PROTOCOLO DE DETECCIÓN E INTERVENCIÓN EN LA ATENCIÓN A VÍCTIMAS DE CIBERDELINCUENCIA DE GÉNERO

JUNTA DE ANDALUCIA
Instituto Andaluz de la Mujer
CONSEJERÍA DE IGUALDAD Y POLÍTICAS SOCIALES

PROTOCOLO DE DETECCIÓN E INTERVENCIÓN EN LA ATENCIÓN A VÍCTIMAS DE CIBERDELINCUENCIA DE GÉNERO.

INSTITUTO ANDALUZ DE LA MUJER
CONSEJERÍA DE IGUALDAD Y POLÍTICAS SOCIALES
JUNTA DE ANDALUCIA

INDICE

1. ANTECEDENTES

1.- ANTECEDENTES

La Tecnología de la Información y Comunicación (TIC) ha cambiado nuestra forma de crear información, transmitirla y recibirla, no sólo en el área profesional sino también en la personal y social. Por eso podemos decir que ha cambiado incluso nuestra forma de relacionarnos.

Pero el uso que se da a las TICs no siempre es igualitario y positivo para la mujer, ya que cada vez con más frecuencia se cometen atentados contra los derechos de las mujeres usando las TICs. **Algo que está afectando especialmente a las adolescentes y jóvenes,** aunque no de manera exclusiva.

Estos atentados al principio parecían corresponder al traslado a la sociedad virtual del machismo de nuestra sociedad física o analógica, de manera que delitos tradicionalmente cometidos contra las mujeres en todos los ámbitos (de la pareja, educativo, laboral, social, familiar) parecía que “simplemente” adoptaban un nuevo modo de ejecución. Pero pronto se ha comprobado que es algo más complejo y grave pues actualmente se ataca como nunca antes -tanto a nivel cualitativo como cuantitativo- el derecho a la imagen, al honor y a la intimidad de las mujeres. Esta realidad afecta con especial intensidad y crueldad a adolescentes y mujeres jóvenes, para muchas de las cuales la comunicación a través de las redes sociales no es opcional, y provoca nuevas necesidades en las víctimas.

Para atender esas necesidades los y las profesionales necesitan a su vez nuevos conocimientos, herramientas y pautas sobre TIC, redes sociales y Ciberdelincuencia de Género.

Por estos motivos, y por entender que ante la velocidad de las TIC y la gravedad de esta nueva dimensión de la violencia de género se precisa una reacción urgente, dentro de la previsión de creación de protocolos existente -como se abordará al exponerse el marco normativo- el IAM crea este Protocolo específico de atención ante la Ciberdelincuencia de Género. Se pretende con este Protocolo dar una atención a las víctimas o posibles víctimas adaptada y completa en la era digital en la que nos encontramos. Y puesto que las TIC evolucionan a una gran velocidad, también se prevé la revisión y actualización periódica del Protocolo.

2. MARCO NORMATIVO

2.- MARCO NORMATIVO

El presente Protocolo se encuadra dentro de nuestro marco normativo como herramienta útil para llevar a cabo lo previsto en normas superiores.

La Comunidad Autónoma de Andalucía asume en su Estatuto de Autonomía (Ley Orgánica 2/2007, de 19 de marzo, de reforma del Estatuto de Autonomía para Andalucía) un fuerte compromiso en la erradicación de la violencia de género en todos los ámbitos y en la **protección integral** de las mujeres, al establecer, en su artículo 16, que las mujeres tienen derecho a una protección integral contra la violencia de género, que incluirá medidas preventivas, medidas asistenciales y ayudas públicas.

En primera línea de las acciones del Gobierno Andaluz, se encuentra la labor que desarrolla el Instituto Andaluz de la Mujer para la promoción de la igualdad, la eliminación de la violencia de género y la atención a las víctimas, con el objetivo de avanzar hacia un modelo de sociedad que incorpore nuevas formas de convivencia más democráticas e igualitarias.

