Informe mensual

Octubre 2022

Observatorio de Violencia Digital

Contenido

Fuente de datos octubre 2022:

Canal de Denuncias del Observatorio de Violencia Digital

Muestra: 126

El Observatorio de Violencia Digital

El convenio de colaboración entre CEDEU y Stop Violencia de Genero Digital, presenta el primer proyecto en común en contra de la violencia Digital: El Observatorio de Violencia Digital.

Este proyecto tiene como objetivos fundamentales la integración de la información, investigación, concienciación y prevención de la violencia digital a través de las nuevas tecnologías y redes sociales.

Debido a la dependencia tecnológica que cada vez tenemos hoy en día, no suele haber ningún lugar en donde esconderse de los ciberacosadores. El ciberacoso puede ocurrir en casa, en el centro de estudios o en cualquier otro lugar donde una persona se pueda conectar a internet.

Es necesario contar con un Observatorio de Violencia Digital que recopile y dé a conocer datos oficiales sobre la situación actual de los delitos informáticos en el ámbito de la **Violencia Digital en España**.

Si contamos con datos oficiales, se podrá actualizar la legislación vigente de acuerdo con los problemas que se están generando en la sociedad hoy en día en el ámbito digital, además que ayudará a la coordinación de organismos públicos y fuerzas y cuerpos de seguridad para combatir este tipo de violencia.

Dentro del observatorio se recogerán los datos, separándolos por tipos de delitos digitales, (Violencia de Genero Digital, Sextorsión, amenazas, suplantación de Identidad, ciberacoso, etc.)

OBJETIVOS DEL OBSERVATORIO DE VIOLENCIA DIGITAL

- Recopilar información de casos de violencia digital en territorio nacional
- Seguimiento y prevención a través de sistemas de rastreo en la red y algoritmos de análisis predictivo

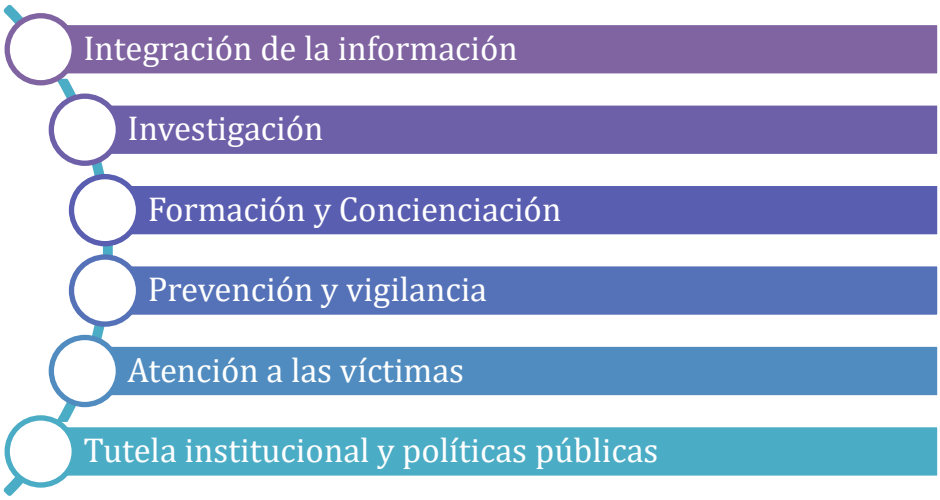
- Realizar informes mensuales y anuales de estadísticas en Violencia Digital de los datos reportados al Observatorio
- Establecer protocolos de actuación ante casos de violencia digital
- Difundir maneras de navegación segura por internet
- Informar a la sociedad para concienciarlos sobre los riesgos y peligros en internet
- Realizar actividades educativas adecuadas para conocimiento de uso de internet (redes sociales, prevención, Ciberseguridad, etc.)

DESTINATARIOS

- Destinatarios directos:
  - ✓ Organismos Públicos
- Destinatarios indirectos:
  - ✓ Familiares y/o personas del entorno de los/as afectados/as .
  - ✓ Víctimas o posibles víctimas que necesiten asesoramiento y/o ayuda.
  - ✓ Todos /as lo que Sufren algún tipo de violencia mediante herramientas digitales

ACTUACIONES

El Observatorio de Violencia Digital fundamenta sus actuaciones en seis ejes, que recogen las actuaciones de distinta naturaleza, pero con un fin conjunto, que es la reducción del impacto de la violencia digital en nuestra sociedad, así como la prevención y atención a sus víctimas.



Integración de la información

El Observatorio de Violencia Digital tiene entre sus objetivos la generación de un conocimiento real sobre las distintas formas de violencia digital y el impacto real que tiene en nuestra sociedad. Para tal fin, el Observatorio desarrollará una base de datos en la que integrará información recogida en distintos sistemas de información como plataformas de violencia de género (VioGen) o bases de datos de organismos de la administración como Incibe, así como los datos recogidos por el propio Observatorio en su seguimiento y gestión de los casos de violencia digital detectados.

Esta base de datos integrada permitirá la investigación y será puesta a disposición de la Administración y Fuerzas de Seguridad del Estado para mejorar sus procedimientos de operación.

Estudio e Investigación

El Observatorio deberá mantener vigilancia tecnológica sobre la evolución de las nuevas tecnologías susceptibles de ser un canal de desarrollo de violencia digital, como redes sociales o dispositivos de comunicación personales. La inmersión de la tecnología en la sociedad aumenta la vulnerabilidad y el impacto de cualquier acto de violencia en este entorno.

Asimismo, el Observatorio mantendrá un estudio activo de la información recopilada e investigará el comportamiento y evolución de la violencia digital en los

distintos grupos de población, con el fin de mejorar los protocolos de actuación y la prevención. Además, el Observatorio publicará sus informes mensuales y anuales con el análisis estadístico.

Formación y concienciación

La normalización de las nuevas tecnologías puede producir insensibilización ante las consecuencias que actos tales como ciberacoso o publicación de material privado pueden producir en una víctima.

Del mismo modo, su creciente papel en las interacciones del día a día abren un gran abanico de posibilidades para que se produzcan comportamientos inadecuados ante los que no siempre existe un conocimiento de cómo actuar.

Por ello, el Observatorio de Violencia Digital trabajará con ciudadanos, colegios, institutos y universidades en campañas de formación presencial y online en la que se abordarán las causas y los procedimientos a seguir en caso de detectar actividades que puedan ser susceptibles de producir violencia digital.

Del mismo modo se trabajará la concienciación y distribución del mensaje a través de campañas, actos y eventos, así como alianzas con otras entidades y organismos que permitan canalizar la importancia de atajar el problema de la violencia digital de raíz.

Prevención y vigilancia

El Observatorio de Violencia Digital tiene como objetivo la prevención activa de la violencia digital. Los casos de violencia digital pueden clasificarse en función del tipo de agresión, del tipo de agresores, de la situación y grupo social de la víctima, del medio, del impacto de la agresión, etc.

El Observatorio de Violencia Digital pondrá a disposición de los usuarios una aplicación multiplataforma que permita al usuario ponerse en contacto con el Observatorio o denunciar un caso de violencia digital. Del mismo modo permitirá, con el consentimiento del usuario, recoger la información del caso.

