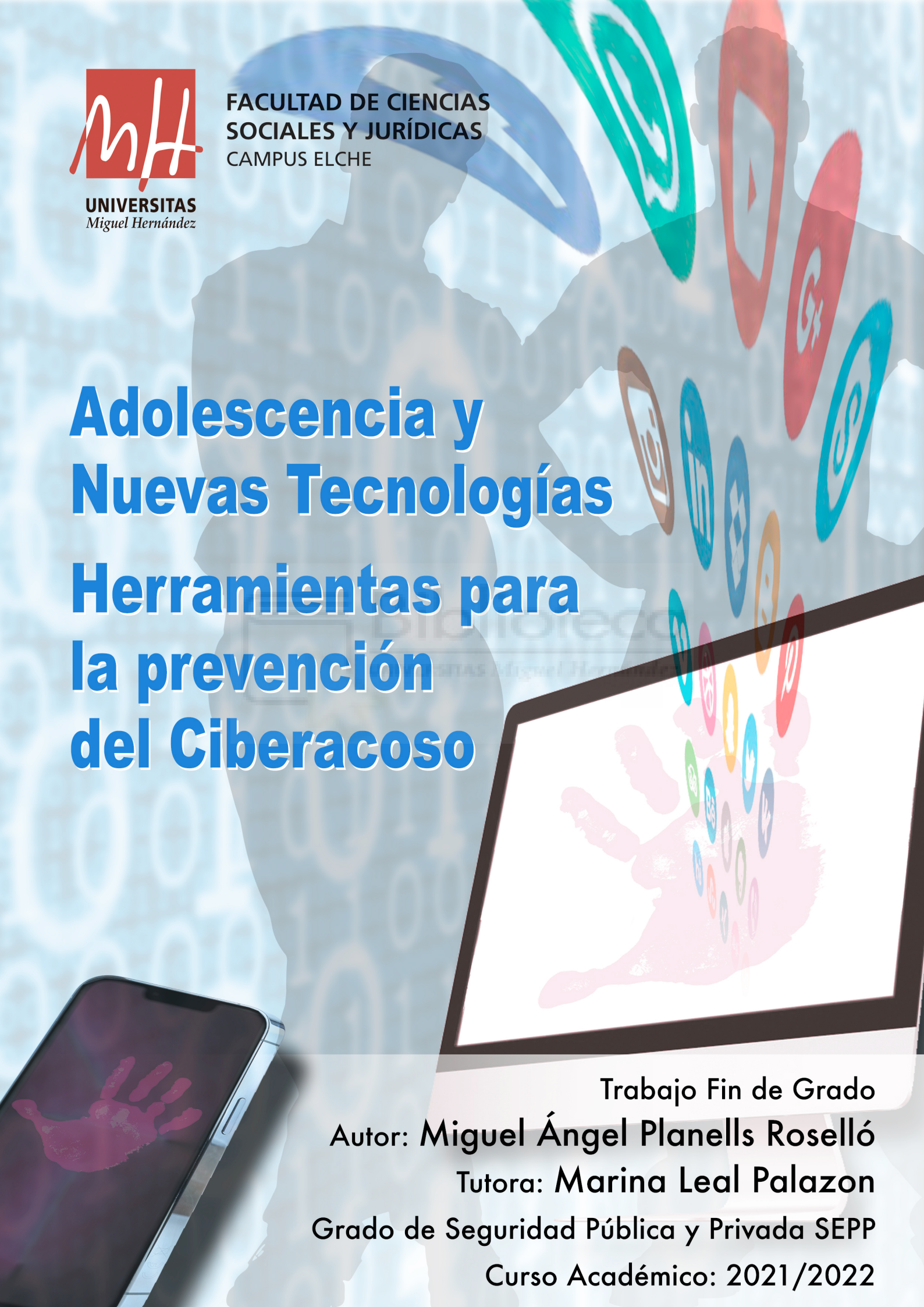
UNIVERSITAS
Miguel Hernández

FACULTAD DE CIENCIAS
SOCIALES Y JURÍDICAS
CAMPUS ELCHE

Adolescencia y Nuevas Tecnologías

Herramientas para la prevención del Ciberacoso



Trabajo Fin de Grado

Autor: Miguel Ángel Planells Roselló

Tutora: Marina Leal Palazon

Grado de Seguridad Pública y Privada SEPP

Curso Académico: 2021/2022

| 1. ÍNDICE |

| 2. RESUMEN |

Las nuevas tecnologías… un concepto fundamental en la sociedad actual que nos está llevando a un mayor bienestar y al cambio de nuestras rutinas de vida, sobre todo con la conectividad e inmediatez que nos aportan los dispositivos móviles. Esta conectividad se ve reforzada con otros sistemas tecnológicos como el denominado “Internet de las Cosas” que permite el almacenamiento de datos en un servidor remoto (nube) y el Big Data que nos posibilita el tratamiento de gran cantidad de datos.

Pero estas tecnologías también conllevan peligros, sobre todo para la población adolescente, ávida de nuevas experiencias y con poca percepción del riesgo, que les lleva a experimentar, mediante las redes sociales, relaciones que pueden ser tóxicas hasta convertirse en víctimas de delitos como la Violencia de Género o el Ciberacoso. Esta nueva forma de comunicación, nos roba privacidad y se escuda en el anonimato.

Para profundizar en el alcance de estos peligros se ha realizado una revisión bibliográfica, relacionada con las palabras clave, también se ha procedido a un sondeo de datos para abordar este problema mediante el análisis de las nuevas formas del ciberacoso, las Redes Sociales y sus herramientas, además de analizar e informar de cómo prevenir o afrontar cuando se es víctima de estos delitos relacionados con las nuevas tecnologías como el Ciberstalking, el Ciberbulliyng, el Sexting y el Grooming.

Por todo ello, en un mundo globalmente comunicado, y creciendo exponencialmente el uso de Internet año tras año, se incide en la prevención, educación y formación del conocimiento de la configuración de las distintas herramientas tecnológicas con el objetivo de impedir intrusiones con perfiles más “seguros”. Todo esto focalizado en el sector juvenil, que son la franja de edad más afectada por esta lacra que intentamos erradicar con los numerosos recursos creados por las Administraciones Gubernamentales.

PALABRAS CLAVE:

Ciberacoso; Nuevas Tecnologías; Violencia de Género; Redes Sociales; Adolescencia.

| 2. ABSTRACT |

New technologies... a fundamental concept in today's society that is leading us to greater well-being and changing our life routines, especially with the connectivity and immediacy that mobile devices provide us. This connectivity is reinforced with other technological systems such as the so-called "Internet of Things" which allows data storaged on a remote server (cloud) and Big Data that enables us to process large amounts of data.

But these technologies also carry dangers, especially for the adolescent population, eager for new experiences and with little perception of risk, which leads them to experience, through social networks, relationships that can be toxic to the point of becoming victims of crimes such as Violence Gender or Cyberbullying. This new form of communication steals our privacy and hides behind anonymity.

To delve into the scope of these dangers, a bibliographic review has been carried out, related to keywords, a data survey has also been carried out to address this problem through the analysis of new forms of cyberbullying, Social Networks and their tools, in addition to analyzing and reporting on how to prevent or deal with when you are a victim of these crimes related to new technologies such as Cyberstalking, Cyberbullying, Sexting and Grooming.

For all these reasons, in a globally connected world, and with use of the Internet growing exponentially year after year, emphasis is placed on prevention, education and training in the knowledge of the configuration of the different technological tools to prevent intrusions with profiles more "insurance". All this focused on the youth sector, who is the age group most affected by this scourge that we try to eradicate with the numerous resources created by Government Administrations.

KEYWORDS:

Cyberbullying; New Technologies; Gender Violence; Social Networks; Adolescence.

| 3. INTRODUCCIÓN |

Este Trabajo de Fin de Grado, (TFG) del Grado de Seguridad Pública y Privada de la Universidad Miguel Hernández de Elche (UMH) pretende analizar las nuevas formas de violencia de género que se están generando sobre todo en la etapa de la adolescencia como consecuencia del avance tecnológico que estamos viviendo. Mucho han cambiado las cosas desde que en los años 90 se introdujeron a nivel doméstico las tecnologías de la Información y la Comunicación **(TIC),** transformando la forma de relacionarnos en todos los ámbitos de nuestras vidas, por la facilidad de acceso para el público con pocos conocimientos tecnológicos y por el abaratamiento de los sistemas electrónicos hasta la actualidad, en que se suma de forma exponencial estas tecnologías pero siendo más eficientes y rápidas, sobre todo desde la irrupción de los **teléfonos inteligentes** o *smartphones,* que nos permiten utilizar todo el potencial del dispositivo como redes sociales, aplicaciones varias con conexión permanente… desde cualquier lugar y tiempo para poder seguir de manera instantánea cualquier cambio o publicación de nuestros contactos. Aunque ya en 2021 las TIC han influido en todos los ámbitos de la sociedad y en todo el mundo, llegando también a cambiar el modo de agresión entre los adolescentes. Como resultado, cada vez resultan más familiares conceptos como el ciberacoso, el *phishing*, el *grooming* o el *sexting*. Estos nuevos delitos han sido ampliamente descritos en la literatura. *(I. Rodríguez-Rodríguez, 2019).*

En la actualidad, estamos viviendo una 3º Revolución Industrial con motivo del uso diario y exagerado, sobre todo por la juventud, que hacemos de los dispositivos tecnológicos destacando el uso del teléfono móvil inteligente.

El teléfono móvil ha superado con creces la funcionalidad básica para la que fue concebido, se ha convertido, especialmente entre los jóvenes, en un instrumento que crea dependencia y que permite cada vez más opciones que favorecen ataduras.

“Internet y móviles, entre otros medios, ocupan un espacio importante en el proceso de socialización, influyendo en los comportamientos y actitudes” *(Levis, 2002).*

Uno de los principales problemas es que la tecnología es dinámica y rápida por lo que las aplicaciones de estos teléfonos inteligentes y los dispositivos electrónicos a nivel general, producen continuamente datos por lo que en pocos años nuestro día a día ha cambiado y así está previsto que continúe. Es decir, estamos en el período del **BIG DATA** que se define como el conjunto de tecnologías y disciplinas que se encargan del almacenamiento y procesamiento de grandes cantidades de información.

Toda esta espiral de rapidez vertiginosa se observa en las características de la información que mueve el BIG DATA, lo que se denomina como las cinco uves (5V´s) por sus características: Volumen, Velocidad, Variedad, Valor y Veracidad.

Para el procesamiento de los datos en el BIG DATA se encargan la Estadística, la Matemática y la Informática haciendo uso de la Minería de Datos, el Aprendizaje Automático (Machine Learning), la Computación Paralela, la Inteligencia Artificial, Deep Learning… *Bagha, A., & Madisetti, V. (2019).*

Internet y las **redes sociales** se han convertido en el principal medio para relacionarse socialmente. "Son sitios webs en donde es frecuente crear perfiles mostrando imágenes, normalmente fotografías u otros. Los adolescentes ven en estas redes la oportunidad de mostrar una imagen de sí mismos, de sus hobbies, de sus gustos, etc. con la intención de encontrar aceptación y sentirse integrados en su grupo de iguales", *(Martín Montilla, et al., 2016)* son la franja de edad más vulnerable para los delincuentes de los entornos virtuales porque a esas edades, con sus experiencias, están forjando la identidad que les va a caracterizar y formar su carácter en el futuro.

"Las redes sociales definen la forma de ser y de aprender, siendo especialmente relevantes en la adolescencia" *(Blanco Ruiz, 2014).*

Las redes sociales se han convertido en auténticas plataformas en las que se puede compartir y buscar todo tipo de información. "La ventaja de dichas redes como medio de comunicación sencillo, gratuito e inmediato, ha supuesto un cambio en los hábitos de comportamiento" *(Urueña, 2011)*. Aunque también tienen su punto negativo y es la proliferación de la **violencia de género** mediante un uso inapropiado de la tecnología. Esto "puede dar lugar a algunos peligros, pudiendo ser utilizados para molestar, dañar o perjudicar de forma intencionada a otras personas o grupos" *(Álvarez-García et al., 2017)*. Nos permite tener una distancia con la víctima por lo que el autor se siente en el anonimato, como detrás de una máscara, en la cual se percibe oculto, con una mayor sensación de impunidad, sin comprometer la identidad que "estimula al agresor a realizar una difusión rápida de la información por toda la red" *(Garaigordobil, 2001)* y de sentirse con el derecho de menoscabar la integridad y dignidad de otra persona, llegando al comportamiento que se ha definido como **ciberacoso o ciberbullying.**

El ciberacoso comienza a investigarse en Estados Unidos en el año 2000. *(Finkelhor, Mitchell & Wolak, 2000; Slonje & Smith, 2008; Hinduja & Patchin, 2008).*

Se define como la “agresión intencional por parte de una persona o grupo a través de dispositivos electrónicos y de forma repetitiva a lo largo del tiempo, a otra persona que no puede defenderse fácilmente”. *(Peter IK, Petermann F. 2018).*

Debemos prestar especial atención a las **víctimas** más vulnerables del ciberacoso, que son el grupo de personas más expuestos al uso de Internet y las redes sociales siendo, como hemos dicho, el segmento de los adolescentes, siendo así las principales víctimas y quienes más lo sufren.

Un mal uso de las redes sociales puede derivar en un riesgo que tiene consecuencias en las víctimas como: padecer “problemas psicosomáticos, depresión, estrés, bajo rendimiento escolar, dificultades para relacionarse con sus pares, e incluso autolesiones e ideación suicida”. *(John A, Glendenning AC, Marchant A, Montgomery P, Stewart A, Wood S, et al. 2018).*

En el ciberacoso existen “tres roles: perpetradores, víctimas o espectadores”. *(Espelage D, Rao M, Craven R. 2015).*

Por otra parte, está lo que se denomina como **Internet de las cosas** (IoT: Internet of Things) se refiere a cosas que tienen identidades únicas y están conectadas a Internet pudiendo enviar la información a servidores centralizados o a la “nube” para su procesamiento.

El World Economic Forum (WEF) ha designado esta revolución de los datos como la 4º Revolución Industrial que se caracteriza “por la fusión de tecnologías que está desdibujando las líneas entre las esferas física, digital y biológica, no habiendo precedentes sobre la velocidad de cambio, transformación y dinamismo de los avances que está experimentando el mundo actual que presagian la transformación de sistemas enteros de producción gestión y gobierno”.

Todos estos avances: Internet de las cosas, el Big Data, Aprendizajes automáticos… “afectan y ayudan a establecer estrategias al amplio abanico de posibilidades que existen para combatir la violencia de género” *(Harikiran G. C., Menasinkai K. y Shirol S. 2016),* pudiendo planificar de una manera adecuada las políticas públicas con el objetivo de realizar una eficiente previsión de los recursos públicos, anticipando campañas de prevención y ejecución contra todo tipo de Violencia de Género.

“Todo lo que sea recopilación de información mediante los sistemas tecnológicos actuales es clave para construir una sólida base de datos mediante la realización de encuestas, estadísticas de los órganos oficiales o monitorización automática que transmitan toda esta información a la nube y en la cual se pueda utilizar de forma eficaz toda su información interna con el fin de recoger toda la información biosensorial del estado de un individuo guardándose los datos en remoto gracias al concepto IoT”. (*Shaik, K. Bogaraju S y Vadepu S. 2017)*.

"La telemonitorización implicará la continua recolección de datos de las víctimas para identificar claramente su condición, ubicación exacta e indicios de riesgos". *(Wu J, Feng Y, y Sun P, 2018)*.

Todos estos avances biométricos pueden permitir una vigilancia permanente de la víctima para monitorizar todos sus estados emocionales para así detectar, anticipar y prevenir situaciones de riesgo gracias a las soluciones tecnológicas enunciadas anteriormente y todo ello a través de aplicaciones mediante los smartphones.

Viendo la gravedad del problema y siendo que el ciberacoso va en aumento, los poderes públicos han elaborado dos versiones del Plan Estratégico de Infancia y Adolescencia (PENIA), en la actualidad ya está licitada la 3º versión del Plan.

En el II Plan cita en su objetivo 3.- "Impulsar los derechos y la protección de la infancia con relación a los medios de comunicación a las tecnologías de la información en general". Se regula porque hoy en día los niños nacen ya con un entorno virtual y cada vez, a edades más tempranas, ya dominan con soltura los recursos tecnológicos como los móviles, ordenadores… continuando su uso en la **adolescencia** en que los utilizan, a veces, de forma excesiva, sin control y límite, demostrando una gran capacidad de dominio de la competencia digital pero sin control de la misma lo que lleva a numerosos riesgos porque los menores, en la franja de la adolescencia "presentan una baja percepción del ciberacoso" *(Quesada, 2015).*

Por otra parte, en muchos casos, "los menores no cuentan con un apoyo educativo de iniciación al mundo tecnológico y muchos de ellos lo aprenden por espontaneidad. Por ello, no tienen un aprendizaje del concepto de la privacidad, una formación que les advierta de los peligros de la utilización de ciertos datos." *(Montoro y Ballesteros, 2016).*

El problema viene dado principalmente porque la tecnología es muy dinámica, avanza muy rápido y la mayoría de los padres/tutores/educadores que tienen a cargo a adolescentes no son capaces de absorber tanto cambio con las nuevas tecnologías, por tanto, los que deben ser "controlados" van por delante de los "controladores", pudiendo aplicar el paralelismo de que "el mal siempre va por delante del bien", con sus consecuencias negativas para el menor.

Uno de los objetivos es que los mismos docentes sean conscientes del problema y se les eduque igualmente a identificar las causas y señales de este tipo de agresiones digitales para poder luchar contra este tipo de maltrato que tanto está dañando a las nuevas generaciones con consecuencias irreversibles como el suicidio de los adolescentes por no saber qué hacer y cómo afrontar este tipo de situaciones.

| 4. OBJETIVOS |

- Analizar las nuevas formas del ciberacoso.

- Estudiar la evolución del futuro de internet, redes sociales y en consecuencia las relaciones sociales.

- Analizar las nuevas herramientas tecnológicas para el conocimiento de los adolescentes y que conozcan cómo usar estas herramientas con el fin de prevenir que sean víctimas de delitos.

- Analizar a las víctimas de estos delitos e informarles de los protocolos para evitar nuevas agresiones: qué deben hacer, cómo deben actuar y dónde deben dirigirse.

| 5. MARCO TEÓRICO |

5.1 La violencia de género:

Para entender en gran medida esta investigación es necesario saber qué es y cómo definen las principales organizaciones la Violencia de Género (VIOGEN), concepto que ha adquirido mucha importancia en todas las civilizaciones desarrolladas por sus consecuencias en la sociedad, convirtiéndose en una lacra social que se debe educar y prevenir para erradicarla.

Según la **Asamblea de la Organización de Naciones Unidas** (**ONU)** en la Declaración sobre la Eliminación de la Violencia contra la Mujer, aprobada en 1993**,** define la VIOGEN como: todo acto de violencia basado en la pertenencia al sexo femenino que tenga o pueda tener como resultado un daño o sufrimiento físico, sexual o psicológico para la mujer, así como las amenazas de tales actos, la coacción o la privación arbitraria de la libertad, tanto si se producen en la vida pública como en la vida privada.

En España se regula mediante la **Ley Orgánica 1/2004 de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Género** en la cual en su artículo 1.1 y 1.3 define la VIOGEN como:

1.1. La presente Ley tiene por objeto actuar contra la violencia que, como manifestación de la discriminación, la situación de desigualdad y las relaciones de poder de los hombres sobre las mujeres, se ejerce sobre éstas por parte de quienes sean o hayan sido sus cónyuges o de quienes estén o hayan estado ligados a ellas por relaciones similares de afectividad, aun sin convivencia.

1.3. La violencia de género a que se refiere la presente Ley comprende todo acto de violencia física y psicológica, incluidas las agresiones a la libertad sexual, las amenazas, las coacciones o la privación arbitraria de libertad.

Cabe destacar, la referencia que hace la **Organización Mundial de la Salud (OMS)** sobre la Violencia de Género en un Informe, en el cual manifiesta que es un problema de salud global de proporciones epidémicas. (Organización Mundial de la Salud [OMS]. 2013, 20 de junio).

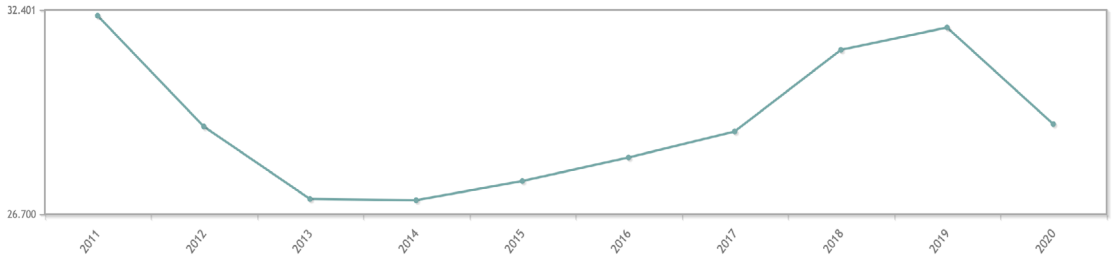
Como datos epidemológicos, el Instituto Nacional de Estadística (I.N.E.), en la estadística de Violencia Doméstica y de Género del año 2020, refleja que:

El **número de mujeres víctimas de Violencia de Género desde 2011-2020** disminuyó un 8,4% en el año 2020, hasta 29.215. La tasa de víctimas de violencia de género fue de 1,4 por cada 1.000 mujeres de 14 y más años.

En el siguiente gráfico se puede observar la evolución de las víctimas de Violencia de Género desde el año 2011 hasta el año 2020.

Figura 1:

Estadística de Violencia de Género desde el 2011-2020.



Nota. (INE: https://www.ine.es/consul/serie.do?d=true&s=VGD25&c=2&)

En el año 2011 se registraron un total de 32.242 personas víctimas de Violencia de Género, disminuyendo progresivamente hasta llegar al año 2014 a 27.087 víctimas. Desde 2014 vuelve a subir de forma moderada con una media de 700 casos más hasta el año 2017 que se sitúa en 29008 víctimas llegando hasta el 2018 con 31.286 casos, es decir con 500 casos más sobre la media, volviendo a subir ligeramente en el año 2019 con 31911 casos y bajar finalmente, y de forma brusca, en el año 2020 a 29.215, situándose en valores del año 2017.

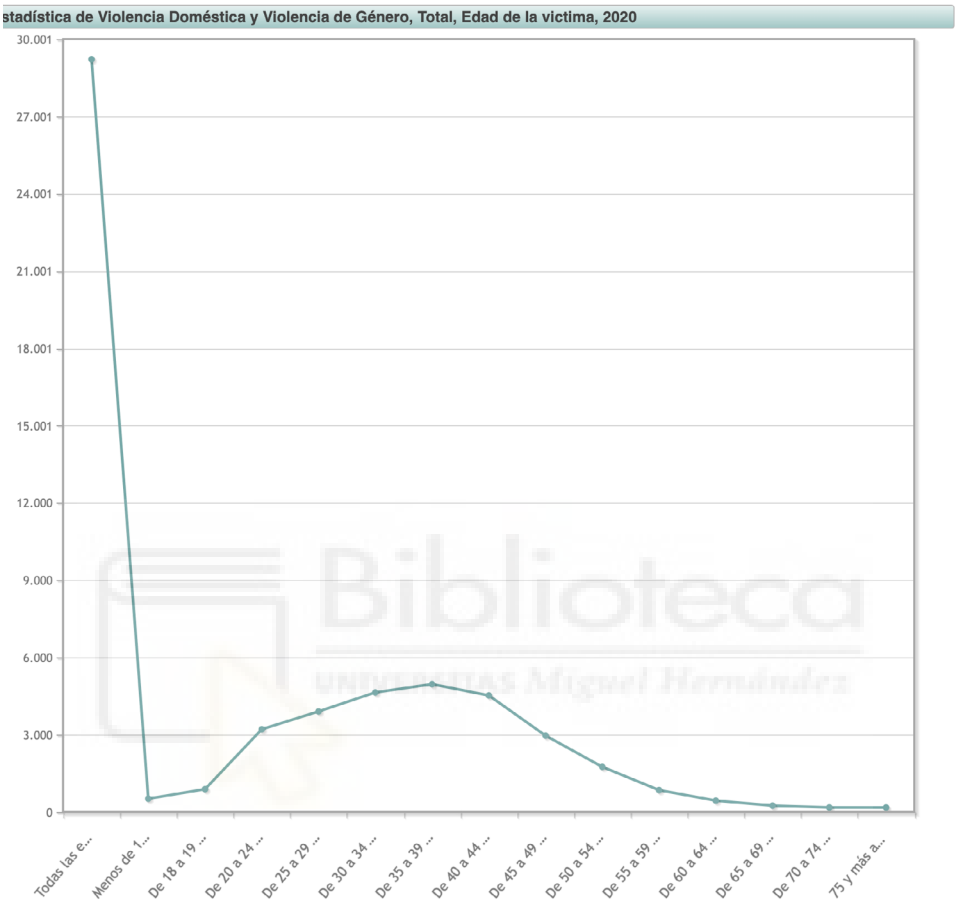
Así se observa que el descenso brusco del año 2020 puede ser debido a la afectación de la pandemia a nivel mundial del COVID-19.

Con estos datos podemos analizar la evolución de las víctimas y estudiar los motivos del por qué aumenta o disminuyen las cifras para poder establecer mediante métodos eficaces la protección a las víctimas de Violencia de Género e informarles de los protocolos con el fin de evitar nuevas agresiones.

En este gráfico podemos valorar **la edad de las víctimas de violencia de género durante el año 2020.**

Figura 2:

Estadística de las víctimas de Violencia de Género y Violencia Doméstica en el año 2020.



Nota. (INE, 2022).

El grupo de edad que presenta más casos de ser víctima de Violencia de Género en el año 2020 se sitúa en la franja de los 35-39 años con 4559 casos, disminuyendo progresivamente según vamos avanzando en los tramos de edad hasta llegar a no más de 100 casos en la franja de edad de más de 75 años de edad, en que prácticamente no existen casos de Violencia de Género.

Respecto a la edad adolescente, que es la que más interesa en este análisis, cabe destacar los 514 casos en los menores de edad, es decir, menores de 18 años, subiendo progresivamente según van avanzando los años situándose en los 884 en la edad en la franja de 18-19 años, apreciando que hay una subida considerable en la franja de los 20-24 años de edad hasta los 3208 casos.

A partir de aquí, ya en la franja que se puede llamar juventud sube de forma más considerada entre los 25-29 años situándose la cifra cercana a 4000 casos hasta llegar al tramo de edad comentado de los 35-39 años que es la franja con más víctimas de Violencia de Género en el año 2020 con 4559 casos.

Respecto a la franja de edad entre 25-29 años existen unos datos alarmantes sobre el maltrato. Según un estudio del año 2015 sobre 'La percepción de la violencia de género en la adolescencia y la juventud', elaborado por el Centro de Investigaciones Sociológicas para la Secretaría de Estado de Servicios Sociales e Igualdad afirma que: "El 33%, de los jóvenes españoles entre 15 y 29 años considera "inevitable" o "aceptable" controlar los horarios de su pareja, impedir que vea a su familia o sus amistades, no permitir que estudie o trabaje o decirle lo que puede y no puede hacer". (*De Miguel, V. 2015).*

Eso es que 1/3 del total de jóvenes en esta franja de edad ve aceptable una violencia de "control". En la mayoría de casos los jóvenes rechazan la violencia física, sexual y verbal pero no lo ven igual, empezando por las mismas víctimas, sobre la violencia ejercida con el control porque se asocia por parte de las chicas que ese "control" no es violencia sino es como una prueba de amor por parte del hombre.

Con esta información percibimos que nos debemos centrar en formar e informar sobre todo a la juventud para educarlos con el objetivo fundamental que sean en un futuro conscientes de lo que implica la Violencia de Género y que al llegar a la edad adulta conozcan los protocolos para evitar las relaciones sociales tóxicas que desembocan en maltrato y así disminuir a corto plazo esa meseta central que nos muestra esta gráfica.

5.1.1. Tipos de violencia de género:

Se clasifican en Violencia:

Física: es la invasión del espacio físico de una persona, de manera no accidental, realizada de diferentes maneras. A través del contacto directo con el cuerpo (golpes, empujones, etc.), limitando los movimientos de la persona (encerrándola, mediante lesiones que impidan el movimiento, muerte, etc.), y/o realizando actos violentos ante la persona (romper objetos, golpear objetos, maltratar animales, destruir cartas o fotos, etc.).

Las consecuencias de esta violencia son los daños físicos directamente derivados de las lesiones producidas, así como daños emocionales que se generan por la vivencia de este tipo de violencia. Además de estos daños, el padecimiento de violencia física afecta al espacio social e intelectual de la persona, reflejándose en sentimientos de vergüenza ante el entorno, agudizándose esto

si las lesiones físicas son visibles, y en una distorsionada interpretación de los hechos, que en ocasiones se minimizan para poder asimilarlos.

Psíquica: es el tipo de violencia en la que se utilizan palabras y/o ruidos para afectar y dañar a la mujer, hacerla creer que está equivocada o hablar en falso de ella. Estos actos tienen como objetivo el menosprecio y control de la mujer mediante el daño de su estabilidad emocional. Se impone de manera directa por medio de amenazas de ejercer violencia física, humillando a través del insulto o, de forma más sutil, haciendo valer la supremacía y el poder masculino.