Ya en el marco de los Planes de acción (I Plan de Actuación del Gobierno Andaluz para avanzar en la erradicación de la violencia contra las mujeres, 1998-2000 y del II Plan de Acción del Gobierno Andaluz contra la violencia hacia las mujeres, 2001-2004), el Gobierno Andaluz impulsó y consolidó destacadas medidas para actuar contra la violencia de género desde un enfoque multidisciplinar, en tres líneas de actuación: **prevención y sensibilización, atención a las víctimas, y coordinación institucional.**

La importancia de explicitar los derechos de las mujeres víctimas de violencia de género así como de establecer unas pautas concretas de coordinación para garantizar el ejercicio de esos derechos, se abordó en el año 2005 mediante el Procedimiento de Coordinación Institucional para la Prevención de la Violencia de Género y Atención a las Víctimas en Andalucía. Según establece dicho documento los derechos de las víctimas de la violencia de género dimanantes de obligaciones asumidas por las Administraciones Públicas con carácter general se articularán en torno a los siguientes Principios Fundamentales:

– Atención especializada y adecuada a sus necesidades
– Protección efectiva de las víctimas
– Recuperación integral

En el año 2007 en nuestra Comunidad Autónoma se aprobó la Ley 12/2007, de 26 de noviembre, para la promoción de la igualdad de género en Andalucía, que tiene como objetivo la consecución de la igualdad real y efectiva entre mujeres y hombres, así como la Ley 13/2007, de 26 de noviembre, de medidas de prevención y protección integral contra la violencia de género, cuyo objetivo es actuar contra la violencia de género que, como manifestación de la discriminación, las situaciones de la desigualdad y las relaciones de poder de los hombres sobre las mujeres, se ejerce sobre éstas. Igualmente es objeto de esta Ley la adopción de medidas para la erradicación de la violencia de género mediante **actuaciones de prevención y protección integral** a las mujeres que se encuentren en esta situación, incluidas las acciones de **detección, atención y recuperación.**

La ley 13/2007 destacó la importancia de que en cada ámbito de actuación se contara con un protocolo y en el art. 60 establece que la Administración de la Junta de Andalucía promoverá la elaboración de **protocolos de actuación,** en particular en los ámbitos judicial, médico legal, policial, de salud, social y de los centros y servicios de información y atención integral a las mujeres. La norma prevé que la elaboración de los protocolos será impulsada por el Instituto Andaluz de la Mujer estableciendo la concreción y el procedimiento de las actuaciones, así como las responsabilidades de los sectores implicados en el tratamiento de la violencia contra las mujeres, con el objetivo de garantizar la prevención, la atención eficaz y personalizada, y la recuperación de las mujeres que se encuentran en situación de violencia de género o en riesgo de padecerla. Dichos protocolos deben diseñar **"circuitos de atención adecuados a las diferentes situaciones de violencia y las necesidades concretas derivadas de estas situaciones".**

Ambas normas están actualmente en proceso de revisión para, manteniendo sus principios y objetivos, adecuarlas a las necesidades actuales, con ocasión del compromiso en el año 2013 del Gobierno Andaluz en el Pacto Andaluz por la Igualdad de Género. Este Pacto **destaca la necesidad de abordar las nuevas realidades de la violencia de género y su incidencia en la población joven.**

A nivel internacional sobre la intervención institucional y los derechos de las víctimas, hay que destacar la Directiva 2012/29/UE del Parlamento Europeo y del Consejo, de 25 de octubre de 2012. Esta Directiva establece normas mínimas sobre los derechos, el apoyo y la protección de las víctimas de delitos, sustituye la Decisión marco 2001/220/JAI del Consejo, y establece que las víctimas deben recibir apoyo especializado y protección jurídica, con independencia de que denuncien o no; así como que los servicios de apoyo especializado deben basarse en un enfoque integrado y preciso que tenga en cuenta, en particular, **las necesidades específicas de las**

víctimas, la gravedad del daño sufrido como consecuencia de un delito, así como la relación entre las víctimas, los infractores, sus hijos e hijas y su entorno social más amplio, incidiendo en la importancia de la evaluación para poder dar la atención necesaria a cada víctima.