El estudio de la información integrada obtenida de las diversas fuentes (bases de datos de fuerzas del estado, otras entidades, casos recogidos por el propio Observatorio) permitirá la modelización de los tipos de agresión con mayores ratios estadísticos e impacto.

A través de plataformas de gestión masiva de datos, también conocido como BigData, se podrá nutrir a las herramientas de rastreo web con los algoritmos y parámetros adecuados. Este proceso cíclico de adquisición y mejora de información permitirá un mayor aprendizaje de la plataforma del Observatorio, a la vez que permitirá generar alarmas cuando se produzcan situaciones de riesgo para potenciales víctimas o víctimas que estén recibiendo vigilancia por parte del Observatorio.

Atención a víctimas de violencia digital

El Observatorio de Violencia Digital colaborará con los distintos organismos y entidades públicos en la atención a las víctimas de violencia digital, incluyendo el asesoramiento ante casos y la atención primaria.

Esto complementa la gestión de incidencias recogidas por la plataforma del Observatorio, en las q se realizará una evaluación del caso y se comunicará directamente con el usuario o se notificará a las Fuerzas de Seguridad en función del resultado de la evaluación.

Tutela institucional y creación de políticas públicas

La resolución progresiva del problema actual de falta de recogida de información sistemática e integrada permitirá al Observatorio, en sus labores de investigación ya mencionadas, proponer aquellas consideraciones o mejoras en los protocolos de actuación de las instituciones y las políticas públicas de la Administración.

Del mismo modo dará soporte a las Fuerzas del Estado en la detección y resolución de todo caso de violencia en la red.

A través de los informes anuales y de la base de datos integrada, así como del análisis de los casos recogidos, el Observatorio participará consultivamente en cualquier propuesta de reforma legal susceptible de mejorar las actuaciones de los cuerpos de seguridad o de sancionar o evaluar correctamente los casos de violencia digital desde un punto de vista jurídico.

Marco Normativo

Código Penal.

Artículo 172 ter.

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 Ciberacoso puede ser constitutivo de un delito de:

- Amenazas (Art. 169 a 171 CP)
- Coacciones (Art. 172 a 173 CP)
- Injurias (Art. 206 a 210 CP)
- Calumnia (Art. 205 CP)

Código penal artículo 197.7

“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."

Marco Teórico Violencia Digital

Entendemos por Violencia Digital a toda aquella acción que mediante medios digitales acose, amenace o extorsione a cualquier individuo.

La **Violencia Digital,** es una manifestación indiscriminada, magnificada por el uso de las nuevas tecnologías e internet, que impide gravemente el goce de derechos y libertades, en donde se vulneran los derechos básicos en cuanto a telecomunicaciones y que llegan a aislar a la víctima apartándolas de su entorno laboral, profesional, social y personal; ya que todos dependemos del teléfono o del correo electrónico, con lo que la sociedad tiene que entender que una persona ciberacosada, sin conocer al ciberagresor, le lleva a vivir situaciones traumáticas que le aíslan de la sociedad y que bien por vergüenza o necesidad, tanto emocional como económica, no saben cómo reaccionar ante estos incidentes.

Podemos diferencias el término Violencia de Género Digital como toda aquella agresión psicológica que realiza una persona través de las nuevas tecnologías como el correo electrónico, sistemas de mensajería como WhatsApp o redes sociales, **contra su pareja o ex pareja** de forma sostenida y repetida en el tiempo, con la única finalidad de discriminación, dominación y intromisión sin consentimiento a la privacidad de la víctima.

La Violencia Digital podemos dividirla en 4 grandes grupos:

Ciberacoso

La Real Academia de la Lengua, define "acosar" como:

1. Perseguir, sin darle tregua ni reposo, a un animal o a una persona
2. Perseguir, apremiar, importunar a alguien con molestas o requerimientos

Por lo que acoso:

1. Acción y efecto de acosar
2. Acoso sexual. El que tiene por objeto obtener los favores sexuales de una persona, cuando quien lo realiza se halla en posición de superioridad respecto de quien lo sufre

El ciberacoso podemos definirla como la acción de llevar a cabo "amenazas, hostigamiento, humillación y otro tipo de molestias realizadas por un adulto contra otro adulto por medio de las nuevas tecnologías como internet, dispositivos móviles, correo electrónico, redes sociales, etc.

Hay que destacar que para que una acción sea catalogada como "ciberacoso" deben existir agresiones *(amenazas, insultos, extorsiones, robos de contraseñas, suplantación de identidad, etc.)* a través de las nuevas tecnologías y **de forma reiterada**, con la única finalidad de socavar la autoestima y la dignidad personal de la víctima, provocándole así una victimización psicológica, estrés emocional y rechazo social.

En algunas situaciones, el ciberacoso es de carácter discriminatorio. Los comentarios intimidatorios o despectivos que se centran en aspectos como el género, la religión, la orientación sexual, la raza o las diferencias físicas de las personas forman parte de este tipo de acoso.

El Ciberacoso puede ser especialmente doloroso y ofensivo incluso más que el físico, ya que suele ser de carácter anónimo y es muy difícil identificar al acosador. La gente puede ser atormentada durante las 24 horas del día y los siete días de la semana, cada vez que mire el teléfono o el ordenador. A veces, puede no ser consciente de lo que se dice a sus espaldas o de dónde procede el ciberacoso.

El ciberacoso resulta más fácil de cometer que otros tipos de acoso, puesto que el acosador no tiene que enfrentarse cara a cara a su víctima.

Actividades que realizan los ciberacosadores que podemos clasificarlas como ciberacoso:

- Distribución por la red de una imagen de carácter sexual para perjudicar la reputación de la víctima
- Publicar en un sitio web información personal (falsa o verdadera) donde pueda estigmatizar y ridiculizar a la víctima
- Crear perfiles falsos en internet en nombre de la víctima para compartir contenido pornográfico o ofertas sexuales explicitas
- Suplantar la identidad de la víctima por las redes sociales
- Con frecuencia los ciberacosadores engañan a las víctimas haciéndose pasar por amigos o por una persona conocida con la que acuerdan un encuentro digital para llevar a algún tipo de acoso *online*.
- Divulgar por Internet grabaciones con móviles o cámara digital en las que se intimida, pega, agrede, persigue, etc. a una persona. El agresor se complace no sólo del acoso cometido sino también de inmortalizarlo, convertirlo en objeto de burla y obtener reconocimiento por ello. Algo que se incrementa cuando los medios de comunicación se hacen eco de ello.
- Dar de alta en determinados sitios web la dirección de correo electrónico de la persona acosada para convertirla en blanco de spam, contactos con desconocidos, etc.
- Asaltar el correo electrónico de la víctima accediendo a todos sus mensajes o, incluso, impidiendo que el verdadero destinatario los pueda leer.
- Enviar mensajes ofensivos y hostigadores a través de e-mail, WhatsApp o redes sociales.
- Perseguir e incomodar a la persona acosada en los espacios de Internet que frecuenta de manera habitual.

- Acosar a través de llamadas telefónicas silenciosas, o con amenazas, insultos, con alto contenido sexual, colgando repetidamente cuando contestan, en horas inoportunas, etc.

