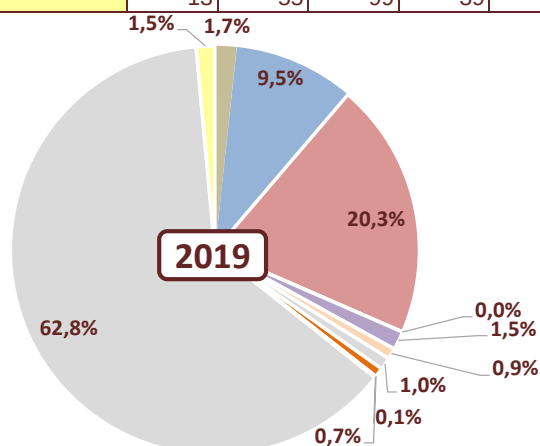


*Véase metadatos explicativos

>> 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

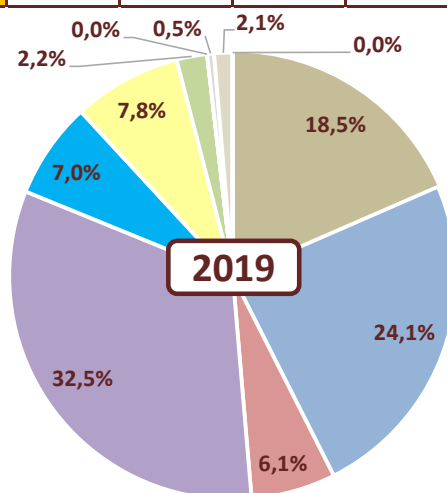


*Véase metadatos explicativos

>> 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



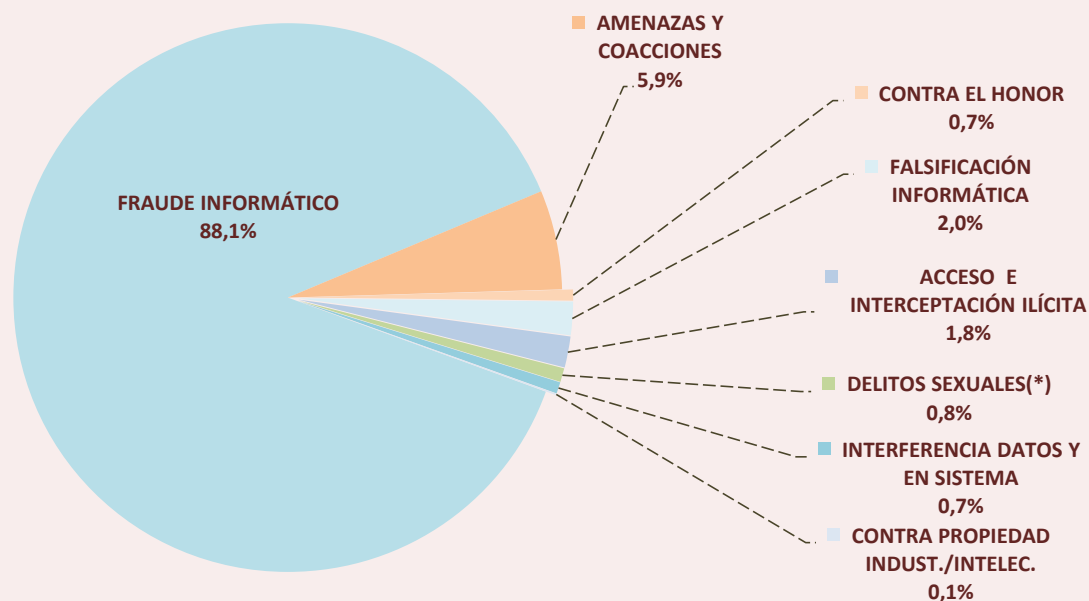
4

DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD

>> 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



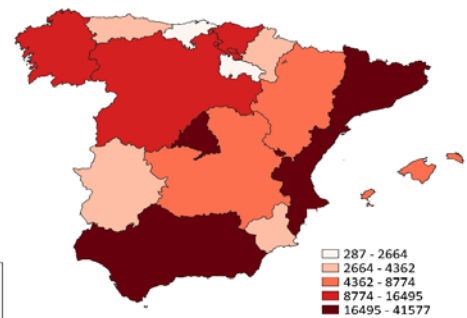
>> 4.3. REPRESENTACIÓN TERRITORIAL DE HECHOS DENUNCIADOS DE CIBERCRIMINALIDAD. AÑO 2019

Hechos denunciados de CIBERCRIMINALIDAD - 2019

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

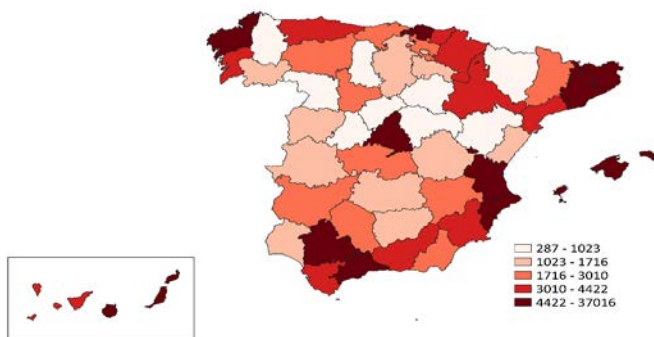
15,1%

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

DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD

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

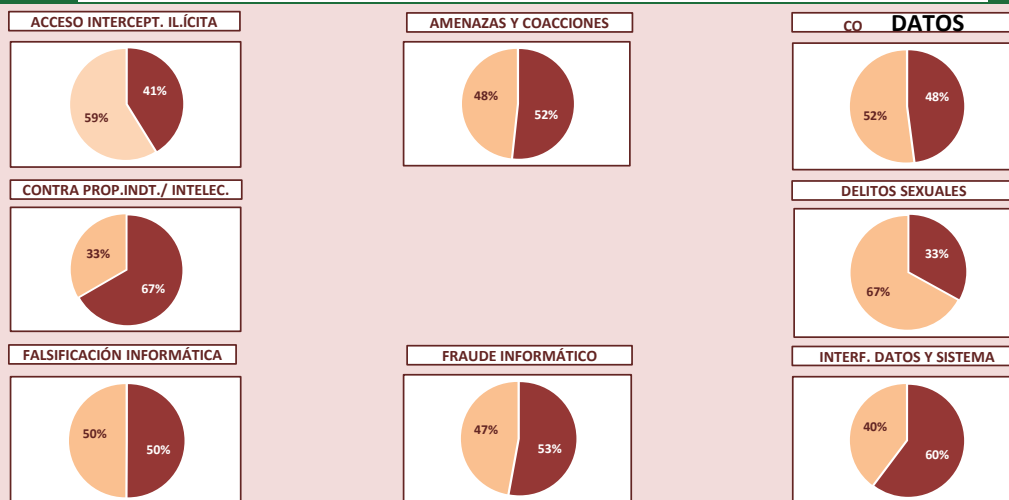
>> 4.4. VICTIMIZACIONES REGISTRADAS SEGÚN GRUPO PENAL Y SEXO. AÑO 2019



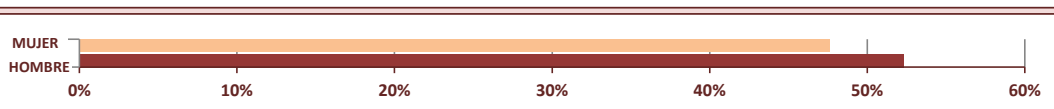
VICTIMIZACIONES	Hombre	Mujer	Desconocido	Total
ACCESO E INTERCEPTACIÓN ILÍCITA	1.455	2.078	3	3.536
AMENAZAS Y COACCIONES	6.767	6.317	32	13.116
CONTRA EL HONOR	728	791	2	1.521
CONTRA LA PROPIEDAD INDUSTRIAL/INTELLECTUAL	38	19	1	58
DELITOS SEXUALES (*)	409	829	5	1.243
FALSIFICACIÓN INFORMÁTICA	1.457	1.452	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