Mediante Acuerdo de fecha 3 de junio de 2013 se aprobó el Procedimiento de Coordinación y Cooperación Institucional para la Mejora de la Actuación ante la Violencia de Género en Andalucía. Entre otras cuestiones se acuerda lo siguiente:

– Instar a la elaboración de Protocolos de Actuación ante la Violencia de Género en aquellos ámbitos en los que aún no se han desarrollado.
– Elaborar un modelo de Plan Individual de Actuación.
– Elaborar un modelo de Sistema de Información Coordinado de Actuaciones que funcione como un “circuito marco” que permita la coordinación de las actuaciones marcadas por los protocolos de los diferentes ámbitos que intervienen.

En cuanto al Marco normativo específico sobre la Ciberdelincuencia y, en concreto sobre la de género, hay que destacar que más allá de lo previsto en el Código Penal, es escaso, dado el carácter novedoso de las TIC y, especialmente, de las relaciones a través de las redes sociales.

A pesar de lo anterior debemos mencionar:

– La Decisión del Consejo, de 29 de mayo de 2000, relativa a la Lucha contra la Pornografía Infantil en Internet.

Esta decisión tiene por objeto prevenir y luchar contra la producción, el tratamiento, la posesión y la difusión de pornografía infantil, así como garantizar que las infracciones que se cometan al respecto sean efectivamente investigadas y perseguidas.

Si bien esta norma no es específica para la violencia de género, la problemática abordada en dicha Decisión tiene una gran actualidad en estos momentos siendo las víctimas mujeres menores de edad involucradas en situaciones de sexting, sextorsión, y porno vengativo.

– El Convenio de Budapest sobre la Ciberdelincuencia, el cual fue firmado el 23 de noviembre de 2001 como consecuencia del desarrollo y utilización cada vez mayor de las Tecnologías de la Información y la Comunicación para cometer crímenes.

El Convenio pretende proteger a la sociedad del Cibercrimen y la persecución de los Ciberdelincuentes, mediante la adopción de normativa interna adecuada y manteniendo una política de cooperación internacional.

Entró en vigor el de julio de 2001 al haber sido ratificado por 22 Estados, y el 20 de mayo de 2010 fue ratificado por España (B.O.E. 17/09/10).

Pone el acento en la gravedad de la Ciberdelincuencia y, dado su carácter imperativo, marca el principio de una evolución hacia un abordaje específico del Cibercrimen, con un tratamiento penal sustantivo, autónomo, unificado y extensivo del fenómeno.

Es un Convenio que parte de los existentes previamente del Consejo de Europa sobre cooperación en materia penal, así como otros tratados similares celebrados entre los Estados miembros del Consejo de Europa y otros Estados, y subraya que **pretende completar dichos Convenios con objeto de dotar de mayor eficacia las investigaciones y los procedimientos penales relativos a los delitos relacionados con los sistemas y datos informáticos, así como facilitar la obtención de pruebas electrónicas de los delitos.**

El Convenio menciona de manera específica la pornografía infantil, que afecta mayoritariamente a niñas, pero no menciona específicamente la captación de menores a través de Internet (Grooming), que también afecta mayoritariamente a niñas y chicas adolescentes, ni hace referencia a la Ciberdelinciencia de Género. Tampoco lo hace el Protocolo Adicional que se aprobó como complemento al Convenio, relativo a la criminalización de los actos de naturaleza racista y xenófoba cometidos a través de sistemas informáticos, y que entró en vigor el 01 de marzo de 2006.