Debido a la dependencia tecnológica que cada vez es mayor, hoy en día, no suele haber ningún lugar en donde esconderse de los ciberacosadores. El ciberacoso puede ocurrir en casa, en el centro de estudios o en cualquier otro lugar donde una persona se pueda conectar a internet.

El 'ciberacoso', al tratarse de una forma de acoso indirecto y no presencial, el ciber agresor no tiene contacto con la víctima, no ve su cara, sus ojos, su dolor, su pena, con lo cual difícilmente podrá llegar a enfatizar o despertar su compasión. El ciberacosador obtiene satisfacción en la elaboración del acto violento y de imaginar el daño ocasionado en el otro, ya que no puede vivirlo in situ.

La particularidad adicional del ciberacoso es el uso principalmente de las nuevas tecnologías. Debido al alcance, difusión, y masificación del uso de Internet, se puede dar ciberacoso prácticamente en todos los ámbitos en los que se mueve una persona ya sea personal o profesional.

Una manifestación muy común de violencia digital, sobre todo entre los jóvenes es el control que tiene el ciberacosador de los dispositivos móviles de la víctima.

Hemos tenido casos en los que la propia víctima acepta que no es consciente que esta sufriendo una relación abusiva y controladora, en la que consideraban "normal" el control total de parte de sus parejas de sus dispositivos móviles, llamadas, WhatsApp y redes sociales. Esas mismas personas aceptaban que como prueba de amor le daban todas sus contraseñas de sus dispositivos y redes sociales a sus parejas. Y cuando no les gustaba algo a sus parejas les obligaban a borrar sus contactos de WhatsApp o redes sociales e incluso les chantajeaban con publicar algo en su Facebook que afectará a su dignidad como persona sino hacia lo que les decía; simplemente por celos e inseguridades.

En violencia de género, el control de las comunicaciones de la víctima se convierte en una herramienta clave para lograr un aislamiento de la misma y obtener un control total de ella; forma parte de una ampliación del hostigamiento y control que el agresor puede ejercer sobre su víctima.

Utilizan los dispositivos móviles ya no solo para controlar con quien habla o donde se encuentra, sino también como medio para amenazar de forma explícita a la víctima y a su entorno; además de suponer un verdadero martirio para aquellas mujeres que se ven obligadas a responder inmediatamente al agresor, repercutiendo en las posibilidades de vivir una vida normalizada e incluso desempeñar una tarea o trabajo. Este tipo de acoso, lejos de desaparecer cuando finaliza la relación, en muchas ocasiones se inicia o se intensifica al poner fin a la misma.

Las víctimas de 'ciberacoso', como las de acoso en la "vida real", sufren problemas de estrés, humillación, ansiedad, depresión, ira, impotencia, fatiga, enfermedad física, pérdida de confianza en sí mismo, pudiendo derivar al suicidio.

Características de un ciberacoso

- **Requiere destreza y conocimientos avanzados sobre Internet.**
- La mayoría de los ciberacosadores intentan dañar la reputación de la víctima manipulando a gente contra él.
- **Publican información falsa** sobre las víctimas en diferentes sitios web y redes sociales
- Los ciberacosadores pueden espiar el entorno social y afectivo de la víctima para obtener información personal de ella. De esta forma, conocen el resultado de sus agresiones y cuáles son los rumores que más efecto están teniendo en la víctima. A menudo monitorizarán las actividades de la víctima e intentarán rastrear su dirección de IP, móviles y ordenadores en un intento de obtener más información sobre ésta.
- **Envían de forma periódica correos difamatorios** al entorno de la víctima para manipularlos.

- **Manipulan a otros para que acosen a la víctima.** La mayoría de los ciberacosadores tratan de implicar a terceros en el hostigamiento. Si consigue este propósito, y consigue que otros hagan el trabajo sucio hostigándole, haciéndole fotos o vídeos comprometidos, es posible que use la identidad de éstos en las siguientes difamaciones, incrementando así la credibilidad de las falsas acusaciones, y manipulando al entorno para que crean que se lo merece.
- **Falsa victimización.** El ciberacosador puede alegar que la víctima le está acosando a él.
- **Ataques sobre datos y equipos informáticos.** Ellos buscan infiltrarse en los dispositivos informáticos y redes sociales de la víctima.
- El ciberacoso no tiene un propósito justificado, más que aterrorizar a la víctima, aunque muchos ciberacosadores están convencidos de que tienen una causa justa para acosarla, usualmente en la base de que la víctima merece ser castigada por algún error o desobediencia que dicen que ésta ha cometido.
- **Repetición:** El ciberataque no es un sólo un incidente aislado. Repetición es la clave del ciberacoso. Un ciberacoso aislado, aun cuando pueda estresar, no puede ser definido como un caso de ciberacoso.
- **El ciberacoso invade ámbitos de privacidad** y aparente seguridad como es el hogar familiar, desarrollando el sentimiento de desprotección total.
- **El ciberacoso se hace público**, se abre a más personas rápidamente.
- **No es necesaria la proximidad física con la víctima.** El 'ciberacoso' es un tipo de acoso psicológico que se puede perpetrar en cualquier lugar y momento sin necesidad de que el acosador y la víctima coincidan ni en el espacio ni en el tiempo.

Sexting / Sextorsión

Podemos definir sexting al intercambio, difusión o publicación de fotografías y videos de carácter sexual, grabados por el remitente haciendo uso de dispositivos informáticos.

Según estudios, el sexting es muy común hoy en día sobre todo en jóvenes de entre los 18 y 24 años, y no está vinculado con conductas sexuales arriesgadas o con problemas psicológicos; más bien se está convirtiendo en una nueva forma de relacionarse sexualmente con tu pareja.

Ahora bien, ¿qué sucede cuando ese contenido sexual que le enviamos a nuestra pareja es publicada y distribuida en internet sin nuestro consentimiento?

Las personas que realizan está práctica no perciben la amenaza que puede llegar a sufrir contra su privacidad ni es consciente de las implicaciones desde el punto de vista de seguridad. No son conscientes de los riesgos de la exposición de datos privados e íntimos, a través de las nuevas tecnologías, y por ello lo difunden. Se colocan a sí mismos en una situación de vulnerabilidad.

Esta muy de moda, utilizar aplicaciones como Snapchat para la práctica de sexting, ya que cada publicación multimedia tiene una duración de segundos y luego se elimina automáticamente; si bien es cierto que se elimina y no puede volver a ser vista, se les olvida que el ciberacosador dispone de segundos para poder hacer una captura de pantalla, y así poder distribuir ese contenido.

Tuvimos un caso de una chica de un pueblo de Madrid, en donde compartía fotografías de carácter sexual con su pareja por Snapchat, a los pocos días el equipo de futbol donde jugaba el y los de los alrededores tenían en su poder las fotografías de la joven, habían sido capturadas con el móvil y distribuida sin su consentimiento.

Riegos que puede conllevar la práctica del sexting

Amenazas a la privacidad.

No nos damos cuenta de que el contenido íntimo generado por nosotros puede terminar en manos de otras personas desde el momento que le damos “enviar”. Una vez enviado, perdemos el control sobre su difusión.