La violencia física y la psíquica, por lo general las más nombradas y visibles, son también las que tienen una dimensión más amplia. La violencia física engloba todas las demás y, por ejemplo, la violencia económica, que a continuación describimos, puede considerarse un tipo de violencia psíquica. Lo que es claro es que todas ellas tienen como finalidad el control de la mujer por parte de su pareja.

Económica: afecta a la subsistencia económica y se puede expresar por acción u omisión. Se manifiesta a través de limitaciones encaminadas a controlar el ingreso de sus percepciones económicas y, por lo tanto, el control del desenvolvimiento social.

Sexual: aunque se considera un tipo de violencia física, merece una mención específica debido a la severidad de los actos incluidos en este tipo de maltrato. Esta violencia afecta a todas las esferas de la víctima a través de la degradación del cuerpo y su sexualidad, mediante la invasión del espacio más íntimo. Como en las anteriores, distinguimos dos formas de llevarla a cabo: la violencia sexual verbal (jactarse de tener otras mujeres, obligar a visualizar películas pornográficas, etc.) y las violaciones, es decir, forzando a la mujer a mantener relaciones sexuales sin su consentimiento, con tocamientos, exhibiciones,etc.

Ambiental: se entiende por violencia ambiental cualquier acto, no accidental, que provoque o pueda producir daño en el entorno al objeto de intimidar. Por ejemplo, dar golpes a puertas, romper cosas, destruir objetos con especial valor sentimental para la mujer, maltratar a los animales domésticos, desordenar o ensuciar a propósito.

Guía Didáctica de Violencia de Género en atención primaria (P.39 y 40)

5.1.2. El ciclo de la violencia de género

Comprender el círculo de la violencia es el primer paso para romperlo. La inequidad de género y la discriminación son las causas raíces de la violencia contra las mujeres, derivado de las normas sociales que prescriben los roles que mujeres y hombres deben desempeñar en la sociedad, generando un desequilibrio de poder entre ellos. *(María de la Luz Vázquez Hernández, 2018)*.

La violencia contra las mujeres se produce de una forma cíclica, intercalando periodos de calma con situaciones límite que ponen en riesgo la propia vida. Tal dinámica se convierte en muchos casos en un vínculo de dependencia emocional y posesión difícil de romper en la pareja.

Figura 3:

Adaptación del Ciclo de la violencia en pareja del Instituto de Mujeres de Xalapa (2020).

Nota. Basada en la teoría de Leonore Walker, (1979). https://www.facebook.com/InstitutoMujeresXalapa/photos/pcb.3661883377187380/3661882037187514/

La investigadora estadounidense Leonore Walker, *(Leonore Walker, 1979)*, describió el ciclo de la violencia, a partir de los testimonios de mujeres maltratadas con las que trabajó y observó que muchas de ellas describían patrones similares en el proceso de maltrato y que éste tenía una forma cíclica, lo que nos ayuda a entender cómo se reproduce la violencia en la pareja.

Este modelo plantea que la violencia de pareja comprende tres fases:

Acumulación de tensión: Se caracteriza por una escalada gradual de la tensión, donde la hostilidad del hombre va en aumento sin motivo comprensible y aparente para la mujer. Las reacciones agresivas de la pareja son impredecibles. Se intensifica la violencia verbal y pueden aparecer los primeros indicios de violencia física. Se presentan como episodios aislados que la mujer cree que puede controlar y que desaparecerán. La tensión aumenta y se acumula. La

formación de la autoridad y ciertas asignaciones, aunque no sean muy explícitas al principio, comienzan a aparecer y la mujer siempre justifica, acomodándose de alguna manera a la situación, precisamente por el falso control que cree poseer de la situación.

Explosión o agresión: Se producen las agresiones físicas, psicológicas y sexuales. El grado de impacto de lo que ha ocurrido, ambivalencia en los sentimientos, llega a su punto máximo. Es en esta fase donde la mujer suele denunciar o pedir ayuda.

Calma, reconciliación o luna de miel: En esta fase, el agresor manifiesta que se arrepiente y pide perdón a la mujer. Utiliza estrategias de manipulación afectiva (regalos, caricias,disculpas, promesas) para evitar que la relación se rompa. La mujer a menudo piensa que todo cambiará (esperanza de cambio). En la medida en que los comportamientos violentos se van afianzando y ganando terreno, la fase de reconciliación tiende a desaparecer y los episodios violentos se aproximan en el tiempo.

El ciclo de la violencia es muy frecuente en las relaciones de pareja en las que se da maltrato, pero es difícil de observar en algunos casos donde hay una situación continua de frustración y amenaza pero donde sólo de forma ocasional aparece la agresión física. En esta llamada forma moderada de violencia serían más difíciles de detectar las fases anteriormente descritas que en las formas más severas de abuso.

En todo este proceso cíclico la mujer sufre lo que Seligman denominó “indefensión aprendida”, *(Seligman, 1975),* que permite explicar muchos de los cambios psicológicos responsables del mantenimiento de la relación violenta. Los acontecimientos violentos entremezclados con episodios de ternura y arrepentimiento actúan como estímulo aversivo administrado al azar que, a largo plazo, provocan en ella una falta de relación entre su comportamiento y las consecuencias del mismo, por lo que queda paralizada y, posteriormente, ya en intervención, la lleva a verbalizar que no sabía qué hacer, ni a qué se debía lo que ocurría. *Guía Didáctica de Violencia de Género en atención primaria (pp.28-29).*

5.2 Nuevas tecnologías de la Información y la Comunicación (TIC)

La Real Academia Española de la Lengua define “Internet” como: “Red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación”.

La palabra “Web” se define como: “red informática” y red se define como: “conjunto de ordenadores o de equipos informáticos conectados entre sí que pueden intercambiar información”. Sobre el año 2000, la llegada del concepto

Web 2.0 revolucionó el concepto de red, las formas de comunicación y adoptó nuevas formas de colaboración y participación. La plataforma Web 1.0 de los años 90 era de sólo lectura y la Web 2.0 pasó a ser de lectura y escritura. Posteriormente, con la Web 3.0 las páginas web se relacionan de manera semántica, añadiendo metadatos, mejorando la búsqueda para encontrar información en la web al comprender el significado de las palabras. Actualmente, nos encontramos en la fase Web 4.0, siendo la etapa de las búsquedas por voz mediante todos los dispositivos inteligentes. Ahora internet puede funcionar de forma predictiva, no sólo recibiendo órdenes del usuario, sino también mediante el empleo de la inteligencia artificial que puede anticipar solicitudes del usuario, así como predecir comportamientos de ese usuario en el futuro. En una etapa no muy lejana, llegará la fase que se está nombrando como la Web 5.0, refiriéndose a la tecnología 5G, que nos permitirá navegar por Internet 10 veces más rápido de lo que es en la actualidad. *(Joaquín Romero, 2020).*

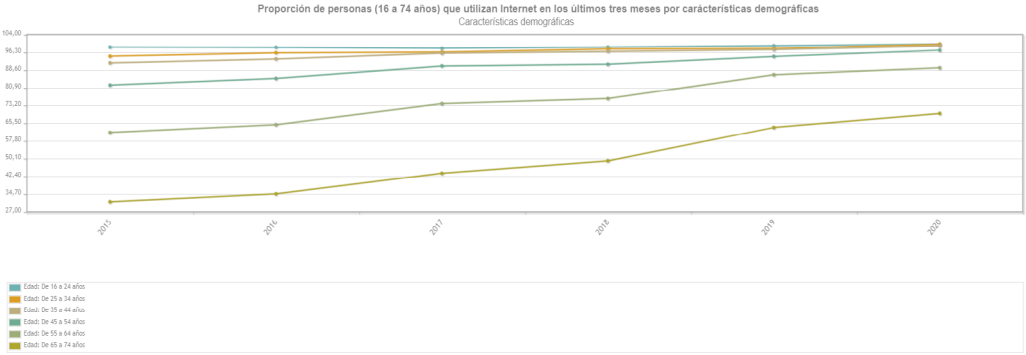
Estamos en una sociedad en la que cada vez es más frecuente la existencia de las nuevas tecnologías en los hogares familiares, en los centros educativos, en los puestos de trabajo y en cualquier ámbito de nuestro entorno, se predispone que cada vez más emerjan generaciones de personas que son dependientes o que necesitan un continuo contacto con las TICs. Este acontecimiento, en el que se promueve la convivencia con la tecnología ha provocado una nueva generación, denominada por Prensky (2001) como los “nativos digitales”, refiriéndose a aquella primera generación que ha nacido y ha crecido con las nuevas tecnologías. Esta generación confluye con otro grupo de personas que no ha crecido con las tecnologías pero que en un momento de sus vidas ha tenido la oportunidad u obligación de tener contacto con ellas. A este segmento de población, Prensky (2010) los denomina “inmigrantes digitales” refiriéndos a aquellos/as que no nacieron en el mundo digital, pero que en algún momento más avanzado de sus vidas han quedado fascinados/as y en su gran mayoría se han tenido que adaptar al uso de las nuevas tecnologías. *(Verdejo Espinosa, 2015).*

Usuarios de internet a nivel nacional

Para ver la trascendencia que están teniendo las T.I.C. en la actualidad sólo hay que ver las estadísticas que realiza el I.N.E., donde observamos como dato más destacable que el uso de Internet en España en los últimos 3 meses alcanza ya prácticamente a la totalidad de la población joven, entre los 16 y los 24 años, con un 99,7 % de usuarios activos, reflejados en la siguiente Tabla donde se reseña los usuarios de Internet a nivel nacional por edades y sexo.

Figura 4:

Estadística de usuarios de internet a nivel nacional en los últimos 3 meses.



Nota. (INE: https://www.ine.es/jaxi/Datos.htm?tpx=48784#!tabs-grafico).

Sin embargo, la mayor subida de los usuarios se produce en la franja de edad de los 65-74 **años de edad que pasa de un** 31,7 % en el año 2015 a un 69,7 % en el año 2020. Datos que muestran que la brecha en el acceso a Internet se reduce drásticamente, pronosticando que un futuro toda la población usará Internet como herramienta de consulta diaria.

También cabe destacar el tramo de edad de los 55-64 años de edad que pasa de un 61,4 % en el año 2015 a un 89,5 % en el año 2020, con ello podemos ratificar mediante estos datos, las palabras de Prensky el cual afirmaba que los "inmigrantes digitales" se quedan fascinados por las nuevas tecnologías.

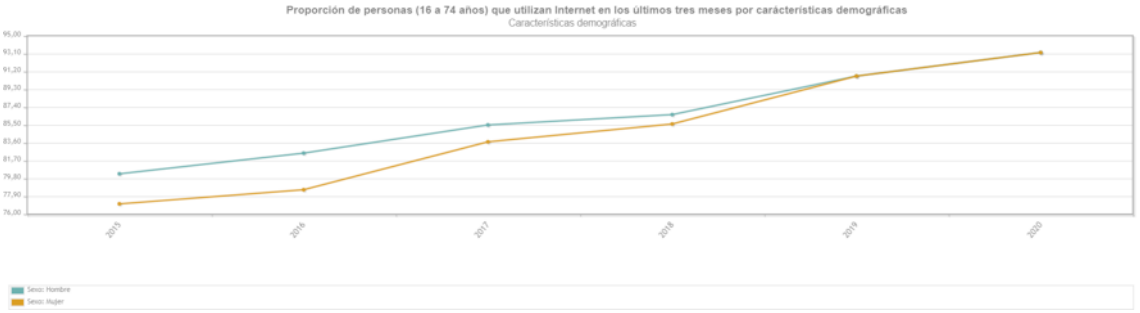
Por lo que respecta al resto de edades se observa que en el año 2015 entre las franjas de edades adultas y jóvenes había 6,9 puntos de diferencia, situándose como valor el 91,6 % la franja de edad de los 35 hasta los 44 años hasta el 98,5 % en la franja de edad de los 16 hasta los 24 años. Mientras que en el año 2020 esa diferencia de los usuarios que han utilizado Internet durante los últimos tres meses se ha reducido a 0,8 puntos de diferencia, situándose con un valor de 99,0 % la franja de edad de los 35 hasta los 44 años, y un valor de 99,8 % en la franja de edad de los 16 hasta los 24 años. Estos datos muestran que entre la población adulta y joven ya se ha igualado el uso de Internet siendo consumidores de la red la práctica totalidad de la población entre 16 y 44 años de edad.

Con esta información percibimos que nos debemos centrar en formar e informar sobre todo a la juventud, indistintamente tanto hombres como mujeres, que es la franja de edad más activa en el uso de las herramientas tecnológicas con el objetivo fundamental que sean conscientes sobre los peligros y riesgos de Internet para que en un futuro puedan detectar y prevenir ser víctimas de delitos a través de estos medios.

Usuarios de internet a nivel nacional por sexo.

Figura 5:

Estadística de usuarios de internet a nivel nacional por sexo



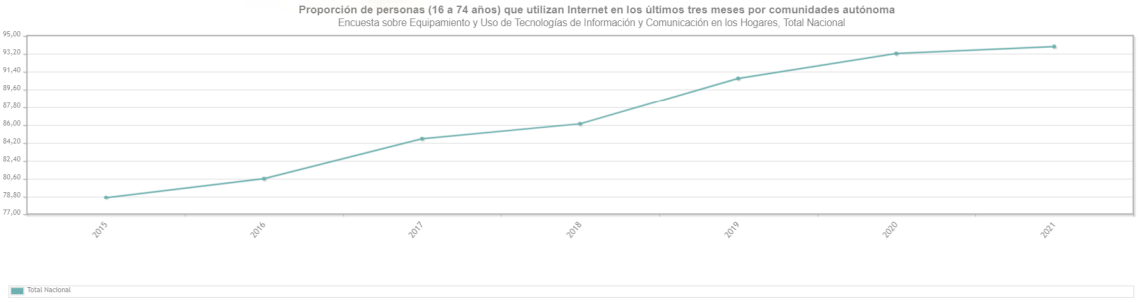
Nota. (INE: https://www.ine.es/jaxi/Datos.htm?tpx=48784#!tabs-grafico).

Respecto al uso de internet por edades se observa que en el año 2015 las mujeres utilizaban menos internet que los hombres con un 77,1% de las mujeres frente a un 80,3% de los hombres, subiendo ambos sexos progresivamente los siguientes años, con un mayor crecimiento por parte de las mujeres hasta el año 2020, en que el % del uso de internet se ha igualado entre los dos sexos llegando a un 93,2% de usuarios tanto en hombres como en mujeres.

Población con acceso a Internet.

Figura 6:

Estadística de población con acceso a Internet.



Nota. (INE: https://www.ine.es/jaxiT3/Datos.htm?t=45877#!tabs-grafico).

La proporción de personas de 16 a 74 años de edad que tienen acceso a Internet asciende en el año 2021 a 93,9% mientras que en el 2015 era del 78,7 %, siendo las comunidades de Madrid y Cataluña los que tienen mayor acceso de población a Internet, situándose la Comunidad Valenciana a un nivel por encima de la media, siendo de un 94,8%.

En el año 2015 Galicia era la comunidad autónoma con menos usuarios conectados a Internet con un 71,9%, siguiendo la misma dinámica en el año 2020

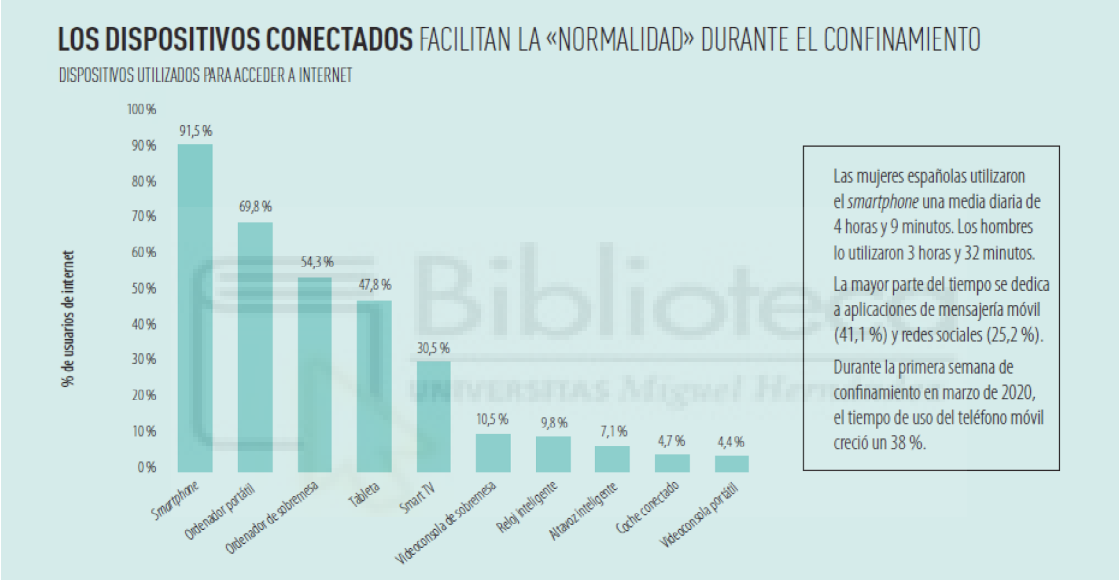
pero ya con un crecimiento destacable de usuarios, situándose en un 90,2% de la población.

En la gráfica nos muestra que cada vez más debemos prestar más atención a los delitos que se realizan a través de las nuevas tecnologías ya que es donde se encuentran el mayor número de posibles víctimas. Analizando los resultados prácticamente la totalidad de la población nacional tiene fácil acceso a la conexión a Internet y a la exposición de los riesgos que conlleva su uso.

Dispositivos utilizados para la conexión a Internet.

Figura 7:

Estadística de dispositivos utilizados para la conexión a Internet



Nota. Informe de la sociedad digital en España. (P.174).

El Smartphone es el dispositivo por excelencia para conectarse a Internet con un 91,5 % durante el año 2020, datos que subieron exponencialmente debido al confinamiento por la pandemia. Cabe destacar el descenso de los dispositivos por excelencia para conectarse a Internet como los ordenadores de sobremesa y los portátiles con un 54,3 y 69,8 % respectivamente. En contraposición suben de forma notable las tabletas electrónicas con un 47,8%. Es necesario recalcar el detalle del aumento de los diferentes aparatos electrónicos que llevan el software adecuado para establecer la conexión a Internet como televisiones, relojes y especialmente las videoconsolas, artilugio usado mayoritariamente por adolescentes y jóvenes, que se sitúa en un 10,5 % sobre el total de dispositivos.

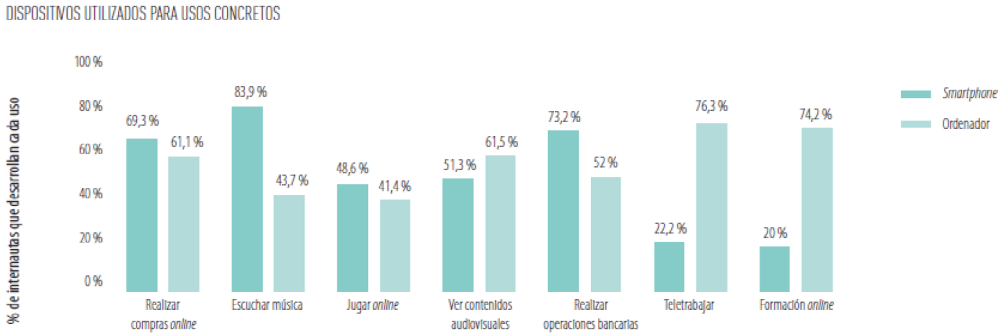
Vemos que nos debemos esforzar en proteger los dispositivos que se conectan a Internet para que los hackers no puedan invadir la intimidad de las posibles víctimas vulnerables mediante un software cada vez más avanzado

porque es fácil que la juventud, las víctimas más frecuentes, no controlen todavía sus dispositivos, siendo objetivos fáciles de corromper, para ello necesitan la ayuda externa de su dispositivo para que haga la función de protección por el usuario.

Uso del dispositivo por materias.

Figura 8:

Estadística de dispositivos utilizados por materias.



Nota. Informe de la sociedad digital en España. (P.174).

Actualmente el smarphone es el dispositivo más utilizado como hemos visto, y los usos más frecuentes son para escuchar música con un 83,9%, mientras que el uso del ordenador, que es el 2º dispositivo más utilizado, se emplea más para teletrabajar con un 76,% dato también alterado con motivo de la pandemia.

A nivel global, el teléfono móvil se usa más para realizar compras online, escuchar música, para juegos online y la realización de operaciones bancarias, mientras que el teletrabajo, la formación online y la visualización de contenidos audiovisuales es más común utilizar el ordenador antes que el teléfono móvil.

En este apartado analizamos que las materias en sí no son peligrosas para los ciberacosadores, no obstante, hay que estar alerta ya que muchas de estas actividades son anzuelos para llegar a intimar con la víctima para que, posteriormente, mediante la violencia, sufra las consecuencias del ciberacoso. Un ejemplo nos lo muestra las altas tasas de los juegos online donde muchos jugadores interactúan con personas desconocidas y donde se esconden cibernautas con unos principios y valores mezquinos, desarrollados por el alto grado de violencia que contienen muchos de los juegos online.

Viviendas con Internet.

Figura 9:

Estadística de hogares con conexión a Internet.

	PORCENTAJE DE VIVIENDAS CON / SIN ACCESO A INTERNET									
	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
Viviendas con internet	62,7	66,6	69,7	74,4	78,7	81,9	83,4	86,4	91,4	95,4
Viviendas sin internet	37,3	33,4	30,3	25,6	21,3	18,1	16,6	13,6	8,6	4,6

Nota. Estudio sobre la Cibercriminalidad en España 2020. (P.27).

El 95,4% de las viviendas españolas tiene acceso a Internet frente al 91,4% del año 2019, con 5 puntos de diferencia entre estos dos años, siendo uno de los años con más crecimiento comparado con años anteriores que la diferencia entre año y año se sitúa sobre los 3-4 puntos porcentuales.

Los datos de 2020 comparados con los del 2011, se observa que en 10 años se ha pasado de un 62,7% de viviendas con Internet a prácticamente a la casi totalidad de los hogares españoles con el 95,4%, habiendo una diferencia de 32,7%, es decir, en los últimos 10 años se han dado de alta 1/3 de los hogares españoles.

Examinando la gráfica podemos deducir que el futuro es Internet, y el futuro de las relaciones sociales serán a través de las Redes, por tanto, hay que enseñar a la población en el uso racional de estos dispositivos y la autonomía que nos da el poder utilizar estas herramientas tan potentes desde la intimidad de nuestra vivienda.

Uso de Internet en los últimos 3 meses por edades.

Figura 10:

Estadística de Uso de Internet en los últimos 3 meses por edades.

	% POR GRUPO DE EDAD DE PERSONAS QUE HAN UTILIZADO INTERNET ÚLTIMOS 3 MESES									
	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
Edad: De 16 a 24 años	94,6	95,8	97,4	98,3	98,5	98,4	98,0	98,5	99,1	**99,8**
Edad: De 25 a 34 años	86,3	87,7	92,1	93,7	94,5	96,0	96,3	97,7	97,9	**99,7**
Edad: De 35 a 44 años	77,7	83,0	83,7	89,8	91,6	93,3	95,8	96,6	97,4	**99,0**
Edad: De 45 a 54 años	64,6	67,4	71,2	78,2	82,0	84,9	90,3	91,0	94,4	**97,1**
Edad: De 55 a 64 años	37,9	43,8	46,5	55,4	61,4	64,8	73,9	76,1	86,5	**89,5**
Edad: De 65 a 74 años	16,2	19,0	21,9	26,2	31,3	34,7	43,7	49,1	63,6	**69,7**

Nota. Estudio sobre la Cibercriminalidad en España 2020. (P.29).

Se observa que la práctica totalidad de la población entre 16 y 44 años ha accedido a Internet en los últimos 3 meses, siendo la franja de los 16-24 años los que más acceden a Internet con el 99,8% de la población, en comparación con la franja de 65 a 74 años en que la franja es la más baja con 69,7%, no obstante, es el segmento de edad que más crece porcentualmente cada año reduciéndose la brecha con todas las franjas de edad.

A partir de ahora en que toda la juventud ya son “nativos digitales”, como enunciaba Prensky, debemos establecer eficaces métodos de protección para todos los usuarios de Internet y con la difícil misión de ir evolucionando a la par que la tecnología para hacer frente, cada vez con recursos más eficientes, a los cambios tan dinámicos en las herramientas tecnológicas para evitar y prevenir los ciberdelitos.

5.2.1. Big Data e Internet de las Cosas (IoT)

Como presentamos en la Introducción, todos los avances tecnológicos como: Internet de las cosas, el Big Data, Aprendizajes automáticos… ayudan a combatir la violencia de género” *(Harikiran G. C., Menasinkai K. y Shirol S. 2016),* pudiendo planificar estrategias sobre políticas públicas con el objetivo de realizar una previsión de recursos anticipando todo tipo de Violencia de Género.

Para conocer mejor el contenido de lo expuesto es necesario definir los conceptos, así que se define el **BIG DATA** como el conjunto de tecnologías y disciplinas que se encargan del almacenamiento y procesamiento de grandes cantidades de información, aunque existen muchas más definiciones que enunciamos a continuación y su fuente. Todas estas definiciones nos permiten comprender la dimensión del Big Data:

Se define el Big Data como colecciones de conjuntos de datos cuyo volumen, velocidad o variedad es tan grande que es difícil almacenar, administrar, procesar y analizar los datos utilizando bases de datos tradicionales

y herramientas de procesamiento de datos." *(libro Big Data Analytics: a Hands-On Approach).*

"Conjunto de técnicas que permiten analizar, procesar y gestionar conjuntos de datos extremadamente grandes que pueden ser analizados informáticamente para revelar patrones, tendencias y asociaciones, especialmente en relación con la conducta humana y las interacciones de los usuarios." (*dpej.rae.es)*

"Se considera Big Data cuando el volumen de los datos se convierte en sí mismo parte del problema a solventar (…)." *(O'Reilly Radar).*

"Las tecnologías de Big Data describen un nuevo conjunto de tecnologías y arquitecturas, diseñadas para extraer valor y beneficio de grandes volúmenes de datos con una amplia variedad en su naturaleza, mediante procesos que permitan capturar, descubrir y analizar información a alta velocidad y con un coste reducido." *(EMC/IDC).*

"Conjuntos de datos cuyo tamaño va más allá de la capacidad de captura, almacenado, gestión y análisis de las herramientas de base de datos." *(McKinsey Global Institute (MGI)).*

Para el análisis del Big Data se requieren herramientas y marcos especializados cuando:

El volumen de datos involucrados es tan grande que es difícil almacenar, procesar y analizar en una sola máquina.

En la velocidad en que se generan los datos es muy alta y es necesario analizarlos en tiempo real.

Hay una variedad de datos involucrados, que pueden ser estructurados, no estructurados o semiestructurado, y se recopila de múltiples fuentes de información.

Varios tipos de análisis deben realizarse para extraer información de los datos: descriptivo, de diagnóstico, predictivo y prescriptivo.

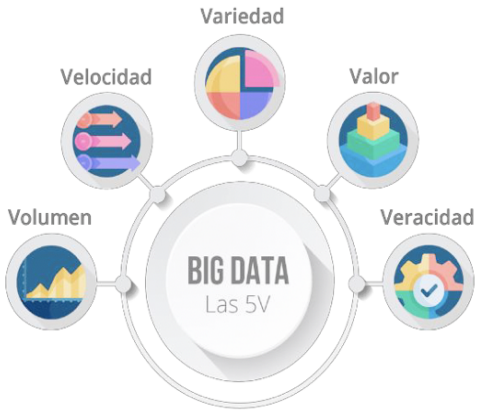
El análisis de Big Data implica varios pasos:

1) Limpieza de datos
2) Manipulación de datos
3) Procesamiento de datos
4) Visualización de datos.

Toda esta espiral de rapidez vertiginosa se observa en las características de la información que mueve el BIG DATA, lo que se denomina como las cinco uves (5V´s) por sus características: Volumen, Velocidad, Variedad, Valor y Veracidad.

Figura 11:

Las 5Vs del Big Data.



Nota. www.auraquantic.com

Conviene resaltar estos 5 elementos para llegar a entender que es el Big Data:

1.- Volumen: En el Big Data el volumen de datos es tan grande que no cabría en una sola máquina, este término se usa para datos de escala masiva que son difíciles de almacenar, administrar y procesar utilizando bases de datos tradicionales y arquitecturas de procesamiento de datos clásicas.

2.- Velocidad: Se refiere a cómo de rápido se generan los datos. Se requieren herramientas especializadas para ingerir datos de alta velocidad en la infraestructura de Big Data y analizar los datos en tiempo real.

3.- Variedad: Se refiere a la forma de los datos. Los datos se presentan como estructurados, no estructurados o semiestructurados. Los sistemas de datos deben ser lo suficientemente flexibles para manejar tal variedad de datos.