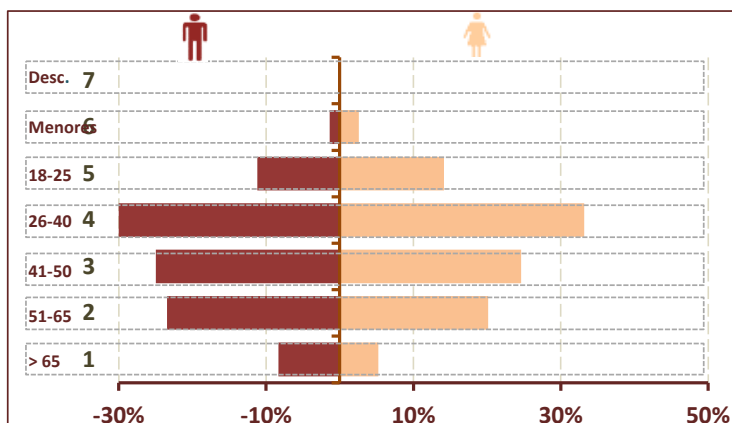
DISTRIBUCIÓN PORCENTUAL DE LAS VÍCTIMAS POR GRUPO PENAL SEGÚN SEXO



DISTRIBUCIÓN GLOBAL POR SEXOS

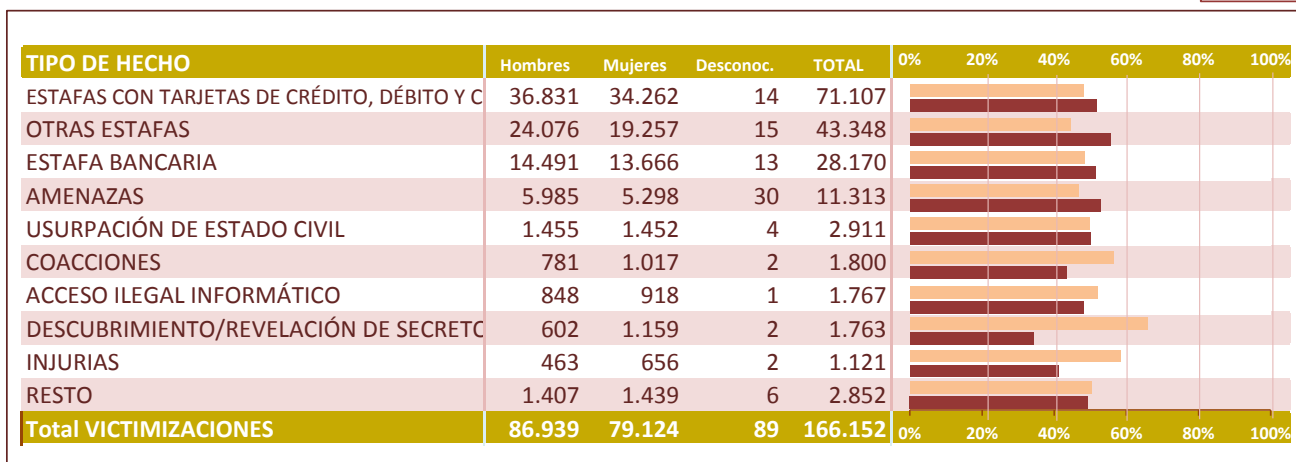


>> 4.5. VICTIMIZACIONES SEGÚN GRUPO DE EDAD Y SEXO. AÑO 2019

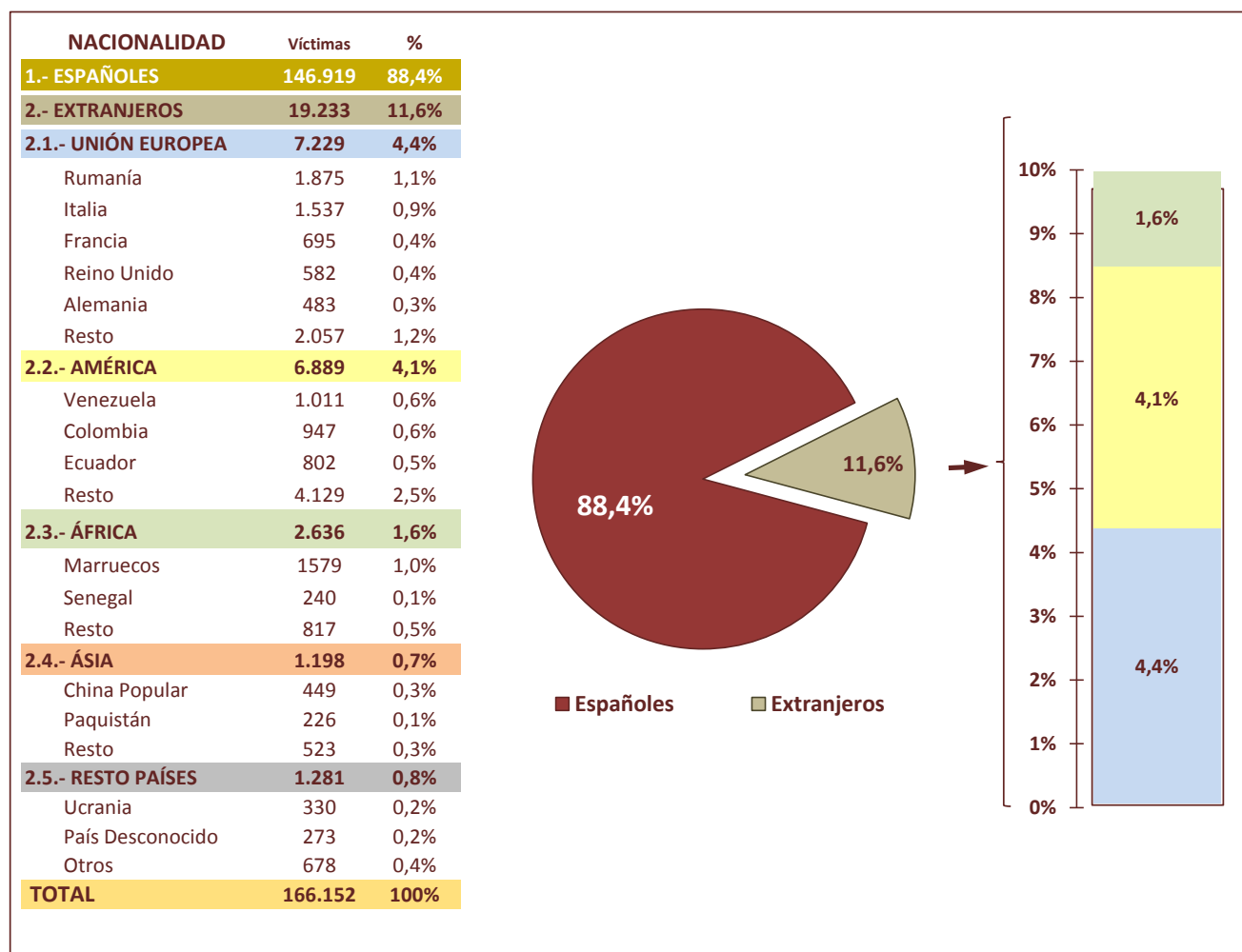


Grupo de edad	Hombre	Mujer	Descon.
Edad descon.	83	69	20
Menores de edad	1.185	2.057	1
De 18 a 25 años	9.737	11.207	2
De 26 a 40 años	26.609	26.248	14
De 41 a 50 años	21.710	19.472	24
De 51 a 65 años	20.364	15.928	18
Mayores 65 años	7.251	4.143	10
TOTAL	86.939	79.124	89