También existen formas involuntarias de perder el control de este tipo de contenido: robo o pérdida del móvil o acceso sin consentimiento por terceros a nuestros dispositivos.

O como comentábamos antes, que ellas mismas le den las contraseñas de sus dispositivos a sus parejas como "prueba de amor y de confianza".

Riesgos psicológicos

Si el contenido cae en terceras personas sin nuestro consentimiento, y son expuestas públicamente entre nuestro entorno, nos podemos ver sometidos a un ensañamiento o humillación pública que puede derivarnos en un daño psicológico: ansiedad, depresión, exclusión social, etc.

Con la práctica del sexting existen dos posibles peligros, por un lado, la publicación por terceros del contenido sexual sin tu consentimiento lo cual es una invasión a tu intimidad, y por otro, la Sextorsión.

Ahora bien, ¿Qué es la Sextorsión?

Un contenido sexual en manos de la persona inadecuada constituye un elemento ideal para poder extorsionar o chantajear a alguien. Se conoce como Sextorsión al chantaje al que es sometida una persona por parte de otra que emplea contenidos de carácter sexual para obtener algún beneficio de la víctima, amenazando con su publicación.

Cabe resaltar, no obstante, que la ley ampara en cierta medida a las víctimas de Sextorsión / sexting. Solo el hecho de publicar las imágenes sin el consentimiento de la otra persona ya es un delito contra la intimidad y está tipificado en la reforma del Código Penal.

Código penal artículo 197.7

"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."

Requisitos para que se contemple el delito de sexting en la legislación vigente:

- La conducta típica debe ser la de **difundir, revelar o ceder a terceros** imágenes o grabaciones audiovisuales.
- **La difusión o divulgación debe haberse realizado sin el consentimiento de la víctima** y ello, aunque tales **imágenes hubieran sido obtenidas con el consentimiento de la víctima** en su domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros.
- La divulgación debe **dañar gravemente la intimidad de la víctima**.

La **difusión, revelación o cesión** de las mismas **a terceros**, puede ser muy variada *(redes sociales, Internet, WhatsApp, SMS, mail, mensajería instantánea, Line o similares....*)

Se distingue claramente entre la **difusión o divulgación** de la imagen o grabación (que debe producirse sin autorización o consentimiento de la víctima) y la **obtención o captación de dichas imágenes o vídeos** (independientemente de que la víctima hubiera dado o no su consentimiento).

Con este artículo del Código Penal se está sancionando dos tipos de conductas:

- La del **receptor inmediato o destinatario de la imagen o grabación**, o que había protagonizado o sido parte de la captación o grabación del vídeo o imagen y difunde la imagen sin el consentimiento de la víctima.
- La de los **terceros receptores** a los que se haya reenviado o *"rebotado"* la imagen o grabación, y éstos a su vez las difunden a otros, sin consentimiento de la víctima.

Suplantación de Identidad

Empecemos definiendo el término "Identidad Digital", el cual es el conjunto de la información sobre una persona u organización expuesta en internet (datos personales, imágenes, etc.) que conforma una descripción de dicha persona en el ámbito digital

Por lo que el uso de dicha información personal para hacerse pasar por otra persona con el fin de obtener un beneficio propio es lo que llamaríamos como Suplantación de Identidad.

Las redes sociales si no tomamos las medidas de seguridad adecuadas, permiten un acceso de terceras personas a nuestra información, publicaciones, comentarios, imágenes, etc.; la cual puede ser utilizada y monitorizada para otros fines sin nuestro consentimiento.

En Violencia de Género Digital, cada vez es más frecuente encontrarse con situaciones de control máximo por parte del agresor hacia la víctima, ya que este conoce previamente la identificación (usuario o correo electrónico) y contraseña de su pareja o expareja, que erróneamente tendemos a compartir dicha información como "prueba de confianza". Por lo tanto, el Ciber agresor puede acceder a nuestros perfiles y correo electrónico, disponiendo de información sobre nuestra persona que puede utilizar para una suplantación de identidad. Por mucho que lo bloquees en las redes sociales, si el conoce tus datos de acceso estamos en un problema, por eso es recomendable el uso contraseñas seguras y el cambio constante de ellas.

Aunque cabe la posibilidad que el Ciber agresor obtenga el usuario y contraseña de manera fraudulenta "hackeando" el ordenador o el móvil de la víctima.

Además, tenemos que considerar que, al interrumpir una relación, no solemos interrumpir nuestra amistad con amistades comunes con nuestra ex pareja e incluso con familiares a los que mantenemos como contacto en las redes sociales a las que pertenezcamos, y que a través de ellos el agresor puede alcanzar cierto grado de conocimiento sobre nuestra actividad personal.

Es más, en aquellos casos en los que las víctimas se abren un perfil tras interrumpir la convivencia con el agresor, se debe prestar mucha atención a no incluir en el mismo dato que las hagan fácilmente localizables por éste a través de cualquiera de los motores de búsqueda existentes. Muchas veces las intenciones del agresor van incluso más allá del puro control y además de monitorizar los actos de la víctima, el objetivo final es la humillación y desacreditación pública de esta, por lo que se hace pasar por la misma y en ocasiones incluso llega a realizar actos propios de ésta.

Entre ejemplos de suplantación de identidad podemos mencionar:

- Registrar un perfil en una red social con el nombre de otra persona sin su consentimiento y utilizando datos o imágenes de la víctima
    - NOTA: Si únicamente se registra un perfil falso por medio del nombre o alias y no se utiliza información o imágenes personales de la víctima, es decir, sin hacer uso de otros datos personales ni realizar ninguna interacción en base a los mismos, la conducta no estaría considerada delito. Solo nos quedaría denunciar en la red social el perfil para su eliminación, ya que la mayoría de las redes sociales considera la suplantación de identidad una falta grave a sus términos y políticas de uso.
- Acceder sin consentimiento a una cuenta ajena para tener acceso a la información almacenada en ella. No solo se está vulnerando la intimidad y privacidad de la víctima, sino que también podría dar lugar a un caso de

suplantación de identidad, si además de acceder a la información se interactuara en nombre de la persona a través de ese canal.

- Acceder sin consentimiento a una cuenta ajena utilizando los datos personales y haciéndose pasar por el suplantado (realizando comentarios, subiendo fotografías, etc.). Se estaría cometiendo un delito de suplantación de identidad unido a obtención ilícita de claves de acceso. Para que sea constitutivo de delito es necesario que el suplantador cometa acciones que solo el suplantado puede realizar por los derecho y facultades que a él le corresponden.
- Una publicación sin consentimiento de anuncios o comentarios en nombre de una tercera persona a través, por ejemplo, de un correo electrónico o WhatsApp, se considera suplantación de identidad

Los principales métodos utilizados por los ciberacosadores para adquirir nuestra información personal para una suplantación de identidad son:

- El diseño y uso de software para recolectar información personal, el cual es instalado silenciosamente en ordenadores o dispositivos móviles. Por ejemplo: malware.
- El uso de correos electrónicos o sitios Web falsos para engañar a las personas haciendo que éstas revelen información personal. Por ejemplo: phishing y spam.

Ciberbullying

Definimos Ciberbullying como el uso de los medios telemático (internet, telefonía móvil, etc.) para ejercer el acoso psicológico entre iguales.

