Protocolo de actuación para la detección e intervención con víctimas de violencia de género digital

Contenido

Justificación

No hay duda de que nos encontramos en la era digital, donde estar conectados a internet y tener presencia en las redes sociales se ha convertido en una prioridad.

La mensajería instantánea como WhatsApp ha pasado a ser el principal medio de comunicación, el correo electrónico provee más rapidez a la hora de comunicarse que el correo ordinario, las redes sociales son un canal para relacionarnos e interactuar con gente de todo el mundo, internet y su infinidad de páginas web son la mayor enciclopedia sin lugar a duda donde todo lo encuentras, incluso hoy en día puedes hasta encontrar trabajo y pareja en la red.

Toda nuestra vida depende de una u otra manera de las nuevas tecnologías, pero no somos conscientes que también **es una forma de exponer nuestra vida privada y no tener control sobre ella**.

Exponemos nuestra vida personal en las redes sociales, **no cuidamos nuestra intimidad ni tomamos las medidas de seguridad básica** para evitar posibles casos de acoso, extorsión e incluso suplantaciones de identidad. O peor aún muchas personas no son ni conscientes de lo expuestos que están y de los peligros que también te puedes encontrar en internet.

Debido al alcance, difusión y masificación que permite internet y los dispositivos móviles, es cada vez más común que el agresor haga daño al autoestima y dignidad de la víctima haciendo un mal uso de las nuevas tecnologías.

Todas aquellas personas que están siendo víctimas de violencia digital (Ciberacoso, Ciberbullying, Grooming, Violencia Genero Digital, etc.) se sienten desprotegidas ante una sociedad cuya legislación y normativa es escasa en materia de delitos informáticos, donde existe un vacío en cuanto a la desinformación que hoy en día sufrimos todos en esta materia.

Es por ello por lo que es imprescindible disponer de profesionales capaces de intervenir en un caso de violencia de género digital, que sean capaces de detectar el

delito, identificando sus canales de actuación para su posterior análisis de evidencias digitales; así como conocer las herramientas de ciberseguridad que ayuden a prevenir, proteger y salvaguardar los dispositivos de la víctima evitando así futuros ataques. No olvidemos que lograr una empatía con la víctima es fundamental para una correcta intervención.

La Asociación SVGD en su estudio "Situación actual de la Violencia Digital en España" del año 2017, concluyó que:

- Un 48,94% de las personas **se han sentido acosadas en alguna red social**.
- Un 42,55% indica que **ha dado, cedido o revelado sus contraseñas de sus correos electrónicos o redes sociales a su pareja**
- Un 79,4% **considera que la desigualdad de género en el ámbito digital provoca violencia**
- Un 47,4% indica que **desconoce cómo reaccionar ante este tipo de delitos informáticos**
- Un 28,4% **afirma que ha recibido insultos o amenazas de su pareja a través de algún medio digital**

La Delegación de Gobierno para la Violencia de Género en su estudio *"El Ciberacoso como forma de ejercer la violencia de género en la juventud: un riesgo en la sociedad de la información y del conocimiento"* determinó:

- **Los chicos muestran una tendencia mayor que las chicas a usar las nuevas tecnologías para compensar dificultades de relación**, es decir, afirman que se han relacionado mejor con la gente a través de internet que "cara a cara" porque así han podido mostrarse como les gustaría ser.
- En cambio, **las chicas afirman en mayor medida que no les hubiera sido posible vivir sin el móvil**, que usan internet cuando se sienten solas, o que se ponen nerviosas cuando no se pueden conectar o no reciben ningún mensaje.

Estas situaciones, más directamente relacionadas con la adicción a las nuevas tecnologías de la comunicación, se dan más en ellas.

- La juventud presenta una percepción muy baja de los efectos perniciosos del Ciberacoso. Determinados patrones de uso de internet que pueden ser interpretados como prácticas de riesgo, tales como intercambiar información o imágenes privadas, **no se perciben como un peligro**.

- **Más de uno de cada cuatro chicos o chicas adolescentes (28,1%) no consideran conducta de riesgo responder a un mensaje en el que le insultan**,

- **Uno de cada dos chicos (49,4%) y una de cada cuatro chicas (26,2%) no consideran muy o bastante peligroso quedar con un chico o una chica que han conocido por internet.**

- Una de cada cuatro chicas (25%) y uno de cada tres chicos (35,9%) **no consideran muy o bastante peligroso responder a un mensaje en el que alguien que no conoce le ofrece cosas.**

- El 4,9% de las chicas y el 16,1% de los chicos **no consideran muy o bastante peligroso colgar una foto suya de carácter sexual**, conducta que reconocen haber realizado en dos o más ocasiones el 1,1% de las chicas y el 2,2% de los chicos.

- Los chicos reconocen realizar muchas más conductas de riesgo de Ciberacoso con las nuevas tecnologías en casi todas las conductas (están sobrerrepresentados en la respuesta de mayor frecuencia: hasta tres veces o más), mientras que las chicas lo están entre quienes dicen no haberlas realizado nunca. Dos ejemplos:

    - el 44,5% de los chicos y el 37,1% de las chicas **han aceptado dos o más veces como amigo o amiga en la red a una persona desconocida**, o

- el 38,3% de los chicos y 30,2% de las chicas **han respondido en dos o más ocasiones a un mensaje en el que le insultan u ofenden**

- En relación con el intercambio de contenidos personales como vídeos o fotos privadas como una prueba de confianza o un acto de intimidad con la pareja ("prueba de amor") se aprecia una puerta abierta para que se de el **sexting** (difusión de imagen de contenido erótico o sexual). En relación a las conductas de riesgo de "sexting":

    - El 2% de las chicas y el 4,5% de los chicos, **han colgado una foto suya de carácter sexual.**

    - EL 1,3% de las chicas y el 2,5% de los chicos **han colgado una foto de su pareja de carácter sexual.**

Todos hemos empezado a utilizar las nuevas tecnologías y las redes sociales, sin lugar a duda, pero cuantos realmente se han preocupado por cuidar su reputación, su vida personal, su intimidad, no quedar expuestos. No entendemos que nuestras contraseñas es información confidencial que nadie más que nosotros debemos de conocerlas.

Sobre todo, cuando hablas con jóvenes, las adolescentes entregan las contraseñas de sus redes sociales con facilidad a su pareja como prueba de "amor" y de confianza, y no se dan cuenta que le dan la herramienta al agresor para poder tener un control total sobre ellas, para poder así manipularlas o bien encontrar información que dañen la reputación y autoestima de la víctima.

Las personas no son conscientes de los peligros a los que están expuestos en las redes sociales e internet. Y una vez que se encuentran con ello no saben ni a quien ni a dónde acudir para solucionarlos. Se sienten indefensos al no saber quién les puede ayudar a solucionar ese problema; llevándolos en caso extremo a unos daños psicológicos más graves que los físicos en dado caso.

Las personas que sufren un caso de Violencia Digital, en la mayoría de los casos **ignora la forma de enfrentarse a la situación que está sufriendo**, igual que ignora sus derechos, porque nadie le proporciona información legal que le indique los recursos de los que puede disponer, y los medios de protección adecuados que existen a cada tipo de ataque.

Existen cuatro grandes problemas en materia de violencia de género digital:

- Desconocimiento sobre este **tipo de violencia, su forma de manifestación y cómo reaccionar ante ella.**
- Desconocimiento **de cómo protegerse** ante este tipo de violencia.
- Desconocimiento de **pautas de prevención** en el uso de los terminales digitales.
- Desconocimiento de la **legislación y sus derechos** en materia de violencia digital.

Objetivos del protocolo

Objetivo General

Establecer una serie de pautas y actuaciones a realizar por cada uno de los profesionales que realizan una atención directa con víctimas de violencia de género digital, para lograr así una correcta intervención y evitar que este tipo de delito quede impune por no realizar correctamente una serie de procesos desde una primera fase de detección.

Objetivos Específicos

1. Proveer de conocimientos y herramientas respecto a la Violencia de Género Digital y Evidencias Digitales a todo aquel profesional que da atención directa a víctimas de violencia de género digital
2. Garantizar que todo profesional dedicado a la atención e intervención de víctimas de violencia de género en el Gobierno de la Rioja cuentan con la formación necesaria para poder intervenir en este tipo de situaciones.
3. Garantizar que los y las profesionales puedan dar una atención integral según las necesidades de cada víctima en el ámbito digital.
4. Proveer de los conocimientos correspondientes para que los y las profesionales puedan realizar una evaluación previa para detectar un posible caso de violencia de género digital
5. Garantizar que la intervención, evaluación, atención y seguimiento sea realizada conforme a la coordinación e implicación de todas las áreas involucradas.
6. Garantizar que los y las profesionales sean capaces de recopilar toda la información fundamental para la intervención en la primera fase del protocolo, identificando y documentando todas aquellas evidencias digitales que sirven de apoyo a la víctima en un proceso judicial.
7. Establecer unas guías de atención para garantizar que toda la información recogida relativa al caso de violencia de género digital, así como las evidencias digitales correspondientes estén expuestas de manera comprensible, así como a disposición de la víctima.

Marco Normativo

NORMATIVA ESTATAL [1]

- Ley Orgánica 1/2004, de 28 de diciembre, Medidas de Protección Integral contra la Violencia de Género
- Ley Orgánica 3/2007, de 22 de marzo, para la igualdad efectiva de mujeres y hombres
- Código de Violencia de Género y Doméstica
- Código de Extranjería
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los derechos digitales.

NORMATIVA EUROPEA

- Carta de los Derechos Fundamentales de la Unión Europea (2000)
- Web de EU JUSTICE- Legislación de la Unión Europea sobre Violencia de Género
- Convenio del Consejo de Europa para prevenir y combatir la violencia contra la mujer y la violencia doméstica de 2011 (Convenio de Estambul)
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la Protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

NORMATIVA INTERNACIONAL

- Declaración universal de los Derechos Humanos
- Convención sobre la eliminación de todas las formas de discriminación contra las mujeres (CEDAW)
- Declaración de Naciones Unidas sobre la eliminación de la violencia sobre la mujer (1993)
- Declaración y Plataforma de Acción de la IV Conferencia Internacional sobre la Mujer de Beijing (1995)
- Manual de Naciones Unidas sobre Legislación en materia de Violencia contra la Mujer (2012)

[1] Fuente: Normativa Violencia de Género: https://violenciagenero.igualdad.gob.es/marcoNormativo/home.htm

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.”