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



>> 4.7. NACIONALIDAD DE LA VÍCTIMA. AÑO 2019

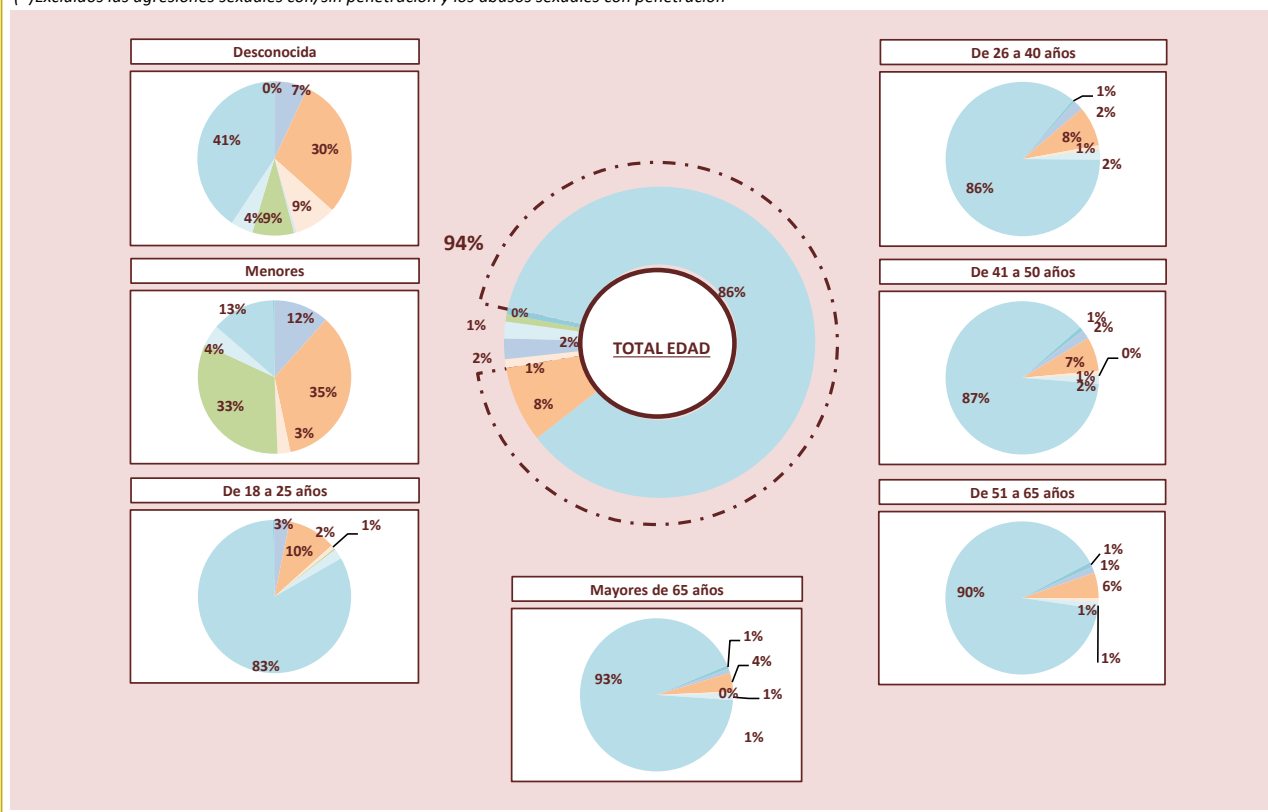


>> 4.8. VICTIMIZACIONES REGISTRADAS SEGÚN GRUPO PENAL Y EDAD. AÑO 2019

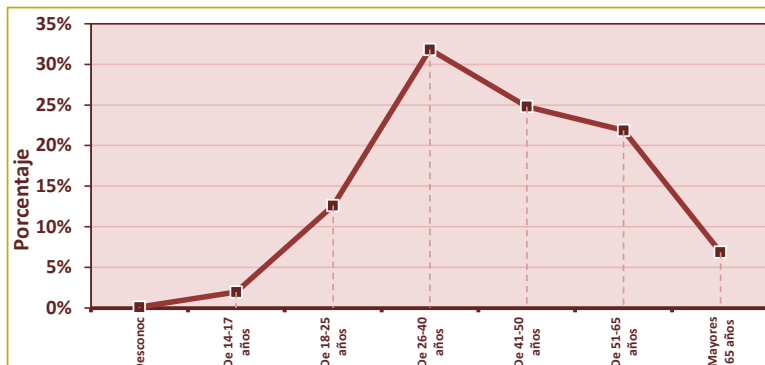


GRUPO PENAL	Rango de edad de la víctima						
	Descon.	Menores	18-25	26-40	41-50	51-65	> 65
ACCESO E INTERCEPTACIÓN ILÍCITA	12	378	663	1.108	790	478	107
AMENAZAS Y COACCIONES	51	1.135	2.140	4.425	2.954	1.961	450
CONTRA EL HONOR	15	88	172	509	402	293	42
CONTRA PROPIEDAD INDUST./INTELEC.	1	0	1	22	14	15	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