Hay que destacar que este tipo de violencia digital se produce a lo largo del periódico escolar y se refiere al uso de las redes sociales, sitios web o blogs para difamar o acosar a compañeros de escuela o, a personas perteneciente al mismo grupo, SIN QUE INTERVENGAN PERSONAS ADULTAS.

El Ciberbullying se caracteriza por 5 aspectos principales:

1. Al igual que el ciberacoso, el Ciberbullying se dilata en el tiempo. Un ataque puntual no se podría considerar Ciberbullying, más bien deben de ser ataques con una continuidad en el tiempo.
2. Un caso de Ciberbullying no cuenta con contenido de índole sexual. En caso de que un acoso a menores sea de carácter sexual se clasificaría como grooming.
3. Tanto víctimas como ciberacosadores son exclusivamente menores
4. Es necesario que ambas partes involucradas tengan algún tipo de relación o contacto previo. Con frecuencia, el Ciberbullying empieza en el "mundo real" siendo el mundo digital una segunda fase de la situación de acoso
5. Se utiliza exclusivamente medios digitales ya sea WhatsApp, redes sociales, etc.; para llevar a cabo el acoso.

El Ciberbullying puede ser constitutivo de un delito de:

- Amenazas (Art. 169 a 171 CP)
- Coacciones (Art. 172 a 173 CP)
- Injurias (Art. 206 a 210 CP)
- Calumnia (Art. 205 CP)

Ahora bien, no olvidemos que en este tipo de violencia digital el ciberacosador es un menor. A este aspecto, la regulación penal aplica la siguiente legislación en función de la edad del sujeto autor del delito:

- Menores entre los 16 y 18 años. Ley Orgánica 10/1995, de 23 de noviembre, por la que se aprueba el Código Penal.
- Mayores de 14 años y menores de 18. Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores (en adelante, LORPM).

Evidencias Digitales

Las evidencias a analizar contienen pruebas que serán utilizadas, en la mayoría de los casos, durante un procedimiento judicial. Su manejo por parte del perito debe ser cuidadoso y escrupuloso.

Podemos definir una "evidencia digital" como un contenedor de información digital que puede ser utilizada como prueba en un procedimiento judicial.

Una evidencia digital es cualquier valor probatorio de una información almacenada o transmitida en formato digital de tal manera que pueda ser aportada por una de las partes en un proceso judicial.

A diferencia de otro tipo de evidencias, una evidencia digital destaca por ser:

- Volátil
- Anónima
- Modificable o Manipulable

Estas tres características hacen que el proceso de adquisición de evidencias digitales sea complejo, ya que pueden desaparecer fácilmente, o dejar de existir o bien ser modificadas con cierta facilidad.

Principios básicos en el manejo de evidencias digitales

Es de vital importancia que el perito informático cumpla tres principios básicos en el tratamiento de evidencias digitales, evitando así una impugnación de dicha prueba.

Principios para el tratamiento de evidencias digitales.

1. Debemos siempre **documentar todas las acciones realizadas**. Detallando cada uno de los pasos a seguir para la extracción y análisis de la evidencia. Es aconsejable realizar fotografías del proceso.
2. No debemos olvidar cuidar la **cadena de custodia** en el momento de la extracción y preservación de la evidencia
3. Hay que garantizar en todo momento **la integridad de la evidencia**.
4. **Nunca se debe trabajar sobre la evidencia original.** Debemos de realizar un clonado de la evidencia, y realizar el análisis sobre el clonado. De esta

forma protegemos y no alteramos ni modificamos la evidencia original, para un posible análisis posterior o bien una contra pericial.

5. Debemos evitar dañar la evidencia (caídas, calor extremo, campos magnéticos, etc.).

Hoy en día, con el auge de las nuevas tecnologías muchas de las infracciones y delitos se realizan a través de un dispositivo o canal digital; acciones como el sexting, Stalking, Sextorsión, Ciberbullying, ciberacoso, etc.; aunque tienen su correspondiente sanción legislativa en mundo "real", en la mayoría de los casos necesitan una evidencia digital como valor probatorio.

Concepto y términos claves

Evidencia Digital: es un registro de la información guardada o difundida a través de un sistema informático que puede utilizarse como prueba en un proceso judicial.

Ciberacoso: acción de llevar a cabo "amenazas, hostigamiento, humillación y otro tipo de molestias realizadas por un adulto contra otro adulto por medio de las nuevas tecnologías como internet, dispositivos móviles, correo electrónico, redes sociales, etc.

Violencia Digital: toda aquella acción que mediante medios digitales acose, amenace o extorsione a cualquier individuo

Stalking: Es la situación que se crea, cuando una persona persigue a otra de forma obsesiva

Sexting: intercambio, difusión o publicación de fotografías y videos de carácter sexual, grabados por el remitente haciendo uso de dispositivos informáticos.

Software Espía: es un **programa** que se instala en nuestro ordenador o móvil con el objetivo de recopilar información sin nuestro consentimiento.

Malware: software con intenciones maliciosas

Tik Tok TikTok, conocido en China como Douyin, es un servicio de redes sociales para compartir videos propiedad de la empresa china ByteDance

Facebook es un servicio de redes y medios sociales en línea estadounidense con sede en Menlo Park, California.

Instagram es una aplicación y red social de origen estadounidense, propiedad de Meta.

WhatsApp es una aplicación de mensajería instantánea para teléfonos inteligentes, propiedad de Meta

Telegram es una plataforma de mensajería y VOIP, desarrollada por los hermanos Nikolái y Pável Dúrov

Resultados Muestra octubre 2022

Los siguientes datos **han sido recogidos a través del canal de denuncias del Observatorio de Violencia Digital**, directamente desde su página web www.observatoriodeviolenciadigital.com

La muestra es de 126 personas.

Como se menciona se ha detectado 126 casos de violencia digital a nivel nacional, el 38% en la Comunidad de Madrid, 20% en Cataluña, 15% en País Vasco, 8% en Comunidad Valenciana.

Los rangos de edad de las víctimas del mes de septiembre 2022 están distribuidos en:

- 18 a 24 8%
- 25 a 30 45%
- 31 a 45 35%
- 46 a 60 12%

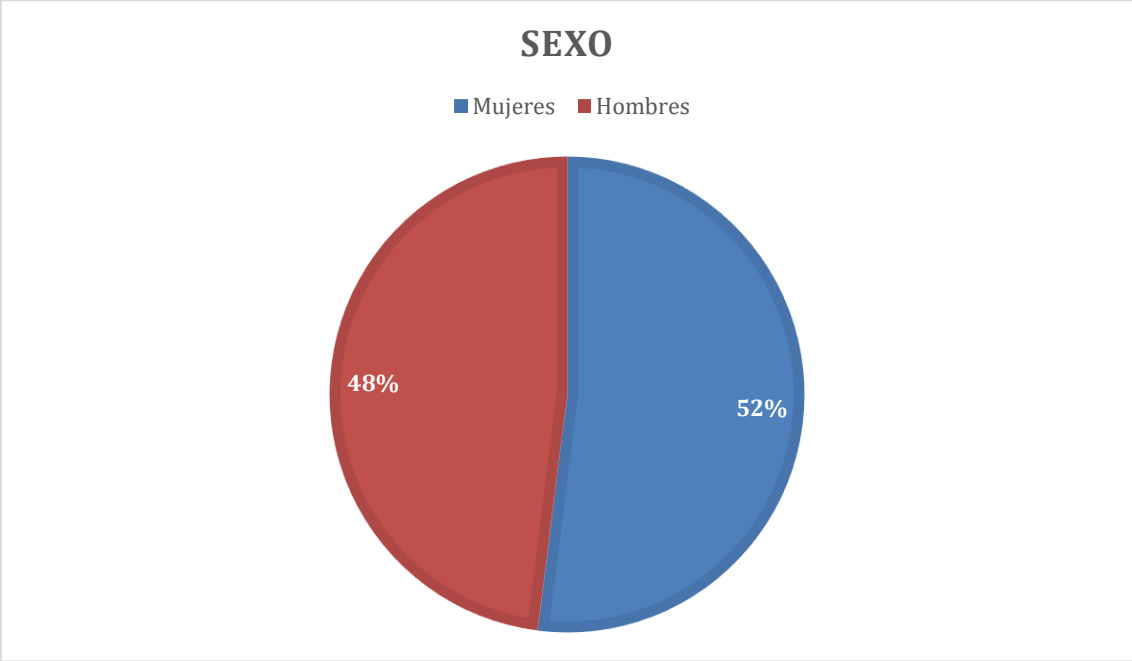
Los principales canales por los que se cometen los delitos informáticos son:

- Whatsapp 38%
- Llamadas telefónicas 12%
- Facebook 19%
- Instagram 26%
- Twitter 5%

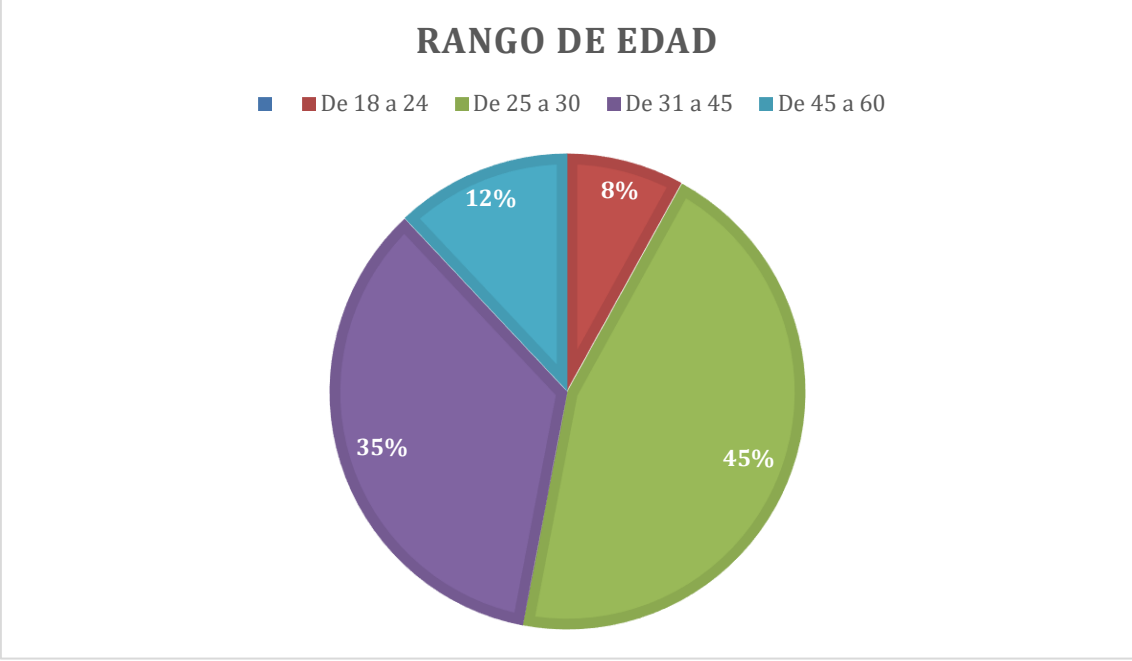
Cabe destacar que el 97% del muestro ha indicado que NO ha denunciado su caso, ya sea por desconocimiento o bien por no saber cómo hacerlo.

Distribución muestra por Sexo

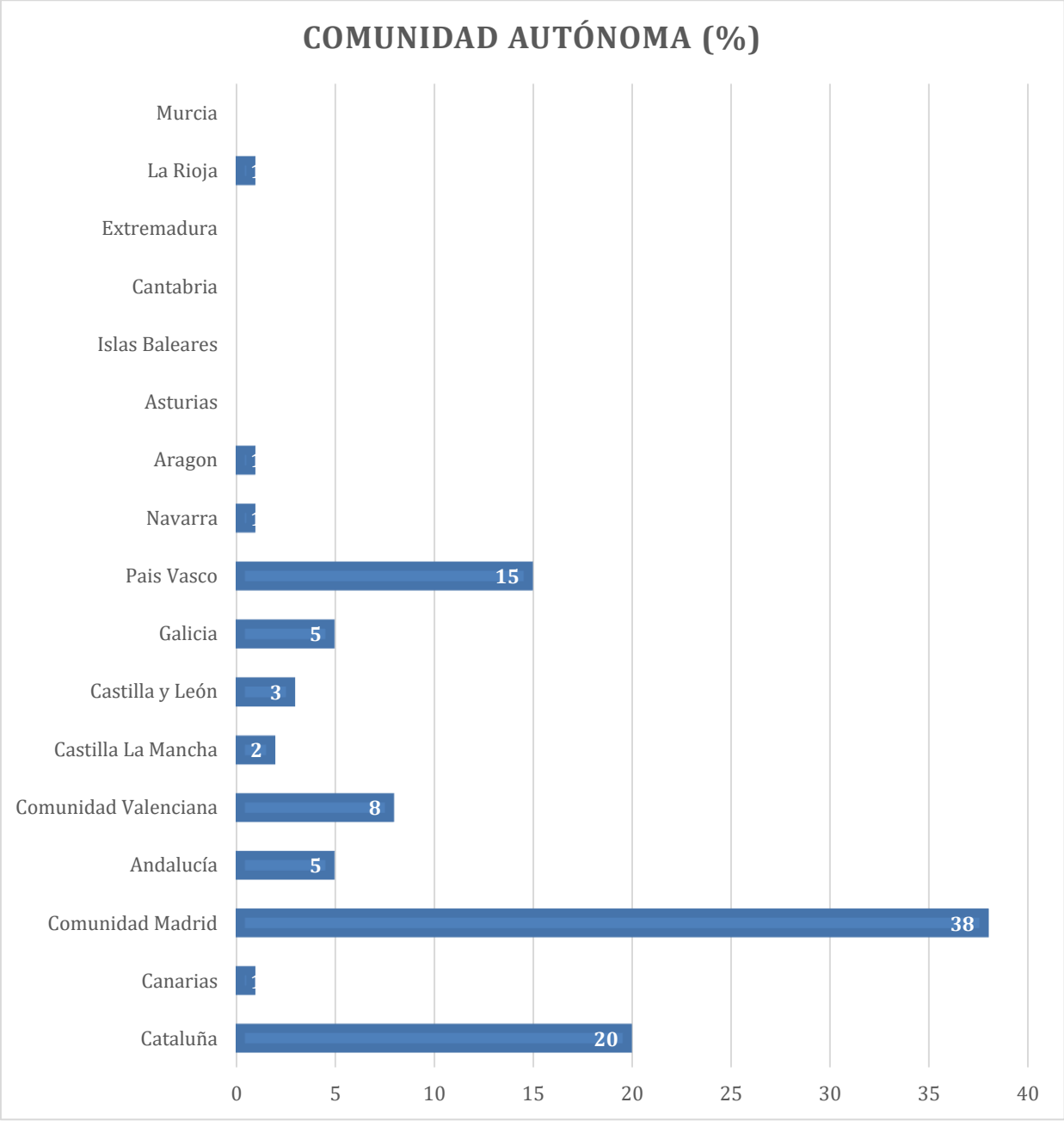
El 52% han sido mujeres y un 48% Hombres