Principios que deben regular la aplicación del protocolo

Innovación

Debemos de tener en cuenta que las nuevas tecnologías están en constante actualización, en un corto periodo de tiempo podemos encontrarnos con nuevas redes sociales, actualizaciones de software, nuevos dispositivos, etc. Por lo que en la fase de detección de este protocolo de intervención debemos de ser conscientes que debemos estar en continua formación e innovando nuestras herramientas y procesos de extracción y captura de evidencias digitales. Debemos de ser capaces de adaptarnos a los cambios tecnológicos.

Complementariedad

Este protocolo es de aplicación a los recursos públicos prestados por el Gobierno de la Rioja a la atención de víctimas de violencia de género digital, por consiguiente, es complementario a normas, protocolos y procedimientos de estos recursos.

Cada una de las fases de este protocolo de intervención se complementa con la anterior, por lo que debe de ser aplicado paso a paso para una correcta intervención con la víctima de violencia digital.

Ámbito de aplicación

El presente Protocolo de actuación para la detección e intervención con víctimas de violencia de género digital se aplica recursos públicos del Gobierno de la Rioja:

- Centro Asesor de la Mujer
- Oficina de Asistencia a las Víctimas del Delito

Concepto y términos claves

Violencia de Género Digital es aquella agresión psicológica que realiza una persona través de las nuevas tecnologías, contra su pareja o ex pareja de forma sostenida y repetida en el tiempo, con la única finalidad de discriminación, dominación e intromisión sin consentimiento a la privacidad de la víctima.

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.

Perito Informático: es una persona especializada en la informática y en las nuevas tecnologías capaz de extraer, analizar y presentar mediante un informe pericial la información de una evidencia digital con todas las garanticas jurídicas.

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.

Grooming: es un tipo de ciberacoso realizado por un adulto hacía un menor con un objetivo de índole sexual

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

Virus Informático: software que tiene por objetivo alterar el funcionamiento de cualquier tipo de dispositivo digital, sin el consentimiento o el conocimiento del usuario.

Marco Teórico

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.

Definimos 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 o violencia de género digital" 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 ciberagresor 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 de género 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 aceptaba que no era consciente que estaba 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. Ellas mismas 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 esta 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 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).

Grooming

El grooming al contrario del Ciberbullying es un tipo de ciberacoso realizado por un adulto hacía un menor con un objetivo de índole sexual.

Si ya de por sí, el Ciberbullying es una modalidad de ciberacoso que conlleva un peligro en los menores de edad, las personas involucradas son menores de edad. En Cambio, cuando hablamos de Grooming el acosador es un adulto y existe una intención sexual para con el menor.

En un caso de Grooming se pueden identificar distintas fases:

1. Una primera fase llamada “Fase de Amistad”. La primera toma de contacto entre el ciberacosador y el menor de edad para conocer sus gustos, preferencias, pero sobre todo crear un vínculo de amistad con el objetivo de ganarse la confianza del menor.
2. Pasamos a una Fase de Relación: En esta fase el atacante se ha ganado la confianza del menor, y profundiza en detalles de su vida personal.
3. Fase Sexual: El atacante empieza a tener conversaciones de carácter sexual con el menor, y sobre todo peticiones de participación en prácticas sexuales, grabación de imágenes y videos o toma de fotografías de índole sexual.

El grooming puede ser considerado como un delito dentro de los denominados exhibicionismo, difusión y corrupción de menores, regulado expresamente en los artículos 185, 186 y 189 del Código Penal.

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.

<u>Principios para el tratamiento de evidencias digitales.</u>

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.

El Concepto de Cadena de Custodia

El término Cadena de Custodia, es un concepto ligado al ámbito legal y judicial, no solamente en el entorno de peritaje informático, ya que concierne al proceso de recopilación, extracción y análisis de cualquier tipo de evidencias.

La Cadena de Custodia establece un procedimiento, que asegura que los elementos probatorios en este caso evidencia digitales, no han sufrido ninguna alteración, modificación o bien, manipulación desde el momento de su recopilación, extracción, análisis y custodia. Se debe de cuidar la cadena de custodia hasta el momento en que se presenta el informe pericial como prueba ante un Tribunal en un proceso judicial.

Consiste en el protocolo de actuación relativo a la seguridad y manipulación que ha de seguirse durante el período de vida de una prueba digital, desde que ésta se recopila, extrae y analiza, hasta que se destruye o deja de ser necesaria.

La Cadena de Custodia controla dónde y cómo se ha obtenido dicha prueba, quien ha realizado la extracción, como y cuando se ha hecho, quien ha entregado y quien ha tenido acceso a la misma, donde se encuentra custodiada y en el caso de las evidencias

digitales comprueba que el clonado de una evidencia digital se ha realizado correctamente y que la evidencia clonada es igual a la evidencia original.

Es importante cuidar la cadena de custodia y ser absolutamente rigurosos, de manera que no pueda dudarse en ningún momento sobre la validez e integridad de la prueba digital.

La cadena de custodia debe realizarse siempre ante un fedatario público, como lo es un Notario. Mediante el acta notarial, el notario da fe de que se ha respetado los principios de la recolección, extracción y análisis de cualquier tipo de evidencias.

Hay que destacar que la evidencia digital tiene ciertas particularidades con respecto a otro tipo de evidencias, y es que la información alojada en ellas la podemos encontrar de diferentes maneras:

1. Almacenada estáticamente. Es decir, la información se encuentra almacenada de manera estática en un dispositivo (móvil, disco duro, etc.) y solo hace falta recuperarla en caso de haber sido borrada o bien podemos utilizarla en caso de estar disponible.
2. Almacenada dinámicamente. Es decir, la información se encontrará disponible de forma temporal en un dispositivo y se perderá en el momento que se apague el dispositivo.
3. En desplazamiento. Tipo de información que se encuentra en la red como paquete de información y puede ser “capturado”.

Para preservar la información contenida en una evidencia digital de manera que a posteriori pueda volver a ser analizada por un perito, se realiza un clonado de la evidencia original. Garantizamos mediante el HASH su validez legal en un procedimiento judicial.

El hash consiste en un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida

tendrá siempre la misma longitud, es decir siempre será de 40 caracteres de longitud. Cada documento, imagen, video, mensaje, disco duro, etc. Tiene un número de hash propio y único. Nunca dos archivos diferentes coincidirán con el mismo hash.

La función del hash en nuestra investigación es comprobar la integridad de la evidencia digital, es decir, como no debemos trabajar sobre la evidencia original realizamos un clonado de esta. El original tiene un hash propio único, que si el clonado esta realizado correctamente, el hash del original y el clonado deberá de coincidir. De esta forma argumentamos que analizando el clonado es como si estuviéramos trabajando en la evidencia original.

Comprobando el hash del original y clonado nos aseguramos que la evidencia no ha sufrido ningún tipo de alteración o manipulación durante el proceso de la extracción. Si los dos hash son idénticos, significa que no ha habido ninguna alteración.

Con el clonado de la evidencia, el original estará siempre protegido de terceros, en un lugar seguro, y libre de posibles manipulaciones o destrucciones. Para en caso de ser necesario pueda volver a analizarse.

Una de las grandes ventajas de las evidencias digitales es que nos permiten trabajar con copias idénticas de la prueba original, evitando así que contaminemos / manipulemos la evidencia.

Si en el momento que estamos realizando el análisis, por alguna razón contaminamos o dañamos la evidencia clonada, podremos volver a realizarse un clonado del original, permitiendo así realizar el análisis nuevamente desde cero de la misma evidencia digital.

Cuando nos encontramos con una evidencia digital en un caso de Violencia Digital, tenemos que ser prudentes a la hora de realizar el análisis, en este sentido debemos de examinar cada elemento con mucho cuidado, ya que una mala praxis en el análisis puede general que manipulemos la prueba y la información no pueda ser recuperada. Se debe de tener en consideración :

1. Podemos encontrarnos con una evidencia digital que desaparece con el tiempo, como resultado del uso constante del dispositivo o modificaciones realizadas por el usuario
2. Cualquier error en el proceso de extracción y análisis puede destruir la información, por lo que debemos de tener cuidado de aplicar bien los procedimientos.
3. No debemos buscar información que no estamos autorizados a buscar. Es decir debemos centrar nuestro análisis en la evidencia que el cliente necesita recuperar y acreditar.

Cuando nos encontramos con una evidencia digital volátil, debemos actuar rápidamente ya que puede desaparecer o encontrarse en el dispositivo de manera temporal. Este tipo de evidencias deben ser recogidas antes de que el dispositivo sea apagado o bien desconectado de la red.

Consideraciones a tomar en cuenta en la extracción de una evidencia:

1. No debemos apagar el dispositivo hasta que haya finalizado todos los procesos de recolección y extracción. Si no esperamos que termine el proceso puede dar lugar a perdida de información o bien alterar o destruir la evidencia.
2. No debemos utilizar programas o aplicaciones para el análisis de dudosa procedencia.
3. Ejecutar de forma correcta de programas de informática forense en los dispositivos a analizar
4. No debemos instalar ningún programa o aplicación en el ordenador donde se encuentra almacenada la evidencia

¿Cómo acreditar una evidencia digital para ser admitida en un proceso judicial?

Las evidencias digitales se rigen por los principios generales para cualquier documento privado como medio de prueba según el art. 325 LEC, aunque existen ciertas especificaciones que cualquier Perito Informático deberá de tener en cuenta al tratar con evidencias digitales.

El artículo 325 de la LEC remite al artículo 268 para conocer la forma de presentación de los documentos privados, y el criterio general es **el de la presentación original o mediante copia autenticada por fedatario público, bastando copia simple del documento privado, siempre que no sea cuestionada por las demás partes**. Es decir, podemos presentar un pantallazo o captura de pantalla autenticado por un fedatario público, siempre que la otra parte no cuestione su autenticidad, en caso contrario, será necesario presentar un informe pericial donde se haga constar la veracidad de dicha prueba. (Art. 326 LEC).