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

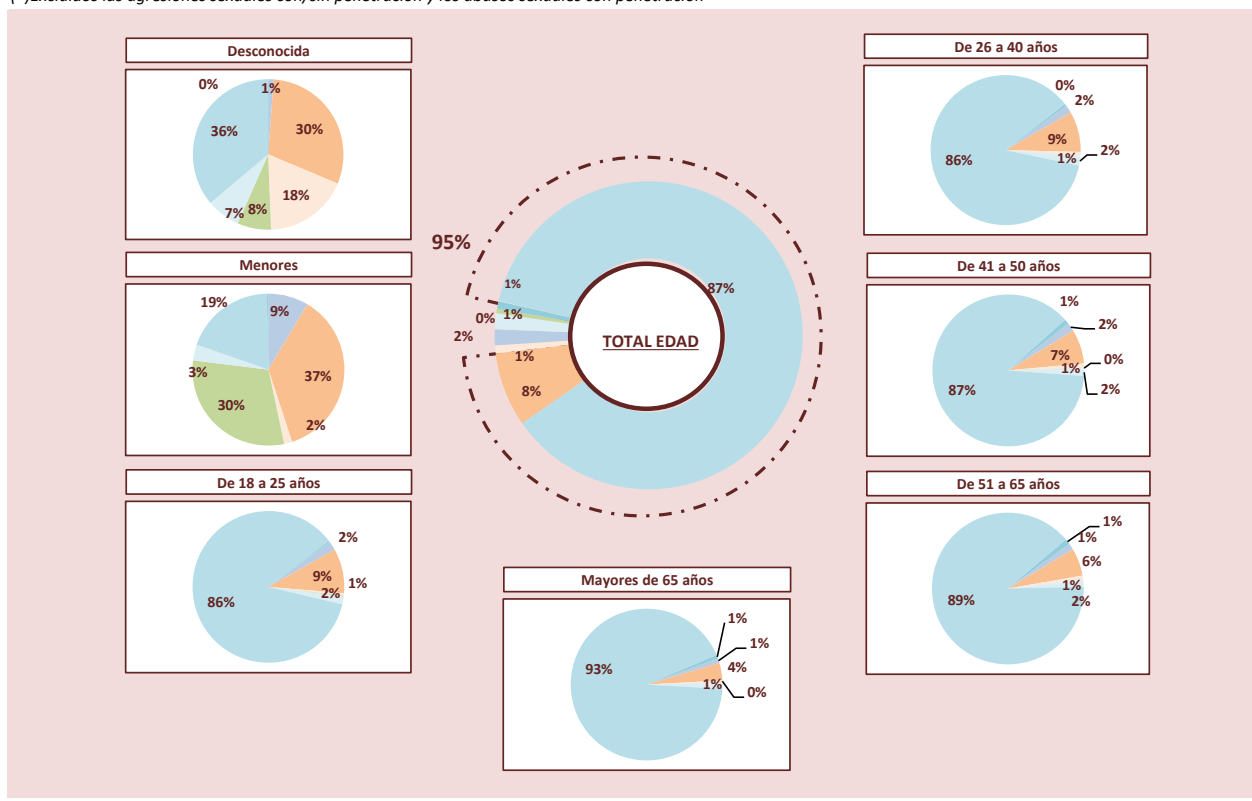
(Fuente de datos: Sistema Estadístico de Criminalidad: Datos de los cuerpos policiales, excepto Ertzaintza)



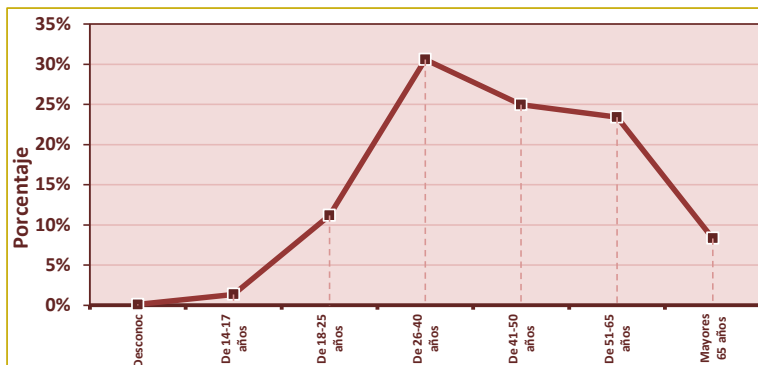
>> 4.10. VICTIMIZACIONES REGISTRADAS SEGÚN GRUPO PENAL Y EDAD. AÑO 2019

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

(*)Excluidas 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

DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil de la VÍCTIMA (MUJER)

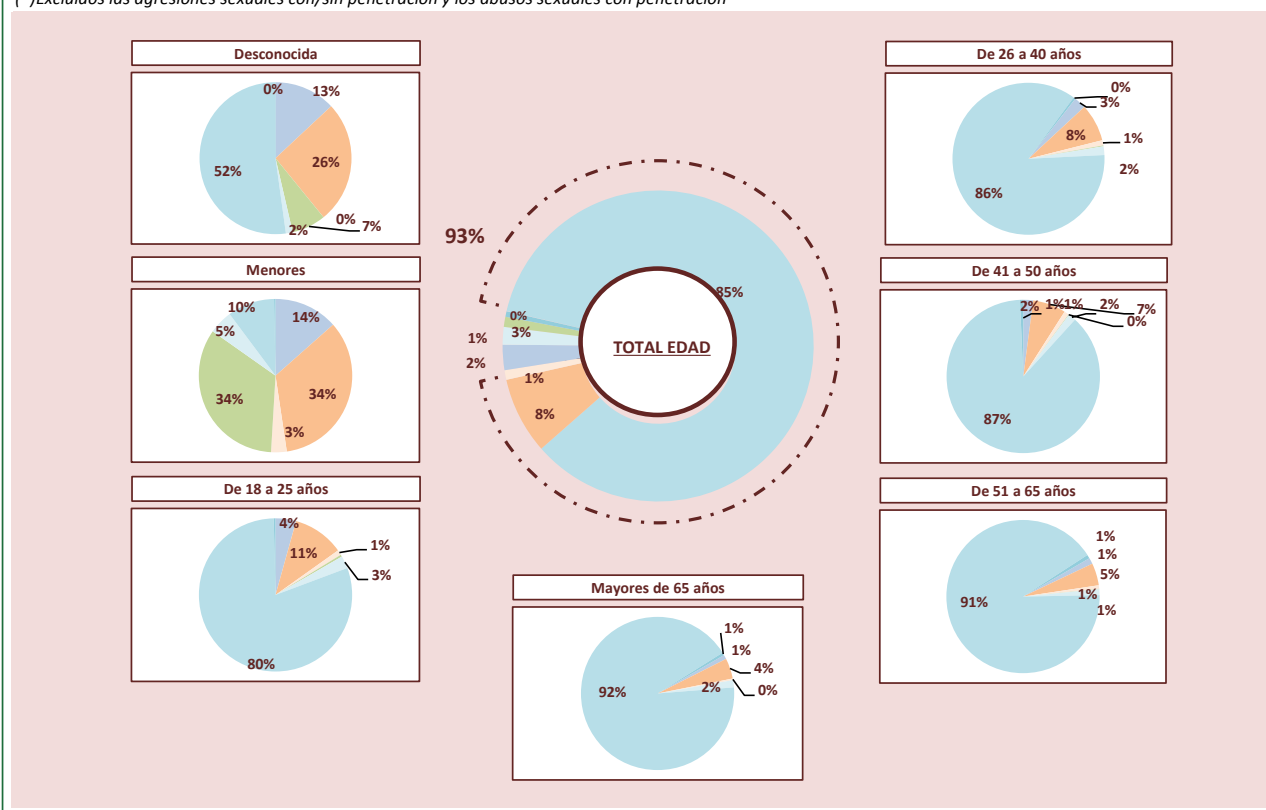
(Fuente de datos: Sistema Estadístico de Criminalidad: Datos de los cuerpos policiales, excepto Ertzaintza)

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

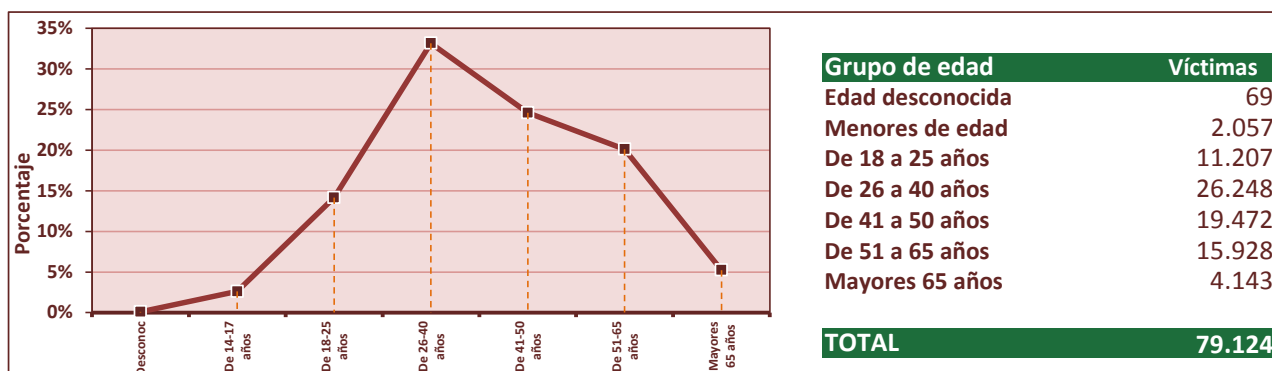


GRUPO PENAL	Rango de edad de la víctima						
	Descon.	Menores	18-25	26-40	41-50	51-65	> 65
ACCESO E INTERCEPTACIÓN ILÍCITA	9	277	485	663	403	204	37
AMENAZAS Y COACCIONES	18	703	1.214	2.099	1.358	746	179
CONTRA EL HONOR	0	68	118	284	189	118	14
CONTRA PROPIEDAD INDUST./INTELEC.	0	0	1	7	6	5	0
DELITOS SEXUALES(*)	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