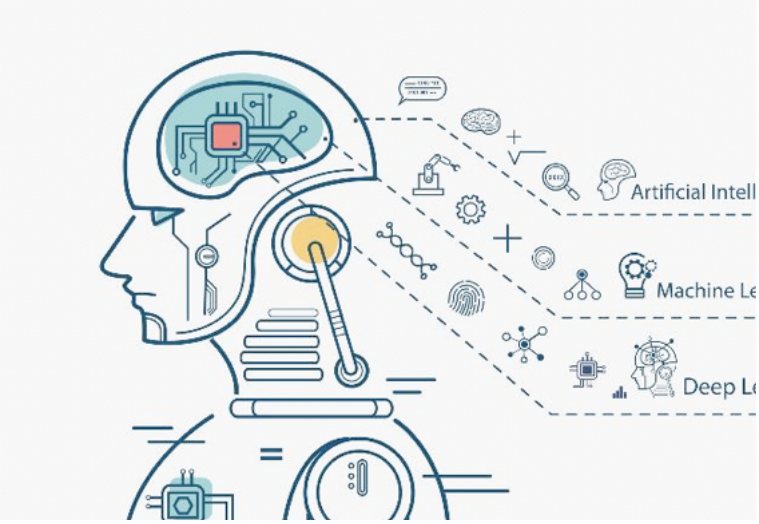
4.- Valor: Se refiere a la utilidad de los datos para el propósito previsto. El objetivo final es extraer valor de los datos.

5.- Veracidad: Se refiere a cómo de precisos son los datos. Para extraer valor de los datos, los datos deben ser limpiados, la limpieza de los datos es importante para que los datos incorrectos y defectuosos se puedan filtrar. (*Bagha, A., & Madisetti, V. 2019).*

Del procesamiento de los datos en el BIG DATA se encargan la Estadística, la Matemática y la Informática haciendo uso de la Minería de Datos, el Aprendizaje Automático (Machine Learning), la Computación Paralela, la Inteligencia Artificial, Deep Learning… *(Bagha, A., & Madisetti, V. 2019).*

Figura 12:

Ilustración sobre Inteligencia Artificial, Machine Learning y Deep Learning.



Nota. www.blogmapfre.com

Para entender mejor cómo funciona el procesamiento de los datos en el Big Data es necesario desarrollar estos conceptos:

Minería de Datos: aplica métodos desde distintas áreas para identificar patrones (conocidos) en los datos. Puede incluir algoritmos estadísticos, machine learning, text analytics, series temporales y otras áreas analíticas. También se incluye en la Minería de Datos el estudio y la práctica del almacenamiento y manipulación de datos.

Machine Learning: es una categoría dentro de la Minería de Datos que usa automatismos y algoritmos interactivos para encontrar patrones en los datos. Aprenden de los datos con una mínima intervención humana.

Inteligencia Artificial: no hay una definición exacta pero se puede resumir la Inteligencia Artificial como el intento de imitar la inteligencia humana usando un robot, o un software.

Deep Learning: el Deep Learning tiene una gran importancia dentro de la Inteligencia Artificial ya que saprovecha la información del pasado y la estructura de las redes neuronales humanas. Actualmente están buscando cómo aplicar estos conocimientos al reconocimiento de patrones, sobre todo en el campo de la medicina, diagnóstico automático por imágenes y en otros campos como la seguridad o el marketing en tiempo real.

Por tanto, una vez planteados los conceptos, la recopilación de información mediante los sistemas tecnológicos actuales es clave y necesaria para construir una gran base de datos mediante la realización de encuestas, estadísticas de

los órganos oficiales o monitorización automática que transmitan toda esta información a la nube que puede utilizarse de forma eficaz con el fin de recoger toda la información biosensorial del estado de un individuo guardándose los datos en remoto gracias al concepto IoT". (*Shaik, K. Bogaraju S y Vadepu S. 2017)*.

Otro recurso, gracias al Big Data es la telemonitorización. Implicará la continua recolección de datos de las víctimas para identificar claramente su condición, ubicación exacta e indicios de riesgos". *(Wu J, Feng Y, y Sun P, 2018)*.

Con estos avances biométricos se puede permitir una vigilancia permanente de la víctima para monitorizar todos sus estados emocionales para así detectar, anticipar y prevenir situaciones de riesgo gracias a estas tecnológicas y todo ello a través de aplicaciones mediante el dispositivo ya global y más utilizado: los smartphones.

Este proceso basado en las TIC, el Big Data y el IoT previenen las situaciones de violencia, que ofrecen amplías posibilidades tanto a nivel global como individualizado. En una situación real el entorno de IoT posibilitará una comunicación rápida y directa con las Fuerzas y Cuerpos de Seguridad, asistencia psicológica… y también una detección automática de una agresión y la correspondiente activación de una alarma. Todo este proceso es posible porque cuando una persona es sometida a una agresión o cualquier tipo de violencia, su cuerpo se altera y mediante los biosensores y dispositivos portátiles recogen datos sobre los cambios fisiológicos como movimientos abruptos, respiración, frecuencia cardiaca, presión sanguínea, glucemia, temperatura, sudoración, presión arterial, conductividad de la piel, actividad cerebral, tensión muscular, voz, entre otras variables. Todos estos datos, ayudados por la tecnología de los automatismos en el entorno de IoT, permiten monitorizar a la víctima y enviar la alerta a sus destinatarios. (G. J. Hunt, 2007).

Concretamente en España, como en muchos otros países llevamos desde el año 2003, se ha estado recopilando datos sobre la Violencia de Género, mediante el Instituto Nacional de Estadística (INE) que ofrece una gran cantidad de datos al respecto, todo gracias al Big Data y al Internet de las Cosas que permite a día de hoy analizar la Violencia de Género con otras variables. Como ejemplo, ahora es posible predecir el número de denuncias que se van a presentar de Violencia de Género en los juzgados en el plaza de 6 meses. Esta predicción se realiza por medio de una Multi-Objective Evolutionary Search Strategy para la selección de variables y con Random Forest como algoritmo predictivo. Todo ello con el objetivo de destinar los más avanzados recursos para reducir el número de víctimas. *(Rodríguez Rodríguez, I. 2021).*

Internet de las Cosas (IoT)

Conviene analizar por otra parte, lo que se denomina como **Internet de las cosas** (*IoT: Internet of Things*): este concepto se refiere a cosas que tienen identidades únicas y están conectadas a Internet pudiendo enviar la información a servidores centralizados o a la "nube" para su procesamiento. Dicho de un modo más sencillo, el IoT se trata de una interconexión total de cualquier dispositivo cercano a Internet que envía de forma continua datos sobre su estado, es decir, remite datos sobre su ubicación, situación, nivel de batería…y cualquier otro dato que pueda percibir mediante sensores. *(Rodríguez Rodríguez, I. 2021).*

Así, los avances tecnológicos, las soluciones de *software* y los nuevos conceptos como IoT con las estrategias de computación en la nube que permiten que la información transferida por los biosensores de la víctima se guarden en remoto, además que para que se pueda producir la monitorización de la víctima y detecte una situación de violencia se requerirá una plataforma de IoT para recoger y gestionar los datos de la información biométrica de la víctima, centrando, gracias a IoT, la detección de la situación de peligro. En consecuencia, se puede observar que IoT ofrece soluciones para enfrentarse y prevenir la Violencia de Género. *(G. C. Harikiran, K. Menasinkai y S. Shirol, 2016) y* Shaik, K. Bogaraju S y Vadepu S. (2017).

Para entender cómo funcionan los entornos de IoT se basa en el llamado "despliegue de capas" que se compone de 5 capas:

Sustrato: Esta es la capa en la que se generan los datos, es decir, la verdadera fuente de información. Aquí distinguimos tres áreas: 1) Ciberespacio: las redes sociales y el uso diario de Internet, 2) Monitoreo del ambiente (trabajo/hogar), y, 3) Sustrato biológico: el estado físico de la superviviente.

Capa de sensorización: Los datos se adquieren a través de aplicaciones, sensores y biosensores, todos conectados a un marco de IoT. Se puede configurar y controlar a distancia a través de Internet, creando una estructura tecnológica. 1) Ciberespacio: aquí utilizamos un software que intercepta la escritura, el vídeo y el audio, ya sea recibido por la superviviente o autogenerado, para la vigilancia; 2) Vigilancia del medio ambiente (trabajo/casa): utilizando recursos domóticos; y 3) Sustrato biológico: utilizando biosensores que vigilan los cambios físicos. Reseñar que si un Juzgado de Violencia sobre la Mujer lo considera apropiado, estos recursos podrían extenderse al agresor.

Capa de comunicación: El objetivo de esta capa es la permeabilidad de los datos en preparación para la siguiente etapa. Utilizando comunicaciones inalámbricas como Wi-Fi, 4G/5G, ZigBee (o 6LowPAN) y conexiones Bluetooth, la información se envía a un dispositivo inteligente más potente (smartphone) que

recoge los datos y actúa como una puerta de enlace. Siguiendo la idea del IoT, esta capa envía comunicaciones a la nube.

Capa de middleware: Como estamos trabajando con diferentes biosensores, sensores domóticos y también software de captura, se requiere un mediador de middleware para transformar y unir todas las fuentes de datos.

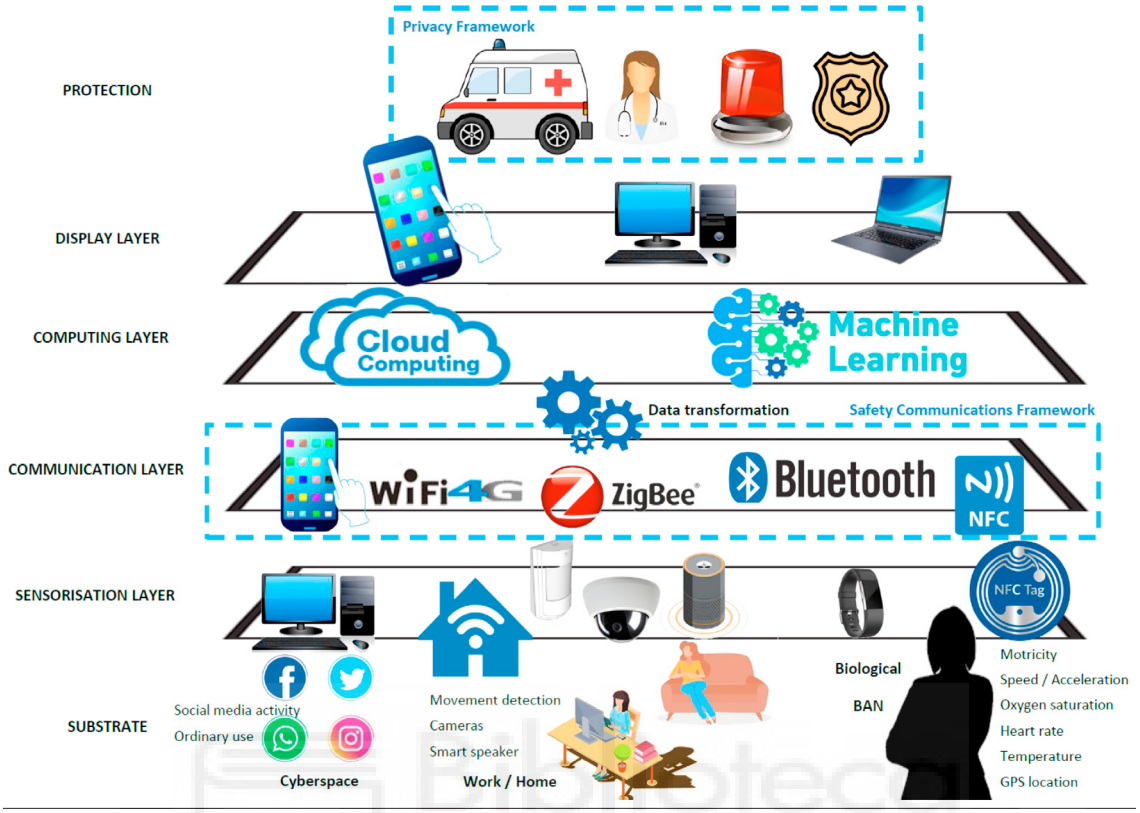
Capa de computación y gestión: En esta capa, los datos recogidos se gestionan para llevar a cabo un análisis de éstos, que podría ser de reconocimiento de texto/voz/imagen/vídeo con el fin de identificar el acoso, pero también para prever y luego anticipar situaciones de riesgo y asaltos. Esta tarea debe realizarse en la nube mediante servidores potentes, ya que los algoritmos de ML utilizados pueden ser muy exigentes en cuanto a recursos informáticos. Por lo tanto, la computación ubicua puede utilizarse para mejorar el proceso y lograr una solución más rápida.

Capa de visualización (interfaz). El acceso al sistema se hará a través de un navegador y una interfaz sencilla con el fin de comprobar la información, ajustar las preferencias del usuario, pero también para lanzar la alarma si se produce un ataque. Así pues, es posible utilizar no sólo un teléfono inteligente para mostrar la interfaz, sino también un ordenador de escritorio. De esta manera, no sólo la superviviente, sino también la policía y los servicios de emergencia pueden tener acceso en caso de alarma, así como también una persona de confianza que puede comprobar que la superviviente está fuera de riesgo.

Salida/Protección: Podemos considerar varios resultados del sistema de gestión, dependiendo de la situación. La plataforma se limita a comprobar la situación de la superviviente, estudiar posibles situaciones de riesgo para mejorar el algoritmo de predicción y, por supuesto, gestionar una situación de riesgo con la cooperación de las fuerzas de seguridad, los servicios médicos y la teleasistencia a distancia en las zonas de TIC. *(Rodríguez Rodríguez, I. 2021).*

Figura 13:

Propuesta de capas de comunicaciones IoT para la gestión de la VG.



Nota. (Rodríguez Rodríguez, I. 2021).

Esta plataforma de"despliegue de capas" permite obtener:

El conocimiento continuo del estado de la víctima y, si es necesario, del infractor. De esta manera, y utilizando la Localización por Posicionamiento Global (GPS), es posible evitar su encuentro accidental. Puede proporcionar ayuda en términos de situaciones de emergencia, pero también en tareas rutinarias.

Manejo de emergencias: un sistema de gestión integral debe estar preparado para hacer frente a una situación de riesgo. El GPS mostraría el punto exacto en el que se ha producido un asalto; las bioseñales sugerirían el estado de la víctima, etc., así como la acción coordinada de los recursos.

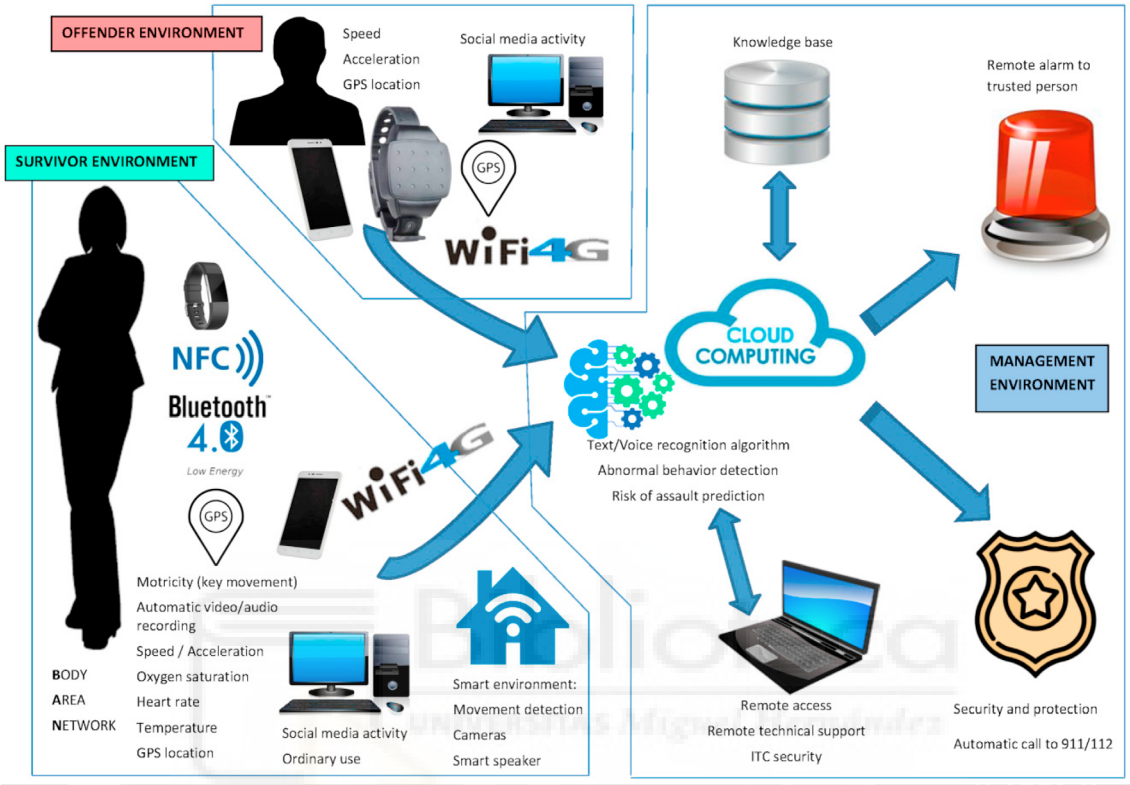
Fácil intercambio de información: entre la persona agredida y la policía, los profesionales de la salud, la persona de confianza, y todas las personas involucradas en el manejo de la VG.

El flujo de datos en la plataforma TIC propuesta puede verse en la siguiente figura. Existe una pasarela local (teléfono inteligente) que se conecta a Internet a través de 4G/5G o mediante WiFi doméstico. Los datos se almacenan en un almacén de datos en Internet, y es desde donde los algoritmos de ML extraen el conocimiento. Finalmente, utilizando varios métodos de comunicación (como

BLE, 6LoWPAN, NFC, etc.), se hace posible el intercambio de datos. *(Rodríguez Rodríguez, I. 2021).*

Figura 14:

Diagrama de los flujos de datos de la plataforma TIC para la gestión de la VG.



Nota. (Rodríguez Rodríguez, I. 2021).

Finalmente, analizando la realidad actual y esta revolución de los datos mediante el Big Data y el IoT, podemos afirmar, tal como se catalogó en El World Economic Forum (WEF), que esta revolución de los datos ha sido designada como la 4º Revolución Industrial que se caracteriza "por la fusión de tecnologías que está desdibujando las líneas entre las esferas física, digital y biológica, no habiendo precedentes sobre la velocidad de cambio, transformación y dinamismo de los avances que está experimentando el mundo actual que presagian la transformación de sistemas enteros de producción gestión y gobierno".

5.3 Adolescentes y las redes sociales

5.3.1. Adolescentes

Según la definición de la Organización de las Naciones Unidas (ONU), la juventud es la edad que se sitúa entre la infancia y la edad adulta. Es una etapa que transcurre entre 10-24 años; abarca la adolescencia inicial (10-14 años), la adolescencia media y tardía (15-19 años) y la juventud plena (20-24 años).

La adolescencia tiene la peculiaridad de que es el periodo donde se muestra gran interés por relacionarse con sus iguales y que derive en una conjunción y aceptación de su persona en un grupo de amistades, también suele ser el periodo en que se inicia una relación con otra persona, desarrollándose una única identidad afectiva, sexual, moral y vocacional. Es la etapa donde frecuentemente se construye nuestra columna vertebral de nuestro carácter, donde decidimos por nuestros gustos… que serán el pilar de nuestro futuro.

Actualmente, con las TIC ya existe una forma de relacionarse que no existía hace 20 años, por lo que el método cambia. El adolescente está mucho más expuesto a la comunicación y a relacionarse con personas fuera de su entorno. Como hemos visto en la Figura 9, la franja de edad entre los 16 y los 24 años, es la edad en la cual se conectan más número de jóvenes con el 99,8%, por lo que prácticamente la totalidad de la población joven en España interactúa con otros iguales o distintas personas de su entorno con los peligros que ello conlleva y con el añadido de que la juventud de hoy en día ya son "nativos digitales" tal como definía Prensky, por lo que los adolescentes conocen esta herramienta de internet y la tienen normalizada como un instrumento para comunicarse entre otras actividades sin valorar ningún riesgo ya que para ellos es la mejor herramienta para interactuar porque tiene un acceso fácil (teléfono móvil) y barato. Suele ser sufragado por los padres ya que entra dentro de un plan familiar de Internet en que los adolescentes no desembolsan cantidad alguna por el acceso a los datos.

Internet se caracteriza porque ofrece a los adolescentes una respuesta rápida, recompensas inmediatas, interactividad e innumerables actividades. *(Echeburúa, E., & De Corral, P., 2010).*

Como hemos comentado anteriormente el mayor hándicap del uso de Internet y las Redes Sociales por parte de los adolescentes entre 16 y 29 años, es el peligro al que se hallan expuestos sin ser conscientes de ello, porque son el grupo más vulnerable, facilitando que sean víctimas exponenciales del ciberacoso. *(Burgess y Baker, 2008)*

El sexo masculino en general toma más riesgos, sobre todo en la etapa adolescente, que el sexo femenino, por tanto, en el ciberespacio no es diferente. Adoptan más riesgos pero también son menos vulnerables que las mujeres adolescentes por los estereotipos existentes en la cultura tradicional y los aún perdurables valores sexistas en los comportamientos de la sociedad. Por ejemplo, las imágenes de las mujeres se valoran de diferente manera a la misma imagen proyectada por los hombres. Esto conlleva que, en general, el uso de la Redes Sociales por las adolescentes y la distribución de contenidos que proporciona Internet y las Redes pueda ser más perjudicial y traumático para este sector de

la población. *(Torrés, C., Manuel, J. y De Marco, S. 2014).*

Según el estudio realizado por *(Díaz-Aguado, M., Martínez, R. y Martínez, J.2014),* las principales condiciones que se puedan dar para que los adolescentes sufran el riesgo de Violencia de Género y en los cuales también se debe enfocar la prevención son:

- La justificación de la Violencia de Género y del dominio y la sumisión en la familia.

- La justificación del sexismo y de la violencia como reacción a una agresión.

- Mensaje escuchados del entorno en que predomina el contenido sobre el dominio y la violencia más que los mensajes enfocados a la igualdad y no violencia.

- Menor tendencia a reconocer como maltrato las conductas específicas por la cual se expresa el maltrato.

- Estereotipo emocional machista: rechazo a la expresión emocional, dureza emocional, en el cual no se debe mostrar debilidad, sensibilidad ni pedir ayuda a otras personas ante situaciones de maltrato.

Finalmente, resaltar que, el uso de las nuevas tecnologías en los adolescentes provoca que la utilicen como herramienta de posesión y control de pareja, además las nuevas tecnologías dificultan el cierre de una relación por todos los hilos que existen entre la pareja, llegando a utilizar esta herramienta para el chantaje, el insulto y las amenazas con el fin de que el agresor intente volver a retomar la relación, con las consecuencias psicológicas para la víctima. *(De Miguel, V. 2015).*

Con todo ello, se debe atender a todos los signos que percibimos de violencia, y mediante estas mismas herramientas, localizarlo, prevenirlo y erradicarlo.

5.3.2. Redes Sociales

Según la Real Academia de la Lengua, una red social es: “Un servicio de la sociedad de la información que ofrece a los usuarios una plataforma de comunicación a través de internet para que estos generen un perfil con sus datos personales, facilitando la creación de comunidades con base en criterios comunes y permitiendo la comunicación de sus usuarios, de modo que pueden interactuar mediante mensajes, compartir información, imágenes o vídeos, permitiendo que estas publicaciones sean accesibles de forma inmediata por todos los usuarios de su grupo”.

Por parte del Observatorio Tecnológico del Ministerio de Educación, Cultura y Deporte define las Redes Sociales como “una estructura social formada

por personas o entidades conectadas y unidas entre sí por algún tipo de relación o interés común".

El término se atribuye a los antropólogos británicos Alfred Radcliffe-Brown y Jhon Barnes. Las redes sociales son parte de nuestra vida, son la forma en la que se estructuran las relaciones personales, estamos conectados mucho antes de tener conexión a Internet.

Un término ya conocido de las Redes Sociales lo aportaron las profesoras estadounidenses, Danah Boyd y Nicole Ellison, definen los servicios de redes sociales como "servicios con sede en la red que permiten a los individuos:

1) Construir un perfil público o semipúblico dentro un sistema delimitado o cerrado, permitiendo contactar con otros usuarios conocidos o no conocidos.

2) Articular una lista de otros usuarios con los que comparten relaciones, estos usuarios comparten información a sus contactos sobre los intereses personales, gustos musicales, preferencias y mucha información personal tanto pasada, como presente e incluso futura. Estos usuarios se pueden comunicar entre ellos mediante una gran variedad de sistemas de comunicación como mensajes privados, chats, comentarios públicos, así como compartir fotos, vídeos o cualquier otro tipo de contenido, en el cual sus contactos pueden ver a través de la red.

3) Ver y recorrer esa lista de relaciones que las personas relacionadas tienen con otras dentro del sistema" estableciendo así una Red Social.

Con la llegada de la Web 2.0, las redes sociales en Internet ocupan un lugar relevante en el campo de las relaciones personales y son, asimismo, paradigma de las posibilidades que nos ofrece esta nueva forma de usar y entender Internet.

El advenimiento de la Web 2.0 revoluciona el concepto de red, las formas de comunicación cambian e Internet adopta características nuevas de colaboración y participación sin precedentes. Como ya se ha indicado, a diferencia de la Web 1.0, de sólo lectura, la Web 2.0 es de lectura y escritura, donde se comparte información dinámica, en constante actualización. La Web 2.0 se ha llamado en muchas ocasiones la Web social y los medios de comunicación que ofrece también han incorporado este adjetivo, denominándose Medios Sociales o Social Media, en contraposición a los Mass Media, para mostrar el importante cambio de modelo que atraviesa la comunicación en la actualidad. Los profesores de la Universidad de Indiana, Andreas M. Kaplan y Michel Haenlein, definen los medios sociales como ""un grupo de aplicaciones basadas en Internet que se desarrollan sobre los fundamentos ideológicos y tecnológicos de la Web 2.0, y que permiten la creación y el intercambio de contenidos generados por el usuario". El cambio se da verdaderamente a nivel usuario, que pasa de ser consumidor de la Web a interactuar con ella y con el resto de usuarios de múltiples

formas. El concepto de medios sociales hace referencia a un gran abanico de posibilidades de comunicación como blogs; juegos sociales; redes sociales; videojuegos multijugador masivos en línea (MMO); grupos de discusión y foros; microblog; mundos virtuales; sitios para compartir vídeos, fotografías, música y presentaciones; marcadores sociales; webcast; etc.

Las herramientas 2.0 fueron en su día una auténtica revolución que actualmente ya se tiene como interiorizada y normalizada pero la web 2.0 nos permitió la participación colectiva a través de colaborar y compartir con otros usuarios. El cambio de mentalidad que supone esta nueva forma de comprender y utilizar Internet desarrolla la auténtica interacción, los individuos establecen relaciones entre ellos y las redes personales se convierten en lo más importante. Los foros permiten crear un perfil, los juegos sociales conocer al resto de jugadores, y los sitios para compartir vídeos enviar mensajes a otros usuarios. Todo esto, al fin y al cabo, posibilita la creación de redes sociales bajo distintos modelos, grupos de personas que se comunican por medio de Internet con un interés común. Cuando hablamos de las redes sociales basadas en Internet nos referimos a un genuino fenómeno social. El deseo de compartir experiencias y la necesidad de pertenencia al grupo provocan esta actividad colectiva, el software traslada los actos cotidianos a un sitio informático, facilitando la interacción de un modo completamente revolucionario que actualmente continua y evoluciona de forma dinámica, permitiendo la globalización en la comunicación, siendo capaces de interactuar y comunicarse instantáneamente con personas de otras culturas y otros lugares del mundo.

Otros especialistas en Redes Sociales plantean estos servicios como herramientas informáticas que permiten la creación de una red social on-line y que, para ello, tratan de operar en tres ámbitos de forma cruzada, "**las 3Cs":**

Comunicación, nos ayudan a poner en común conocimientos;

Comunidad, nos ayudan a encontrar e integrar comunidades; y

Cooperación, nos ayudan a hacer cosas juntos, compartir y encontrar puntos de unión.