Artículo 268 Forma de presentación de los documentos privados

***1.** Los documentos privados que hayan de aportarse se presentarán en original o mediante copia autenticada por el fedatario público competente y se unirán a los autos o se dejará testimonio de ellos, con devolución de los originales o copias fehacientes presentadas, si así lo solicitan los interesados. Estos documentos podrán ser también presentados mediante imágenes digitalizadas, incorporadas a anexos firmados electrónicamente.*

***2.** Si la parte sólo posee copia simple del documento privado, podrá presentar ésta, ya sea en soporte papel o mediante imagen digitalizada en la forma descrita en el apartado anterior, que surtirá los mismos efectos que el original, siempre que la conformidad de aquélla con éste no sea cuestionada por cualquiera de las demás partes.*

***3.** En el caso de que el original del documento privado se encuentre en un expediente, protocolo, archivo o registro público, se presentará copia auténtica o se designará el archivo, protocolo o registro, según lo dispuesto en el apartado 2 del artículo 265.*

Artículo 326 Fuerza probatoria de los documentos privados

***1.** Los documentos privados harán prueba plena en el proceso, en los términos del artículo 319, cuando su autenticidad no sea impugnada por la parte a quien perjudiquen.*

2. *Cuando se impugnare la autenticidad de un documento privado, el que lo haya presentado podrá pedir el cotejo pericial de letras o proponer cualquier otro medio de prueba que resulte útil y pertinente al efecto.*

Si del cotejo o de otro medio de prueba se desprendiere la autenticidad del documento, se procederá conforme a lo previsto en el apartado tercero del artículo 320. Cuando no se pudiere deducir su autenticidad o no se hubiere propuesto prueba alguna, el tribunal lo valorará conforme a las reglas de la sana crítica.

3. *Cuando la parte a quien interese la eficacia de un documento electrónico lo pida o se impugne su autenticidad, se procederá con arreglo a lo establecido en el artículo 3 de la Ley de Firma Electrónica.*

Es posible según el artículo 382 LEC, la aportación al proceso como medio de prueba de cualquier instrumento de filmación, grabación y semejantes, refiriéndose a la reproducción de la palabra, el sonido y la imagen y de los instrumentos que permiten archivar y conocer datos relevantes para el proceso.

Artículo 382 Instrumentos de filmación, grabación y semejantes. Valor probatorio

1. *Las partes podrán proponer como medio de prueba la reproducción ante el tribunal de palabras, imágenes y sonidos captados mediante instrumentos de filmación, grabación y otros semejantes. Al proponer esta prueba, la parte podrá acompañar en su caso, transcripción escrita de las palabras contenidas en el soporte de que se trate y que resulten relevantes para el caso.*

2. *La parte que proponga este medio de prueba podrá aportar los dictámenes y medios de prueba instrumentales que considere convenientes. También las otras partes podrán aportar dictámenes y medios de prueba cuando cuestionen la autenticidad y exactitud de lo reproducido.*

3. *El tribunal valorará las reproducciones a que se refiere el apartado 1 de este artículo según las reglas de la sana crítica.*

Cuando nos encontramos que la prueba es un correo electrónico o cualquier otra vía de comunicación como puede ser un mensaje de whatsapp, no debemos olvidar que la otra parte puede valerse para impugnar dicha evidencia, alegando una manipulación o mal presentación; ya que puede indicar la facilidad que existe hoy en día de realizar un "pantallazo" y modificarlo para dar fe de una supuesta comunicación no realizada; o bien siempre puede alegar que se esta violando el derecho de la intimidad o comunicaciones de su cliente.

Ante este tipo de alegaciones la jurisprudencia actual indica que una vez enviado el correo electrónico, ya no le pertenece su contenido a su emisor, por tanto, una vez finalizada la comunicación en sí misma, no hay secreto de comunicaciones, lo que no indica que no se puede vulnerar el derecho a la intimidad. En cualquier caso, y dejando a criterio de la sana crítica de los letrados, la existencia de un acto de comunicación permite a cualquier de los involucrados la aportación de una prueba que acredite dicha comunicación en un procedimiento judicial.

Existen unos requisitos mínimos exigidos por el Poder Judicial para admitir una evidencia digital como prueba en un proceso judicial. Estos son:

1. La evidencia digital debe ser lítica. Es decir el proceso de obtención de la evidencia no debe ni puede vulnerar el derecho de la intimidad de la persona involucrada ni su derecho de el secreto de las comunicaciones.
2. La integridad de la evidencia. Se debe de garantizar la integridad de la evidencia obtenida. Debemos de realizar la extracción de la evidencia haciendo un clonado del original calculando el valor HASH tanto del original como de la copia. Documentarlo correctamente bajo el protocolo de la cadena de custodia mediante un fedatario público.
3. Garantizar la autenticidad de la evidencia. Debemos de garantizar que la evidencia analizada es identifica a la original. Garantizando que la evidencia no ha sido manipulada ni alterada durante el proceso de recopilación y extracción.
4. Debemos de realizar el análisis de forma clara, que pueda ser comprendido por cualquier persona que no conozca los tecnicismos.

Uno de los principales problemas que nos encontramos al utilizar este tipo de pruebas en un caso de violencia digital, es la facilidad con la que pueden ser manipuladas por terceras personas, por lo que siempre resaltamos la importancia de demostrar en un proceso judicial el uso correcto de la cadena de custodia, para garantizar la integridad y la autenticidad de la prueba digital.

Es común encontrar que la evidencia digital se encuentre en discos duros, memorias USB, móviles (aplicaciones, conversaciones de whatsapp, imágenes, videos, etc.), tablets, en la nube (dropbox, google drive, etc.) o bien ser correos electrónicos o publicaciones en redes sociales.

Una vez hemos identificado donde se encuentra la evidencia, debemos de tener claro cual es la forma más adecuada para adquirirla. Esta primer fase es la más importante, ya que es el primer punto de contacto con la evidencia, y es donde existen mas probabilidades de modificarla o dañarla.

Si por error, modificamos o dañamos la prueba, perdería cualquier valor probatorio en un proceso judicial, y quedaría impugnada. La otra parte podría alegar que hemos modificado la evidencia a conveniencia de nuestro cliente.

Además de una correcta adquisición, no debemos olvidar los requerimientos legales para no vulnerar derechos de terceros que puedan estar afectados.

En una investigación el Perito Informático puede encontrarse con diferentes tipos de evidencia digitales, siendo los más comunes:

- Correos electrónicos,
- Capturas de Pantalla o Pantallazos
- SMS
- Conversaciones de WhatsApp
- Memorias USB
- Documentos PDF

- Páginas Web

WhatsApp, como evidencia digital

WhatsApp, una aplicación de mensajería instantánea que permite enviar mensajes y contenido multimedia a tus contactos a través de una sencilla aplicación de tu móvil se ha convertido en uno de los principales medios de comunicación, dejando atrás al SMS e incluso por encima de las llamadas telefónicas.

Ahora bien, así como es un medio que facilita la comunicación entre dos o más personas, también puede ser utilizado para amenazar, insultar, coaccionar a otra persona.

¿Como se puede aportar a un proceso judicial una conversación de whatsapp?

La primera solución sería, presentar capturas de pantalla de las conversaciones realizadas por WhatsApp, solicitar al letrado que levante acta sobre su contenido, dando fe pública del mismo a través de una trascripción de los mensajes recibidos y enviados, y de que corresponde con el smartphone y el número de teléfono de una de las partes, etc.

Otro modo sería a través de un acta notarial. Ante un notario presentamos la conversación de whatsapp, así el notario da fe de su existencia y de su contenido. Y adjuntamos el acta notarial al proceso.

Ahora bien, eso esta muy bien si al presentar la prueba al proceso, la otra parte no presenta queja alguna y acepta la veracidad de esa conversación. ¿Pero que sucede cuando niega haber establecido esa conversación o enviado ese mensaje? ¿Y si indica que esa conversación o pantallazo ha sido manipulada? O peor aún que ha obtenido dicha prueba de forma ilícita y vulnerando sus derechos fundamentales.

Como mencionamos antes la impugnación de una prueba documental (conversaciones de whatsapp) se rige por tres aspectos:

1. La Autenticidad. Que el autor de dicha conversación corresponda con su “autor real”

2. La integridad. Que corresponda el contenido de la prueba con el original
3. Licitud. Que en el proceso de obtención de dicha prueba documental no se vulnere ningún derecho fundamental.

Estos tres aspectos son muy importantes a tomar en cuenta, ya que si el Juez percibe una posibilidad de que la prueba documental presentada pudo haber sido alterada, manipulada o modificada; o bien se ha vulnerado algún derecho fundamental para obtenerla, denegará dicha prueba. Aparte que la parte perjudicada por dicha prueba, la impugnaría.

Es importante mencionar que la captura de una conversación de whatsapp que tiene lugar entre dos o más personas, y que uno de los involucrados desea conservar dicha conversación, como prueba fidedigna de la conversación mantenida, no supone una invasión de la intimidad.

Por otro lado, la prueba de mensaje de whatsapp deberá respetar el derecho fundamental del secreto de las comunicaciones. Por lo que, cualquiera interferencia o intervención de la comunicación de cualquier persona, convertirá dicha prueba en ilícita. Es decir, no debemos nunca ingresar de forma ilícita a un dispositivo móvil de un tercero en búsqueda de una evidencia.

Si consideramos que dicha conversación de whatsapp, es verdadera y es fundamental presentarla para corroborar una hecho delictivo, la mejor forma de presentarla para evitar impugnaciones o que sea denegada por el Juez, es mediante un **informe pericial de un perito informático.**

En dicho informe pericial, el perito informático acreditará todo el proceso de recopilación, extracción y análisis de la evidencia, así como da fe del contenido de la misma. En ningún momento el perito deberá de favorecer a una de las partes, recordemos que la figura del perito es imparcial y deberá de presentar su informe con la información obtenida sin dar su opinión solamente exponer los hechos que muestran la evidencia.

Ahora bien, antes de analizar cualquier dispositivo móvil, no debemos olvidar que solamente los propietarios del terminal móvil o bien los que dispongan de autorización podrán solicitar un informe pericial para el análisis de una evidencia digital. El análisis, extracción y adquisición de evidencias de un terminal de propiedad de un tercero, es un acto ilícito.