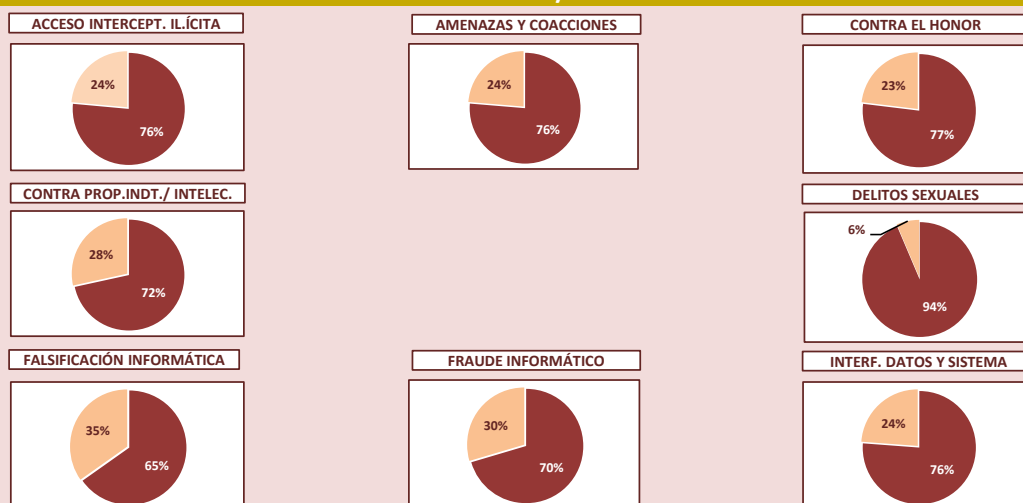
>> 4.14. DETENCIONES/INVESTIGADOS REGISTRADOS SEGÚN GRUPO PENAL Y SEXO. AÑO 2019



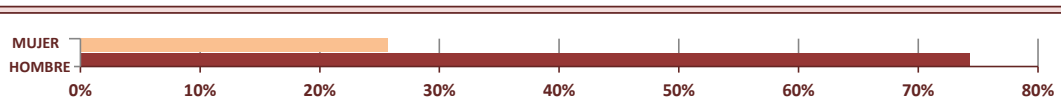
DETENCIONES/INVESTIGADOS REGISTRADOS	Hombre	Mujer	Total
ACCESO E INTERCEPTACIÓN ILÍCITA	357	110	467
AMENAZAS Y COACCIONES	1.334	414	1.748
CONTRA EL HONOR	120	36	156
CONTRA LA PROPIEDAD INDUSTRIAL/INTELLECTUAL	141	56	197
DELITOS SEXUALES(*)	907	62	969
FALSIFICACIÓN INFORMÁTICA	266	142	408
FRAUDE INFORMÁTICO	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

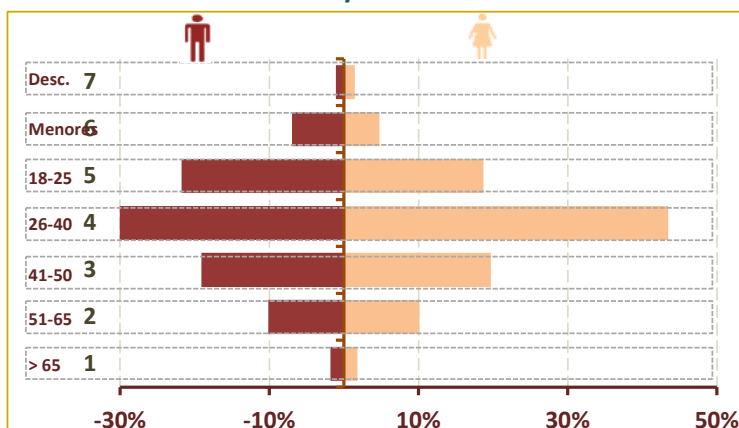
DISTRIBUCIÓN PORCENTUAL DE LAS DETENCIONES/INVESTIGADOS POR GRUPO PENAL SEGÚN SEXO