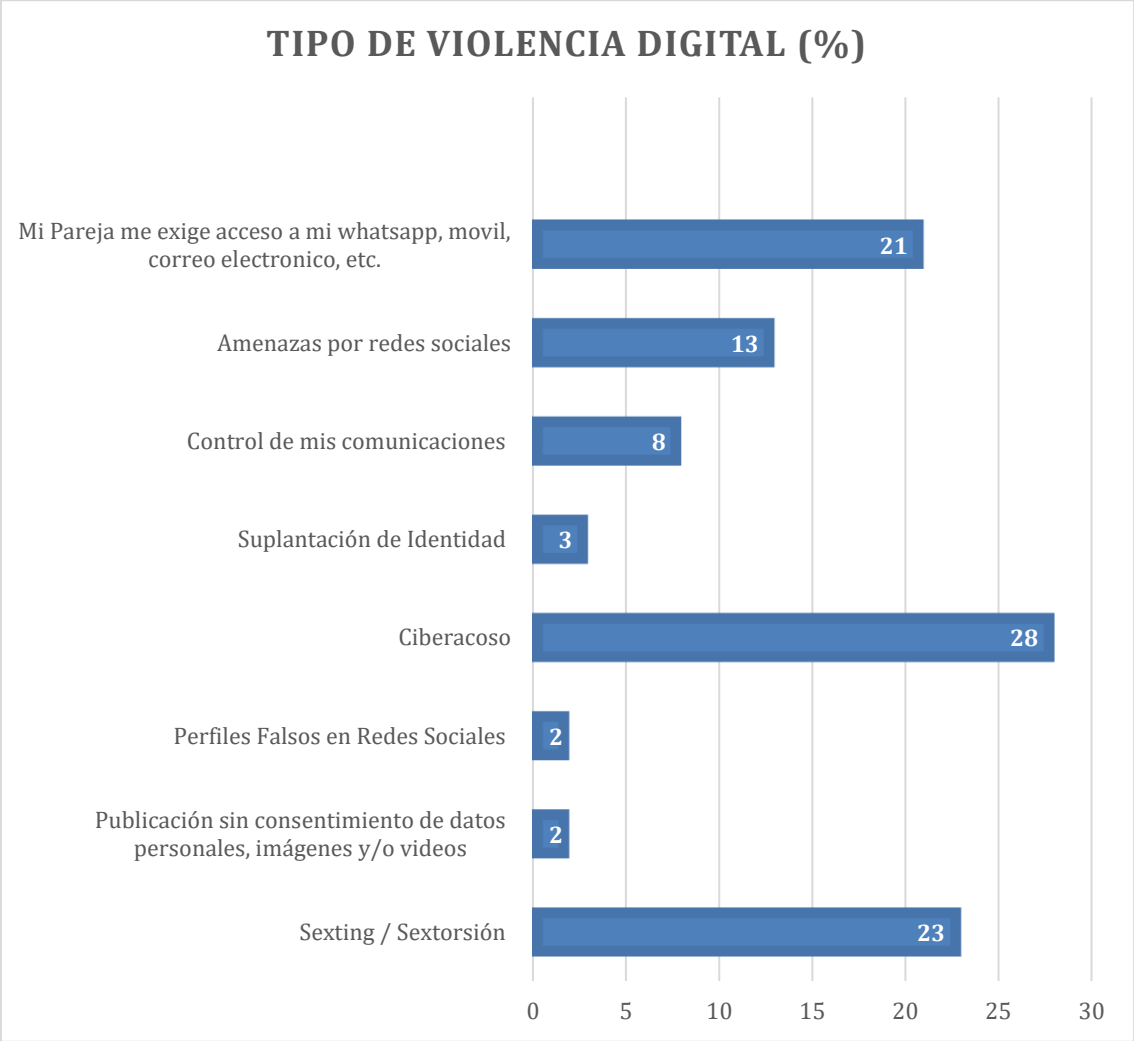
Distribución muestra por Rango de Edad



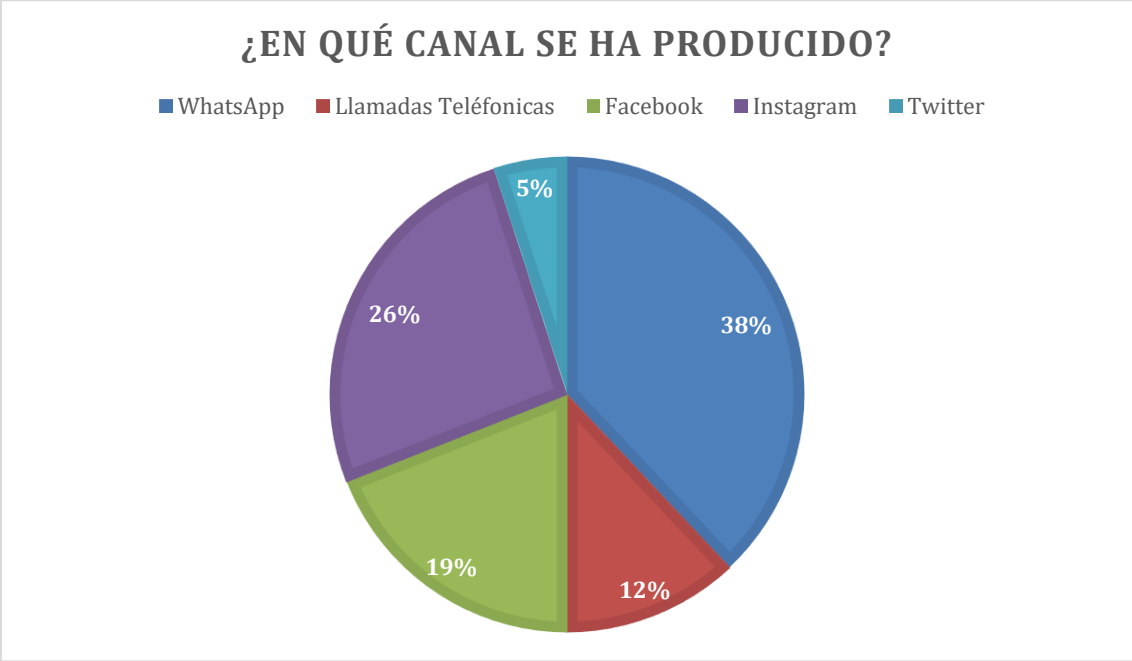
Distribución muestra por Comunidad Autónoma