Destacamos la Sentencia del Tribunal Supremo nº 300/2015 de 19 de mayo que dice que *"la prueba de una comunicación bidireccional mediante cualquiera de los múltiples sistemas de mensajería instantánea debe ser abordada con todas las cautelas. La posibilidad de una manipulación de los archivos digitales mediante los que se materializa ese intercambio de ideas, forma parte de la realidad de las cosas"*.

Protocolo de Actuación

Este protocolo busca dictar unas pautas para la intervención correcta de mujeres víctimas de violencia de género digital, debemos señalar que se debe de tener presente en todo momento la necesidad manifestada por la mujer antes, durante y después de la intervención.

La actuación en cada una de las áreas de intervención estará a cargo de profesionales previamente especializados y formados en intervención ante casos de violencia de género digital por el Gobierno de la Rioja.

Este tipo de intervenciones serán multidisciplinar abarcando conocimientos de áreas sociales, psicológicas, jurídicas y técnicas según las necesidades de cada mujer.

Pautas Comunes entre las áreas de intervención

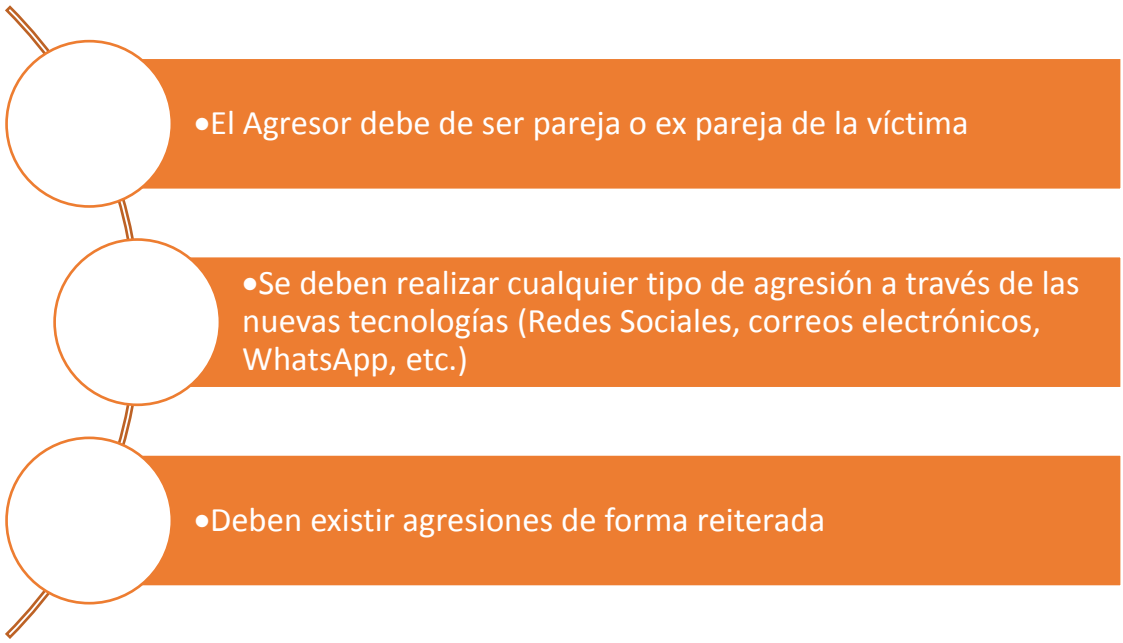
- En todo momento la atención con la víctima debe de ser de una manera cordial, haciéndola sentir en todo momento comprendida, apoyada y a salvo.
- El profesional responsable deberá de presentarse a la mujer e indicar el servicio del Gobierno de la Rioja que prestará
- Se debe de interactuar en todo momento en un lenguaje comprensivo acorde al nivel socio - cultural y edad de la víctima
- Con las mujeres menores de edad, al ser nativas digitales, se usará el propio lenguaje de las nuevas tecnologías, redes sociales e internet. Es por eso por lo que en este protocolo se cuenta con un glosario de términos claves.
- En ningún momento se debe de culpabilizar a la mujer o hacerle ver que por culpa de su desconocimiento digital esta sufriendo un caso de violencia de género digital. Ni mostrar mensajes de rechazo o sorpresa.
- Se debe de potenciar mensajes de cercanía y empatía.
- En ningún momento se debe de dudar de la mujer sobre si está siendo realmente ciberacosada

- Si la mujer muestra una crisis de ansiedad, miedo o vergüenza se debe de intentar calmarla y hacerle ver que no tiene porque avergonzarse, que se está aquí para ayudarle.
- La intervención puede llevarse a cabo mediante una comunicación personal, por teléfono o bien por escrito
- Todas las intervenciones se deberán de documentar conforme a las pautas establecidas por los recursos del Gobierno de la Rioja.

Generalidades

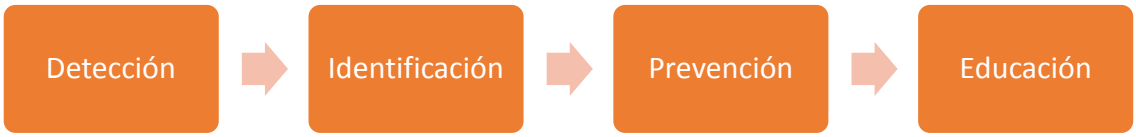
La Violencia de Género Digital es entendida como aquella agresión psicológica que realiza una persona través de las nuevas tecnologías como el correo electrónico, sistemas de mensajería como WhatsApp o redes sociales, contra su pareja o ex pareja de forma sostenida y repetida en el tiempo, con la única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

No debemos olvidar las características que se deben cumplir para determinar si es un caso de violencia de género digital o no:



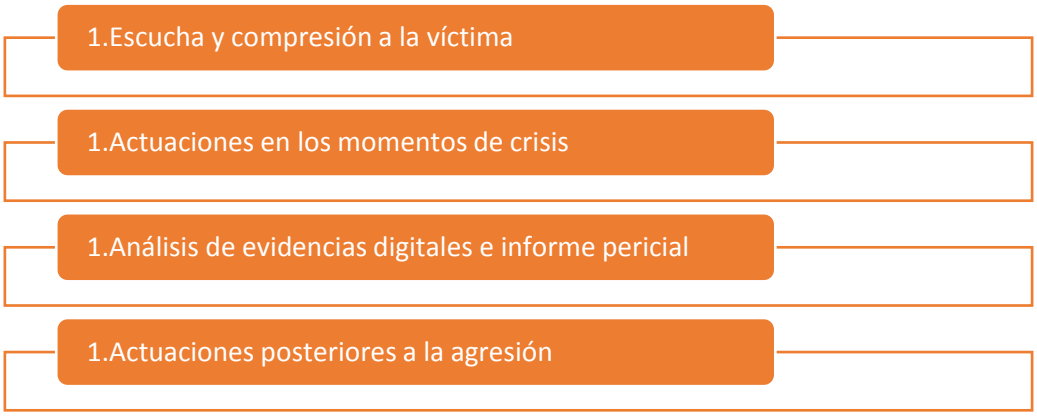
La Asociación Stop Violencia de Género Digital mediante su Protocolo de Actuación de víctimas de Violencia de Género Digital (Protocolo DIPE, Detección, Identificación, Prevención y Educación) marca una serie de pautas a seguir para una intervención óptima a víctimas de violencia de género digital.

Los 4 pilares fundamentales de este protocolo son:

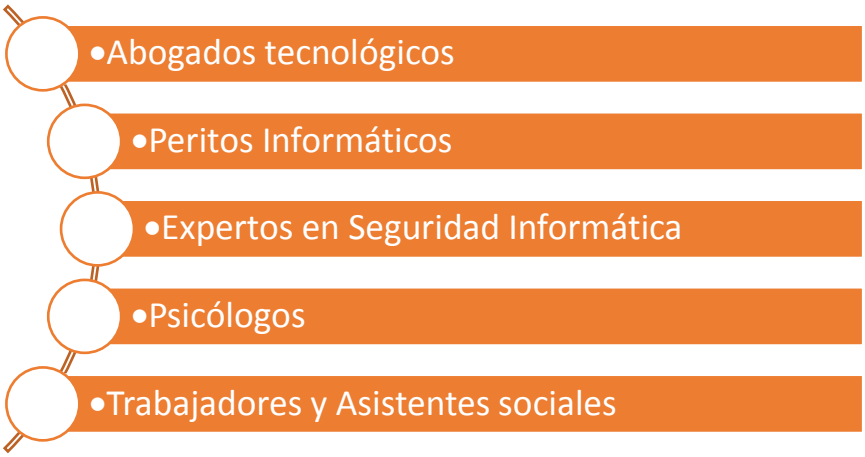


- Detectar el tipo de violencia digital que está sufriendo la víctima, así como los canales por donde está sufriendo las agresiones
- Identificar y analizar las evidencias digitales, como herramienta de prueba ante una denuncia de violencia de género digital
- Proveer de herramientas de prevención a la víctima para evitar futuros ataques
- Educar y concientizar la víctima de un uso correcto y seguro de las nuevas tecnologías

El protocolo se sustenta en los siguientes aspectos:



Para ello, se necesita una comisión de trabajo que este formada por distintos profesionales:



FASE 1: Detección

Cuando una mujer está siendo víctima de violencia de género digital buscará ayuda e información ya que lastimosamente en muchos casos la víctima desconoce por que medios o dispositivos está siendo ciber acosada, puede incluso en pensar que se está volviendo loca por que desconoce los métodos que utiliza un ciberacosador para cumplir su objetivo.

Una vez la víctima se ha animado a buscar ayuda y contacta con nosotros, no olvidemos que debemos hacerla sentir **comprendida, apoyada, y sobre todo que no está sola y que juntos superaremos su problema.**

Podemos encontrarnos con dos vertientes fundamentalmente:

- **Las mujeres que buscan ayuda y asesoría porque están siendo víctimas de violencia de género digital pero no tienen pensando denunciar**
- **Y aquellas mujeres que saben que están siendo víctimas de violencia de género digital y quieren denunciar.**

El Gobierno de la Rioja cuenta con dos recursos, el **Centro Asesor de la Mujer**, y la **Oficina de Asistencia a las Víctimas del Delito**.