DISTRIBUCIÓN GLOBAL POR SEXOS



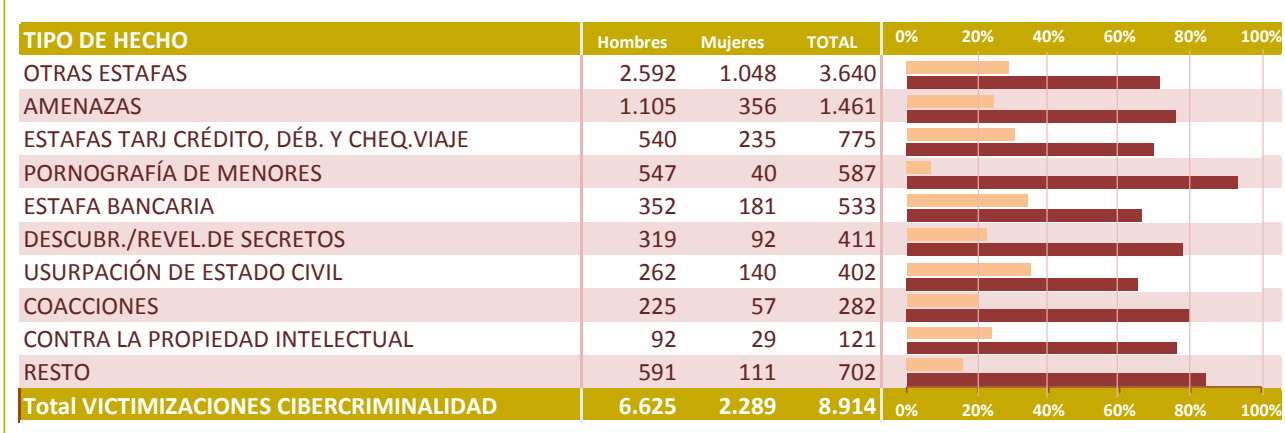
>> 4.15. DETENCIONES/INVESTIGADOS SEGÚN GRUPO DE EDAD Y SEXO. AÑO 2019



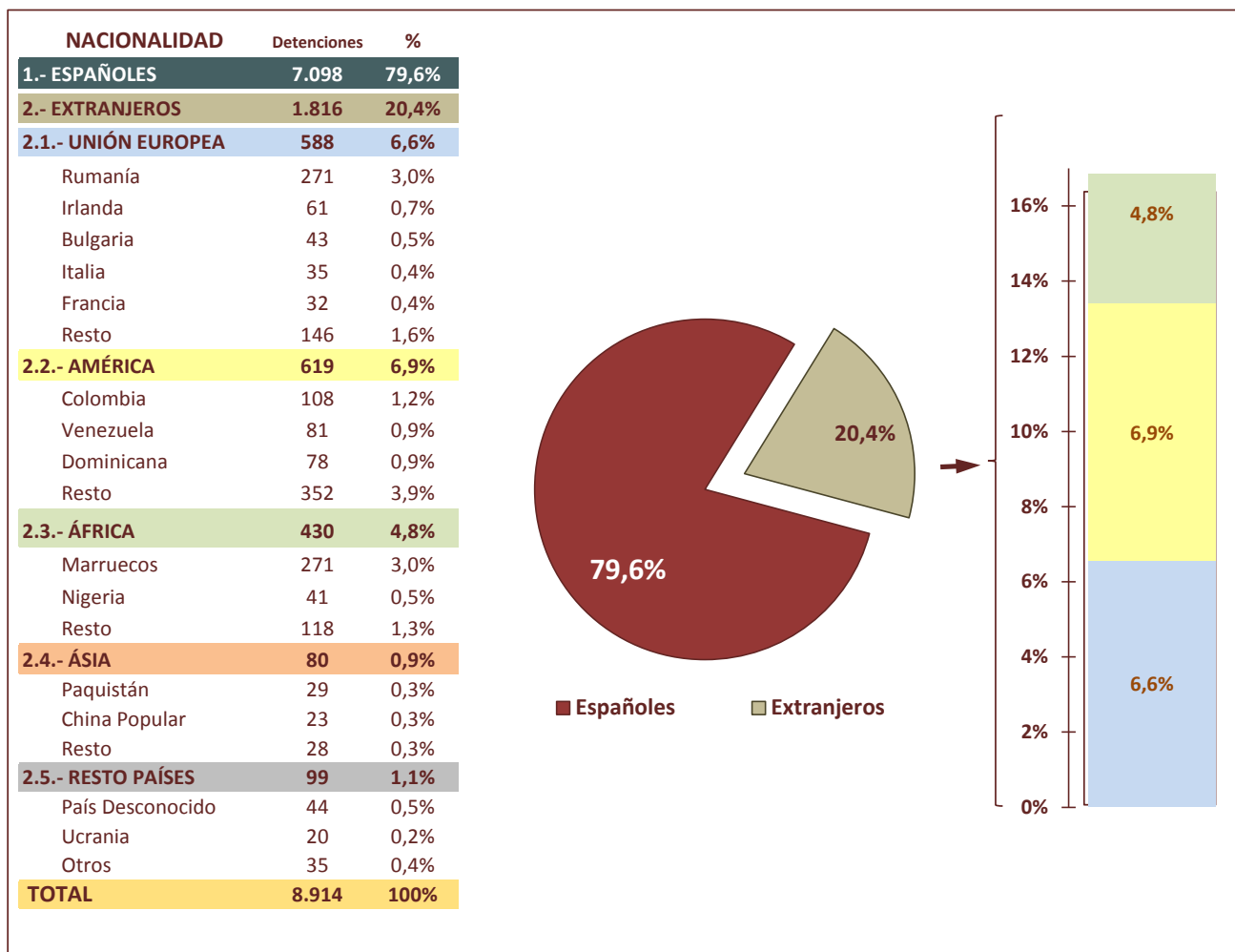
Grupo de edad	Hombre	Mujer
Edad desconocida	71	33
De 14 a 17 años	461	109
De 18 a 25 años	1.441	428
De 26 a 40 años	2.596	995
De 41 a 50 años	1.265	451
De 51 a 65 años	671	232
Mayores 65 años	120	41
TOTAL	6.625	2.289



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



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



DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD - Perfil del RESPONSABLE

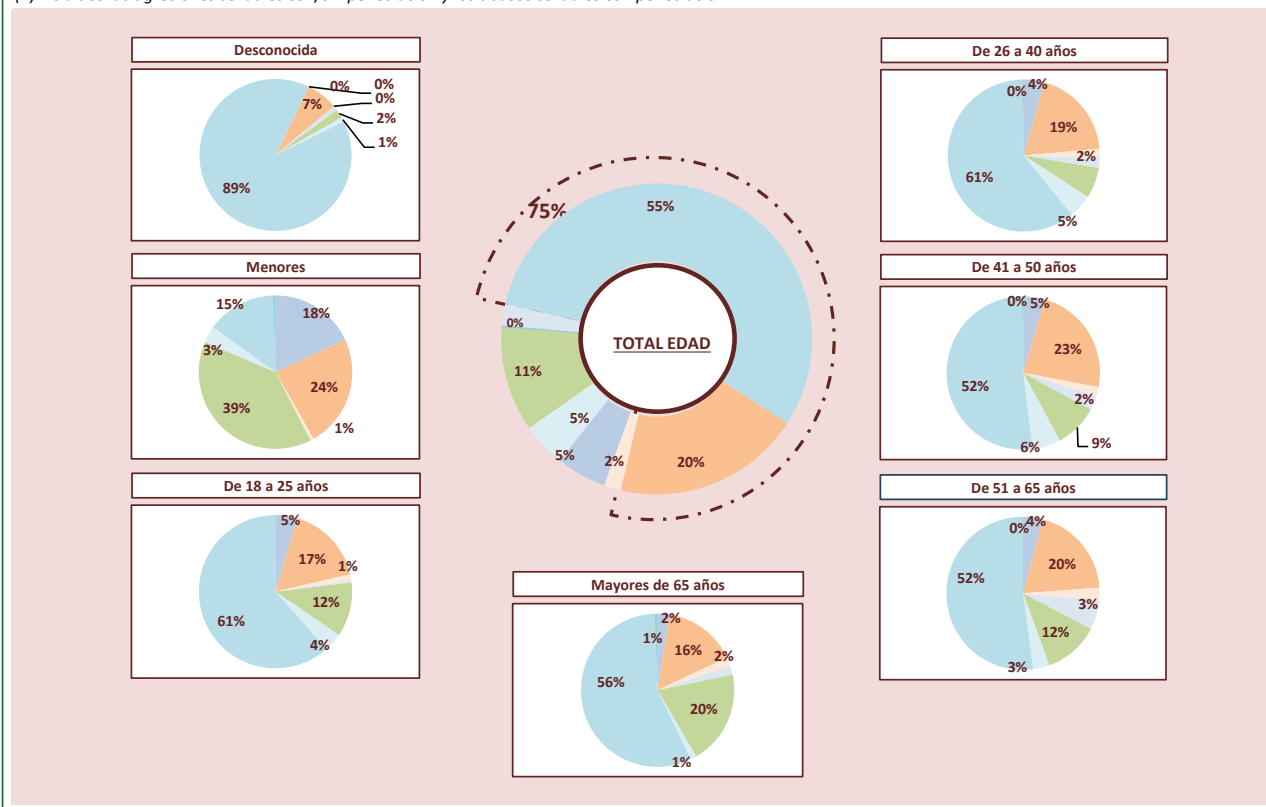
(Fuente de datos: Sistema Estadístico de Criminalidad: Datos de los cuerpos policiales)