Con todo ello, podemos definir las redes sociales on-line como estructuras sociales compuestas por un grupo de personas que comparten un interés común, relación o actividad a través de Internet, donde tienen lugar los encuentros sociales y se muestran las preferencias de consumo de información mediante la comunicación en tiempo real, aunque también puede darse la comunicación diferida en el tiempo, como en el caso de los foros. (*Ponce I. 2012).*

Por esta razón, las Redes Sociales atraen tanto a la juventud, porque son muy dinámicas, rápidas, dan una respuesta inmediata al tiempo, con la interacción con otras personas y pueden realizar diferentes actividades para compartirlas con sus contactos, esto les permite ser visibles ante los demás, reafirma su identidad grupal y están permanentemente conectados con sus amigos. *(Echeburúa, E., & De Corral, P. 2010).*

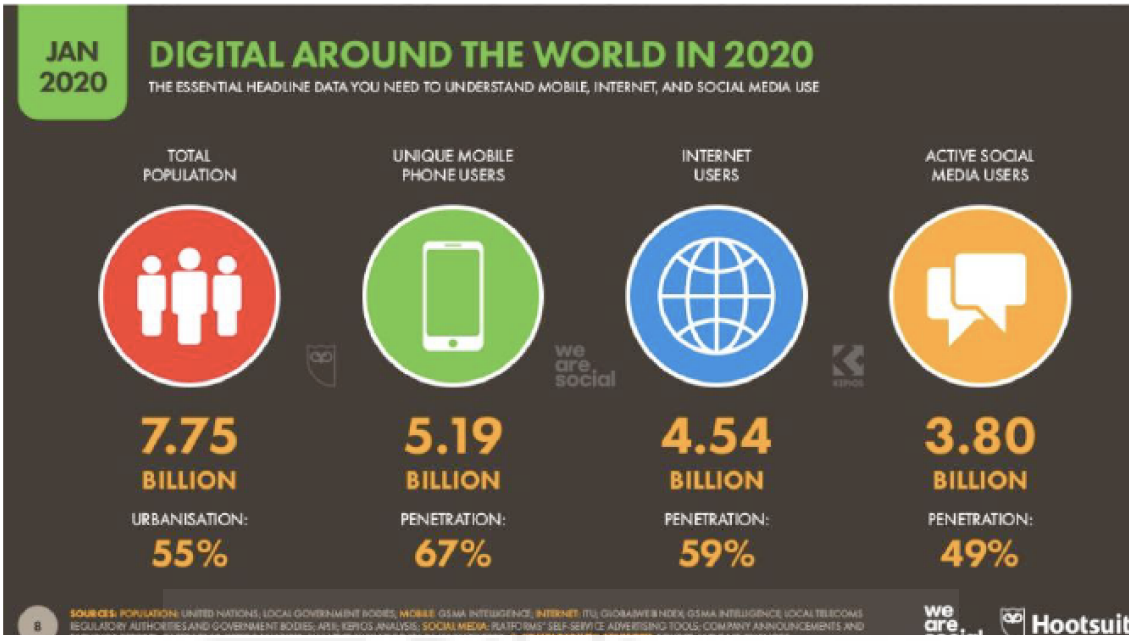
Esta preocupación de los adolescentes en adoptar una posición social carismática y de validación social provoca que los deseos hayan cambiado radicalmente con generaciones pasadas. Actualmente la aspiración es tener un teléfono móvil de alta gama, con acceso a Internet, buena y rápida transferencia de datos, con capacidad de almacenamiento y capaz de realizar fotos con la máxima calidad para después, a través de las Redes Sociales, compartir e intercambiar experiencias vividas a través de las distintas plataformas sociales bien a través de audios, vídeos, fotos…

Con los datos desarrollados es preciso contrastarlos mediante gráficas para darnos cuenta de la trascendencia de las Redes Sociales en la actualidad tanto en los adolescentes como a nivel global. Para ello, enfatizamos en las altas tasas de uso de las nuevas tecnologías. Para darnos cuenta de la repercusión de las redes mostramos las dos siguientes tablas el informe realizado por Digital Report 2020: Global Digital Overview en el cual se puede apreciar la visión global a nivel mundial del uso de las nuevas tecnologías.

Usuarios RRSS a nivel mundial.

Figura 15:

Estadística de Uso de Redes Sociales a nivel mundial.



Nota. Estudio sobre la Cibercriminalidad en España 2020. (P.7).

Como se puede comprobar en la Figura 10, existe un 55% de penetración de los usuarios de internet a nivel mundial con un total de 7.75 billones de usuarios.

De estos usuarios 5.19 billones de personas son usuarios únicos del teléfono móvil siendo el dispositivo por excelencia con un 67% de penetración respecto al año 2019.

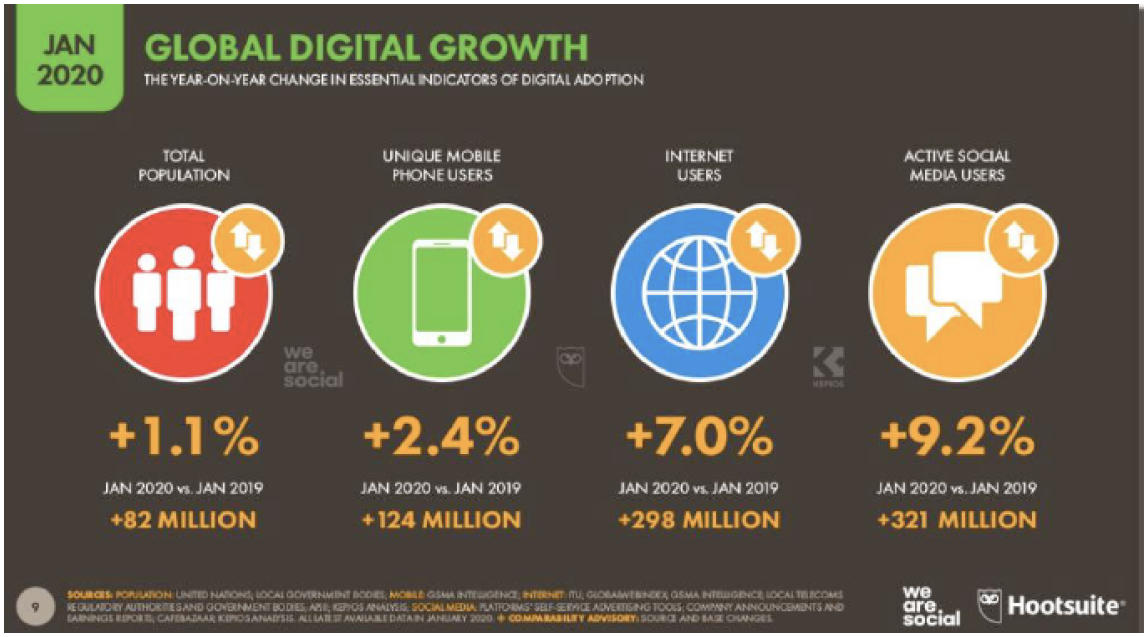
Respecto a la evolución de usuarios de Internet en el mundo ha experimentado un 59% de nuevos usuarios estableciéndose en 4.54 billones de personas que usan Internet.

Finalizando con la evolución de usuarios de Redes Sociales en el mundo con 3.80 billones de personas teniendo una subida del 49% respecto al año anterior del año 2019.

Todas estas diferencias en los porcentajes tan altos ha sido como consecuencia de la pandemia mundial que hemos sufrido que ha “obligado” a billones de personas a conectarse a Internet para tener contacto con sus familiares y allegados. *(Sociedad digital en España, 2020, p.168).*

Figura 16:

Estadística de Uso de Redes Sociales a nivel mundial.



Nota. Estudio sobre la Cibercriminalidad en España 2020. (P.7).

Los usuarios de Redes Sociales a nivel mundial aumenta cada año teniendo un incremento del 1.1%, 2.4% 7.0% y 9.2% en el total de la población, usuarios teléfono móvil, usuarios de Internet y usuarios de Redes Sociales activos respectivamente.

Para ver más detalladamente la subida en un año que ha experimentado el uso de Internet y las Redes Sociales, tan sólo en un año (2020), se ha visto incrementado en 82 millones de personas el número total de usuarios de internet respecto al año 2019 con un incremento del 1.1%.

Mientras que los usuarios que se han convertido en consumidores únicos de teléfono móvil se han incrementado en 124 millones de personas significando un aumento de 2.4% respecto al año 2019.

Por otra parte, destacar que ha subido un 7% los usuarios que se han conectado a Internet, es decir, se ha incrementado el valor en 298 millones de personas desde el año 2019.

Finalmente, reseñar que la mayor subida se ha producido en los usuarios totales a las Redes Sociales, en 321 millones de personas más, siendo un 9,2% más que el año anterior lo que denota que a nivel global la población está mucho más conectada sobre todo por las redes sociales en que se ha demostrado que son un instrumento eficaz para la comunicación entre las personas.

Considerando los datos que aporta esta figura con muchos billones de cibernautas. Internet es comunicación, y esa comunicación se establece mediante

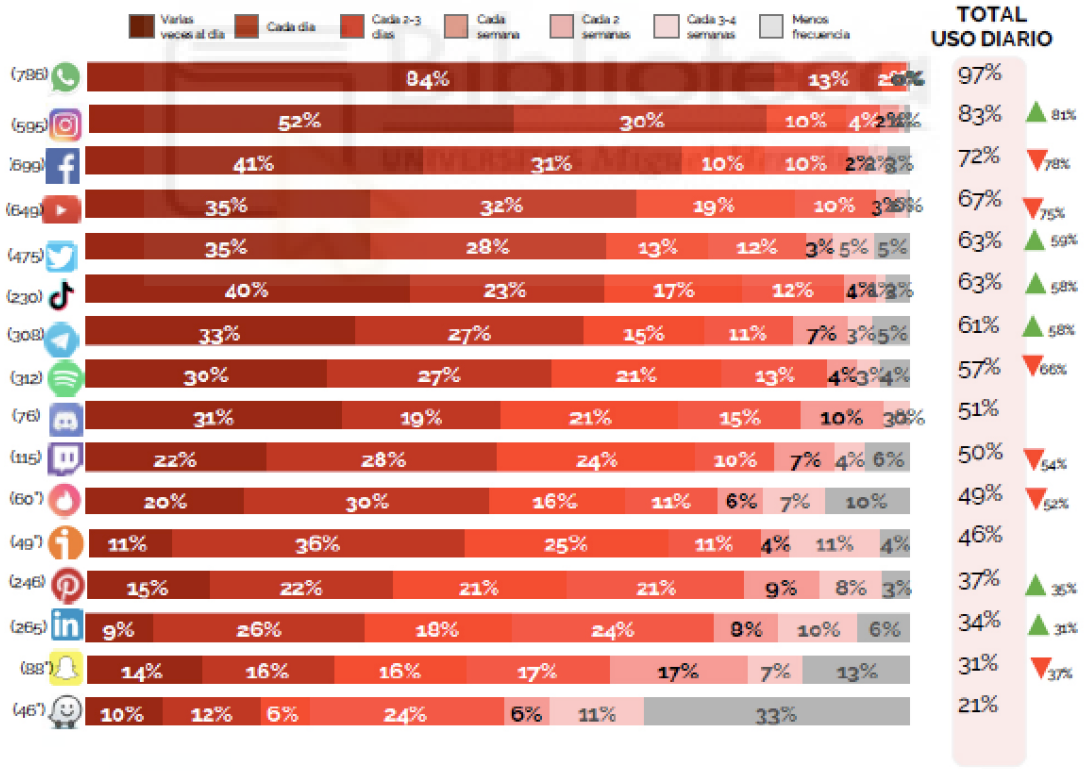
las Redes Sociales, las cuales las empresas responsables de su gestión ya establecen protocolos muy estrictos con lo que respecta a la privacidad de los perfiles, a diferencia de sus orígenes a finales de los años 90, en que los chats grupales, cualquier persona podía entablar una conversación sin ningún tipo de filtro. Este sistema ya desapareció por ser tremendamente inseguro estando los internautas expuestos a todo un mundo de peligros.

En las gráficas siguientes podemos observar la penetración de las Redes Sociales en la población, estas gráficas han sido realizadas por el Estudio Anual que publica la empresa IAB Spain y elaborada por la empresa Elogia, con estos datos podemos cuantificar el impacto de la Redes Sociales en el año 2021 destacando los siguientes resultados:

RRSS más utilizadas.

Figura 17:

Estadística de Redes Sociales más utilizadas a nivel nacional.



Nota. Estudio de Redes Sociales 2021. (P.22).

Las Redes Sociales más utilizadas en el año 2021 son Whatssap, Instagram y Facebook, la que más ha aumentado su uso diario es la Red Social Instagram con un 81% más que el año 2020, mientras que la caída más notable se sitúa en la Red Social Facebook que disminuye su uso en un 78%, siendo

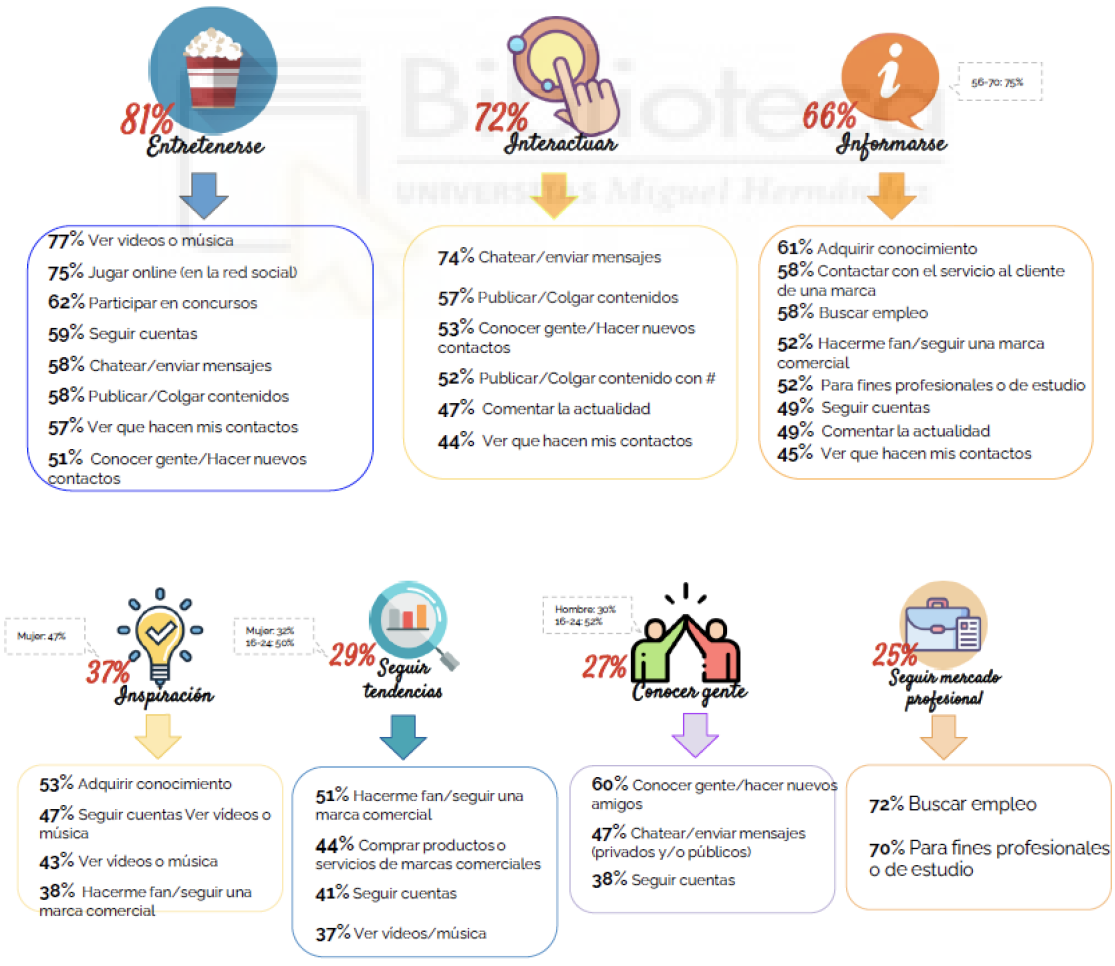
Whatsapp la que se mantiene en comparación con el año 2020, con un 97% de usuarios que la usan diariamente.

Subrayar que todavía no se poseen datos sobre en qué Red Social es más propensa a que se materialicen conductas relacionadas con la Violencia de Género o de Ciberacoso. Como detallaremos a continuación, en la sección 5.4. de este trabajo, actualmente se están recopilando datos a través de un proyecto técnico llamado: "Estudio sobre las conductas saludables de los adolescentes escolarizados" en que se recogerán y estudiarán este tipo de datos, sobre todo en la población joven que es la más vulnerable de sufrir y materializar estos tipos de delitos.

Actividades más realizadas.

Figura 18:

Estadística de Actividades más realizadas en Redes Sociales a nivel nacional.



Nota. Estudio de Redes Sociales 2021. (P.26-27).

Como actividades más realizadas tenemos que las redes sociales se utilizan principalmente para el entretenimiento, la interacción y la información, mientras que la inspiración, el seguimiento de tendencias, conocer gente y el seguimiento del mercado profesional son las actividades con menos frecuencia de uso.

Dentro del entretenimiento 81% de las ocasiones, los usuarios utilizan las redes principalmente para ver vídeos o escuchar música y jugar online. Chatear o enviar mensajes baja a la 3º posición con un 74% de uso.

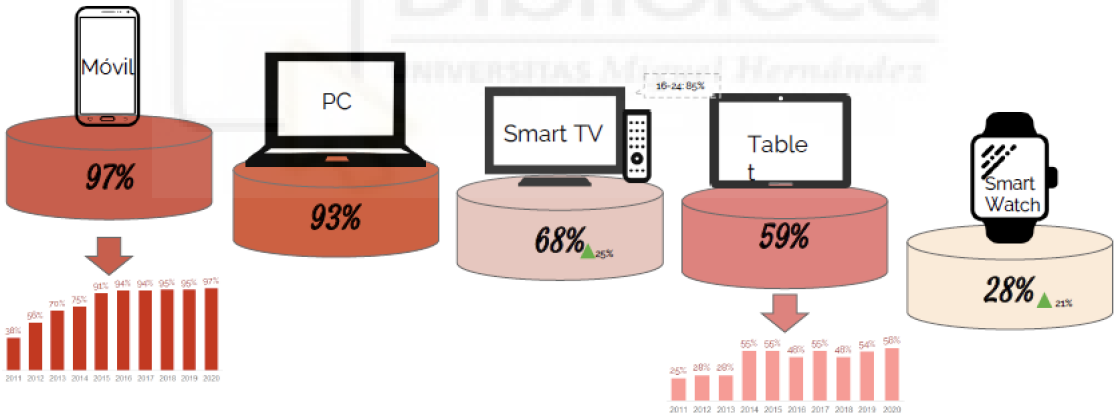
Sobre la actividad con menor interacción de los usuarios con las Redes Sociales es la búsqueda de empleo y los fines profesionales o de estudio.

Así que podemos deducir que las Redes Sociales las usamos principalmente como una herramienta de entretenimiento.

Dispositivos de conexión

Figura 19:

Estadística de dispositivos más usados para conectarse a las Redes Sociales a nivel nacional.



Nota. Estudio de Redes Sociales 2021. (P.34).

El Móvil sigue siendo el principal dispositivo para conectarse a Redes, superando al dispositivo por excelencia hasta ahora que ha sido el Ordenador con un 93%.

El dispositivo que más crece es el SMART TV, que aumenta en un 25% en un año, situándose en un 68% de uso en el año 2021.

Respecto a la Tablet ha ido creciendo progresivamente su uso hasta estabilizarse en la actualidad aunque con pequeños altibajos en el año 2016 y 2018.

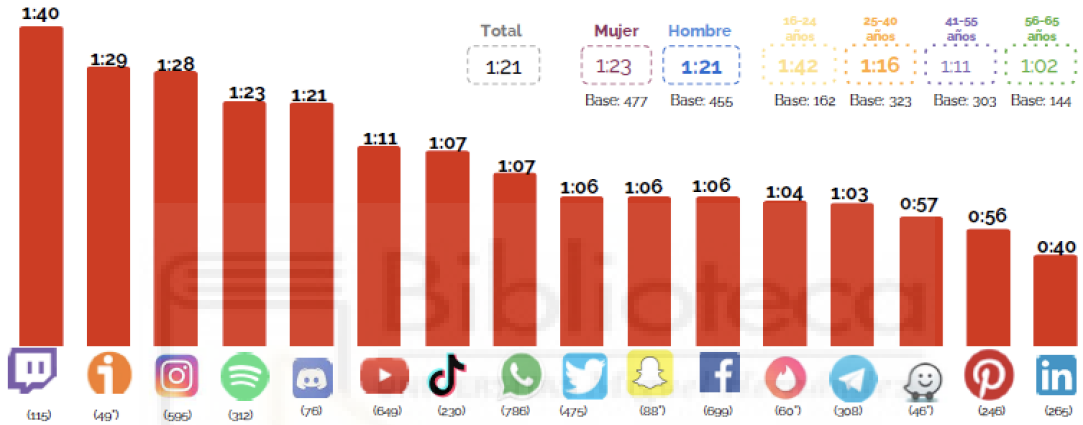
Le sigue el Smart Watch, el reloj inteligente que aunque presenta todavía un 28%, su uso sigue creciendo.

Por tanto, se observa la peculiaridad de que los dispositivos de conexión cada vez son más autónomos y portátiles por lo que podemos interactuar y explotar los recursos tecnológicos de estos dispositivos en cualquier momento y lugar.

Frecuencia de uso o conexión a RRSS a nivel nacional

Figura 20:

Estadística sobre la frecuencia de uso a las Redes Sociales a nivel nacional.



Nota. Estudio de Redes Sociales 2021. (P.23).

La frecuencia de uso de las redes sociales se mantiene en un total de 1h 21 min. al día respecto al año 2020 con 1h 19 min. de media. La franja de los 16-24 años son los que más usan las redes sociales con 1h 42 min. y la red social Twitch pasa a ser la red social más utilizada con 1h 40 min. al día, seguida de iVoox, Instagram, Spotify y Discord siendo, en global, las app´s de contenido de vídeo/audio las más usadas.

Respecto al género la frecuencia de uso es indistinta, la suelen usar tanto las mujeres como los hombres dedicándoles de media 1h 23 min. las mujeres y 1h 21 min. los hombres.

La Red Social menos utilizada es la app de Linkedin, utilizada para la búsqueda de empleo, con una media de 40 min. al día, que coincide con los datos de la Figura 12 en que las Redes Sociales para buscar empleo son las menos usadas.

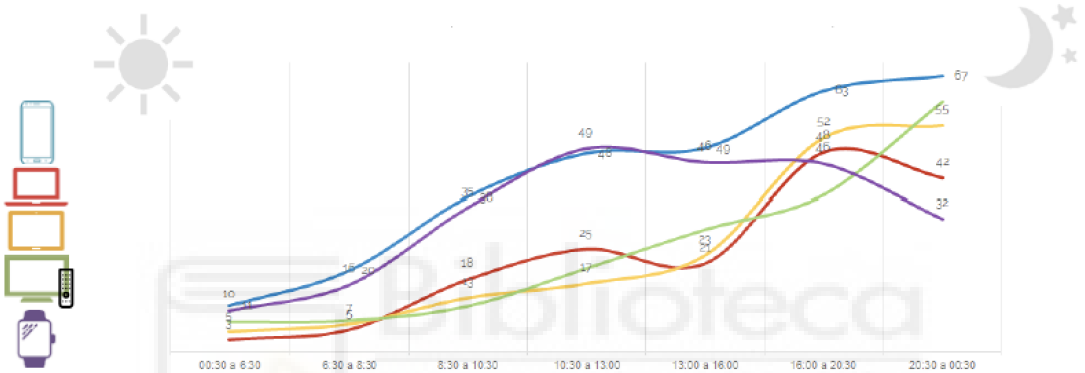
Durante esta media de uso es importante que, a diario, sobre todo en la población juvenil, haya un control parental sobre el uso de las Redes Sociales

para saber qué está haciendo el consumidor adolescente y con qué personas mantiene el contacto con el objetivo de educarle y formarle para prevenir ciertas actitudes ciberdelictivas. Actualmente, cabe especificar que en los dispositivos electrónicos, como en las plataformas de las Redes Sociales, hay "controles parentales" que monitorizan y controlan la actividad de los perfiles, avanzando así hacia un futuro con menos ciberdelincuencia.

Momento de conexión

Figura 21:

Estadística sobre el momento de conexión a las Redes Sociales a nivel nacional.



Nota. Estudio de Redes Sociales 2021. (P.35).

El momento de más conexión durante el día es la franja de 20:30 a 00:30 horas, siendo el móvil el dispositivo por excelencia con 67 puntos porcentuales, siendo la franja de madrugada la menos usada con unos escasos 3-10 puntos según el dispositivo utilizado, subiendo progresivamente durante las horas diurnas, y según los dispositivos utilizados, llegando a su punto álgido durante la tarde.

Este punto también es importante para la prevención de los delitos, ya que los posibles acosadores utilizarán las horas en las que más usuarios estarán conectados. Esta gráfica nos muestra que su conocimiento por parte de los padres les haga sospechar, si monitorizan los dispositivos familiares, que el uso de las Redes Sociales utilizados de madrugada puede ser un indicio de que se pueda estar realizando un uso indebido o pueda existir algún peligro, con el beneficio de poder corregir esas actitudes en el adolescente que en un futuro pueda derivar en una víctima del ciberacoso.

5.4. Ciberacoso

En primer lugar, se debe diferenciar entre varios conceptos para entender qué es el ciberacoso.

Primeramente, cabe explicar, qué significa la palabra bullying y se define como acoso físico o psicológico, pero con la diferencia que ese acoso se tiene que dar entre escolares, es decir, entre su mismo grupo de iguales. De ahí viene el vocablo "ciberbullying". Definimos, por una parte, el prefijo "ciber" que es el acortamiento de la palabra "cibernético" que significa: relacionado con las redes informáticas o realidad virtual. *(Real Academia de la Lengua Española. RAE, 2022).* Por tanto, el ciberbullying es el acoso entre personas con edades escolares a través de las redes informáticas, usando generalmente, las redes sociales.

Conociendo estas definiciones podemos definir también lo que se denomina el ciberstalking. El ciberstalking es una combinación de dos palabras inglesas "ciber" (como la hemos definido anteriormente) y "stalking" que se puede traducir de una forma literal como acecho o persecución, dando el resultado que conocemos de forma más regular en el castellano que es el ciberacoso que lo podremos definir como: el acecho o violencia de género a través de la red. Se diferencia con el ciberbullying de que este tipo de violencia de género es a nivel global abarcando todas las edades.

Dicho esto, observamos que las redes sociales e Internet han traído grandes beneficios a nivel de comunicación global, pero también se han agravado problemas como el acoso, en que los autores han traspasado su amenazas físicas, mensajes vejatorios, etc. al nivel del anonimato o avance que suponen las nuevas tecnologías, para acosar a través de las redes, o la utilización de las redes para robar información de las víctimas, uso de Internet como base para causar violencia psicológica mediante falsas acusaciones o mostrar información falsa, así como fotografías de la víctima en situaciones comprometidas (llamado sexting, que hablaremos en la sección 5.5), también se utilizan las nuevas tecnologías como herramienta para dañar de forma remota el equipo de la víctima e imposibilitarle la interactuación con sus semejantes, entre otras muchas acciones.

Para entender mejor que es el ciberacoso es preciso aludir a varias definiciones de varios autores para conocer qué importante es el concepto en la actualidad por el uso constante de las nuevas tecnologías sobre todo por la población joven, enfatizar que los estudios sobre el ciberacoso están centrados en los jóvenes que son los usuarios que más expuestos están al ser el grupo de edad que está más conectado a las nuevas tecnologías:

Empezamos por lo que enuncia la legislación española vigente sobre el

ciberacoso que la define como la violencia de género cuya práctica se da en el mundo digital que constituye Internet. También se define como una forma de desigualdad digital en la medida en que unos ciudadanos, con más poder en otros ámbitos, limiten las posibilidades de otras per-sonas para disfrutar de Internet con libertad y autonomía. Esta circunstancia transforma a Internet en una puerta de entrada para la des-trucción de la vida íntima de la persona acosada. *(Torrés, C., Manuel, J. y De Marco, S., 2014).*

Otra definición es el ciberacoso como forma de violencia de género que implica, agresión psicológica, sostenida y repetida en el tiempo, contra su pareja o expareja, utilizando para ello las nuevas tecnologías a través de plataformas o sistemas virtuales como el correo electrónico, sistemas de mensajería, redes sociales, blogs o foros…, siendo su objetivo la dominación, la discriminación, el abuso de la posición de poder y debe su-poner una intromisión, sin consentimiento, en la vida privada de la víctima. *(Verdejo Espinosa, 2015).*

"….el ciberacoso es un tipo de práctica digital en la que el agresor ejerce dominación sobre la víctima mediante estrategias vejatorias que afectan a la privacidad e intimidad de las víctimas. Es decir, el acosador ejerce su poder sobre elementos que la víctima considera privados y personales. Esta irrupción, abrupta en la mayoría de casos, trata de poner en evidencia aspectos de su vida personal que la víctima desearía mantener en el ámbito de lo privado" *(Hensler-McGinnis, 2008).*

El ciberacoso es un conjunto de comportamientos mediante los cuales una persona, un conjunto de ellas o una organización usan las TIC para hostigar a una o más personas. Dichos comportamientos incluyen, aunque no de forma excluyente, amenazas y falsas acusaciones, suplantación de la identidad, usurpación de datos personales, daños al ordenador de la víctima, vigilancia de las actividades de la víctima, uso de información privada para chantajear a la víctima, etc. *Bocij y McFarlane (2002).*

El ciberacoso es una forma de invasión en el mundo de la vida de la víctima de forma repetida, disruptiva y sin consentimiento utilizando las posibilidades que ofrece Internet. Estas actividades tienen lugar entre personas que tienen o han tenido alguna relación y se produce por motivos directa o indirectamente vinculados a la esfera afectiva. De esta forma, en alguna medida, el ciberacoso tiene un importante componente emotivo como los celos, la envidia o el género. Los actos separados que componen la intrusión no tienen por qué significar, por sí mismos, abuso. Sin embargo, tomado en su conjunto (efecto acumulativo) sí constituyen un problema. *(Royakkers, 2000).*

Por eso es tan importante conocer por parte de los usuarios los peligros que esconde Internet y saber los conceptos para ser conscientes de los riesgos

que conllevan ciertos comportamientos o relaciones con otros usuarios de las redes. Se ha demostrado que ciertas prácticas en el uso de Internet pueden producir en la víctima graves consecuencias emocionales y psicológicas como el suicidio, *(United Nations, 2016)*, por ello también es tan importante la formación en la materia y la prevención de la cual hablaremos en el próximo punto.