Área Social

El área social será la encargada del primer contacto con la víctima y dará la información inicial, así como toda aquella información que se considere relevante para la víctima.

Será la encargada de escuchar por primera vez a la mujer, de identificar el tipo de violencia de género digital que está sufriendo, así como los canales por lo que está siendo agredida.

Será el área encargada de:

- Establecer el primer contacto con la víctima
- Identificar el tipo de violencia de género digital
- Los canales por los que se está realizando la agresión
- Identificar la necesidad de apoyo psicológico en caso de ser necesario
- Tomar nota del relato y el estado de la víctima. Por ejemplo: Si está bloqueada, siente vergüenza, etc.
- La derivación correspondiente en base a la información ofrecida por la mujer
- Realizar un primer diagnostico y evaluación, teniendo en cuenta las necesidades de cada situación. Por ejemplo: Si cuenta o no con evidencias digitales, si necesita apoyo jurídico o psicológico, etc.
- Apertura del expediente en el registro del recurso del Gobierno de la Rioja
- Indicar unas pautas básicas de seguridad informática
- Analizar junto con la mujer la documentación y evidencias digitales que debe de ir recopilando y guardando en un lugar seguro para su análisis posterior por el profesional correspondiente.
- Incorporar en el expediente de la víctima, las situaciones de violencia de género digital que la mujer ha manifestado verbalmente, documentalmente o por alguna otra vía
- En cada intervención con la víctima se debe dar información sobre herramientas para la detección de violencia de género digital

- Indicarle a la víctima la forma segura de salvaguardar una evidencia digital

Esta primera fase conlleva la primera toma de contacto y entrada de la mujer al protocolo de intervención, es seguramente el paso más importante ya que es primordial que la mujer se sienta comprendida, apoyada y sobre todo NO JUZGADA, si logramos transmitirle correctamente que no está sola, ella tendrá la confianza para poder seguir adelante.

Todos los hechos e información proporcionada por la mujer deben de quedar registrado en el expediente correspondiente a la víctima. **Se debe de describir lo más detalladamente posible el caso de violencia de género digital**, si se han difundidos contenido sexual de la víctima, calumnias por redes sociales, ciberacosos o suplantaciones de identidad, etc.

En esta primera fase de detección la empatía es muy importante, sobre todo en la toma del primer contacto ya que poniéndonos en el lugar de la víctima nos hará comprender mejor por lo que está pasando y como poderle ayudar a superarlo.

Es importante saber que se debe escuchar a la víctima atentamente, **sin juzgarla.**

Una vez hemos escuchado su caso, procedemos a detectar:

- El tipo de violencia digital
- Historial de agresiones por medios digitales
- Canales por los que se realiza dichas agresiones
- Las Evidencias Digitales*

* Las evidencias que son imprescindibles analizar y que serán de utilidad para aportar a un juzgado junto a la denuncia.

Ahora bien, no todas las personas que nos contacten estarán siendo víctimas de violencia de género digital, recordemos que para catalogarlo como tal se deben cumplir:

- **El Agresor debe de ser pareja o ex pareja de la víctima**
- **Se deben realizar cualquier tipo de agresión a través de las nuevas tecnologías (Redes Sociales, correos electrónicos, WhatsApp, etc.)**
- **Deben existir agresiones de forma reiterada**

¿Cómo reconocemos que está sufriendo una violencia digital?

Hay distintas pautas, además de las anteriores *(que son imprescindibles)* que debemos de tomar en cuenta para catalogarla como víctima de violencia de género digital.

Desde el punto de vista del agresor

- Ignora los sentimientos de la víctima
- Busca ridiculizar, insultar e humillar a la víctima por medios digitales
- Tiene un control sobre los dispositivos digitales de la víctima
- No permite a la mujer tener libertad para el uso de las redes sociales
- Controla las comunicaciones de la víctima, con quien habla, sus amigos de redes sociales, con quien se escribe un correo electrónico
- Realiza amenazas por mensajería instantánea como WhatsApp
- Acosa a la víctima con excesivas llamadas telefónicas
- Castiga a la víctima privándola del uso de sus terminales

Desde el punto de vista de la víctima

- Padece ansiedad, confusión, depresión, sentimiento de culpa, etc.
- Considera alejarse de las nuevas tecnologías como solución a su problema
- Baja autoestima
- Reputación perjudicada por publicaciones en redes sociales e internet
- Han podido distribuir contenido sexual sin su consentimiento

- Ha recibido mensajes, correos electrónicos amenazantes y hostigadores con cierta regularidad
- Tiende a tener miedo de utilizar las nuevas tecnologías
- No puedes realizar ninguna acción (agregar amigos, comentar, subir fotos, etc.) en alguna red social sin consultarle a su pareja

El siguiente cuadro os ayudará a identificar el caso según el tipo de violencia digital que está sufriendo:

La víctima ha sufrido…	Ciberacoso	Sextorsión	Suplantación de Identidad	Ciberbullying	Grooming
Amenazas, humillaciones, etc. a través de medios digitales	X			X	
Difusión y/o publicación de contenido sexual sin su consentimiento		X			X
Acoso psicológico, busca hacerla sentir responsable	X			X	
Acoso sexual por un adulto, siendo la víctima menor					X
Existe un perfil con sus datos, fotografías, etc.; creado sin su consentimiento			X		
Recibe email difamatorios	X			X	
Tiene instalado software espía en algún dispositivo móvil	X				
Invade la vida privada de la víctima sin consentimiento	X				
Robo de contenido sexual en sus dispositivos informáticos		X			X
Se produce durante el período escolar				X	
El agresor conoce las contraseñas de sus correos electrónicos, redes sociales, etc.	X		X		
Distribución de contenido de carácter vejatorio para perjudicar	X			X	

la reputación de la víctima			
Creación de perfiles falsos en redes sociales para controlar a la víctima	X		
Perseguir, controlar e intimidar por medios digitales	X	X	X

Una vez se detecta el tipo de violencia digital que está sufriendo la víctima, debemos de identificar los canales por donde está sufriendo el acoso, estos pueden ser:

- Dispositivos móviles
- Ordenadores sobremesa y/o portátiles
- Redes Sociales
- Correos electrónicos
- Sitios Web

Dependerá del tipo de violencia digital con el que nos encontremos, pero algunas evidencias digitales que podremos analizar según el canal son:

- Documentos y contenido multimedia (imágenes y videos)
- Conversaciones de WhatsApp
- Correos electrónicos
- Publicaciones en Redes Sociales
- Mensajes Privados en Redes Sociales
- Perfiles Sociales
- Publicación en Páginas Web
- Programas y aplicaciones de ordenadores y móviles
- Registro de llamadas en dispositivos móviles
- SMS en móviles
- Registros de accesos a un ordenador

En esta primera fase del protocolo, es de vital importancia que cuando una mujer busca ayuda para superar, terminar y como denunciar un caso de violencia de género

digital se le brinde de toda la información necesaria que por desconocimiento desconoce de sus derechos, formas de protegerse y sobretodo de comprobar que está siendo víctima de un caso de violencia de género digital.

La persona según el organismo donde la víctima acuda procederá a abrir el expediente, anotando cada uno de los aspectos que ayude a tipificar el tipo de violencia digital a la que está siendo sometida la víctima, tomando en cuenta los canales digitales por donde se realiza el acoso, así como toda información que la víctima aporte y la persona considera importante adjuntarla al expediente.

En esta primera fase, debemos de indicarle a la víctima que cualquier tipo de violencia de género digital o ciberacoso es considerado un delito y está tipificado en el código penal. Se le debe en todo momento incentivar a denunciar, ya que es primordial contar con una denuncia para poder continuar el proceso judicial.

Se analizará dicha documentación, y en el caso que la víctima decida denunciar se trasladará dicha información al área jurídica que será la encargada de guiarla durante la denuncia y el análisis de evidencias digitales.

A la víctima se le deberá de informar sobre:

- Los derechos con los que cuenta ante este tipo de casos
- La forma de salvaguardar toda aquella evidencia digital que aloje las pruebas oportunas para demostrar la violencia digital
- Medidas básicas de seguridad para evitar que siga siendo sometida ante este tipo de violencia

Se deberá de informar que en ningún caso la víctima deberá de:

- Eliminar conversaciones de WhatsApp
- Eliminar fotografías, videos o archivos de audio
- Formatear ordenador, portátil o móvil
- Desinstalar aplicaciones móviles
- Cambiar de dispositivo móvil sin hacer antes una copia de seguridad

- Borrar correos electrónicos

Se les proporcionará a las personas que tienen el primer contacto con la víctima toda aquella documentación que le será de ayuda para detectar el tipo de violencia digital que está sufriendo la víctima, así como los canales por donde está sufriendo las agresiones y el tratamiento adecuado para las evidencias digitales para evitar su impugnación en sede judicial.

Consejos básicos de Seguridad Informática que debemos de informar a la víctima

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
7. No debemos subir contenido a las redes sociales que puedan ayudar a localizarnos
8. Desactivar la webcam en sobremesas y portátiles, o al menos tener tapada con algun protector
9. Desactivar el GPS en nuestro móvil
10. Debemos cambiar periódicamente nuestras contraseñas de correos electrónicos, dispositivos y redes sociales
11. Es recomendable crear una cuenta de correo electrónico personal diferente para el contacto con abogados, psicólogos o cualquier profesional

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.