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

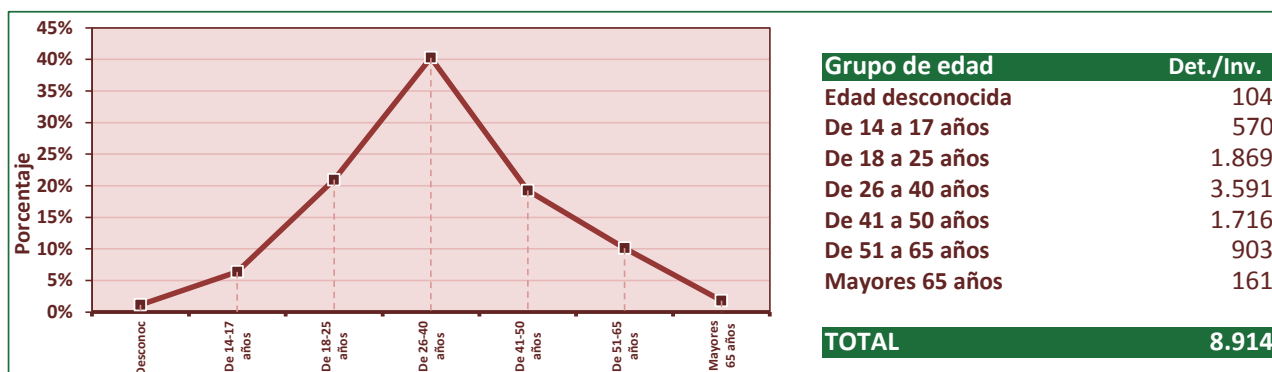


GRUPO PENAL	Rango de edad de los detenidos/investigados						
	Descon.	14-17	18-25	26-40	41-50	51-65	> 65
ACCESO E INTERCEPTACIÓN ILÍCITA	0	103	86	158	78	38	4
AMENAZAS Y COACCIONES	7	135	313	689	402	177	25
CONTRA EL HONOR	0	4	24	68	33	24	3
CONTRA PROPIEDAD INDUST./INTELEC.	1	0	8	77	52	56	3
DELITOS SEXUALES(*)	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

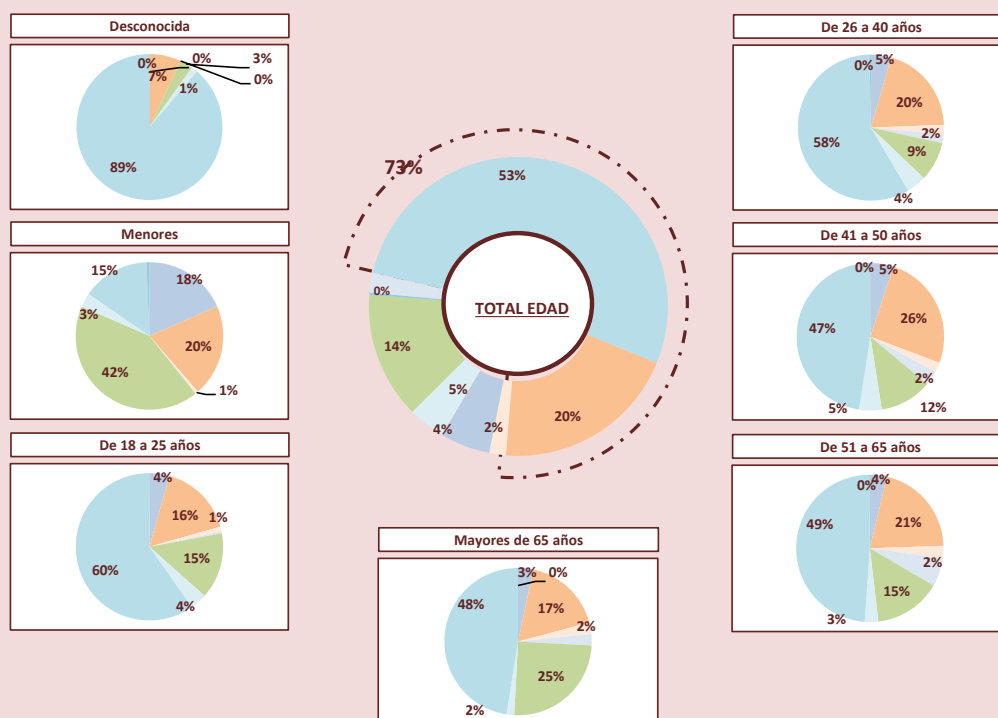


>> 4.20. DETENCIONES/INVESTIGADOS REGISTRADAS SEGÚN GRUPO PENAL Y EDAD. AÑO 2019

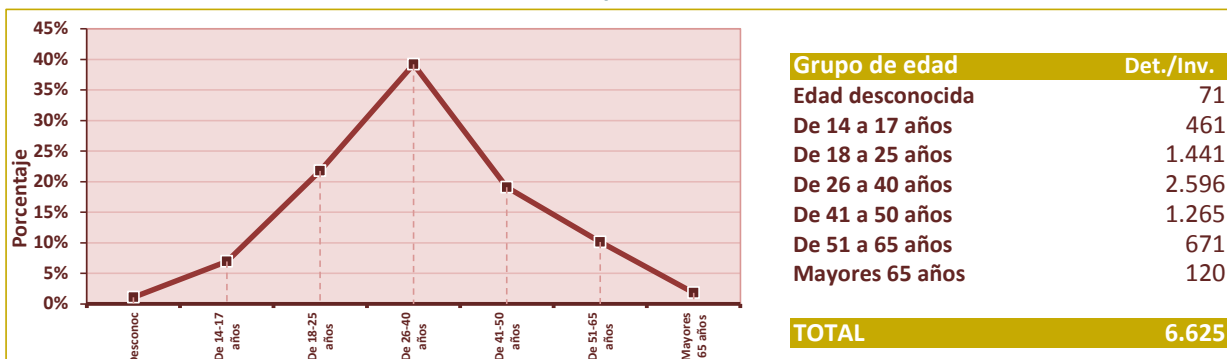


GRUPO PENAL	Rango de edad de los detenidos/investigados						
	Descon.	14-17	18-25	26-40	41-50	51-65	> 65
ACCESO E INTERCEPTACIÓN ILÍCITA	0	85	63	116	64	25	4
AMENAZAS Y COACCIONES	5	93	234	517	325	139	21
CONTRA EL HONOR	0	3	15	54	27	18	3
CONTRA PROPIEDAD INDUST./INTELEC.	0	0	6	50	40	42	3
DELITOS SEXUALES(*)	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