Respecto a las estadísticas, la trascendencia y las consecuencias que está tomando este tipo de Violencia de Género. El ciberacoso (Violencia de género a través de las nuevas tecnologías) todavía no se han obtenido datos objetivos, aunque se ha investigado para encontrar datos sobre el ciberacoso a nivel nacional, hallamos en la página del I.N.E. información en la cual comunica que el estudio de las estadísticas sobre el ciberacoso está como proyecto piloto y empezarán a tener datos estadísticos a partir del año 2023.

Este proyecto técnico se elabora en el año 2021 como un "Estudio sobre las conductas saludables de los adolescentes escolarizados" en el cual se estudia a la población de estudiantes entre 11 y 18 años mediante una encuesta que abarcan preguntas para obtener información de los últimos 7 días, último mes, últimos 2 meses, últimos 6 meses, último año, desde el inicio del curso e incluso de toda la vida, además de los momentos específicos de cada persona: "La primera vez que" o "la última vez que" sucedió un hecho.

Este proyecto se basa en unas variables de estudio como el consumo de sustancias, la conducta sexual, relación entre iguales y de pareja (apoyo percibido, satisfacción con el grupo, tener pareja, duración relación de pareja, además de la recogida de datos sobre el bullying/acoso y el ciberbullying/ciberacoso como también datos sobre la frecuencia y motivo de uso de medios electrónicos.

Respecto a las variables de clasificación, este proyecto técnico abarca datos sobre el sexo, grupos de edad, hábitat, estatus socioeconómico familiar y país de origen.

En lo que refiere al diseño muestral, durante la última edición se tomaron datos a un total de 40.495 alumnos de un total de 511 centros educativos. Para la próxima edición tienen pensado recoger un tamaño muestral similar. El método de selección de la muestra se aplica sobre un muestreo aletorio polietápico estratificado por conglomerados, teniendo en cuenta la edad, la comunidad autónoma y la titularidad del centro educativo (público o privado) de los adolescentes; de esta forma es como obtienen una muestra representativa de la población española de estas edades.

Finalmente destacar el planteamiento de futuro que se desea realizar de este proyecto técnico, enunciando que:

En el año 2021 elaboran el cuestionario y realizan el primer estudio piloto.

En el año 2022 están recogiendo los datos para su posterior análisis.

Y a partir del año 2023 y siguientes ya realizarán la elaboración de informes y su difusión. *(Subdirección General de Promoción, Prevención y Calidad, 2021).*

Finalmente destacar, que actualmente existe un protocolo de Intervención para erradicar el Ciberacoso enfocado para los jóvenes y en el cual intervienen de forma indistinta, los familiares, los alumnos, el centro escolar y el profesorado componiéndose de 5 fases: la **Prevención**, la **Detección**, la **Protección**, la **Intervención** y la **Evaluación**. *(Castro Clemente, C., 2017).*

En la fase de **"Prevención"**, orientada a familias, profesores y alumnos, tiene como objetivo principal proporcionar una amplia información sobre el fenómeno del ciberacoso así como la de incrementar el conocimiento sobre los riesgos potencialmente negativos en el uso de las nuevas tecnologías a fin de prevenir la victimización en los adolescentes.

Para ello, se realizan diferentes acciones globales con toda la comunidad educativa como son reuniones, conferencias públicas y profesionales, presentación de gráficas, cartelería, información sobre el problema o principales signos para identificar su manifestación.

Asimismo, se relaciona una serie de acciones y materiales específicos en distintos niveles con el fin de aumentar y fortalecer su conocimiento a nivel:

Familiar: Introducción y definición terminológica; formas en las que se manifiesta el cyberbullying, pautas sobre cómo se manifiesta dentro de casa e información de espacios web de ayuda y consulta.

Profesorado: Formación y capacitación para abordar el problema; utilización de instrumentos didácticos en su acción tutorial; acompañar a los estudiantes en el uso de las TIC; promover en los alumnos no silenciar esta situación así como rechazar las prácticas abusivas; mantener una interacción abierta y activa con los estudiantes; realizar debates y escenificaciones con los alumnos.

Cabe destacar la propuesta novedosa realizada por la Comunidad de Madrid (2016) en la que incluye una guía docente sobre la prevención del suicidio en escolares en la que ofrece, además de información, indicadores y síntomas de alerta susceptibles de ser observados por el centro educativo y grupo familiar, contiene también recursos a los que pueden dirigirse los padres y los profesores.

Alumnado: Presentar a los estudiantes situaciones de riesgo en Internet mediante la utilización de material didáctico (vídeos o videojuegos) con la finalidad de adquirir un mayor conocimiento sobre sus peligros y desarrollar habilidades de protección para evitar la violencia. Involucrar a los alumnos como protagonistas y neutralizadores de la violencia impartiendo formación e información con los demás estudiantes del centro.

Como material didáctico, existe un videojuego educativo llamado “Tabby plays - Cyberbullying Gameover” cuyo objetivo principal es cambiar las conductas arriesgadas de los adolescentes cuando navegan por Internet.

Por otra parte, existen guías elaboradas por el Colegio Oficial de Psicólogos de Madrid y la Fundación Atresmedia e INCIBE en las cuales se pueden analizar un conjunto de actividades propuestas en sus programas para que los estudiantes sean los protagonistas en sensibilizar y formar con sus conocimientos a otros alumnos en la erradicación de la violencia.

El módulo **“Detección”** tiene como objetivo identificar los factores de riesgo y evaluar una amenaza de peligro en la web. Algunos de los programas analizados destacan que los cuestionarios, o tests online, representan la mejor herramienta para detectar y autoevaluar distintas situaciones de maltrato así como para obtener recomendaciones de actuación sobre las distintas modalidades de acoso.

Hay cuestionarios a nivel internacional, a nivel Europeo, con el programa “Tabby” que dispone de un cuestionario online de preguntas de autoevaluación dirigido a los jóvenes cuyo objetivo es ayudarles a reconocer si están en una situación de peligro; y a nivel nacional, en que podemos consultar la aplicación “SociEscuela”, desarrollada por la Comunidad Autónoma de Madrid, cuya finalidad es la detección temprana y avanzada de posibles víctimas e informar a los centros educativos para activar su plan de intervención.

Además de los tests, existen unos indicadores sintomatológicos (físicos, psíquicos y relacionales) que permiten detectar un episodio de acoso.

En las “Guías S.O.S. contra el Ciberbullying”, elaboradas por el Instituto Nacional de Tecnologías de la Comunicación (2014) y dirigidas a padres y profesorado, se proporciona información y recomendaciones para detectar un episodio de ciberacoso:

A nivel **familiar** se les relaciona una serie de pautas para aclarar y determinar la situación, así como un conjunto de síntomas que les puede ayudar a reconocer un episodio de maltrato aunque el adolescente silencie el acoso.

A nivel **educacional**, la guía presenta una conjunto de recomendaciones en su acción tutorial para detectar un posible caso de ciberacoso, además de indicar los pasos a dar y colaboradores a los que consultar en caso de que se confirme el acoso.

Como medidas de **“Protección”**, y dentro del objetivo de prevenir y evitar la victimización, se relacionan distintas acciones protectoras -institucionales, escolares y familiares- detalladas por niveles:

Familiar: Acompañar a los hijos en la navegación por Internet; establecer normas familiares y criterios sobre el uso de los dispositivos: edad, horarios,

conexión, desconexión, tiempo, acceso a aplicaciones…; instalar herramientas de protección y de alerta ante el acceso a contenidos inapropiados y peligrosos en todos los dispositivos: ordenadores, teléfonos móviles y tabletas; elegir contraseñas seguras y diferentes para cada servicio de Internet; cambiar las contraseñas router y establecer otras más seguras.

Centro escolar, profesorado y estudiantes: Además de aplicar el Plan de Convivencia elaborado por la institución escolar y dar a conocer las medidas disciplinarias que se adoptarían en un episodio de violencia, se pueden implantar un conjunto de acciones encaminadas a fortalecer la protección del menor como: vigilancia de recreos, pasillos, entradas-salida del centro, cambio de aulas, etc.; habilitar un sistema de comunicación interno y confidencial (e-mail, teléfono, etc.) entre estudiantes y tutores o personas adultas a las que poder acudir a pedir ayuda o implantar vigilantes con chalecos reflectantes en las instituciones escolares con el fin de recordar a los estudiantes que su labor es ser responsables de la seguridad de todos.

Una vez se presenten posibles indicios de un episodio de violencia entre iguales, como medida de **"Intervención"** es de muy buena aplicación el programa elaborado por la Comunidad de Madrid (2016) porque es en la actualidad uno de los mejores protocolos disponibles ya que mediante un único documento, se recoge todo el procedimiento de intervención escolar (fases, herramientas y líneas de actuación). Simultáneamente, presentar distintas recomendaciones para detener con rotundidad la situación:

Familia: Reconocer la situación de acoso sobre sus hijos y acudir al centro educativo para saber si han detectado la situación; realizar preguntas abiertas al adolescente para investigar lo que está sucediendo y conocer al hostigador; acudir a los amigos del menor para ampliar información y escuchar y dialogar con el adolescente.

En las guías de INTECO (2014) y de INCIBE (2016), se ofrecen recomendaciones específicas de actuación para que los padres pueden consultar cómo deben abordar un episodio de ciberacoso sobre sus hijos y, en el caso de episodios graves en el que se deban tomar medidas de atención urgente, se facilita los datos de contacto con el Ministerio Fiscal y Fuerzas y Cuerpos de Seguridad.

Centro escolar y alumnado: Activar el Plan de Actuación escolar establecido en el Plan de Convivencia que cada centro tenga elaborado así como entrevistarse con las familias y actores implicados e informarles del procedimiento y medidas a adoptar.

La última fase, **"Evaluación"**, persigue tres objetivos:

1) valorar la efectividad del programa y comprobar si ha cambiado la situación.

2) evaluar a profesores, alumnos y padres con el fin de estimar su conocimiento acerca del acoso y ciberacoso; actitudes y comportamientos ante el problema; probabilidad en ser ciberacosador o cibervíctima; modalidades y formas de ejercer la intimidación; familiaridad con la terminología y conocimiento de soluciones ante un episodio ocurrido.

3) acción investigadora con el fin de actualizar y mejorar aquellas áreas del programa que necesiten reforzarse.

Esta etapa de evaluación también debería integrarse la celebración de dos encuentros en el contexto educativo. Uno en el propio centro para que alumnos, profesores y familias valoren las actividades desarrolladas y realicen propuestas de mejora; y un segundo en el que el Equipo Directivo y la Comisión de Convivencia del Consejo Escolar de todos los centros participantes en el programa compartan sus experiencias, información y resultados a fin de establecer o mejorar acciones orientadas a la optimización del plan antiviolencia escolar.

Para realizar esta fase evaluativa, se puede consultar, entre otros, distintos programas en el que se indican las distintas fases para celebrar con éxito estos encuentros destacando la "Guía de prevención del ciberbullying" desarrollado por el Colegio Oficial de Psicólogos de Madrid y la Fundación Atresmedia (2014). *(Castro Clemente, C., 2017).*

5.4.1. Víctimas vulnerables y la Prevención

Tal como hemos visto anteriormente, concretamente en la Figura 9 , los usuarios que más se han conectado a Internet con un 99.8% en los últimos 3 meses es la franja de edad que abarca desde los 16 a los 24 años, es decir, la juventud, y con la práctica totalidad de jóvenes conectándose a Internet son a la misma vez los que más riesgo tienen de sufrir sus peligros, además se junta la casuística de que los jóvenes son la franja de edad que más curiosidad tienen por experimentar nuevas vivencias, bajo sentido del riesgo, tienen la necesidad de estar en contacto continuo con sus amigos/as, necesitan saber, hablar o ver fotos de sus amistades o de gente de su entorno. La adolescencia es una etapa en la que se empieza a crear una identidad propia, identidad que no puede entender sin tener ningún tipo de relación, sobre todo con su grupo de iguales.

En la adolescencia también es el momento que el individuo busca su intimidad, es cuando se empiezan a distanciar de sus progenitores y es aquí cuando las nuevas tecnologías y las redes sociales adquieren una especial relevancia para ellos, necesitan explorar continuamente su entorno, buscan

integrarse y pertenecer a un grupo social, contemplando la necesidad que tienen de disponer de conocimientos y vivencias como una curiosidad adolescente, y es esto precisamente lo que les hace especialmente vulnerables ante los peligros que puedan presentar las TICS; no saben qué deben publicar y qué no, aceptan a amigos/as que no conocen por el mero hecho de tener muchos contactos y ser así más populares, suben fotos de amigos/as en situaciones comprometidas, dan datos que no deben dar poniendo en peligro su intimidad, etc. *(Morduchowicz, R., 2012)*.

Además, porque con el uso de Internet obtienen las respuestas de una amplia gama de preguntas, consiguen información rápida y actual, mantienen el contacto con nuevos y/o existentes contactos, y en definitiva se divierten. *(Tsitsika, A., Tzavela E. y Mavromati, F., 2012)*.

El uso y/o abuso de Internet en sus diferentes y atractivas vertientes por parte de los menores genera, sin lugar a dudas, que aumenten las posibilidades de que estos jóvenes sufran distintos riesgos o lleguen a ser vulnerables a sufrirlos. El uso de Internet les hace pasar menos tiempo con su familia o sus amigos. Los cuatro tipos de riesgos fundamentales que pueden producir al usar Internet por parte de los menores son: el acceso a contenidos sexuales, el ciberbullying o ciberacoso escolar, la recepción de mensajes de tipo sexual y el encuentro con extraños conocidos a través de la red. *(Garmendia, M. et Al., 2012)*.

En lo que se refiere a los/as menores, en los últimos años, esta gran herramienta educativa ha demostrado ser un arma de doble filo, ya que engendra muchos peligros para los más vulnerables. Son muchos los riesgos que corren los niños/as navegando por Internet si no siguen los consejos de una navegación segura y no han recibido una correcta información acerca de los peligros y trampas que les acechan. Este colectivo tiene que valorar la comunicación física por encima de la que pueden entablar a través de las nuevas tecnologías. Las ventajas de conocer al interlocutor frente a los riesgos de no hacerlo.

Por otra parte, hay que señalar que todavía nos encontramos un porcentaje de población que básicamente no utiliza Internet por no tener conocimientos para su uso o por no tener la capacidad para afrontar los gastos que supone tener un ordenador y contratar una tarifa de Internet. Otros autores extienden el alcance de la Brecha Digital para explicarla también en función de lo que se ha denominado “analfabetismo digital”, que consiste en la escasa habilidad o competencia de un gran sector de la población, especialmente entre aquellos que han nacido antes de la década de 1960, para manejar las herramientas tecnológicas de computación y cuyo acceso a los servicios de Internet es por tanto muy limitado. Esto constituye un entorno de indefensión por la carencia de conocimientos que generen espacios de seguridad y protección para aquellos

menores de esta población que este en contacto con las TIC e Internet en otro lugar de su contexto, como podrían ser los centros educativos o los centros públicos. De este modo, aquellos menores que convivan en este tipo de entornos, son menores aún más vulnerables al no tener un entorno protector ya que sus progenitores o personas de referencia están inmersos en esta brecha digital o son analfabetos digitales, los cuales no pueden prestarle el apoyo que precisan para prevenir, controlar o intervenir en caso de riesgo.

Respecto al comportamiento de los adolescentes por género, los chicos realizan conductas de riesgo de ciberacoso con mayor frecuencia que las chicas.

Las mujeres jóvenes son más vulnerables al daño del ciberacoso por la desigualdad en la consideración y valoración social a la que se someten los comportamientos y las imágenes de las mujeres en la relación de pareja, por lo que su vivencia es muy traumática. *(Torres. C; Robles J. M.; de Marco, S., 2013).*

En cuanto a los grupos de mujeres en situación de especial vulnerabilidad, más de una quinta parte de los adolescentes justifica en cierta medida la violencia como reacción a una agresión; una de cada diez mujeres universitarias reconoce que se ha sentido obligada a conductas de tipo sexual en la que no quería participar, o que le han difundido mensajes, insultos o imágenes por Internet o teléfono móvil sin su permiso o que la han intentado aislar de sus amistades; aparecen nuevas formas de ejercer violencia como consecuencia del uso de las nuevas tecnologías que tienen una especial incidencia en la juventud, como el ciberacoso: la juventud, ya ”nativa digital”, presenta una percepción muy baja de sus efectos perniciosos; el intercambio de contenidos personales es una prueba de confianza o un acto de intimidad con la pareja (“prueba de amor”) y constituye una puerta abierta para que se dé el sexting (difusión de imagen de contenido erótico o sexual); tras la ruptura de la pareja, los ciberacosadores utilizan Internet para alcanzar a la víctima;

Las recientes encuestas y estudios acreditan que la población juvenil y adolescente resulta ser un colectivo especialmente vulnerable frente a la violencia de género. La población juvenil puede ser muy vulnerable a muchos casos desapercibidos de maltrato psicológico u otras formas más sibilinas y escondidas de violencia. Aunque este fenómeno se reconoce como “un problema social de primer orden”. *(Ministerio de Sanidad, Servicios Sociales e Igualdad, 2013-2016).*

Una vez comprobado que los jóvenes adolescentes y entre ellos en mayor medida las chicas son las víctimas más vulnerables, es preciso detallar las herramientas que existen para prevenir el ciberacoso para evitar futuras victimizaciones. La formación del usuario es básica a la hora de utilizar Internet y actualmente, aunque tenemos la sensación que Internet ha estado toda la vida

con nosotros, aún nos encontramos en el período inicial de uso de esta "gran arma de la comunicación", que es Internet, por lo que su utilización esconde peligros como el ciberacoso que pueden llegar a graves consecuencias o secuelas permanentes a los/las que lo padecen.

Primero debemos inculcar la importancia de los datos personales y que valoren la privacidad los jóvenes para prevenir que expongan sus datos públicamente y sean conscientes de los riesgos que estas publicaciones llevan anidadas como la usurpación de identidad y los fraudes, especialmente han aumentado los ataques cibernéticos como consecuencia del aumento del uso de estas tecnologías con motivo de la pandemia de la COVID-19. *(Lopez Gutiérrez, J. et al., 2020).*

Para evitar estos comportamientos La Agencia Española de Protección de Datos (AEPD), el Instituto Nacional de Ciberseguridad (INCIBE) y la Oficina de Seguridad del Internauta (OSI), han colaborado y editado una "Guía de Privacidad y Seguridad en Internet" con el fin de promover el uso seguro y responsable de Internet, explicando los riesgos de la navegación pero también enseñando a los usuarios a navegar sin comprometer nuestra seguridad y privacidad mediante la explicación de cómo establecer contraseñas seguras, privacidad en Redes Sociales… **conceptos** que vamos a desarrollar a continuación:

El **primero** de los conceptos trata sobre la protección de nuestros dispositivos móviles. El elemento en sí, el teléfono no tiene en realidad valor, lo que realmente vale y es de interés para los supuestos hackers es nuestra información por eso debemos salvaguardarla, además del resto de personas que nos comunicamos como: los contactos, fotografías, vídeos, correos electrónicos… en general, información que no nos gustaría perder y que cayesen en manos de terceros. Para ello, debemos proteger la información de nuestro móvil con información cifrada, mediante el bloqueo por código para entrar al terminal; herramientas de seguridad, para poder localizar el dispositivo en caso de pérdida; copias de seguridad, para tener nuestra información en otro lugar seguro por si se daña o perdemos el móvil; descargas en sitios seguros, es decir, de sitios oficiales; revisión de comentarios, los mismos usuarios nos darán pistas de cómo es la aplicación; e instalación de antivirus, para detectar aplicaciones que dañen o roben información de nuestro dispositivo; Todos estos consejos se muestran tal como se muestra en la siguiente figura:

Figura 22:

Consejos para la protección de los móviles.

Nota. Guía de Privacidad y Seguridad en Internet, AEPD e INCIBE.(P.4).

El **segundo** de los consejos es utilizar contraseñas robustas, con ello evitamos que entren en nuestras áreas privadas como los bancos y puedan usurpar nuestra identidad, realizar fraudes… aparte de que la contraseña sea robusta debe ser diferente para cada sitio. Al final tenemos tantas contraseñas que es difícil acordarse de todas, entonces es buen momento para usar un gestor de contraseñas y usar reglas nemotécnicas para acordarse. En la siguiente figura podemos ver una muestra de cómo crear contraseñas fuertes.

Figura 23:

Cómo crear contraseñas robustas.

Nota. Guía de Privacidad y Seguridad en Internet, AEPD e INCIBE.(P.5).

Tercer consejo: Verificación en dos pasos. ¿Qué quiere decir esto? Que al acceder a un sitio web no dependamos solamente de una contraseña, sino de un factor de verificación mediante un mensaje al móvil el cual generará un código que se acompañará a la dirección de la contraseña, ganando en seguridad y confianza.

Figura 24:

Sistema de verificación en dos pasos.

Nota. Guía de Privacidad y Seguridad en Internet, AEPD e INCIBE.(P.6).

Cuarto: Realizar copias de seguridad. Ello conlleva guardar toda la información de tu dispositivo en otro lugar, bien sea disco duro externo, ordenador, "nube" virtual donde se almacenan datos… con el objetivo de si ocurre alguna incidencia al dispositivo móvil, con la copia de estos datos podamos introducir de nuevo los mismos datos en el dispositivo u otro nuevo preservando así nuestros contactos, fotos, anotaciones y documentos importantes. En la actualidad existen herramientas muy eficaces que realizan copias automáticas en servidores virtuales y que se realizan de forma automática de forma diaria por lo que la pérdida de información es mínima.

Figura 25:

Realizar copias de seguridad.

Nota. Guía de Privacidad y Seguridad en Internet, AEPD e INCIBE.(P.7).

Quinta recomendación: Navegar por páginas fiables. ¿Cómo se consigue? Los que no están muy familiarizados con las nuevas tecnologías tienen miedo de realizar acciones comprometidas en Internet como entrar en el área privada de la banca electrónica y que por desconocimiento, les lleva al miedo porque temen que les roben el dinero de su cuenta bancaria… para ello debes seguir ciertos pasos como: Ver el protocolo de la página que empiece por "https://" la "s" final nos dice que es una web segura, además de un símbolo de un candado cerrado en la barra de direcciónes, también debemos tener instalado en el ordenador un buen antivirus para prevenir amenazas y que las detecte para hacer de barrera cortafuegos, tener los programas y navegadores actualizados para que puedan detectar las nuevas amenazas, evitar conectarse a redes WIFI públicas ya que es fácil robar datos sin demasiados conocimientos informáticos, saber utilizar la banca online para saber reconocer las presuntas estafas o correos eléctrónicos fraudulentos que solicitan claves o datos personales, el banco nunca envía este tipo de correos electrónicos, igualmente pasa con las compras online, mirar el precio, que no lleve cargas adicionales, opiniones de los usuarios, formas de pago o políticas de devoluciones.

Figura 26:

Navegar por páginas fiables.

Nota. Guía de Privacidad y Seguridad en Internet, AEPD e INCIBE.(P.8).

Sexta: Introducción de datos personales. En la mayoría de páginas web no tenemos la obligación de introducir todos los datos personales. Con el D.N.I, nombre, apellidos, dirección y número de teléfono ya es suficiente. Sin embargo, sí que existen lugares que tienes obligación de facilitar más datos personales como por ejemplo la contratación de un seguro médico. En la siguiente figura aparecen las recomendaciones a seguir para facilitar datos personales.

Figura 27:

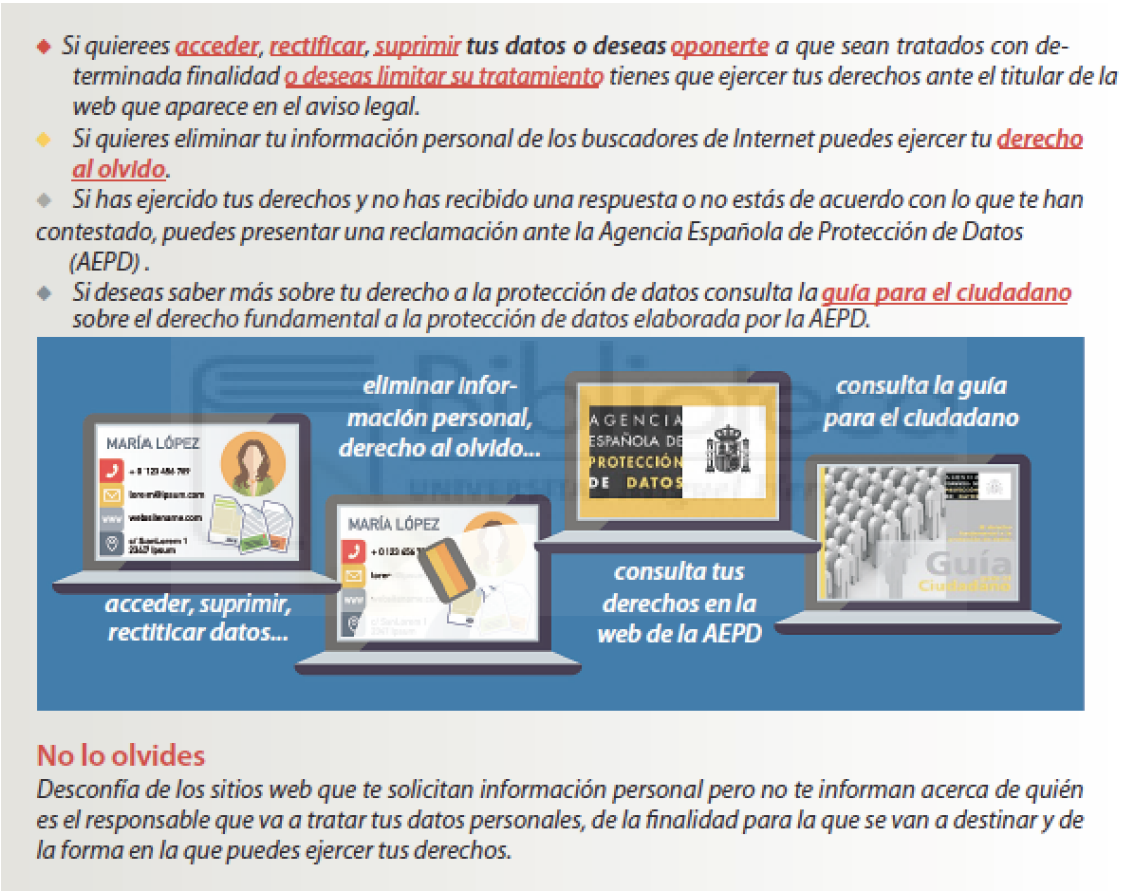
Introducción de datos personales.

Nota. Guía de Privacidad y Seguridad en Internet, AEPD e INCIBE.(P.9).

Séptima: ¿Cómo eliminar datos personales de la red? En ocasiones facilitar datos personales en webs puede provocar que pierdas el control sobre tu propia información. Para evitar estas situaciones, antes de facilitar datos, debes asegurarte a quién puedes dirigirte para el tratamiento, rectificación, cancelación o eliminación de tus datos personales, si no lo encuentras, desconfía. Si llega el caso que no puedes reclamar siempre puedes presentar una reclamación a la Agencia Española de Protección de Datos (AEPD).

Figura 28:

Cómo eliminar datos personales de la red

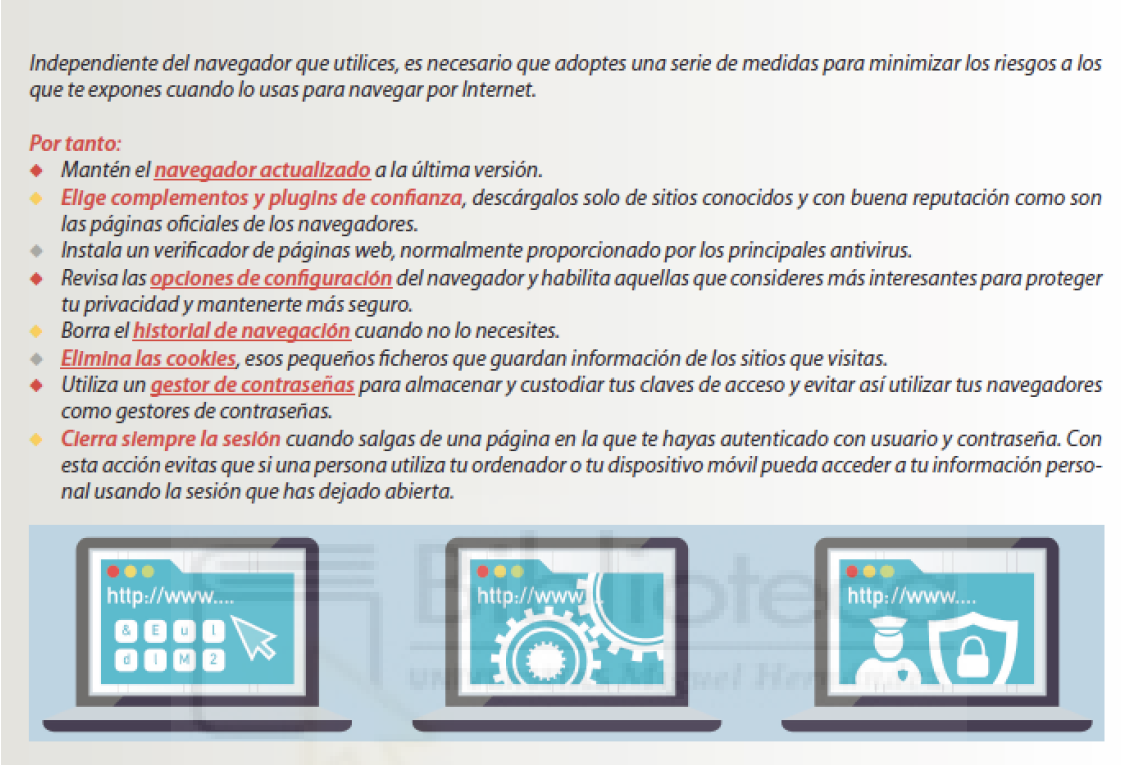


Nota. Guía de Privacidad y Seguridad en Internet, AEPD e INCIBE. (P.10).