Consejos para preservar una evidencia digital

- Si nuestra prueba digital se encuentra en un dispositivo móvil es recomendable mejor no utilizarlo, ya que podríamos modificar o alterar la prueba sin darnos cuenta, causando su nulidad en un proceso judicial o bien dificultar su extracción
- Proteger el dispositivo en un lugar seguro fuera del alcance de terceros, para evitar su manipulación, borrado o alteración
- Si contamos con una tarjeta de memoria externa en nuestro dispositivo, es probable que la evidencia se almacene en ella. Por lo que tenemos que tener cuidado de que no la encuentren terceras personas que pueden borrar o alterar dicha prueba
- Si la prueba es una conversación de whatsapp, bajo ningún concepto debemos de borrar el chat o mensaje.
- Un ordenador sobremesa tiene un registro de acceso y evento que pueden ser una evidencia de que terceros han accedido a nuestro ordenador, bajo ningún concepto debemos de formatearlo o cambiar el disco duro o sistema si tenemos sospechas de que alguien tiene acceso a nuestro ordenador sin nuestro consentimiento
- En caso de que queramos grabar una conversación para ser utilizado como prueba documental en un proceso judicial, debemos de tener instalado en nuestro móvil alguna aplicación que realice esta acción. Recuerda que no deberás de perder el móvil ni borrar el registro de llamadas para que podar presentar dicho registro y la grabación en sede judicial.
- Si la prueba se encuentra en nuestro ordenador, se guardará en su disco duro. Si desconoce la forma de extraerlo para protegerlo, bajo ningún concepto

debemos de hacerlo nosotros mismos, sino que deberíamos llamar a un experto para que lo haga por nosotros.

- Realizar capturas de pantalla de cualquier evidencia digital
- La extracción, análisis y presentación de la evidencia digital en sede judicial deberá de estar a cargo de un perito informático o del organismo de la fuerza de seguridad pertinente, bajo ningún concepto presentamos una evidencia digital sin su respetivo informe por un profesional especializado.

Área Psicológica

En esta primera fase del protocolo en muchas ocasiones las psicólogas y los psicólogos tendrán un papel fundamental.

Una vez el área social considera que la víctima necesita ser atendida a nivel psicológico, procederá a contactar con un o una psicóloga para la correcta intervención.

Este profesional deberá de

- Escuchar el relato de la víctima, dejando constancia en su expediente las barreras que puede llegar a tener la víctima para socializar en su entorno digital, así como las dificultades que puede presentar para recordar los hechos sufridos.
- Deberá de indicar en el expediente toda aquella información relevante en cuanto al uso de las Tics se refiere, así como las situaciones de violencia de género digital
- En las entrevistas se profundizará sobre la situación de violencia de género digital.
- Se analizará el impacto en la reputación, vida social, familiar y/o laboral de la mujer el hecho de violencia de género digital sufrido

- Deberá de realizar una evaluación y diagnostico incluyendo lo expresado por la mujer y terceras personas.
    - Descripción de hechos documentados en referencia al caso de violencia de género digital
    - Consecuencias por la difusión del contenido en redes sociales
    - Los riesgos que pueden perjudicar psicológicamente a la mujer
    - Se analizarán necesidades específicas como recuperación de reputación social, etc.
    - Pronostico de la mujer en caso de que cese los hechos de violencia de género digital o en caso contrario los objetivos de la terapia, etc.
- Cuando la mujer sea menor de edad y necesite terapia o terapia en grupo se explicará en un lenguaje que pueda comprender sobre porque de la terapia, sus objetivos, en que consiste etc.
- Se concienciará a la mujer sobre el uso de pautas de ciberseguridad en redes sociales y en el uso de las TICS
- Se indicará estrategias terapéuticas para combatir los efectos de la crisis reputación a través de las TICS
- En caso de que la víctima tenga que afrontar un procedimiento jurídico, se hará hincapié en herramientas de fortalecimiento ante la posible exposición de la intimidad de la mujer en los procedimientos.

Consejos básicos de Seguridad Informática que debemos de informar a la víctima

- Nunca se debe de dar las contraseñas de nuestros dispositivos, redes sociales y correos electrónicos a nadie.
- Tener instalado un antivirus en nuestros dispositivos digitales
- No descargar archivos adjuntos de correos electrónicos desconocidos
- No debemos abrir archivos sospechosos en nuestras conversaciones de whatsapp o correos electrónicos

- Debemos de tener nuestros perfiles en redes sociales privados, de esta forma nos seguirán las personas que nosotros aceptemos
- Configurar la doble autentificación en las redes sociales, para evitar que terceras personas accedan sin nuestro consentimiento
- No debemos subir contenido a las redes sociales que puedan ayudar a localizarnos
- Desactivar la webcam en sobremesas y portátiles, o al menos tener tapada con algun protector
- Desactivar el GPS en nuestro móvil
- Debemos cambiar periódicamente nuestras contraseñas de correos electrónicos, dispositivos y redes sociales
- Es recomendable crear una cuenta de correo electrónico personal diferente para el contacto con abogados, psicólogos o cualquier profesional

Consejos para prevenir una sextorsión

- Evita hacerte fotografías de contenido sexual. Si no existen esas fotografías no te pueden extorsionar con ellas
- 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.
- 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.
- No cedas al chantaje. No accedas a las peticiones del chantajista, si aceptas le haces más fuerte y nunca parará de extorsionarte
- Elimina Malware. Asegúrate de que no tienes ningún software malicioso, aunque tu no compartas las fotografías o videos pueden espiarte el ordenador y conseguirlas.

- 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
- No confundas relaciones sentimentales, de amistad, etc. Identifica bien las relaciones sanas, basadas en la confianza y el respeto
- 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
- 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

- **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
- **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.
- **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.
- **Restringe el acceso a tus redes sociales.** Cambia tu privacidad en redes sociales. Haz tu perfil solo accesible a tus contactos.
- **Comprueba que tu conexión sea segura.** Cambiar la contraseña del router que trae por defecto, es una manera de asegurar tu conexión.
- **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

- **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.
- **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.
- **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
- **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.

Área Jurídica

El área jurídica deberá de:

- Recoger en el expediente de la mujer todos aquellos aspectos jurídicos respecto al caso de violencia de género digital que ella ha manifestado verbal o documentalmente

- Ofrecer asesoramiento jurídico en procedimientos derivados del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la Protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los derechos digitales, y de la Ley Orgánica 1/1982, de 5 de mayo, de protección

civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

- Recopilar toda aquella documentación, información y evidencias digitales a aportar en los posibles procedimientos judiciales en apoyo a la mujer
- Deberá de informar a la mujer la forma correcta de recopilar y custodiar una evidencia digital con garantías procesales.
- Se explicará la importancia de plasmar en la denuncia todos aquellos hechos de violencia de género digital que se ha sufrido, aunque el incidente se realizará de forma anónima, aunque deberá de explicarse los motivos de sospechar de una persona en concreta.
- Asesorar y elaborar medidas de protección a solicitar con especial atención a las relativas a las TIC.
- Indicarle nuevamente las pautas de seguridad informática y la forma de salvaguardar una evidencia digital.
- Asesorar y solicitar el derecho del olvido a las plataformas de redes sociales y a la Agencia Española de Protección de Datos

Consejos básicos de Seguridad Informática que debemos de informar a la víctima

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

- Desactivar la webcam en sobremesas y portátiles, o al menos tener tapada con algun protector
- Desactivar el GPS en nuestro móvil
- Debemos cambiar periódicamente nuestras contraseñas de correos electrónicos, dispositivos y redes sociales
- Es recomendable crear una cuenta de correo electrónico personal diferente para el contacto con abogados, psicólogos o cualquier profesional

Consejos para prevenir una sextorsión

- Evita hacerte fotografías de contenido sexual. Si no existen esas fotografías no te pueden extorsionar con ellas
- 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.
- 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.
- No cedas al chantaje. No accedas a las peticiones del chantajista, si aceptas le haces más fuerte y nunca parará de extorsionarte
- Elimina Malware. Asegúrate de que no tienes ningún software malicioso, aunque tu no compartas las fotografías o videos pueden espiarte el ordenador y conseguirlas.
- 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
- No confundas relaciones sentimentales, de amistad, etc. Identifica bien las relaciones sanas, basadas en la confianza y el respeto

- 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
- 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

- **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
- **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.
- **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.
- **Restringe el acceso a tus redes sociales.** Cambia tu privacidad en redes sociales. Haz tu perfil solo accesible a tus contactos.
- **Comprueba que tu conexión sea segura.** Cambiar la contraseña del router que trae por defecto, es una manera de asegurar tu conexión.
- **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
- **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.

- **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.
- **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
- **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.

Consejos para preservar una evidencia digital

- Si nuestra prueba digital se encuentra en un dispositivo móvil es recomendable mejor no utilizarlo, ya que podríamos modificar o alterar la prueba sin darnos cuenta, causando su nulidad en un proceso judicial o bien dificultar su extracción
- Proteger el dispositivo en un lugar seguro fuera del alcance de terceros, para evitar su manipulación, borrado o alteración
- Si contamos con una tarjeta de memoria externa en nuestro dispositivo, es probable que la evidencia se almacene en ella. Por lo que tenemos que tener cuidado de que no la encuentren terceras personas que pueden borrar o alterar dicha prueba
- Si la prueba es una conversación de whatsapp, bajo ningún concepto debemos de borrar el chat o mensaje.
- Un ordenador sobremesa tiene un registro de acceso y evento que pueden ser una evidencia de que terceros han accedido a nuestro ordenador, bajo ningún concepto debemos de formatearlo o cambiar el disco duro o sistema si

tenemos sospechas de que alguien tiene acceso a nuestro ordenador sin nuestro consentimiento

- En caso de que queramos grabar una conversación para ser utilizado como prueba documental en un proceso judicial, debemos de tener instalado en nuestro móvil alguna aplicación que realice esta acción. Recuerda que no deberás de perder el móvil ni borrar el registro de llamadas para que podar presentar dicho registro y la grabación en sede judicial.
- Si la prueba se encuentra en nuestro ordenador, se guardará en su disco duro. Si desconoce la forma de extraerlo para protegerlo, bajo ningún concepto debemos de hacerlo nosotros mismos, sino que deberíamos llamar a un experto para que lo haga por nosotros.
- Realizar capturas de pantalla de cualquier evidencia digital
- La extracción, análisis y presentación de la evidencia digital en sede judicial deberá de estar a cargo de un perito informático o del organismo de la fuerza de seguridad pertinente, bajo ningún concepto presentamos una evidencia digital sin su respetivo informe por un profesional especializado.

Una vez la víctima decide denunciar, el área jurídica toma las riendas del protocolo. El área social ha identificado el tipo de violencia digital que está siendo sometida la víctima, así como los diferentes canales y evidencias digitales que serán de utilidad para poder demostrar el hecho.