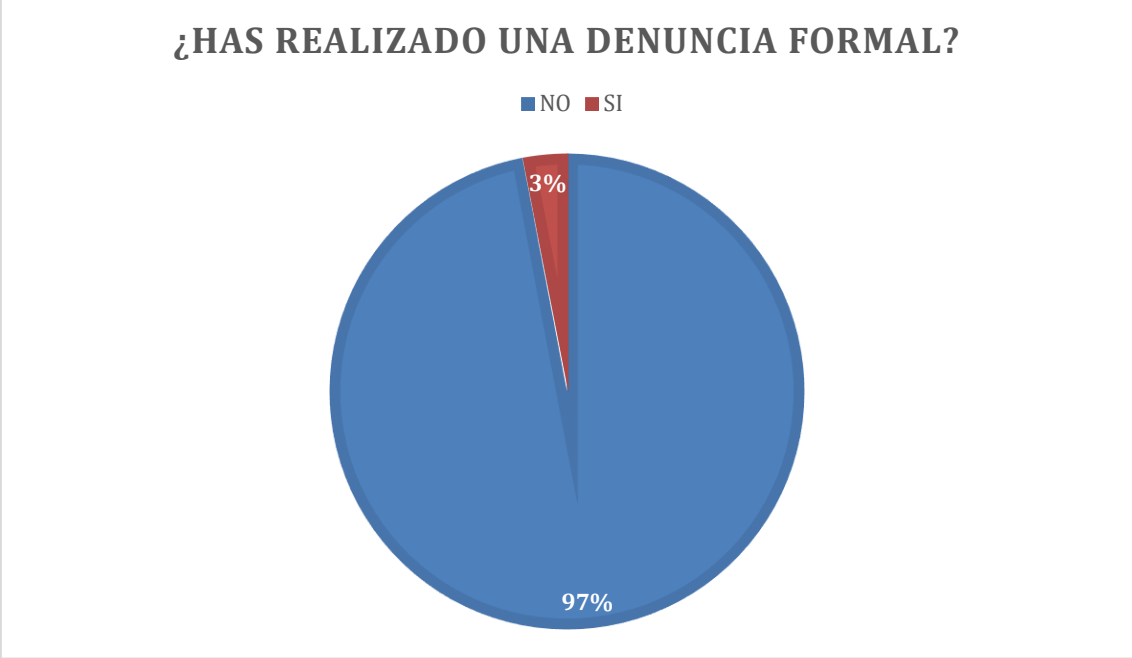
¿Qué tipo de violencia digital has sufrido?



¿En qué canal se ha producido?



¿Has realizado una denuncia formal ante Policía, Guardia Civil o Juzgado?



Medidas de Seguridad para evitar ser víctima de violencia digital

1. Nunca se debe de dar las contraseñas de nuestros dispositivos, redes sociales y correos electrónicos a nadie.
2. Tener instalado un antivirus en nuestros dispositivos digitales
3. No descargar archivos adjuntos de correos electrónicos desconocidos
4. No debemos abrir archivos sospechosos en nuestras conversaciones de WhatsApp o correos electrónicos
5. Debemos de tener nuestros perfiles en redes sociales privados, de esta forma nos seguirán las personas que nosotros aceptemos
6. Configurar la doble autentificación en las redes sociales, para evitar que terceras personas accedan sin nuestro consentimiento

Consejos para prevenir una sextorsión

1. Evita hacerte fotografías de contenido sexual. Si no existen esas fotografías no te pueden extorsionar con ellas
2. No envíes contenido a personas desconocidas. Si ya hay que tener cuidado con personas que conocemos, debemos estar alerta del tipo de contenido que compartimos con personas desconocidas; pueden estar en busca de fotografías comprometedoras para extorsionarte.
3. Cuida tu imagen en internet. Recuerda que toda actividad que realizamos en internet deja una huella y las imágenes o videos compartidos pueden seguir en internet indefinidamente.
4. No cedas al chantaje. No accedas a las peticiones del chantajista, si aceptas le haces más fuerte y nunca parará de extorsionarte
5. Elimina Malware. Asegúrate de que no tienes ningún software malicioso, aunque tu no compartas las fotografías o videos pueden espiarte el ordenador y conseguirlas.
6. Cambia tus contraseñas. Es probable que intenten acceder a tus cuentas y redes sociales en busca de contenido sexual para extorsionarte. Cambia la contraseña cada cierto tiempo

7. No confundas relaciones sentimentales, de amistad, etc. Identifica bien las relaciones sanas, basadas en la confianza y el respeto
8. Evita imágenes con tu rostro. Si practicas sexting, evita enviar fotografías y videos con tu rostro o algún rasgo identificable (lunares, cicatrices, tatuajes, etc) de tu persona
9. Borra el contenido sexual de tu móvil. Los móviles y ordenadores pueden ser robados o puedes perderlo y una tercera persona puede tener acceso a este tipo de contenido.

Consejos para prevenir una suplantación de identidad

1. **Contraseñas.** Es importante asegurar nuestras cuentas y dispositivos con contraseñas "fuertes" (de más de 8 caracteres). Intenta ser creativo usando combinaciones de números y letras
2. **Utiliza Antivirus.** Estos programas te ayudan a mantener tu ordenador libre de algún malware o virus. Recuerda que pueden instalarte software espía o robarte información sin que te enteres.
3. **Análisis constante en busca de virus o malware.** No es suficiente con tener instalado un antivirus, es también importante realizar un análisis completo del sistema con frecuencia, y mantener nuestro antivirus actualizado.
4. **Restringe el acceso a tus redes sociales.** Cambia tu privacidad en redes sociales. Haz tu perfil solo accesible a tus contactos.
5. **Comprueba que tu conexión sea segura.** Cambiar la contraseña del router que trae por defecto, es una manera de asegurar tu conexión.
6. **Estar alerta ante posible caso de Phishing.** No hagas caso a correos sospechosos o de dudosa procedencia. Suelen enviarte correos haciéndose pasar por distintas marcas para robarte información personal
7. **No accedas desde equipos públicos a tus cuentas bancarias.** No utilices ordenadores públicos como en locutorios o wifi gratuitas para acceder a tu banca online. No se sabe si estarán infectados y puedan robarte tus datos bancarios.

8. **Ten cuidado en donde realizar compras y pagos en línea.** Pueden hacerte creer que estás comprando en un sitio que no es el "verdadero" y robarte los datos de tu tarjeta.
9. **Evitar ingresar tu usuario y contraseña en links extraños que te lleguen por email.** No hagas caso a correos electrónicos que te indican que has ganado un premio o un descuento especial y parte dartelo te solicitan tus datos bancarios y usuario / contraseña
10. **Nunca utilices el correo electrónico para compartir información personal.** Incluso si conoces al remitente de un correo electrónico, podría ocurrir que alguna persona sin autorización haya obtenido acceso a la cuenta de correo electrónico del remitente.