Octava: Modo “navegación privada” en los navegadores para preservar tus consultas e historial para evitar posibles filtraciones sobre todo en los ordenadores compartidos.

Figura 29:

“Navegación privada”



Nota. Guía de Privacidad y Seguridad en Internet, AEPD e INCIBE. (P.11).

Novena: ¡Cuidado con la información personal que introduces en las Redes Sociales! De forma común tendemos a rellenar los formularios que nos ofrecen las redes sociales para introducir nuestros datos personales. Destacar que no es necesario completar los datos de la dirección de tu domicilio, trabajo, etc. Puede ser vista por terceras personas y ser utilizada de forma fraudulenta.

En la próxima imagen aparecen una serie de recomendaciones y consejos para evitar introducir más información que la estrictamente necesaria.

Figura 30:

¡Cuidado con la información personal que introduces en las Redes Sociales!

Nota. Guía de Privacidad y Seguridad en Internet, AEPD e INCIBE. (P.12).

Décima: Identificar los riesgos y los timos en servicios de mensajería instántanea. Aplicaciones como Whatssap no están exentas de timos ya que en ella se reúnen gran cantidad de usuarios que pueden llegar a ser potenciales víctimas, por ello, es importante detectar mensajes fraudulentos como mensajes de personas no conocidas, enlaces a páginas web con direcciones/dominios sospechosos, mensajes en cadena, mensajes que tienen un premio como reclamo… todo ello tiene como riesgo el robo de información personal, en la siguiente figura se muestran consejos para evitar la exposición a los riesgos que esconden estas aplicaciones.

Figura 31:

Identificar los riesgos y los timos en servicios de mensajería instántanea.

Nota. Guía de Privacidad y Seguridad en Internet, AEPD e INCIBE. (P.13).

Undécima recomendación: ¡Cuidado con la información falsa en Internet! ¿Cómo identificarla? Si recibimos noticias que capten nuestra atención mediante enlaces, desconfía. Estos enlaces es la puerta de entrada para que se inicie la instalación de aplicaciones fraudulentas que tienen por objeto "espiar" y robar datos de tu teléfono. En la siguiente figura se muestra información para prevenir este tipo de estafa.

Figura 32:

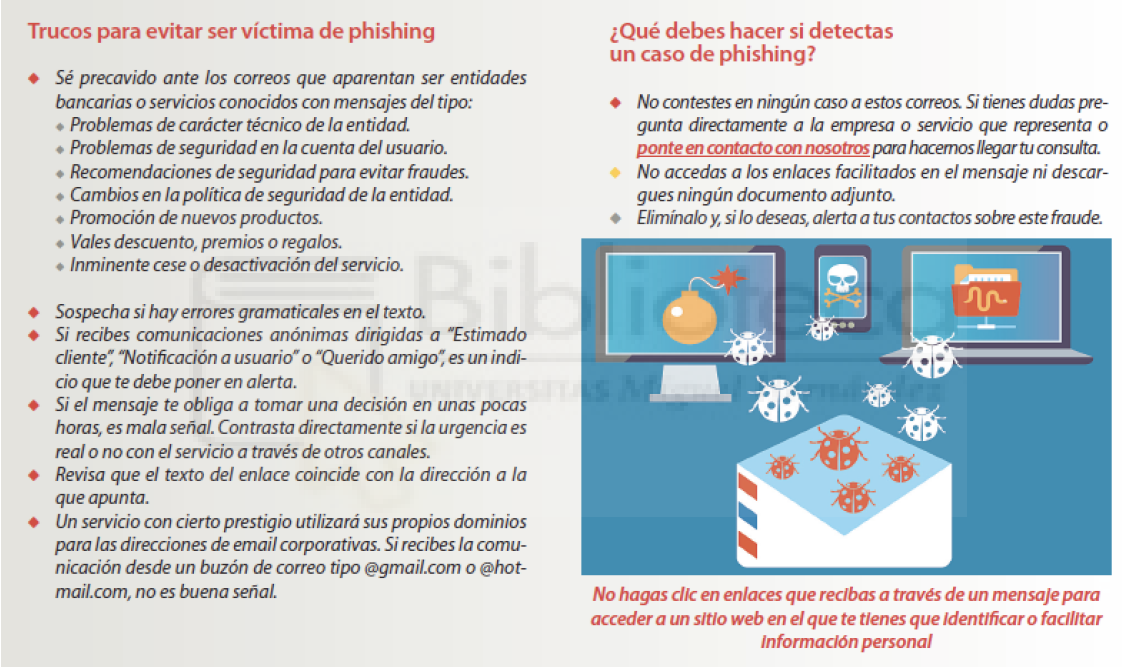
¡Cuidado con la información falsa en Internet!

Nota. Guía de Privacidad y Seguridad en Internet, AEPD e INCIBE. (P.14).

Duodécima: Phishing: Fraude que intenta robar nuestros datos personales y bancarios. El phishing se muestra generalmente mediante una suplantación gráfica de una página oficial, tipo banco, empresa de comunicaciones… con un mensaje que se envía a través de cualquier medio, generalmente, correo electrónico para comunicar que ha habido un error técnico y necesitan que vuelvas a introducir tus datos personales y los envíes a la dirección del remitente… con ello consiguen datos personales que utilizarán de forma fraudulenta. Para evitar ser víctima de Phishing en la próxima figura se muestran las recomendaciones principales para conocer su "modus operandi".

Figura 33:

Phishing.

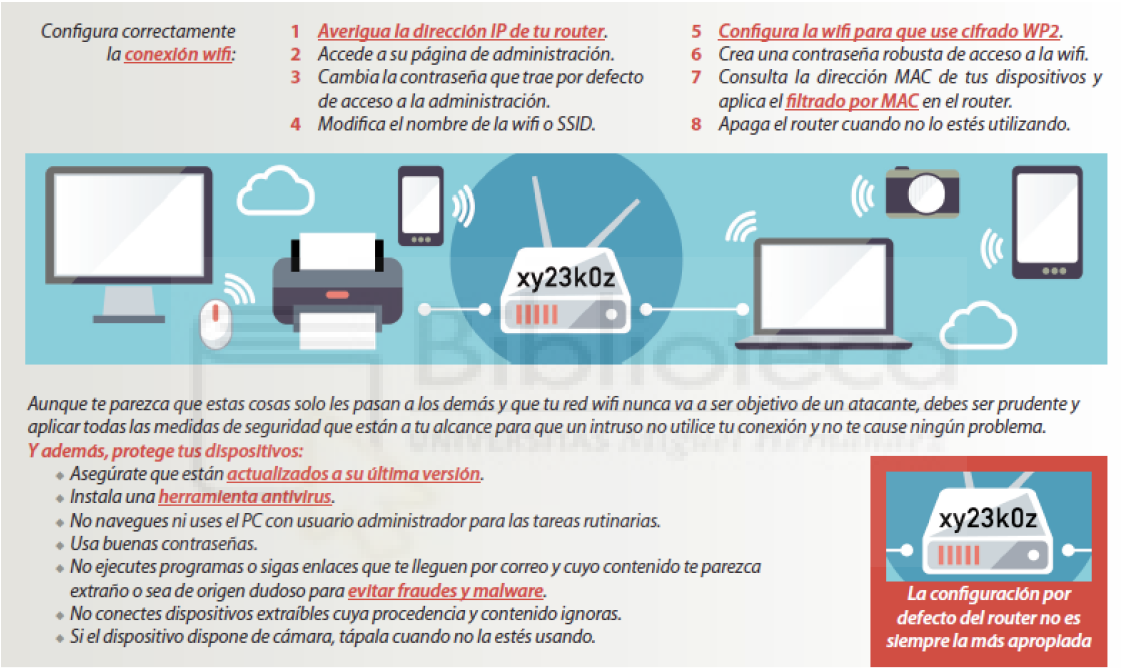


Nota. Guía de Privacidad y Seguridad en Internet, AEPD e INCIBE. (P.15).

Décimotercera: ¡Ojo si te falla la conexión a Internet! Actualmente, como hemos visto, la mayoría de hogares españoles tienen conexión a Internet. Si detectas que la conexión wifi va a velocidad anormalmente lenta, puede ser que tengas intrusos en tu router wifi, para ello debes tener instauradas una serie de recomendaciones para evitar que personas ajenas a tu vivienda puedan robarte información o conectarse con los dispositivos vinculados a tu router. En la Figura 33 se muestran los consejos y recomendaciones para proteger de forma efectiva tu conexión wifi y evitar acciones ilícitas.

Figura 34:

¡Ojo si te falla la conexión a Internet!



Nota. Guía de Privacidad y Seguridad en Internet, AEPD e INCIBE. (P.16).

Decimocuarta: Protección del correo electrónico. Actualmente el correo electrónico es una herramienta muy eficaz y en la cual se guarda mucha información personal. Tal como hemos visto anteriormente, a través del correo se pueden producir muchas situaciones fraudulentas, por esta razón es también muy importante protegerlo como por ejemplo: el inicio de sesión en dos pasos, establecer una contraseña robusta y sobre todo detectar posibles correos maliciosos eliminándolos y marcándolos como correo basura. En la Figura 34 podemos ver cuáles pueden ser las consecuencias de una deficiente seguridad en la cuenta de correo electrónico.

Figura 35:

Protección del correo electrónico.

Nota. Guía de Privacidad y Seguridad en Internet, AEPD e INCIBE. (P.17).

Decimoquinta: Información personal en la nube. La nube posee innumerables ventajas y te proporciona un servidor virtual que puedes acceder desde cualquiera de tus dispositivos, actualizándose desde el terminal con el cual trabajes, además de realizar la buena labor de copia de seguridad ya que los datos no están en el interior del teléfono, pero para evitar poner en peligro esta información hay que tener en cuenta varios factores que se muestran en la siguiente figura:

Figura 36:

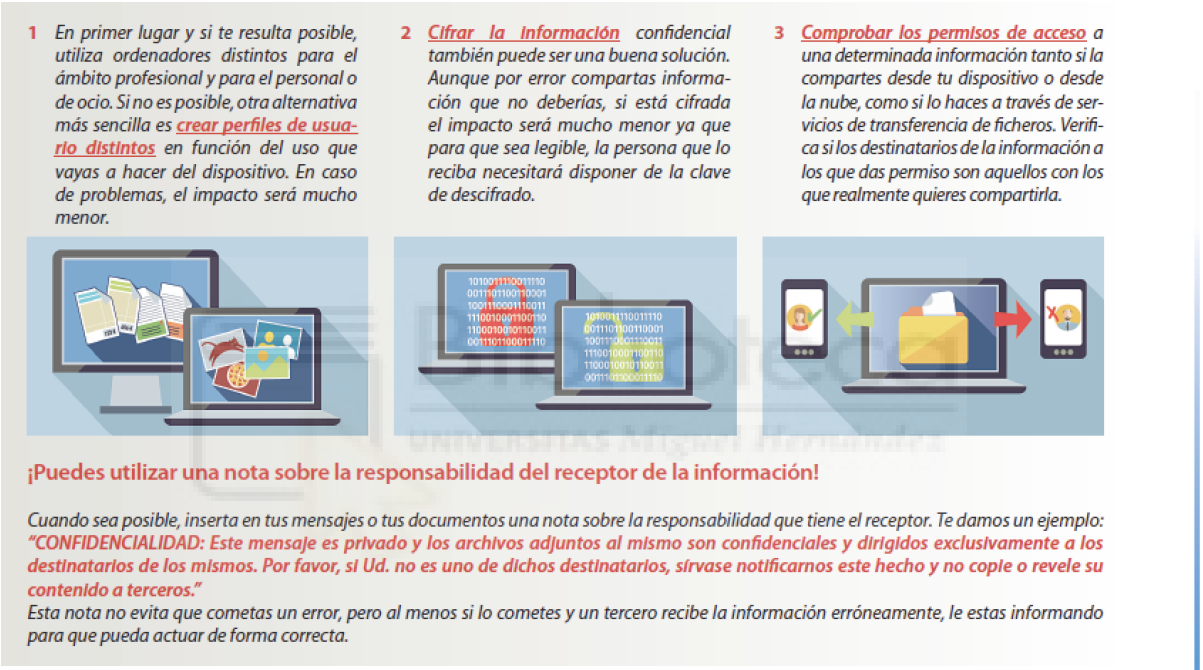
Información personal en la nube.

Nota. Guía de Privacidad y Seguridad en Internet, AEPD e INCIBE.(P.18).

Decimosexta: ¿Cómo compartir ficheros con las aplicaciones con el sistema P2P? Las aplicaciones P2P es un sistema avanzado de transferencia de ficheros pero lo más importante es su correcta configuración ya que si la carpeta raíz compartida es la opción “c:\” de tu disco duro, estarás compartiendo toda la información de tu ordenador a todos los usuarios. Por tanto, se debe asegurar que compartes sólo la carpeta en la cual tienes los archivos que quieres compartir. En la siguiente figura están relacionados los consejos y recomendaciones que se deben seguir para que la configuración de las aplicaciones P2P sea la correcta.

Figura 37:

¿Cómo compartir ficheros con las aplicaciones con el sistema P2P?

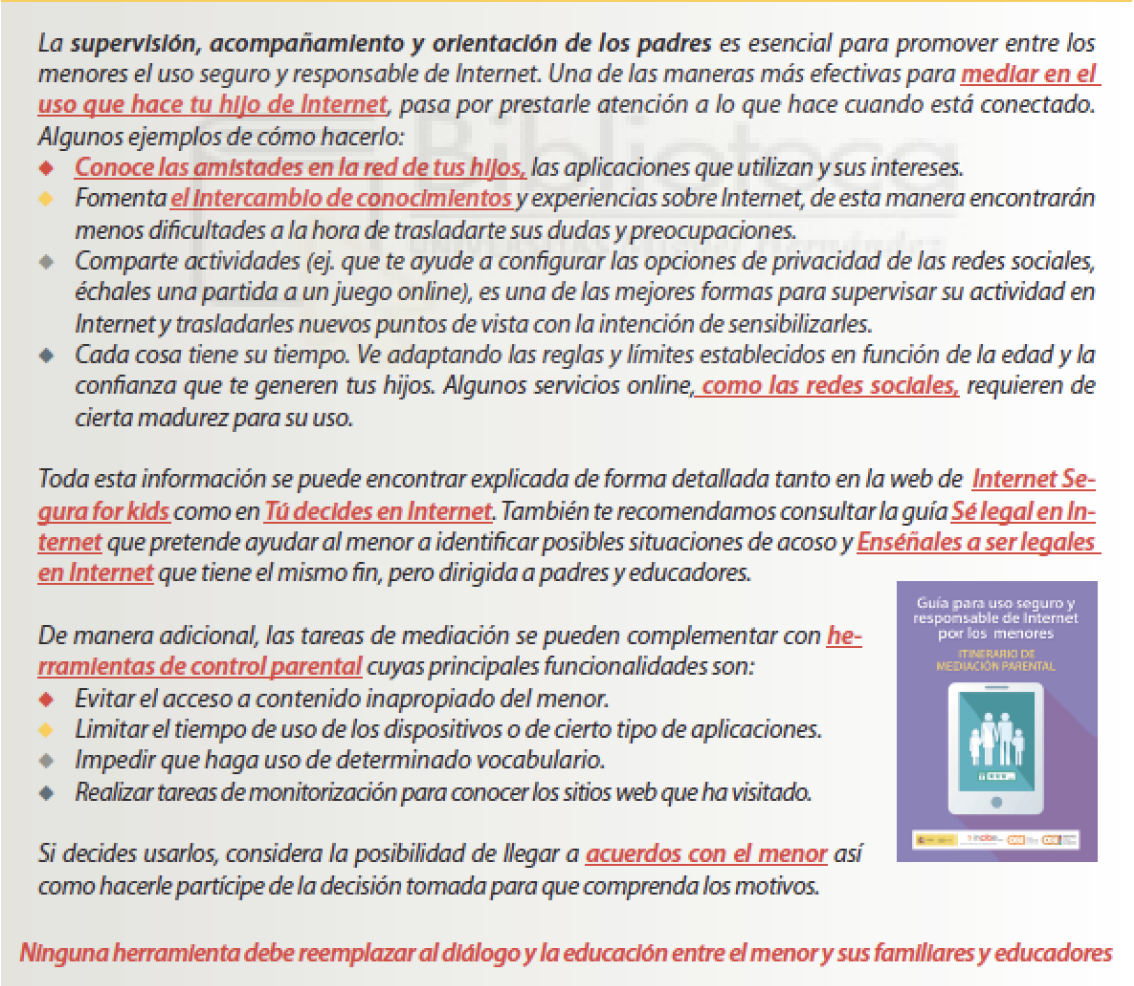


Nota. Guía de Privacidad y Seguridad en Internet, AEPD e INCIBE. (P.19).

Decimoséptima: ¿Cómo utiliza mi hijo Internet? Uno de los mayores problemas a los cuales se enfrentan los padres actualmente es a su "analfabetismo digital" que hablamos anteriormente, eso provoca que el menor navegue libremente por el espacio web con los peligros que ello conlleva mediante el riesgo de ver contenidos inapropiados, publicación excesiva de información privada, incorrecta gestión de información, ser víctima de suplantación de identidad, así como convertirse en víctimas de delitos como el sexting, el grooming y el ciberbullying de los cuales hablaremos en la sección 5.5. de este trabajo. La solución no está en prohibirle esta herramienta ya que actualmente es beneficiosa para el desarrollo del menor. Pero para evitar que nuestro hijo sea víctima de nuestro analfabetismo, en la Figura 37 nos muestra consejos y recomendaciones para favorecer un uso responsable y eficiente de Internet.

Figura 38:

¿Cómo utiliza mi hijo Internet?



*La **supervisión, acompañamiento y orientación de los padres** es esencial para promover entre los menores el uso seguro y responsable de Internet. Una de las maneras más efectivas para mediar en el uso que hace tu hijo de Internet, pasa por prestarle atención a lo que hace cuando está conectado. Algunos ejemplos de cómo hacerlo:*

- *Conoce las amistades en la red de tus hijos, las aplicaciones que utilizan y sus intereses.*
- *Fomenta el intercambio de conocimientos y experiencias sobre Internet, de esta manera encontrarán menos dificultades a la hora de trasladarte sus dudas y preocupaciones.*
- *Comparte actividades (ej. que te ayude a configurar las opciones de privacidad de las redes sociales, échales una partida a un juego online), es una de las mejores formas para supervisar su actividad en Internet y trasladarles nuevos puntos de vista con la intención de sensibilizarles.*
- *Cada cosa tiene su tiempo. Ve adaptando las reglas y límites establecidos en función de la edad y la confianza que te generen tus hijos. Algunos servicios online, como las redes sociales, requieren de cierta madurez para su uso.*

Toda esta información se puede encontrar explicada de forma detallada tanto en la web de Internet Segura for kids como en Tú decides en Internet. También te recomendamos consultar la guía Sé legal en Internet que pretende ayudar al menor a identificar posibles situaciones de acoso y Enséñales a ser legales en Internet que tiene el mismo fin, pero dirigida a padres y educadores.

De manera adicional, las tareas de mediación se pueden complementar con herramientas de control parental cuyas principales funcionalidades son:

- *Evitar el acceso a contenido inapropiado del menor.*
- *Limitar el tiempo de uso de los dispositivos o de cierto tipo de aplicaciones.*
- *Impedir que haga uso de determinado vocabulario.*
- *Realizar tareas de monitorización para conocer los sitios web que ha visitado.*

Si decides usarlos, considera la posibilidad de llegar a acuerdos con el menor así como hacerle partícipe de la decisión tomada para que comprenda los motivos.

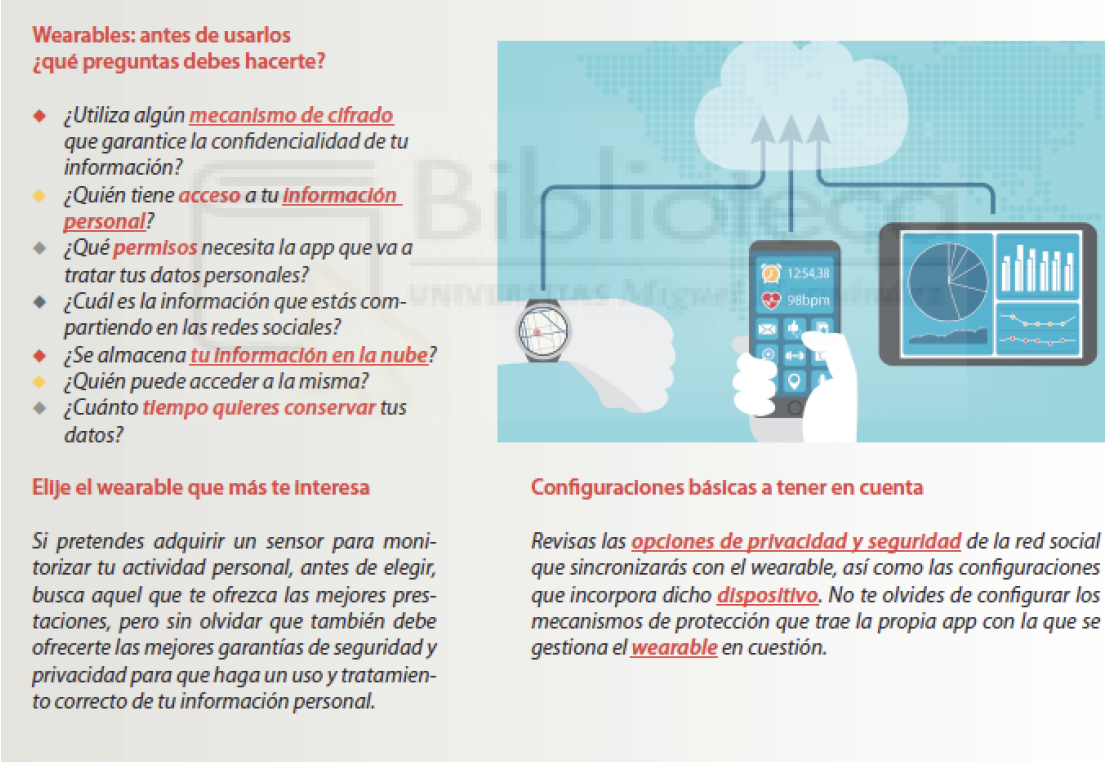
Ninguna herramienta debe reemplazar al diálogo y la educación entre el menor y sus familiares y educadores

Nota. Guía de Privacidad y Seguridad en Internet, AEPD e INCIBE. (P.20).

Decimoctava: ¿Las pulseras y relojes (wearables) son seguros? Actualmente existen muchos dispositivos que recogen todo tipo de información sobre nosotros, uno muy novedoso es los wearables o relojes inteligentes que tienen la virtud de monitorizar todos los datos de salud y avisarnos de cualquier anomalia, además de ponernos en la muñeca todo un mundo de conectividad con otros dispositivos. Ante esta avalancha de tecnología la mejor recomendación es estar alerta y ser consciente de la configuración del dispositivo para compartir los datos que nos interesen para evitar el riesgo de que todos tus datos sean expuestos y publicados en Redes Sociales. En la siguiente figura se muestran consejos y recomendaciones que debemos seguir para evitar mostrar todos los datos que recogen estos dispositivos inteligentes.

Figura 39:

¿Las pulseras y relojes (wearables) son seguros?



Nota. Guía de Privacidad y Seguridad en Internet, AEPD e INCIBE. (P.21).

Ahora que conocemos todos los riesgos de Internet y cómo prevenirlos es conveniente informar que no todos los adolescentes están educados para hacer frente a cualquiera de estos peligros, es por ello que, desde las diferentes entidades gubernamentales, a nivel estatal y autonómico, han creado aplicaciones para el teléfono móvil muy eficientes para ayudar a las víctimas de Violencia de Género en todas sus vertientes como el Ciberacoso. Con ello, se pretende llegar al objetivo de facilitar herramientas a la víctima para su seguridad y seguimiento

de una forma cómoda, tanto para la víctima como para los "vigilantes", en la cual mediante el dispositivo del teléfono móvil se pueda monitorizar su actividad preservando su intimidad para poder dar la protección adecuada a la víctima y ser capaces de erradicar y disuadir las conductas ilícitas por parte de los agresores.

Por consiguiente, pasamos a enumerar las diferentes aplicaciones móviles:

App "Libres": Fue creada por el Ministerio de Sanidad, Servicios Sociales e Igualdad en agosto del año 2013, que desde entonces ha tenido una gran aceptación contabilizando 9500 descargas.

El objetivo principal de la aplicación es informar y apoyar a las mujeres que sufren Violencia de Género y a cualquier persona que detecte en su entorno cualquier situación de maltrato.

A través de un menú principal, la mujer que se descargue "LIBRES" puede tomar conciencia de su situación como víctima de violencia de género detectando los primeros signos del maltrato, informarse acerca de los pasos a seguir ante una situación de violencia de género, conocer los recursos telefónicos y presenciales que están a su alcance para asesorarse y denunciar y las medidas de autoprotección que puede y debe tomar para salvaguardar su seguridad y la de sus hijos y, finalmente, puede sentir que todos estamos con ella, que otras mujeres han pasado por su misma situación y han conseguido salir y comenzar una nueva vida alejada de la violencia.

La última novedad introducida es que mejora la accesibilidad pudiendo ser usuadas por personas con discapacidad.

Todo ello de una forma gratuita, ágil, sencilla y confidencial ya que el icono de la misma se ha diseñado para que no sea reconocible. *(Delegación del Gobierno para la Violencia de Género, 2022).*

Figura 40:

Pantalla inicial de la app. "LIBRES".

Nota.https://violenciagenero.igualdad.gob.es/laDelegacionInforma/pdfs/DGVG_Informa_ACCESIBILIDAD_APP_LIBRES_2016.pdf

ALERTCOPS: es una aplicación elaborada por el Ministerio del Interior que sirve para cualquier ciudadano estar en contacto directo con las Fuerzas y Cuerpos de Seguridad ante una situación de emergencia, incluida la Violencia de Género. Actualmente, entre otras funcionalidades de seguridad, dispone de un botón de socorro que está desde la pantalla del menú que si se pulsa 5 veces en menos de 6 segundos se conecta el micrófono del teléfono y se inicia una grabación de audio que se envía inmediatamente a tus "guardianes" (personas de confianza) y en el caso de los colectivos vulnerables, a las Fuerzas y Cuerpos de Seguridad además se activa la función de geolocalización para que alerte del lugar dónde se encuentra la víctima y que la atención sea inmediata.

Figura 41:

Captura de la pantalla inicial de la app. "ALERTCOPS".

Nota. https://alertcops.ses.mir.es/mialertcops/

SMS ¡Actualízate! Amor 3.0: siguiendo el camino iniciado en el año 2009 con la creación, de forma pionera en España, de la primera App para la prevención de la violencia machista, se presenta ahora una versión más actualizada y adaptada a los modernos smartphones: "*SMS ¡Actualízate! Amor 3.0".*

Bajo el concepto del M-Learning o aprendizaje mediante la utilización de teléfonos móviles, surge esta aplicación con la finalidad de sensibilizar y prevenir la violencia machista en la juventud a través del uso coeducativo de las nuevas tecnologías.

Los divertidos tests para jóvenes, la interpretación de sus resultados y los recursos disponibles en Canarias constituyen el contenido de la aplicación además, con la última actualización, han creado una PROPUESTA DIDÁCTICA con actividades y recomendaciones para trabajar sus diferentes pantallas con jóvenes y adolescentes.

Figura 42:

Composición de varias de las pantallas de la app. "SMS ¡Actualízate! Amor 3.0".