La persona encargada de la asesoría jurídica deberá de indicarle los pasos a realizar.

- Firmar un acuerdo de confidencialidad
- Realizar el acta de la recepción de los dispositivos digitales
- Interponer la Denuncia, con las respectivas evidencias digitales para su análisis.
- En caso de que el organismo correspondiente de la Fuerza y Cuerpo de Seguridad cuenta con los medios para realizar el análisis de evidencias digitales,

se deberán presentar junto con la denuncia. En caso contrario, se deberá contratar a un perito informático para el análisis de dichas evidencias.

A continuación, veremos diferentes modelos que el área jurídica deberá de utilizar según sea necesario:

- Acuerdo de confidencialidad. Siempre será necesario firmar un acuerdo de confidencialidad entre el área jurídica y la víctima ANEXO I
- Acta Recepción y Entrega Dispositivos. Cuando la víctima presente dispositivos para analizar, se deberá firmar un acta de recepción de ellos ANEXO II
- Acta de entrega Documentos. Cuando la víctima haga entrega de cualquier documento digital, como archivos en PDF, Word, jpg, etc,; se deberá de firmar un acta de recepción de dichos documentos ANEXO III
- Acta de Acceso a Redes Sociales. Cuando el delito se este cometiendo a través de una red social, se deberá de firmar el acta de acceso a redes sociales para indicar que la víctima ha dado su consentimiento para poder acceder a sus perfiles sociales para realizar la comprobación. ANEXO IV
- Acta de acceso a correos electrónicos. Al igual que el apartado anterior, si tenemos que ingresar al correo de la víctima es necesaria la respectiva acta donde se acredita el consentimiento de la víctima para acceder a sus cuentas de correos electrónicos. ANEXO V

Es importante que en todo momento la denuncia este acompañada de las evidencias digitales que comprueben que está siendo víctima de una violencia de género digital.

En una denuncia de violencia de género digital o ciberacoso es primordial la preservación y análisis de la evidencia digital, para que no pueda ser invalidada en sede judicial, es por eso por lo que debemos de indicar unas pautas para su correcta preservación.

Se deberá de informar que en ningún caso la víctima deberá de:

- Eliminar conversaciones de WhatsApp

- Eliminar fotografías, videos o archivos de audio
- Formatear ordenador, portátil o móvil
- Desinstalar aplicaciones móviles
- Cambiar de dispositivo móvil sin hacer antes una copia de seguridad
- Borrar correos electrónicos

Una vez hemos detectado el tipo de violencia digital, los canales y los medios por donde se está realizando el acoso digital, debemos de extraer y analizar cada evidencia digital, ya que servirá de soporte ante una denuncia por violencia de género digital.

El análisis y la extracción de la evidencia digital ya sea de un teléfono móvil, ordenador o cualquier dispositivo digital deberá de realizarse bien por un perito informático acreditado o por el cuerpo de seguridad especializado.

Un perito judicial debe afrontar todas sus investigaciones siguiendo unos procedimientos y principios en el análisis de evidencias digitales y ratificaciones de sus actuaciones, para evitar una posible manipulación de la evidencia o bien dar la posibilidad de que se impugne la prueba en un proceso judicial.

Retirada de Contenidos sensibles en internet. Canal Prioritario AEPD

El área jurídica será la encargada de gestionar la retirada de contenido sensible en internet mediante el canal prioritario de la Agencia Española de Protección de Datos.

Antes de solicitar ayuda al canal prioritario, si el contenido ha sido publicado a través de una red social, se deberá acudir primeramente a ellas.

Facebook

https://www.facebook.com/help/428478523862899

Twitter

https://help.twitter.com/es/rules-and-policies/twitter-report-violation#specific-violations

Google

https://support.google.com/legal/troubleshooter/1114905?hl=es

Instagram

https://help.instagram.com/122717417885747/?ref=hc_fnav

Si la víctima tiene conocimiento de la existencia de determinadas imágenes de **contenido sexual** o que muestran actos de **agresión**, cuya difusión sin el consentimiento de las personas afectadas está poniendo en ALTO RIESGO sus derechos y libertades, y no se ha logrado la retirada de dicho contenido por otras vías se deberá de utilizar el canal de la AEPD.

El área jurídica deberá describir detalladamente las circunstancias en que se ha producido la difusión no consentida de las imágenes, indicando en particular si la persona afectada es víctima de violencia de género, abuso o agresión sexual o acoso y si pertenece a cualquier otro **colectivo especialmente vulnerable**: menores de edad (especificando si es menor de catorce años), personas con discapacidad o enfermedad grave o en riesgo de exclusión social.

Si las imágenes están siendo difundidas a través de internet, se deberá presentar la **dirección o direcciones web de acceso** o identificar claramente el **perfil social** a través del que se están difundiendo

Es recomendable que se especifique si se ha llevado a cabo acciones para denunciar los hechos ante las **instancias policiales**, detallando, en tal caso, las instancias administrativas o judiciales concretas y la referencia de los procedimientos que se estén tramitando.

Además, se deberá especificar si ha llevado a cabo acciones para limitar la difusión de los datos personales, identificando claramente, en tal caso, a los **prestadores de servicios** (la red social, el portal de vídeo o de blogs, …) a los que se ha dirigido.

Adjunte los **documentos** que considere relevantes para la tramitación de su reclamación, particularmente **una copia de la pantalla o del dispositivo** donde pueda apreciarse claramente el servicio (la red social, el portal de vídeo o de blogs …) a través del cual se están difundiendo las imágenes.

Tras el análisis de la reclamación, la Agencia determinará la posible adopción de **MEDIDAS URGENTES** que limiten la continuidad del tratamiento de los datos personales.

La tramitación se puede realizar electrónicamente si se cuenta con certificado digital

Enlace para la tramitación:

https://sedeagpd.gob.es/sede-electronica-web/vistas/formNuevaReclamacion/nuevaReclamacion.jsf

FASE 2: Identificación

Antes de continuar con la fase de identificación, debemos de:

- Considerar el caso como violencia de género digital
- Conocer el tipo de acoso digital al que está siendo sometida la víctima
- Identificado los canales por donde se está realizando o se ha realizado el acoso
- Identificar el tipo de evidencia que debemos de analizar

La fase de identificación es donde la figura del perito informático especializado en violencia de género digital toma un papel importante, ya que es el encargado de la extracción, análisis y comprobación de las evidencias digitales, así como de redactar el informe pericial que será adjuntado a la denuncia de violencia de género como prueba del acoso al que está siendo sometida la víctima.

Algunas las actuaciones que el perito informático realiza en la fase de identificación son:

- Detectar Software espía en dispositivos móviles y ordenadores
- Detectar casos de Suplantación de Identidad en Redes Sociales
- Validar y certificar conversaciones de WhatsApp, registro de llamadas, SMS, etc.
- Recuperar imágenes, videos y aplicaciones borrados en dispositivos móviles y tablets
- Recuperar documentos, y contenido multimedia en ordenadores
- Certificar acciones de ciberacoso en correos electrónicos y redes sociales
- Detectar software de geo localización en móviles
- Detectar la intrusión de terceros sin consentimiento en dispositivos móviles y ordenadores

Área Psicológica

Una vez activado el protocolo, en las posteriores entrevistas se deberá de ahondar en el caso de violencia digital detectado, para analizar los daños psicológicos causados a la víctima.

Una vez analizado el impacto que pudo haber tenido el vivir este tipo de episodio en la vida de la víctima la psicóloga o psicólogo en coordinación con la trabajadora social. Además, deberá de realizar un informe de evaluación y diagnóstico de cómo ha ido superando la mujer su situación desde que se activó el protocolo.

FASE 3: Prevención y Protección

Hemos detectado el caso, identificado y analizado las evidencias, así como el informe pericial, pero la intervención aún no ha terminado, debemos de proveer a la víctima de las herramientas de prevención necesarias para evitar futuros ataques de su agresor.

Área social

El área social será la encargada de informar a la víctima sobre medidas de seguridad y prevención para evitar ser víctima de violencia de género digital.

Es importante que la víctima que ha realizado la denuncia y aportado las evidencias digitales correspondientes, sienta que no la hemos abandonado, que estamos con ella, que no la dejaremos sola por si el agresor vuelve a acosarla; además que sea consciente que debe tomar las medidas preventivas necesarias para evitar futuros ataques.

Medidas de Seguridad para evitar ser víctima de violencia de género digital

- Nunca se debe de dar las contraseñas de nuestros dispositivos, redes sociales y correos electrónicos a nadie.
- Tener instalado un antivirus en nuestros dispositivos digitales
- No descargar archivos adjuntos de correos electrónicos desconocidos
- No debemos abrir archivos sospechosos en nuestras conversaciones de whatsapp o correos electrónicos
- Debemos de tener nuestros perfiles en redes sociales privados, de esta forma nos seguirán las personas que nosotros aceptemos
- Configurar la doble autentificación en las redes sociales, para evitar que terceras personas accedan sin nuestro consentimiento
- No debemos subir contenido a las redes sociales que puedan ayudar a localizarnos
- Desactivar la webcam en sobremesas y portátiles, o al menos tener tapada con algun protector
- Desactivar el GPS en nuestro móvil
- Debemos cambiar periódicamente nuestras contraseñas de correos electrónicos, dispositivos y redes sociales
- Es recomendable crear una cuenta de correo electrónico personal diferente para el contacto con abogados, psicólogos o cualquier profesional

Consejos para prevenir una sextorsión

- Evita hacerte fotografías de contenido sexual. Si no existen esas fotografías no te pueden extorsionar con ellas
- 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.
- 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.
- No cedas al chantaje. No accedas a las peticiones del chantajista, si aceptas le haces más fuerte y nunca parará de extorsionarte
- Elimina Malware. Asegúrate de que no tienes ningún software malicioso, aunque tu no compartas las fotografías o videos pueden espiarte el ordenador y conseguirlas.
- 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
- No confundas relaciones sentimentales, de amistad, etc. Identifica bien las relaciones sanas, basadas en la confianza y el respeto
- 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
- 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

- **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
- **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.
- **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.
- **Restringe el acceso a tus redes sociales.** Cambia tu privacidad en redes sociales. Haz tu perfil solo accesible a tus contactos.
- **Comprueba que tu conexión sea segura.** Cambiar la contraseña del router que trae por defecto, es una manera de asegurar tu conexión.
- **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
- **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.
- **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.
- **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

- **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.