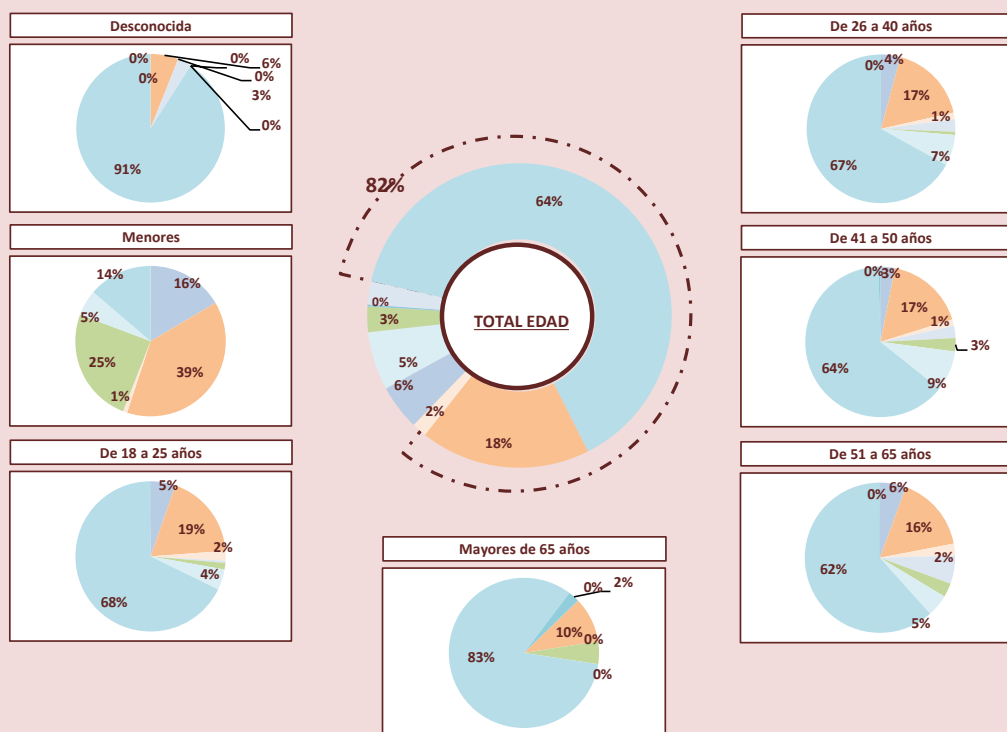
>> 4.21. EDAD DE LAS PERSONAS DETENIDAS/INVESTIGADAS. AÑO 2019



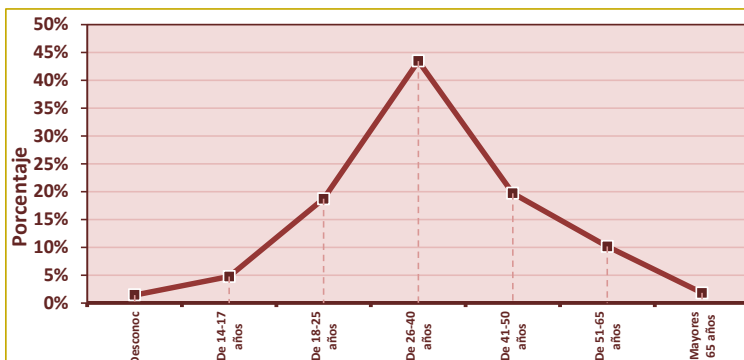
>> 4.22. DETENCIONES/INVESTIGADOS REGISTRADAS SEGÚN GRUPO PENAL Y EDAD
AÑO 2019

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

ESTUDIO SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA	2019
--	------

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/I0/&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/I0/&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/I0/&file=02004.px&L=0

ESTADÍSTICA DE CRIMINALIDAD	ESTADÍSTICA DE CRIMINALIDAD	ESTADÍSTICA DE CRIMINALIDAD	ESTADÍSTICA DE CRIMINALIDAD	ESTADÍSTICA DE CRIMINALIDAD	ESTADÍSTICA DE CRIMINALIDAD
ESTADÍSTICA DE CRIMINALIDAD	ESTADÍSTICA DE CRIMINALIDAD	ESTADÍSTICA DE CRIMINALIDAD	ESTADÍSTICA DE CRIMINALIDAD	ESTADÍSTICA DE CRIMINALIDAD	ESTADÍSTICA DE CRIMINALIDAD
ESTADÍSTICA DE CRIMINALIDAD	ESTADÍSTICA DE CRIMINALIDAD	ESTADÍSTICA DE CRIMINALIDAD	ESTADÍSTICA DE CRIMINALIDAD	ESTADÍSTICA DE CRIMINALIDAD	ESTADÍSTICA DE CRIMINALIDAD
ESTADÍSTICA DE CRIMINALIDAD	ESTADÍSTICA DE CRIMINALIDAD	ESTADÍSTICA DE CRIMINALIDAD	ESTADÍSTICA DE CRIMINALIDAD	ESTADÍSTICA DE CRIMINALIDAD	ESTADÍSTICA DE CRIMINALIDAD
ESTADÍSTICA DE CRIMINALIDAD	ESTADÍSTICA DE CRIMINALIDAD	ESTADÍSTICA DE CRIMINALIDAD	ESTADÍSTICA DE CRIMINALIDAD	ESTADÍSTICA DE CRIMINALIDAD	ESTADÍSTICA DE CRIMINALIDAD
ESTADÍSTICA DE CRIMINALIDAD	ESTADÍSTICA DE CRIMINALIDAD	ESTADÍSTICA DE CRIMINALIDAD	ESTADÍSTICA DE CRIMINALIDAD	ESTADÍSTICA DE CRIMINALIDAD	ESTADÍSTICA DE CRIMINALIDAD
ESTADÍSTICA DE CRIMINALIDAD	ESTADÍSTICA DE CRIMINALIDAD	ESTADÍSTICA DE CRIMINALIDAD	ESTADÍSTICA DE CRIMINALIDAD	ESTADÍSTICA DE CRIMINALIDAD	ESTADÍSTICA DE CRIMINALIDAD
ESTADÍSTICA DE CRIMINALIDAD	ESTADÍSTICA DE CRIMINALIDAD	ESTADÍSTICA DE CRIMINALIDAD	ESTADÍSTICA DE CRIMINALIDAD	ESTADÍSTICA DE CRIMINALIDAD	ESTADÍSTICA DE CRIMINALIDAD
ESTADÍSTICA DE CRIMINALIDAD	ESTADÍSTICA DE CRIMINALIDAD	ESTADÍSTICA DE CRIMINALIDAD	ESTADÍSTICA DE CRIMINALIDAD	ESTADÍSTICA DE CRIMINALIDAD	ESTADÍSTICA DE CRIMINALIDAD
ESTADÍSTICA DE CRIMINALIDAD	ESTADÍSTICA DE CRIMINALIDAD	ESTADÍSTICA DE CRIMINALIDAD	ESTADÍSTICA DE CRIMINALIDAD	ESTADÍSTICA DE CRIMINALIDAD	ESTADÍSTICA DE CRIMINALIDAD

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/I0/&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

53



MÓDULO DE CONSULTA DE CIBERCRIMINALIDAD				
DENOMINACIÓN	CÓDIGO PENAL ESPAÑOL	TIPO HECHO SEC	VARIABLES SECA 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	
Interferencia en los datos y en el sistema	Arts. 263 a 267 y 625.1. Daños y daños informáticos	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.	
		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.	
Falsificación informática	Arts CP 388-390, 399bis, 400 y 401	ATAQUES INFORMÁTICOS	Ninguna	
		FALSIFICACIÓN DE MONEDA, SELLOS Y EFECTOS TIMBRADOS FABRICACIÓN/ TENENCIA DE ÚTILES 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	ESTAFAS	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 BANCARIAS ESTAFAS CON TARJETAS DE CRÉDITO, DÉBITO Y CHEQUES DE CUBIERTA OTRAS ESTAFAS	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 sexuales	Arts. CP 181, 183.1, 183 bis, 184, 185, 186, 189	EXHIBICIÓN SMO	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	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.	
		ACOSO SEXUAL	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.	
		ABUSO SEXUAL	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.	
		CORUPCIÓN DE MENORES/INCAPACITADOS	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.	
		PORNOGRAFÍA DE MENORES	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.	
		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	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.	
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	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 y coacciones	Arts 169 a 172 y 620 del CP 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	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.	
		COACCIONES	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.	



SECRETARÍA DE ESTADO
DE SEGURIDAD

GABINETE DE COORDINACIÓN
Y ESTUDIOS