*Nota.*https://www.gobiernodecanarias.org/icigualdad/organismo/los_servicios_al_publico/ediciones_publicaciones/recursos_interactivos/sms_sin_machismo_si/propuesta_didactica_sms.html

DETECTAMOR: Al igual que el Gobierno Canario, que fue el pionero, el Instituto Andaluz de la Mujer, basándose en el Proyecto DETECTA, desarrolló esta aplicación con el objetivo de sensibilizar y prevenir la violencia machista en la juventud andaluza mediante la educación afectivo-amorosa para que los adolescentes andaluces aprendan a percibir lo que es el abuso, el maltrato y la Violencia de Género, y huyan de la mitología del "amor romántico", el machismo y las relaciones desiguales. La aplicación se compone de 10 juegos enfocado a los adolescentes y educadores para aprender y enseñar e informar sobre la prevención de la violencia machista en las parejas jóvenes mientras juegan y se divierten en la uso de la aplicación para que les haga reflexionar e interpretar cualquier signo de Violencia de Género.

Figura 43:

Captura de la pantalla inicial de la app. "DETECTAMOR".

Nota. http://www.juntadeandalucia.es/iamindex.php/areas-tematicas-coeducacion/app-detectamor.

ENRÉDATE SIN MACHISMO: EnrédateSinMachismo.com, es una campaña que se desarrolla desde el **Área de Educación Juventud e Igualdad del Cabildo de Tenerife** desde noviembre de 2010, para la PREVENCIÓN, SENSIBILIZACIÓN, E INFORMACIÓN sobre la violencia de género a jóvenes.

Enrédate sin machismo está pensada para jugar, divertirse y al mismo tiempo chequear tu relaciónde pareja. La aplicación tiene tres tres niveles de dificultad, si consigues desbloquearlo podrás compartir la medalla que te acredita como un tío o una tía que tiene las **cosas claras** en las relaciones.

Y si algo no va bien, reflexiona y busca información en la Guía o en la web.

Enrédate Sin Machismo al igual que Adolescentes SIN Violencia de Género se desarrolla desde las redes sociales más comunes como: F*acebook, Twitter, Tuenti, Spotify, el Blog y la web*. Un espacio para reflexionar, compartir y actuar contra la violencia de género.

Figura 44:

Cartel promocional de la campaña "enREDate sin machismo".

Nota. https://www.enredatesinmachismo.com/enredate-para-jovenes/#descargarApp

RELACIÓN SANA: Aplicación desarrollada por el Gobierno de Murcia en el año 2012, está enfocada a las desigualdades que se producen en las relaciones de pareja indicada principalmente para adolescentes.

La interfaz está diseñada de una forma cuidada para que los jóvenes se sientan más cómodos en su utilización y adaptada a sus necesidades.

Esta aplicación tiene como objetivo desnaturalizar la violencia en las relaciones de pareja adolescentes. Conductas tales como el control de las amistades y de los tiempos, los celos o el querer controlar los contenidos personales en los perfiles de distintas redes sociales, son indicativos de una relación tóxica y no deben permitirse.

La aplicación muestra consejos, cuestionarios de autodiagnóstico, pautas de actuación para saber si estás siendo víctima de Violencia de Género ofreciendo asistencia telefónica a través del 112 o la Red CAVI (Red regional de Murcia de centros de atención especializada para mujeres víctimas de la Violencia de Género).

Figura 45:

Captura de pantalla de la pantalla principal de la app. "RELACIÓN SANA".

Nota. http://adolescentesinviolenciadegenero.com/relacion-sana-aplicacion-para-smartphones/

OTROS RECURSOS:

016: Al igual que el 112 es el teléfono para todo tipo de emergencias, incluidas las relativas a la Violencia de Género, el número 016 es el teléfono especializado para las víctimas de Violencia de Género creado por el Ministerio de Igualdad por medio de la Delegación del Gobierno para la Violencia de Género. El 016, presta el Servicio telefónico de información, de asesoramiento jurídico y de atención psicosocial inmediata por personal especializado a todas las formas de violencia contra las mujeres, a través del número telefónico de marcación abreviada 016; por WhatsApp en el número 600 000 016 y por correo electrónico al servicio 016 online: 016-online@igualdad.gob.es.

Servicios que ofrece:

- Gratuito.
- Confidencial.
- Accesible para personas con discapacidad auditiva y/o del habla y baja visión.
- Atención en 53 idiomas por teléfono (24 horas): castellano, catalán, euskera, gallego, inglés, francés, alemán, portugués, chino mandarín, ruso, árabe, rumano, búlgaro, tamazight y otros 39 idiomas a través de un servicio de tele-traducción.
- Atención 24 horas en 16 idiomas por correo electrónico y chat online: castellano, catalán, euskera, gallego, valenciano, inglés, francés, alemán, portugués, chino, mandarín, ruso, árabe, rumano, búlgaro, italiano.
- Servicio de información general (servicio 24 horas de lunes a domingo).
- Servicio de asesoramiento jurídico (de 8 a 22h de lunes a domingo).
- Atención psicosocial inmediata para todas las personas que necesiten contención emocional y acompañamiento psicosocial inmediato (servicio 24 horas de lunes a domingo): Realizada por personal especializado.
- Atención consultas procedentes de todo el territorio.
- Derivación de llamadas de emergencia al 112.
- Coordinación de servicios similares de las Comunidades Autónomas.
- Información a las mujeres víctimas de violencia de género y a su entorno sobre qué hacer en caso de maltrato.
- Información sobre recursos y derechos de las víctimas en materia de empleo, servicios sociales, ayudas económicas, recursos de información, de asistencia y de acogida para víctimas de este tipo de violencia.
- Derivación de llamadas realizadas por menores de edad al Teléfono ANAR de Ayuda a Niños y Adolescentes: 900202010
- Derivación de llamadas relacionadas con la trata de mujeres y niñas con fines de explotación sexual al teléfono del Ministerio del Interior: 900105090.

- Como novedad señalar que cada vez más, más modelos de teléfono móvil están configurados de forma prederteminada para que al llamar al número 016 no deje rastro en el registro de llamadas tanto entrantes como salientes.

Figura 46:

Captura de pantalla de la página web del teléfono 016 para víctimas de Violencia de Género.

Nota. https://violenciagenero.igualdad.gob.es/informacionUtil/recursos/telefono016/home.htm

024: Nuevo teléfono contra el suicidio que se ha puesto en marcha el 10 de mayo de 2022, es nacional, gratuito y accesible y responde a una "demanda social" tras registrarse en 2020 el pico máximo de muertes por esta causa de la serie histórica. Los últimos datos de suicidios son alarmantes. El primer año de la pandemia marcó un récord en las muertes por esta causa en España. 3.941 decidieron acabar con su vida, un 7% más que un año antes, según los últimos datos del INE. Y psicólogos, psiquiatras y estudios de diferente calado constatan un empeoramiento de la salud mental a raíz del coronavirus.

El teléfono está pensado para atender a los pacientes con ideaciones suicidas, pero también a sus entornos y a los supervivientes, aquellas personas que han perdido a un ser querido por un suicidio. La Organización Mundial de la Salud (OMS) advirtió ya hace 20 años que un suicidio individual afecta íntimamente, al menos, a otras seis personas.

El servicio estará gestionado por Cruz Roja. Los casos catalogados como de alto riesgo o en curso de suicidio se alertará a los servicios de emergencia para que no llegue a consumarse.

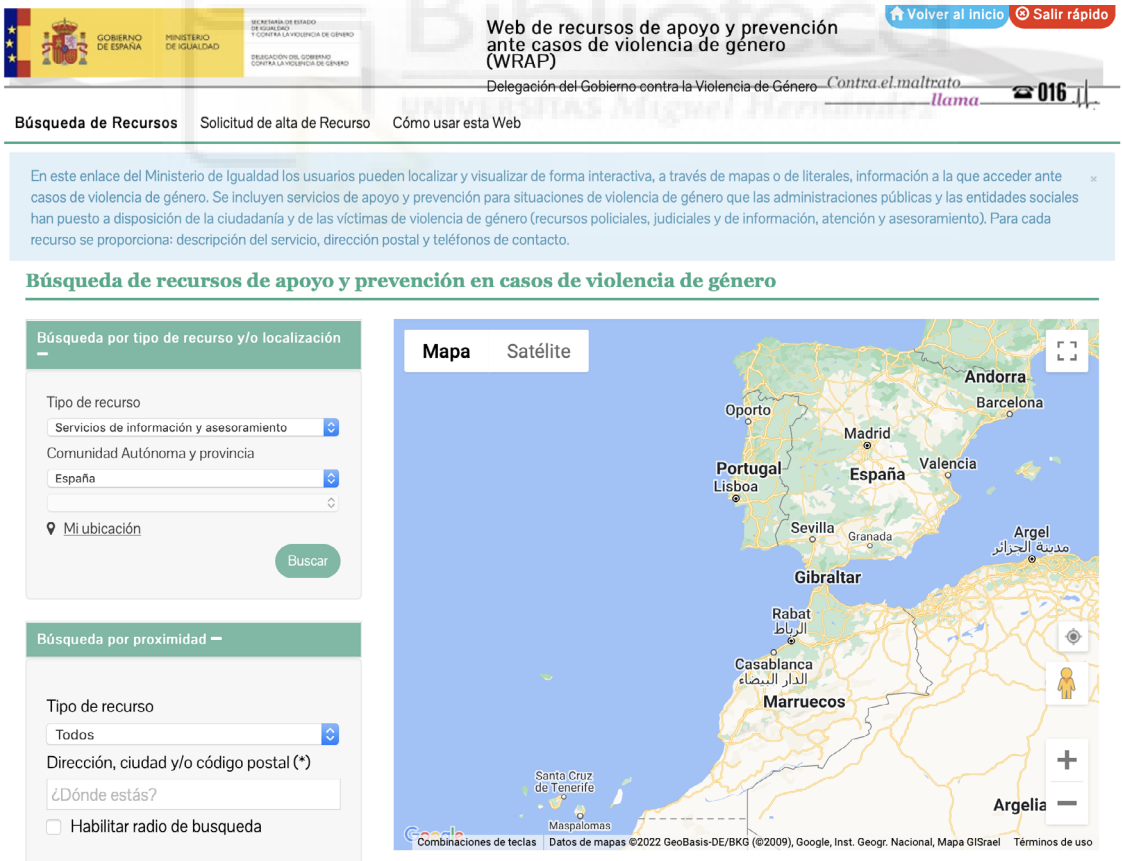
España ya disponía de recursos de prevención al suicidio puestos en marcha al margen de la administración, como el de la Fundación Anar, que veremos a continuación, pero no existía un teléfono público.

https://www.eldiario.es/sociedad/sanidad-pone-marcha-024-nuevo-telefono-suicidio_1_8978229.html

WRAP (Web de Recursos de Apoyo y Prevención ante casos de Violencia de Género): en este enlace del Ministerio de Igualdad los usuarios pueden localizar y visualizar de forma interactiva, a través de mapas o de literales, información a la que acceder ante casos de violencia de género. Se incluyen servicios de apoyo y prevención para situaciones de violencia de género que las administraciones públicas y las entidades sociales han puesto a disposición de la ciudadanía y de las víctimas de violencia de género (recursos policiales, judiciales y de información, atención y asesoramiento). Para cada recurso se proporciona: descripción del servicio, dirección postal y teléfonos de contacto.

Figura 47:

Captura de pantalla de la pantalla de inicio de la página web de la WRAP.



Nota. https://wrap.igualdad.gob.es/recursos-vdg/search/SearchForm.action

Fundación ANAR (Ayuda a Niños y Adolescentes en Riesgo): La Fundación ANAR es una organización sin ánimo de lucro que ayuda a niños/as y adolescentes en riesgo, cuyos orígenes se remontan a 1970, y se dedica a la promoción y defensa de los derechos de los niños/as y adolescentes en situación de riesgo y desamparo, mediante el desarrollo de proyectos tanto en España como en Latinoamérica, en el marco de la Convención de los Derechos del Niño de Naciones Unidas.

En el Teléfono ANAR de Ayuda a Niños/as y Adolescentes (900202010) dan respuesta inmediata a cualquier problema que pueda afectar a un menor de edad: dificultades de relación, violencia en sus diferentes formas, problemas psicológicos entre otros. Cualquier niño/a o joven puede ponerse en contacto con la Fundación, que es gratuito y confidencial, y encontrará al otro lado un psicólogo/a que le va a escuchar el tiempo necesario, que le orientará en su problema y que le ayudará a encontrar una solución.

Esta Fundación tiene como objetivo principal facilitar a niños, niñas y adolescentes un espacio seguro y confidencial en el que se sientan escuchados y respetados, y donde puedan expresar libremente aquello que les ocurre para encontrar alternativas a sus problemas de manera conjunta.

Los datos de esta organización, publicados en el mes de abril del año 2022, son preocupantes: las llamadas de ayuda por problemas de salud mental en menores se han disparado un 54% en un año. El abanico de causas que se esconde detrás de las cifras es amplio, según ha analizado la organización. Muchos son los niños, niñas y adolescentes que trasladan en sus llamadas “la sensación de soledad acompañada” producida “por las nuevas formas de comunicación”. La fundación ha identificado una “falta de referentes emocionales, problemas de comunicación, una mayor exposición a la violencia a través de la tecnología”. El informe señala el “preocupante” incremento en las víctimas de violencia de género menores de edad, una tendencia observada desde hace 13 años, que en 2021 ha escalado un 49,5% (3.440 chicas).El 43,6% de las adolescentes, además, no eran conscientes de estar siendo víctimas de la violencia machista. A lo largo de la última década, estos casos se han multiplicado por diez.

¿Por qué aumentan estos problemas? Según Benjamín Ballesteros, director de programas de la Fundación, “la soledad acompañada producida por las nuevas formas de comunicación y las tecnologías, la falta de referentes emocionales, los problemas de comunicación, la mayor exposición a la violencia a través de la tecnología y otros problemas graves como el coronavirus o la invasión de Ucrania en la actualidad generan problemas psicológicos, sociales y económicos que aumentan la frustración, la desmotivación, la incertidumbre, el malestar y, en ocasiones, la desesperanza”. Ésto puede ser algunas de las claves.

Figura 48:

Captura de pantalla de la página web de la "Fundación ANAR".

Nota. https://www.anar.org

https://www.eldiario.es/sociedad/llamadas-ayuda-problemas-salud-mental-menores-disparan-54-ano_1_8950059.html

https://es.scribd.com/document/572002351/Informe-Telefono-Chat-Anar-2021#from_embed

5.5. La nueva violencia de género en la era cibernética.

La ciberdelincuencia se ha convertido en un fenómeno complejo y global y tal como hemos hablado anteriormente, las nuevas tecnologías suponen un avance, pero también esconde sus peligros que afectan a todos los usuarios, especialmente los más vulnerables.

Internet nos ha cambiado la forma de vivir, pero también es el medio más potente en la actualidad para atentar contra los derechos de las personas, la intimidad, por la potencialidad que ofrece para la difusión de imágenes e información, la libertad sexual, la dignidad, el honor… es decir, el mal uso de Internet perjudica a la columna vertebral de nuestra estructura vital por eso es tan

peligrosa y problemática provocando consecuencias muy graves a las víctimas.

Por este motivo, en la actualidad los poderes públicos ya asumen la cibercriminalidad como un problema de primer orden incorporando este tipo de amenazas a la legislación con el fin de penalizar y proteger los derechos fundamentales de las personas mediante la reforma de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal en el año 2015 en las que se reglamentó los delitos tecnológicos relacionados con la ciberdelincuencia para catalogarlas como antijurídicas reforzando así la protección penal de estas víctimas de ciberdelitos.

Por ende, se regulan como nuevos delitos en el Código Penal (C.P.) el Stalking y el Sexting que pasaremos a detallar a continuación.

Stalking o Acoso ilegítimo (Art. 172 ter): Regulado en el Título VI: Delitos contra la libertad. Capítulo III: De las Coacciones del C.P.:

1. Será castigado con la pena de prisión de tres meses a dos años o multa de seis a veinticuatro meses el que acose a una persona llevando a cabo de forma insistente y reiterada, y sin estar legítimamente autorizado, alguna de las conductas siguientes y, de este modo, altere gravemente el desarrollo de su vida cotidiana:

1.ª La vigile, la persiga o busque su cercanía física.

2.ª Establezca o intente establecer contacto con ella a través de cualquier medio de comunicación, o por medio de terceras personas.

3.ª Mediante el uso indebido de sus datos personales, adquiera productos o mercancías, o contrate servicios, o haga que terceras personas se pongan en contacto con ella.

4.ª Atente contra su libertad o contra su patrimonio, o contra la libertad o patrimonio de otra persona próxima a ella.

Si se trata de una persona especialmente vulnerable por razón de su edad, enfermedad o situación, se impondrá la pena de prisión de seis meses a dos años.

2. Cuando el ofendido fuere alguna de las personas a las que se refiere el apartado 2 del artículo 173, se impondrá una pena de prisión de uno a dos años, o trabajos en beneficio de la comunidad de sesenta a ciento veinte días. En este caso no será necesaria la denuncia a que se refiere el apartado 4 de este artículo.

3. Las penas previstas en este artículo se impondrán sin perjuicio de las que pudieran corresponder a los delitos en que se hubieran concretado los actos de acoso.

4. Los hechos descritos en este artículo sólo serán perseguibles mediante denuncia de la persona agraviada o de su representante legal.

El delito de Stalking fue introducido por el número noventa y uno del artículo único de la L.O. 1/2015, de 30 de marzo, por la que se modifica la L.O. 10/1995, de 23 de noviembre, del Código Penal, entrando en vigor el día 1 de julio de 2015.

El bien jurídico protegido es la libertad individual con el fin de proteger esas conductas reiteradas en la cual se menoscaba la libertad y el sentimiento de seguridad de la víctima, a la que se somete a persecuciones o vigilancias constantes, llamadas reiteradas u otros actos continuos de hostigamiento, tal como se muestra en la exposición de motivos de la L.O. 1/2015.

https://noticias.juridicas.com/actualidad/noticias/10989-el-nuevo-delito-de-acoso-ilegitimo-o-stalking-art-172-ter-cp/

Sexting. (Art. 197.7): Regulado en el Título X: Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio. Capítulo I: del descubrimiento y revelación de secretos del C.P.:

7. Será castigado con una pena de prisión de tres meses a un año o multa de seis a doce meses el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona.

La pena se impondrá en su mitad superior cuando los hechos hubieran sido cometidos por el cónyuge o por persona que esté o haya estado unida a él por análoga relación de afectividad, aun sin convivencia, la víctima fuera menor de edad o una persona con discapacidad necesitada de especial protección, o los hechos se hubieran cometido con una finalidad lucrativa.

Sexting viene de una palabra heredada del Inglés que se descompone en dos palabras Sex-Texting, es decir, Sexo y Texto. Originariamente el Sexting era el delito que regulaba la conducta de enviar mensajes de texto con connotación sexual desde los primeros teléfonos móviles. Con el desarrollo de la tecnología, actualmente esta conducta abarca también al envío de todo contenido multimedia (videos, fotografías, mensajes…) que conlleve connotaciones sexuales y se haga un uso ilícito de ese material.

Por último, destacar otra práctica que entra dentro del rango del ciberacoso y es la denominada conducta llamada **“Grooming”,** que viene de la palabra inglesa “engatusamiento”, que consiste en establecer lazos de amistad con un menor, de manera deliberada por parte de un adulto, para obtener satisfacción sexual mediante el envío de imágenes eróticas o pornográficas del menor,

solicitando éstas, o incluso como medio y preparación a un encuentro sexual posterior. Efectivamente, se refiere a la pederastia y supone un grave problema sobre la seguridad de los menores en Internet.

El “modus operandi” es: prácticas online de ciertos adultos para ganarse la confianza de un (o una) menor fingiendo empatía, cariño, etc., normalmente bajo una falsa identidad de otro/a menor, con fines de satisfacción sexual. Esos fines incluyen casi siempre como mínimo la obtención imágenes del/a menor desnudo/a o realizando actos sexuales.

En este sentido, la información y educación sexual preventiva es fundamental, más aún si los menores tienen acceso a móviles, ‘tablets’ u ordenadores.

Pero, aunque sea el mayor peligro, no solo los niños y adolescentes pueden ser víctimas del mal uso digital. La “sextorsión” o chantaje sexual aparece en todas las edades y se combate sin duda con menos herramientas y más miedos entre los menos maduros emocionalmente. Los delincuentes que lo realizan juegan con la vergüenza y la culpa para extorsionar y conseguir que la persona realice lo que su “sextorsionador” le pida, a cambio de no contar nada de lo sucedido. Lo cual tampoco suele respetarse, porque los chantajistas no son el perfil de personas que respeten los mínimos códigos de conducta.

https://www.elmundo.es/vida-sana/sexo/2018/07/20/5b50b3eb468aeb2a7d8b464e.html

| 6. METODOLOGÍA |

Este trabajo es consecuencia de la asignatura del Trabajo Final de Grado (TFG) en el segundo cuatrimestre del 4º curso de la primera promoción del Grado de Seguridad Pública y Privada de la Universidad Miguel Hernández de Elche (UMH).

La elección del tema la hice pensando principalmente en un problema de actualidad. Entre diversos temas propuestos, enfoqué el trabajo a las nuevas tecnologías porque están teniendo un creciente impacto en nuestra vida diaria. Pero en este tipo de trabajo hacer una investigación sobre nuevas tecnologías es un asunto muy basto por lo que requería más concreción. Es por lo que teniendo como referencia las asignaturas del grado relacionadas con la criminología pensé en un concepto delictivo que estuviera de actualidad y que se aplicara con las nuevas tecnologías y ese delito es la violencia de género.

Por tanto, se estuvo tratando sobre ese tema y todos los tipos delictivos que se asocian actualmente con la violencia de género como es el sexting, grooming, robo de datos personales, cámaras espías, phishing para utilizar las contraseñas de la pareja, virus para espiar a la pareja, ataques informáticos… destacando sobre todos ellos el ciberbullying o el ciberacoso, llamado también ciberstalking, recogido en el art. 172.ter de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal qué es el acoso a través de las tecnologías. Con toda esta información, se llegó a unas conclusiones por medio de una revisión sistemática sobre el tema de la Violencia de Género, pero focalizado en el tramo de edad de la adolescencia, que es donde más casos se dan sobre ciberacoso.

Una vez localizado el tema a tratar, para poder continuar con la investigación, se trazaron los objetivos y se basó sobre cinco palabras claves: Ciberacoso; Nuevas Tecnologías; Violencia de Género; Redes Sociales y Adolescencia para facilitar la posterior localización de información mediante varios motores de búsqueda más conocidos como: Google Scholar, Proquest, Base de datos de la biblioteca UMH y Dialnet, y se analizó que estos motores de búsqueda se adaptaban perfectamente a nuestra búsqueda, arrojando los siguientes resultados cuantitativos:

Representación cuantitativa:

Para la búsqueda de información sobre la materia se utilizó diferentes motores de búsquedas con diferentes tesauros basados en las palabras clave y acompañados por diferentes criterios de búsqueda y por los booleanos (AND y OR), para definir la búsqueda se hizo de cada palabra clave una búsqueda con diferentes criterios de búsqueda según el motor utilizado.

En consecuencia, en **Google Scholar** se adoptaron los criterios de los trabajos de los últimos 5 años: 2017-2022, por relevancia, en cualquier idioma y que fueran artículos de revisión, esto unido a la inclusión de los booleanos, pasamos de una búsqueda inicial de 5710 resultados (del término "Nuevas Tecnologías") a 53 utilizando el filtro de las palabras claves más los booleanos.

Detallando, más concretamente, cómo se obtuvieron estos resultados lo explicamos a continuación: Se buscaron en el motor de "Google Scholar", (que es el motor de búsqueda de trabajos académicos creados por Google, el mayor y más eficiente motor de búsqueda en la web), las cinco palabras claves elegidas de forma individual, así se buscó por la palabra clave "Ciberacoso" con los siguientes criterios de búsqueda que nos ofrecía el motor, desde los años 2017 hasta 2022, por relevancia, en cualquier idioma y por artículos de revisión, saliendo como resultado 176 búsquedas o trabajos que se adecuaban a nuestros intereses.

Seguidamente, se realizó al igual que el ciberacoso, la búsqueda individual sobre otra de nuestras palabras clave: "Nuevas Tecnologías" arrojando un resultado de 5710 trabajos que coincidían con nuestros criterios, habiendo, además, trabajos recientes de este mismo año 2022. Con motivo de tratar con un trabajo que implica nuevas tecnologías, debemos tener en cuenta sacar información lo más reciente posible por la idiosincrasia y dinámica del cambio que nos aportan las nuevas tecnologías, por eso la importancia de encontrar trabajos recientes. No obstante, para completar más resultados, realicé más búsquedas a nivel individual sobre las palabras clave utilizadas en este trabajo como: "Violencia de Género": Dando una cifra de 2100 resultados encontrados; "Redes Sociales": 4710 resultados; y "Adolescencia": 2820 resultados. Con este tanteo, teníamos demasiados trabajos para realizar una revisión, por lo que se utilizaron los "booleanos "AND y OR" para especificar y acotar las búsquedas.

En consecuencia, resaltar de esta Tabla 1 que los booleanos nos ayudaron a concretar mucho la búsqueda. Por ende, la búsqueda de trabajos que contenían las palabras de nuevas tecnologías con miles de resultados encontramos 57 trabajos que especificamente contenían las palabras "Ciberacoso AND Nuevas Tecnologías", posteriormente añadimos las siguientes palabras claves "Violencia de Género" y "Redes Sociales" con el "booleano: OR" añadiendo el booleano "AND" en la palabra clave "Adolescencia" porque nos interesaba buscar trabajos que trataran sobre las nuevas tecnologías pero específicamente refirieran contenido sobre el ciberacoso y adolescencia, a la misma vez, de estos trabajos que pudieran versar, de forma indistinta, sobre temas como: "Violencia de Género" o "Redes Sociales", arrojando resultados de entre 50 y 60 trabajos encontrados en esta Tabla 1.

Tabla 1

Resultados obtenidos de la búsqueda en la base de datos de Google Scholar.

Google Scholar										
Criterios de búsqueda	**2017-2022 / Relevancia / Cualquier idioma / Artículos revisión**									
Palabras Clave	Resultados	Año	Booleano	1º Resultado	Booleano	2º Resultado	Booleano	3º Resultado	Booleano	4º Resultado
Ciberacoso	176	2022								
Nuevas Tecnologías	5710	2022	AND	57	AND		AND		AND	
Violencia de Género	2100	2022			OR	59	OR		OR	
Redes Sociales	4710	2022					OR	55	OR	
Adolescencia	2820	2022							AND	53

Nota. Fuente: elaboración propia.

En la Tabla 2, efectuamos la misma búsqueda que la Tabla 1, con el mismo motor "Google Scholar" pero con las palabras claves en Inglés y mismos criterios arrojando un resultado de 26200 trabajos que contienen la palabra "New Technologies" hasta los 32 resultados utilizando las palabras clave "Ciberbullying AND New Tecnologies". Sin embargo, en esta Tabla 2, al añadir más booleanos nos amplió la búsqueda a varios centenares de resultados.

Así que, la búsqueda de Ciberbullying AND New Tecnologies OR Gender Violence arrojó un resultado de 963 trabajos, mientras que la búsqueda de Ciberbullying AND New Tecnologies OR Gender Violence OR Social Media AND Adolescence nos dio 785 resultados buscados. Es decir, utilizando todas las palabras claves arrojó un resultado parecido, sin poder acotar demasiado la búsqueda.

Tabla 2

Resultados obtenidos de la búsqueda en la base de datos de Google Scholar con las palabras claves en Inglés.

Google Scholar										
Criterios de búsqueda	**2017-2022 / Relevancia / Cualquier idioma / Artículos revisión**									
Palabras Clave	Resultados	Año	Booleano	1º Resultado	Booleano	2º Resultado	Booleano	3º Resultado	Booleano	4º Resultado
Ciberbullying	171	2021								
New Technologies	26200	2022	AND	32	AND		AND		AND	
Gender Violence	18900	2022			OR	963	OR		OR	
Social Media	39600	2022					OR	857	OR	
Adolescence	28000	2022							AND	785

Nota. Fuente: elaboración propia.

Respecto a la Tabla 3, utilizamos el motor de búsqueda de **Proquest.** Los criterios de búsqueda se basaron en Tesis doctorales y tesinas dando sorprendentemente un resultado de una sola tesis con la palabra “Ciberstalking”, por lo que denotó que no había demasiados trabajos sobre la materia, debiendo ampliar los campos mediante la ampliación de palabras claves y booleanos, llegando a conseguir 132 tesis con las palabras “Ciberstalking AND Nuevas Tecnologias OR Violencia de Género OR Redes Sociales AND Adolescencia.”

Resaltar que, en esta Tabla 3, la búsqueda de Ciberstalking AND Nuevas Tecnologías proporcionó 3 resultados, dos resultados más que la anterior búsqueda por lo que se observa que hay una mayor relación entre las Nuevas Tecnologías y el Ciberstalking.

Tabla 3

Resultados obtenidos de la búsqueda en la base de datos de Proquest.

Proquest										
Criterios de búsqueda	**Tesis doctorales y tesinas**									
Palabras Clave	Resultados	Año	Booleano	1º Resultado	Booleano	2º Resultado	Booleano	3º Resultado	Booleano	4º Resultado
Ciberstalking	1	2019								
Nuevas Tecnologías	3	2021	AND	3	AND		AND		AND	
Violencia de Género	105	2021			OR	109	OR		OR	
Redes Sociales	173	2022					OR	204	OR	
Adolescencia	76	2022							AND	132

Nota. Fuente: elaboración propia.