FASE 4: Educación

Desde la Asociación Stop Violencia de Género Digital, creemos que la mejor arma para prevenir episodios de violencia de género digital es la educación.

Muchas de las víctimas que hemos recibido en la asociación no son conscientes de:

- Los peligros con los que se pueden encontrar en internet
- La importancia de contar con contraseñas seguras
- La configuración de medidas de seguridad en sus dispositivos móviles y ordenadores
- Las formas en las que pueden salvaguardar su privacidad en redes sociales
- Un uso correcto y seguro de internet
- Las formas en las que puedan sufrir violencia digital

Área Social

Se deberá coordinar acciones formativas donde participaran mujeres que han sido víctimas de violencia de género digital o desean conocer herramientas para una navegación segura por internet.

Las ofertas de formación se deberán de centrarse en:

- Igualdad y Nuevas tecnologías
- Uso correcto de las redes sociales
- Medidas de seguridad en dispositivos digitales
- Privacidad, LOPD y Redes Sociales

ANEXOS

ANEXO I Modelo de Acuerdo de Confidencialidad

ACUERDO DE CONFIDENCIALIDAD Y SECRETO #

En La Rioja a __ de _____ de 2020

REUNIDOS

Don _____-___ mayor de edad, con DNI _____ y con domicilio _____ en calidad de Perito Informático, y

Dña. _____, mayor de edad, con CIF: _____ y con domicilio en _____ en adelante EL CLIENTE

EXPONEN

Que ambas partes se reconocen capacidad jurídica suficiente para suscribir el presente documento.

Que ambas partes desean iniciar una relación y colaboración mutua a nivel profesional.

Que durante la mencionada relación las partes intercambiarán o crearán información que están interesadas en regular su confidencialidad y secreto mediante las siguientes:

CONDICIONES

I. OBJETO

Con el presente contrato # _____ las partes fijan formalmente y por escrito los términos y condiciones bajo las que las partes mantendrán la confidencialidad de la información proporcionada y creada entre ellas.

*Que, a los efectos de este acuerdo, tendrá la consideración de **información confidencial,** toda la información susceptible de ser revelada por escrito, de palabra o*

por cualquier otro medio o soporte, tangible o intangible, actualmente conocido o que posibilite el estado de la técnica en el futuro, intercambiada como consecuencia de este acuerdo.

Este acuerdo no constituye ningún acuerdo de licencia, contrato de desarrollo o similar, obligándose las partes a adoptar las medidas oportunas para asegurar el tratamiento confidencial de dicha información, medidas que no serán menores que las aplicadas por ellas a la propia información confidencial de su organización o persona.

II. DURACIÓN

Este acuerdo tendrá una duración indefinida desde la firma del contrato

Cada parte se compromete a mantener el compromiso de confidencialidad respecto a la información y material intercambiado entre las partes, de forma indefinida tras la finalización del presente acuerdo.

III. CONFIDENCIALIDAD

Las partes se obligan a entregarse todo el material que sea necesario para la actuación profesional, y en el caso de ser este confidencial se comprometen a:

Utilizar dicha información de forma reservada.

No divulgar ni comunicar la información técnica facilitada por la otra parte.

Impedir la copia o revelación de esa información a terceros, salvo que gocen de aprobación escrita de la otra parte, y únicamente en términos de tal aprobación.

No utilizar la información o fragmentos de ésta para fines distintos de la ejecución de este contrato.

IV. DERECHOS PREVIOS SOBRE LA INFORMACIÓN

Toda información puesta en común entre las partes es de propiedad exclusiva de la parte de donde proceda, y no es precisa la concesión de licencia para dicho

intercambio. Ninguna de las partes utilizará información previa de la otra parte para su propio uso, salvo que se autorice lo contrario.

V. CLÁUSULA PENAL

Las partes se comprometen a cumplir con todos los términos fijados en el presente contrato, y muy especialmente aquellos relativos a las cláusulas sobre propiedad intelectual e industrial, confidencialidad y obligación de secreto.

Independientemente de las responsabilidades que pudieran derivarse del incumplimiento del presente acuerdo, así como de las eventuales indemnizaciones por daños y perjuicios de cualquier naturaleza que pudieran establecerse, el incumplimiento de estas obligaciones determinará a elección de la parte que no incumplió el contenido de los términos fijados en el presente contrato:

La resolución del contrato.

VI. DERECHOS DE PROPIEDAD

Toda información intercambiada es de propiedad exclusiva de la parte de la cual proceda. Ninguna de las partes utilizará información de la otra para su beneficio independiente.

VII. PROTECCIÓN DE DATOS

Para la correcta aplicación del presente acuerdo, ambas partes podrían tener acceso a datos de carácter personal protegidos por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la Protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y la Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los derechos digitales, por lo que se comprometen a efectuar un uso y tratamiento de los datos afectados que será acorde a las actuaciones que resulten necesarias para la correcta prestación de servicios regulada en este acuerdo, según las instrucciones facilitadas en cada momento.

Asimismo, las partes asumen la obligación de guardar secreto profesional sobre cuanta información pudieran recibir, gestionar y articular con relación a los datos personales y a no comunicarlos a terceros, salvo las excepciones mencionadas, así como a destruirlos, cancelarlos o devolverlos en el momento de la finalización de la relación contractual entre ambas partes, así como a aplicar las medidas de seguridad necesarias.

Los derechos de acceso, rectificación, cancelación y oposición podrán ejercitarse mediante escrito dirigido a las direcciones de contacto de los firmantes del presente documento que constan en el encabezamiento.

VIII. CONFIDENCIALIDAD DEL ACUERDO

Las partes acuerdan que este acuerdo reviste el carácter de confidencial y por tanto se prohíbe su divulgación a terceros.

IX. MODIFICACIÓN O CANCELACIÓN

Este acuerdo sólo podrá ser modificado con el consentimiento expreso de ambas partes, en documento escrito y mencionando la voluntad de las partes de modificar el presente acuerdo.

X. JURISDICCIÓN.

Las partes se comprometen a resolver de manera amistosa cualquier desacuerdo que pueda surgir en el desarrollo del presente contrato.

ESTE ACUERDO CONSTA DE CUATRO HOJAS NUMERADAS.

Y en prueba de conformidad de cuanto antecede, firman el presente acuerdo por duplicado y a un solo efecto en el lugar y fecha citados.

Firmado en La Rioja a _____ de _____de 2020.

ANEXO II Modelo entrega – recepción de dispositivos digitales

ACTA DE ENTREGA-RECEPCIÓN DISPOSITIVOS

A fecha de _____ de _____de 2020, estando reunidos de una parte D/Dña. _____ como Representante de la Asociación Stop Violencia de Género Digital, con D.N.I _____ y de otra parte Don/Doña _____., con D.N.I. _____en la Calle _____ Nº _____- provincia de _____ , se procede al levantamiento de la Presente Acta de Entrega-Recepción de los terminales Modelo _____ con número de serie _____

Según manifiesta de su propiedad, siendo consciente de las posibles consecuencias penales que puedan surgir ante la falta a la verdad para su realizar un estudio pericial sobre el mismo.

DECLARACIONES:

D/Dña. _____ declara que recibe dicho terminal y D/Dña. _____ declara que entrega los terminales indicado anteriormente de manera totalmente voluntaria

Se cierra la presente acta a las horas del día _____ de _____- de 2020.

Entrega *Recibe*

D/Dña. _____ *D/Dña. _____*

ANEXO III Modelo acta de entrega recepción de documentos

ACTA DE ENTREGA-RECEPCIÓN DE DOCUMENTOS

A fecha de __ de ___de 2020, estando reunidos de una parte D/Dña. _____ como Representante de la Asociación Stop Violencia de Género Digital, con D.N.I _____ y de otra parte Don _____., con D.N.I……..en la Calle _____ Nº provincia de _____ , se procede al levantamiento de la Presente Acta de Entrega-Recepción de los siguientes documentos:

Según manifiesta de su propiedad, siendo consciente de las posibles consecuencias penales que puedan surgir ante la falta a la verdad sobre el mismo.

DECLARACIONES:

D. _____ declara que recibe dichos documentos y D. _____ declara que entrega los documentos indicado anteriormente de manera totalmente voluntaria

Se cierra la presente acta a las horas del día __ de __ 2020.

Entrega *Recibe*

Don _____ *Don _____*

ANEXO IV Modelo autorización acceso a redes sociales

AUTORIZACIÓN ACCESO A REDES SOCIALES

A fecha de 19 de Septiembre de 2018, Dña. _____ , mayor de edad, con DNI: _____ y con domicilio en La Rioja en adelante EL CLIENTE, ***AUTORIZA*** *a Don _____ mayor de edad, con DNI _____- y con domicilio en La Rioja en calidad de Perito Informático, a* ***acceder*** *a su perfil en la red social Facebook a estudio de la pericial solicitada por el cliente, con las siguientes credenciales:*

Usuario:

Contraseña:

El cliente manifiesta que el perfil social es de su propiedad, y es consciente de las posibles consecuencias penales que puedan surgir ante la falta a la verdad para su realizar un estudio pericial sobre el mismo.

Se procede al levantamiento de la Presente Acta de autorización de acceso a redes sociales.

ANEXO V Modelo autorización acceso a correos electrónicos

AUTORIZACIÓN ACCESO A CORREOS ELECTRONICOS

A fecha de 4 de Abril de 2018, Dña. _____, mayor de edad, con DNI _____- y con domicilio en La Rioja en adelante EL CLIENTE, ***AUTORIZA*** *a Don _____-- mayor de edad, con DNI _____ y con domicilio en La Rioja en calidad de Perito Informático, a* ***acceder*** *a los siguientes correos electrónicos:*

Con las contraseñas proporcionada por el cliente.

El cliente manifiesta que estos correos electrónicos son de su propiedad, y es consciente de las posibles consecuencias penales que puedan surgir ante la falta a la verdad para su realizar un estudio pericial sobre el mismo.

Se procede al levantamiento de la Presente Acta de autorización de acceso a correos electrónicos.