Por lo que concierne a la Tabla 4, la búsqueda se realizó con el motor de la **biblioteca UMH.** En esta tabla, se observa que la búsqueda con los criterios de los últimos 5 años, y sólo elaboraciones de Trabajos Final de Grado (TFG), los resultados más numerosos se dieron con la palabra clave "Redes Sociales" con 128 trabajos encontrados y los resultados más escasos fueron los trabajos que contenían la palabra "Ciberacoso" con 3 resultados, siendo el trabajo más reciente del año 2019, mientras que trabajos que tratan sobre Nuevas Tecnologías, Violencia de Género, Redes Sociales y Adolescencia son todos trabajos más recientes del año 2021, indicándonos que son temas muy actuales y tratados frecuentemente por lo que podemos deducir que su estudio es a raíz de los problemas actuales que plantea.

Tabla 4

Resultados obtenidos de la búsqueda en la base de datos de la biblioteca de la UMH.

Biblioteca UMH									
Criterios de búsqueda	**2017-2022 / TFG**								
Palabras Clave	Resultados	Año	Booleano	1º Resultado	Booleano	2º Resultado	Booleano	3º Resultado	Booleano	4º Resultado
Ciberacoso	3	2019					Acoso			
Nuevas Tecnologías	44	2021	AND	2	AND		AND		AND	
Violencia de Género	34	2021			OR	0	OR		OR	
Redes Sociales	128	2021					OR	3	OR	
Adolescencia	22	2021							AND	0

Nota. Fuente: elaboración propia.

Por último, en la Tabla 5, nos servimos del motor de búsqueda de **Dialnet**, es el buscador de origen de la Universidad de la Rioja, desde el año 2002 se ha convertido en uno de los buscadores con más documentos sobre las Ciencias humanas, jurídicas y Sociales, que es la rama que más nos interesó para la elaboración de esta revisión bibliográfica. Las búsquedas se caracterizaron por ser las más relevantes y que fueran Tesis, resultando que la temática con más tesis era la de "Nuevas Tecnologías" con 8597 tesinas y la materia menos tratada era la del "Ciberacoso" con 42 resultados. Resaltar que, de todos los resultados sobre las nuevas tecnologías, solo 20 trabajos tratan del Ciberacoso aplicado a las nuevas tecnologías. Por otra parte, en esta Tabla 5, nos interesó acotar aún más la búsqueda por lo que se realizó un nuevo filtro con todas las palabras claves y los booleanos utilizados: "Ciberacoso AND Nuevas Tecnologias OR Violencia de Género OR Redes Sociales AND Adolescencia", acotando la búsqueda a 5 tesinas las cuales tenían temas comunes a los objetivos de nuestra investigación.

Tabla 5

Resultados obtenidos de la búsqueda en la base de datos de Dialnet.

Dialnet										
Criterios de búsqueda	**Relevancia / Tesis**									
Palabras Clave	Resultados	Año	Booleano	1º Resultado	Booleano	2º Resultado	Booleano	3º Resultado	Booleano	4º Resultado
Ciberacoso	42	2021								
Nuevas Tecnologías	8597	2022	AND	20	AND		AND		AND	
Violencia de Género	1282	2022			OR	9	OR		OR	
Redes Sociales	4231	2021					OR	8	OR	
Adolescencia	3796	2022							AND	5

Nota. Fuente: elaboración propia.

Representación cualitativa:

De estos resultados se seleccionaron los siguientes estudios que cumplían con los requisitos de inclusión, los cuales contenían información sobre las cinco palabras clave, siendo éstos:

Revisión bibliográfica sobre el bullying y ciberbulluying en alumnado de Educación Secundaria (Arellano Aguado, J.J. 2017).

Violencia a través de las TIC: El ciberacoso en escolares de la Comunidad

Autonóma de Madrid. (Castro Clemente, C. 2017).

El continuo de las (ciber) violencias sexuales en las mujeres: la educación sexual como prevención. (Martínez Román, R. 2021).

De víctimas, perpetradores y espectadores: una meta etnográfica de los roles en el ciberbullying. (Moretti, C. y Herkovits, D. 2020).

Transversalidad de las Tecnologías de la Información y las Comunicaciones en la Prevención de la Violencia de Género desde un Enfoque Multinivel-Propuestas de Aplicación. (Rodríguez Rodríguez, I. 2021).

Mientras que la tutora de este trabajo aportó tres selecciones más:

Una modalidad actual de violencia de género en parejas de jóvenes: Las redes sociales. (Martín Montilla, A.; Pazos Gómez, M.; Montilla Coronado, M. V. C. y Romero Oliva, C. 2016).

Ciberacoso y Violencia de Género en Redes Sociales. Análisis y herramientas de prevención. (Verdejo Espinosa, M.A. 2015).

Violencia de Género en entornos virtuales: una aproximación a la realidad adolescente. (Villar Varela, M.; Mendez-Lois, M.J. y Barreiro Fernández, F. 2021).

Realizada la selección, se efectuó una lectura analítica de los trabajos que tenían más relación y se ajustaban más a los objetivos planteados, dando como resultado la extracción de los datos más relevantes para la investigación y dirigirnos a las conclusiones explicadas en la sección 8.

Por otra parte, se trabajó paralelamente en el marco teórico de la investigación, buscando las diferentes definiciones y los tipos que existen de Violencia de Género, además de toda la estructura del trabajo, finalizando primeramente la Introducción, para poder avanzar de una forma más precisa en la investigación.

A continuación, se llevó a cabo la búsqueda de gráficas en el Instituto Nacional de Estadística (INE) para realizar un sondeo de los datos, posteriormente se encontró diverso material muy interesante sobre estadísticas acerca de la cibercriminalidad, guías didácticas sobre violencia de género y ciberacoso enfocadas en los adolescentes editadas por organismos oficiales, documentos sobre el uso de las Redes Sociales editados por empresas de telecomunicaciones y tratados sobre Nuevas Tecnologías publicados por Fundaciones, aportando toda esta documentación los resultados expuestos en la sección 7 y que derivaron en las conclusiones antes mencionadas.

| 7. ANÁLISIS DE LOS RESULTADOS Y DISCUSIÓN |

Los principales resultados que se obtuvieron en este trabajo están relacionados con los objetivos propuestos en esta revisión bibliográfica:

Analizar las nuevas formas de ciberacoso; estudiar la evolución del futuro de internet, redes sociales y en consecuencia las relaciones sociales; analizar las nuevas herramientas tecnológicas para el conocimiento de los adolescentes y que conozcan cómo usar estas herramientas con el fin de prevenir que sean víctimas de delitos. Y, por último, analizar a las víctimas de estos delitos e informarles de los protocolos para evitar nuevas agresiones: qué deben hacer, cómo deben actuar y dónde deben dirigirse.

La evolución de las relaciones sociales, a corto plazo se ha visto que pasa básicamente a través de Internet y las Redes Sociales. Observamos que las nuevas tecnologías, aparte del avance que supone en las comunicaciones, presentan el hándicap de que estas comunicaciones son más globales y, por tanto, también hay más facilidad para comunicarse con gente anónima.

Estas actividades delictivas que han aumentado son el acoso a las personas en sus múltiples formas a través de la red. En la red está conectada la mayoría de la población, tanto hombres como mujeres, destacando la franja de edad de la adolescencia y la juventud (16-24 años). Por consiguiente, el acoso ha pasado de ser físico en épocas anteriores a ser mayoritariamente a través de la red mediante múltiples dispositivos, siendo el teléfono móvil el dispositivo por excelencia mediante el cual se produce este delito. Unido a la tecnificación y al tratamiento masivo de datos denominado el “Big Data y el Internet de las Cosas” hace que el delincuente se sienta protegido bajo el paraguas del anonimato y puedan consumir el delito regulado en nuestro código penal llamado “Stalking” (Acoso). Este delito engloba todas sus formas derivadas como el ciberstalking, el bullying, el ciberbullying, el sexting y el grooming, términos ingleses que describen distintas formas de acosar a las personas a través de las nuevas tecnologías. Aunque estas formas de delito existen, nos encontramos con el problema de que aún no hay resultados sobre el ciberacoso a nivel nacional, aunque está previsto que el I.N.E. tenga resultados estadísticos a partir del año 2023.

Actualmente, existen muchas herramientas para relacionarnos, pero la nueva herramienta para la comunicación por excelencia es Internet y dentro de Internet son las Redes Sociales. El 55% de la población mundial está conectada a Internet, por lo que más de la mitad de la población mundial es capaz de relacionarse e interactuar con cualquiera de las 7.75 billones de personas que están conectadas a la red en cualquier lugar del mundo. Cabe destacar, el gran aumento que están experimentando las Redes Sociales. Cada año van

aumentando los usuarios exponencialmente, poniendo como ejemplo que en enero del año 2020 aumentaron en 82 millones de personas los usuarios de Redes Sociales comparado con el año 2019.

Dentro de las Redes Sociales, destacar, que las Redes más utilizadas a nivel nacional durante el año 2021 ha sido Whatssap, con un 97% de usuarios, seguidas de Instagram y Facebook. Mientras que las actividades más realizadas en las redes sociales son con el "objetivo de entretenerse", con un 81% de usuarios, e "interactuar con el resto de personas", con un 72% de usuarios.

Respecto a la frecuencia en el uso de Redes Sociales los usuarios emplearon 1 hora y 21 minutos al día a gestionar sus cuentas en Redes Sociales, siendo la red social "Twitch" la más utilizada con una media de 1h 40 min. al día.

Y el momento por antonomasia para conectarse a las redes sociales se situó en el tramo desde las 20:30 horas de la tarde hasta las 00:30 horas de la madrugada.

En conclusión, la población está mucho más conectada, sobre todo por las redes sociales, en que se ha demostrado que son un instrumento eficaz para la comunicación entre las personas, esta comunicación eficaz conlleva unos peligros que hay que tener en cuenta para evitar ser víctimas de delitos con sus graves consecuencias.

Como hemos visto, la juventud (16-24 años) es la franja de edad que más utilizan Internet y también el sector de edad más expuesto y vulnerable a la violencia a través de las redes, también es el sector que muestra más prevalencia a la violencia, porque es el sector de edad que más identifica cualquier modo de violencia (física, psíquica, económica, sexual o ambiental) y son las más proclives a contarlas.

Para evitar ser víctimas de cualquier violencia o acoso a través de la red, es preciso conocer las herramientas que estamos utilizando y configurarlas de modo que aseguren la evitación de intrusos en nuestras redes y filtraciones de datos, mediante el conocimiento de: cifrar nuestra información, las herramientas de seguridad a nuestro alcance, copias de seguridad, conocer si estamos realizando descargas seguras, instalación de antivirus... Además, debemos dotar nuestros accesos a las redes y aplicaciones con contraseñas robustas con la verificación en dos pasos, navegar por páginas fiables que tengan el protocolo de seguridad, saber dónde y qué datos debemos introducir en las páginas web y las Redes Sociales, conocer cómo podemos eliminar datos de la red, tener conocimiento de cómo navegar de forma privada para preservar tu intimidad en las consultas, estar enterado de los riesgos y timos que se producen en las aplicaciones de mensajería instantánea además de saber e identificar la información falsa en Internet, así como el Phishing. También debemos estar al corriente de interpretar

las causas del por qué nos quedamos sin conexión, pueden haber personas utilizando nuestro wifi, proteger de forma segura el acceso a nuestro correo electrónico y la información personal en la nube, asegurarse a quién compartes tus ficheros, sobre todo en plataformas P2P, proteger igualmente todos tus dispositivos incluso las pulseras o relojes inteligentes. Además, los padres deben controlar cómo los hijos menores utilizan internet, controlando su actividad a diario, estando al tanto de qué está haciendo en internet y con qué personas mantiene el contacto, con el objetivo de educarle y formarle para prevenir ciertas actitudes ciberdelictivas. Actualmente, cabe especificar que en los dispositivos electrónicos como en las plataformas de las Redes Sociales hay "controles parentales" que monitorizan y controlan la actividad de los perfiles, avanzando así hacia un futuro con menos ciberdelincuencia y previniendo el daño que puedan ocasionar a los menores.

Y, aun así, conociendo todas las herramientas de prevención y control podemos ser víctimas de ciberdelitos porque no todos los usuarios están educados para hacer frente a todos estos peligros. Pero para ello también existen soluciones que ayudan a los usuarios a informarles y recomendarles una vez han sido víctimas del delito. Este tipo de delitos se han convertido en una lacra a nivel mundial que afecta a todas las naciones, por eso desde los gobiernos crearon políticas públicas para erradicar este tipo de conductas mediante la creación de aplicaciones para móviles para facilitar a las víctimas su seguridad y seguimiento de una forma cómoda y discreta. En España se crearon y existen diversas aplicaciones como:

"Libres" que informa y apoya a las mujeres que sufren cualquier tipo de Violencia de Género y cualquier persona que detecte estas conductas en su entorno.

"Alertcops" tal como dice el título es una aplicación que envía una alerta a la policía en caso de ser víctima de cualquier delito, entre ellas las relacionadas con la Violencia de Género.

"SMS ¡Actualizaté! Amor 3.0 destinada para prevenir la violencia machista entre los jóvenes y lanzada por el Gobierno Canario.

"Detectamor" con el mismo objetivo que la anterior aplicación pero promovido por el Gobierno Andaluz.

"Enrédate sin machismo" es una campaña a través de la Web propuesta por el Cabildo de Tenerife para combatir la Violencia de Género destinada principalmente a los jóvenes.

"Relación Sana" en este caso es el Gobierno de Murcia el que crea esta aplicación para aconsejar a los adolescentes cómo deben de relacionarse en pareja y evitar las conductas patriarcales que induzcan a la Violencia de Género.

Y para completar los servicios a los ciudadanos tanto a nivel nacional como autonómico, desde hace años se crearon otros recursos como números de teléfono en que la asistencia es inmediata, como el conocido teléfono de emergencias: 112., el específico para la Violencia de Género: 016 o el recientemente número creado para las personas que tienen intención o ideas suicidas: 024, el cual en su primer día de atención telefónica, el pasado 10 de mayo de 2022, arrojó un resultado de 1000 llamadas. Resultado que evidencia que este tipo de recursos son necesarios implantarlos para el bienestar de la población.

En otro orden, existen otros recursos que luchan contra toda clase de conductas sobre la Violencia de Género, y éstas son la web de Recursos de Apoyo y Prevención ante casos de Violencia de Género (WRAP) y financiada por el Ministerio de Igualdad y la Fundación ANAR (Ayuda a Niños y Adolescentes en Riesgo) en que psicólogos ayudan a niños y adolescentes, creando un espacio seguro y confidencial en el que se sientan escuchados y respetados, y donde puedan expresar libremente aquello que les ocurre para encontrar alternativas a sus problemas de manera conjunta.

| 8. CONCLUSIONES |

En esta investigación llegamos a las conclusiones de que en la actualidad todos los detalles son importantes.

Respecto al tema tratado sobre las formas de la Violencia de Género a través de las nuevas tecnologías observamos que, la comisión de ciberdelitos relacionados con Violencia de Género, con delincuentes que se protegen en la sencillez del anonimato o en la suplantación de identidades, avanza a la misma velocidad que la tecnología, la evolución de los móviles, la cantidad de datos tratados mediante Big Data...

A esta problemática se unen otros factores como el uso masivo de la Redes Sociales que está provocando cambios, generalmente negativos, en la personalidad y la educación de los usuarios más jóvenes. Estos jóvenes no son conscientes de los efectos nocivos de las Redes. No perciben la importancia de preservar la privacidad porque buscan la inmediatez obviando lo realmente importante que es la lectura de las condiciones de uso.

En relación a las variadas formas de la Violencia de Género utilizando las nuevas tecnologías, comprobamos que el móvil es el dispositivo tecnológico por excelencia y el más utilizado. Con los teléfonos inteligentes y las aplicaciones que tenemos instaladas en ellos generamos, entre todos, enormes cantidades de datos cada día. A través del Big Data se genera, con estos datos, información sobre nosotros, nuestros gustos o nuestras necesidades.

Toda esta nueva tecnología tiene un denominador común, avanza muy rápido y esta rápidez va en consonancia con la rapidez que evolucionan los delitos cibernéticos. Estos delitos cibernéticos se caracterizan por la facilidad que tienen los delincuentes de proteger su anonimato o la suplantación de identidades por lo que convierte el uso de las tecnologías en peligrosas si no se toman las medias oportunas para protegerse a uno mismo.

Junto a esta rapidez del avance de la tecnología, se unen múltiples factores que se mezclan entre sí, destacando el factor del uso de las Redes Sociales que son utilizadas por la mayoría de la población.

Este uso intensivo de las Redes Sociales esta originando que los jóvenes evolucionen en su personalidad y su educación, siendo de forma diferente a las generaciones anteriores, porque las Redes Sociales provocan que no se perciba, por parte de los usuarios jóvenes, sus efectos nocivos. El principal efecto nocivo de las Redes Sociales es la falta de la privacidad debido a la búsqueda de la inmediatez porque obviamos las condiciones de uso (lectura de la “letra pequeña”) y en consecuencia lo realmente importante: Las condiciones de uso que son fundamentales para que se respete nuestra privacidad.

Con motivo de la gran mayoría de población conectados a Internet, los ciberdelincuentes se focalizan con las víctimas más vulnerables que son los jóvenes entre los 16 y 24 años, y que afecta más a las mujeres por los estereotipos sociales que todavía perduran.

Este tipo de delitos virtuales afectan a la persona las 24 horas al día porque tenemos al lado el dispositivo móvil que es la herramienta por la cual recibimos toda la comunicación, incluidas las personas acosadoras. Por tanto, todos los usuarios de las nuevas tecnologías, estamos expuestos a los actos de acecho, a la intromisión de nuestra intimidad y a la persecución permanente, convirtiéndonos en potenciales víctimas, desencadenando progresivamente los síntomas de los delitos derivados de la Violencia de Género y agravando sus consecuencias, que llegan hasta el suicidio de la víctima por la angustia, presión, ansiedad, estrés y descontrol que cambia las costumbres y hábitos de la víctima.

Los datos reflejan un paréntesis en el año 2020 sobre las víctimas de Violencia de Género debido a la pandemia mundial, pero no debemos relajarnos, sino que debemos seguir luchando contra esta lacra. Para ello, la solución pasa por la prevención, y la educación de los usuarios mediante los docentes, la familia y personal especializado. En el caso de los adolescentes, como prevención, debemos enseñarles a identificar cualquier signo de violencia online, a comportarse ante estas situaciones y hacer frente a los riesgos, mediante la presentación de denuncias para atajar estas conductas, que no sufran daños y extinguirlas.

Pero las nuevas tecnologías no son todo desventajas, sino que debemos aprovecharnos de sus beneficios mediante la utilización de instrumentos que atraigan a la adolescencia para socializarlos en la igualdad de género y así convertir los riesgos en oportunidades para la transformación y erradicación de la Violencia de Género.

Actualmente, existen numerosos recursos que abarcan todo tipo de soluciones ante la Violencia de Género, desde la telemonitorización, sensores biométricos y la gestión de los datos gracias al Big Data e Internet de las Cosas, hasta la instauración de aplicaciones móviles promovidas por entidades Gubernamentales, así como teléfonos de ayuda y fundaciones, con el único objetivo de detectar, prevenir y erradicar la Violencia de Género.

| 9. REFERENCIAS BIBLIOGRÁFICAS |

Álvarez-García, D.; Barreiro-Collazo, A. y Núñez, J.C. (2017). *Cyberaggression among Adolescents: Prevalence and Gender Differences. [Ciberagresión entre adolescentes: prevalencia y diferencias de género]* Comunicar. XXV (50), 89-97. https://doi.org/10.3916/C50-2017-08

Arellano Aguado, J.J. (2017). *Revisión bibliográfica sobre el bullying y ciberbulluying en alumnado de Educación Secundaria.* Facultad de Ciencias de la Educación de Granada.

Bagha, A. & Madisetti, V. (2019). *Big Data Analytics: A Hands-On Approach,* 26, 460.

Blanco Ruiz, M.A. (2014). *Implicaciones del Uso de las Redes Sociales en el aumento de la violencia de género en adolescentes*. Comunicación y medios. (30), 124-141.

Castro Clemente, C. (2017). *Violencia a través de las TIC: El ciberacoso en escolares de la Comunidad Autonóma de Madrid.* Universidad Pontificia Comillas de Madrid.

De Miguel, V. (2015). *Percepción de la Violencia de Género en la Adolescencia y la Juventud.* Madrid: Ministerio de Sanidad, Política Social e Igualdad. Centro de Publicaciones. https://www.lainformacion.com/asuntos-sociales/un-tercio-de-los-jovenes-considera-aceptable-prohibir-a-su-pareja-que-trabaje-o-vea-a-sus-amigos_UdReQmBpjbLN3Yj2b0SjD4//

Díaz-Aguado, M., Martínez, R. y Martínez, J. (2014). *La evolución de la adolescencia española sobre la igualdad y la prevención de la violencia de género.* Madrid: Ministerio de Sanidad, Política Social e Igualdad. Centro de Publicaciones, 323

Echeburúa, E., & De Corral, P. (2010). *Adicción a las nuevas tecnologías ya las redes sociales en jóvenes: un nuevo reto.* Adicciones, vol. 22 (2), 2.

Elogia (2021). *Estudio de Redes Sociales.* Madrid: Iab·spain. https://iabspain.es/estudio/estudio-de-redes-sociales-2021/

Espelage D, Rao M, Craven R. (2015). *Theories of cyberbullying*. *[Teorías del Ciberacoso].* In: Bauman S, Cross D, Walker J, editors. Principles of cyberbullying research: definitions, measures, and methodology. New York: Routledge; p. 49-64.

Finkelhor, D., Mitchell, K.J., & Wolak, J. (2000). *Online victimization: A report on the nation´s youht. [Victimización en línea: un informe sobre la juventud nacional].* Alexandria: VA: National Genter for Missing and Exploteid Children.

Fundación telefónica y Taurus. (2021). *Informe de la Sociedad Digital en*

España 2020-2021. Penguin Random House Grupo Editorial, S. A. U. Barcelona (España). https://www.fundaciontelefonica.com/cultura-digital/publicaciones/sociedad-digital-en-espana-2020-2021/730/

Garaigordobil, M. (2001). *Bullying y Cyberbullying: Conceptualización, Prevalencia y Evaluación.* FOCAD, Formación Continua a Distancia. 12, 2-22.

Harikiran G. C., Menasinkai K. y Shirol S., *Smart security solution for women based on Internet Of Things (IOT), [Solución de seguridad inteligente para mujeres basada en el Internet de las Cosas (IOT)]* (2016) International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT).

Hinduja, S. & Patchin, J.W. (2008). *Cyberbullying: An exploratory analysis of factors related to offending and victimization. [Ciberacoso: un análisis exploratorio de los factores relacionados con la delincuencia y la victimización]*. Deviant Behavior, 29, 129-156.

Hunt, G. J. (2007) *Flight and fight: a comparative view of the neurophysiology and genetics of honey bee defensive behavior*. Journal of insect physiology, vol. 53, p. 399–410.

John A, Glendenning AC, Marchant A, Montgomery P, Stewart A, Wood S, et al.(2018). *Self-harm, suicidal behaviours, and cyberbullying in children and young people: systematic review. [Autolesiones, conductas suicidas y ciberacoso en niños y jóvenes: revisión sistemática].* J. Med Internet Res; 20:e129.

Joshi, R. C., & Gupta, B. B. (Eds.). (2019). *Security, Privacy, and Forensics Issues in Big Data.* IGI Global, 363-379.

Levis, D. (2002). *Videojuegos: cambios y permanencias.* Comunicación y pedagogía, 184, 65-69.

Lopez Gutiérrez, J. et al. (2020) *Estudio sobre la cibercriminalidad en España.* Dirección General de Coordinación y Estudios Secretaría de Estado de Seguridad. Ministerio del Interior. http://www.interior.gob.es/documents/10180/11389243/Estudio+sobre+la+Cibercriminalidad+en+España+2020.pdf/ed85b525-e67d-4058-9957-ea99ca9813c3

Martín Montilla, A.; Pazos Gómez, M.; Montilla Coronado, M. V. C. y Romero Oliva, C. (2016). *Una modalidad actual de violencia de género en parejas de jóvenes: Las redes sociales.* Educación XX1, 19(2), 405-429, doi: 10.5944/educXX1.13934.

Martínez Román, R. (2021). *El continuo de las (ciber) violencias sexuales en las mujeres: la educación sexual como prevención.* Universidad de Vigo.

Montoro, E., y Ballesteros, M. (2016). *Competencias docentes para la prevención del ciberacoso y delito de odio en Secundaria.* RELATEC, 15(1), 131-143.

Moretti, C. y Herkovits, D. (2020). *De víctimas, perpetradores y espectadores: una meta etnográfica de los roles en el ciberbullying.* Instituto de Salud Colectiva, Universidad Nacional de Lanús (Argentina), 1-18.

Organización Mundial de la Salud [OMS]. (2013, 20 de junio). *Violencia contra la mujer un problema de salud global de proporciones epidémicas.* https://www.who.int/es/news/item/20-06-2013-violence-against-women-a-global-health-problem-of-epidemic-proportions-

Peter IK, Petermann F. (2018) *Cyberbullying: a concept analysis of defining attributes and additional influencing factors.[Ciberacoso: un análisis conceptual de atributos definitorios y factores de influencia adicionales].* Comput Human Behav; 86:350-66.

Pochiraju, B., & Seshadri, S. (Eds.). (2019). *Essentials of Business Analytics: An Introduction to the Methodology and Its Applications* (Vol. 264). Springer, 459, 507, 569.

Ponce, I. (2012). *Definición de redes sociales.* Observatorio Tecnológico del Ministerio de Educación, Cultura y Deporte. http://recursostic.educacion.es/observatorio/web/en/internet/web-20/1043-redes-sociales?start=1

Quesada, M. S. (2015). *La violencia de género y el ciberacoso en las redes sociales: análisis y herramientas de detección*. En M. A. Verdejo (Coord.), 111-126. Universidad Internacional de Andalucía.

Rodríguez-Rodríguez, I. (2019) *How can we tackle gender-based violence in cyberspace?*, [¿Cómo podemos abordar la violencia de género en el ciberespacio?], de UNIRE-Gender Violence is also a Cultural Issue! – Uníversitá degli Studi di Trento (Italy).

Rodríguez Rodríguez, I. (2021). *Transversalidad de las Tecnologías de la Información y las Comunicaciones en la Prevención de la Violencia de Género desde un Enfoque Multinivel-Propuestas de Aplicación.* Universidad de Alicante.

Romero, Joaquín, (2020). *En qué se diferencian la web 1.0, la 2.0, la 3.0 y la 4.0.* https://www.trecebits.com/2020/12/05/que-es-y-en-que-se-diferencian-la-web-1-0-la-2-0-la-3-0-y-la-4-0/

Shaik, K. Bogaraju S y Vadepu S. (2017). *Implementation of Novel Application for Woman and Child Protection Using IOT Enabled Techniques*. *[Implementación de una aplicación novedosa para la protección de mujeres y niños utilizando técnicas habilitadas para IOT],* International Journal of Advanced Research in Computer Science, vol. 8.

Slonje, R. & Smith, P.K. (2008). *Cyberbullying: Another main type of bullying? [Ciberacoso: ¿Otro tipo principal de acoso?].* Scandinavian Journal of Psychology, 49, 147-154.

Subdirección General de Promoción, Prevención y Calidad (2021), *Estudio HBSC Health Behaviour in School-aged Children (Estudio sobre las conductas saludables de los adolescentes escolarizados).*

Torrés, C., Manuel, J. y De Marco, S. (2014). *El Ciberacoso como forma de ejercer la Violencia de Género en la juventud: un riesgo en la sociedad de la información y del conocimiento*. Madrid: Ministerio de Sanidad, Política Social e Igualdad. Centro de Publicaciones.

Urueña, A (coord.) (2011). *Las redes sociales en Internet.* Madrid: Observatorio Nacional de las Telecomunicaciones y de la SI.

Vazquez Hernández, María de la Luz. (2018). *Círculo de la Violencia*. Instituto Municipal de la Mujer en Amaxac. Guerrero. México. https://gentetlx.com.mx/2018/06/12/amaxac-llevo-a-cabo-platica-circulo-de-la-violencia/

Verdejo Espinosa, M.A. (2015). *Ciberacoso y Violencia de Género en Redes Sociales. Análisis y herramientas de prevención.* Universidad Internacional de Andalucía, p.228.

Villar Varela, M.; Mendez-Lois, M.J. y Barreiro Fernández, F. (2021). *Violencia de Género en entornos virtuales: una aproximación a la realidad adolescente.* Departamento de Pedagogía y Didáctica, Universidad de Santiago de Compostela.

Walker, Leonore (1979). *El círculo de la violencia de Leonor Walker.* https://lamenteesmaravillosa.com/el-circulo-de-la-violencia-de-leonor-walker/

Wu J, Feng Y, y Sun P, (2018). *Sensor fusion for recognition of activities of daily living*, *[Fusión de sensores para reconocimiento de actividades de la vida diaria].* Sensors, vol. 18, p. 4029.

UNIVERSITAS
Miguel Hernández