A pesar de ello, es un documento relevante ya que destaca la importancia de dar un abordaje específico a la Ciberdelincuencia y la Prueba Electrónica. Además, la Ciberdelincuencia de Género es una parte del Cibercrimen, como veremos a continuación, vinculada a la violencia sobre las mujeres por el hecho de serlo, que se ha manifestado de manera alarmante con posterioridad a la elaboración del Convenio y su Protocolo Adicional, y que sin duda será abordada en documentos internacionales posteriores.

- El Primer Plan Estratégico para la Igualdad de Mujeres y Hombres en Andalucía (2010-2013), ya destaca la importancia de las T.I.C. en la actualidad y la necesidad de garantizar la igualdad en ese ámbito, indicando:

“La oportunidad de cambios radicales en la eliminación definitiva de las desigualdades de género que proporciona esta nueva etapa, hace imprescindible considerar la incorporación de las mujeres en pie de igualdad a los procesos de innovación tecnológica y científica como elemento irrenunciable del cambio perseguido, y no sólo como usuarias, sino como portadoras de elementos diferenciales de enriquecimiento y desarrollo de la sociedad del conocimiento y de la sociedad de la información.”

3. PRINCÍPIOS

3.- PRINCIPIOS

3.1.- PRINCIPIOS GENERALES

Los principios generales de aplicación en la organización y funcionamiento del Instituto Andaluz de Mujer, atendiendo a lo establecido en el Decreto 1/1989, de 10 de enero, por el que se aprueba su Reglamento, son:

a) Simplificación, racionalización, eficacia y coordinación administrativa.
b) Descentralización y desconcentración de la gestión.
c) Actuación con criterios de planificación y evaluación continuada, de acuerdo con el sistema de información actualizada, objetiva y programada.

Este Protocolo, como no puede ser de otro modo, mantiene esos Principios de actuación, incorporando los siguientes Principios Específicos en cuanto a la interpretación, aplicación y concordancia del Protocolo con otras normas del mismo rango.

3.2.- PRINCIPIOS ESPECÍFICOS

Principio de Innovación.

En estos momentos las Tecnologías de la Información y Comunicación, que tanto afectan a las relaciones, cambian a una gran velocidad, promoviendo nuevas formas de contacto, relación e intercambio y difusión de datos. Por ello el presente Protocolo parte de dicha capacidad de innovación de las TIC, y deberá aplicarse buscando siempre, respetando sus objetivos, cubrir las necesidades que surjan ante nuevas estrategias de Ciberdelincuencia de Género. Para ello deberá aplicarse la analogía, previa evaluación por parte del personal técnico, aunque no se encuentren detalladas de manera expresa esas nuevas formas de Ciberdelincuencia de Género, sin perjuicio de las revisiones periódicas del mismo.

Principio de Complementariedad

El presente protocolo es de aplicación en numerosos servicios prestados por el IAM directa o indirectamente y por tanto es un complemento a las normas y a los protocolos internos de dichos servicios para que la atención en los casos de posible violencia de género incorpore la perspectiva del fenómeno de las TIC, y muy especialmente de las redes sociales.

Principio de Proceso

Este Plan es el primer paso en la protocolización de la actuación ante la

Ciberdelincuencia de Género y a su vez está enmarcado en una etapa en la que -por lo acordado en el Procedimiento de Coordinación y Cooperación Institucional para la Mejor Actuación ante la Violencia de Género en Andalucía- se prevé la creación de un modelo común de Plan Individual de Actuación, así como de un Circuito Marco en la intervención.

Cuando se dicten dichas normas o se llegue a los acuerdos correspondientes, serán un paso más de este proceso común de adecuación continuada a las necesidades de las víctimas. Por ese motivo este Protocolo perderá su vigencia en todo lo que contravenga a lo que se establezca por las normas y acuerdos que surjan con ocasión del citado Procedimiento.

4. CONCEPTOS Y TÉRMINOS CLAVES

4.- CONCEPTOS Y TÉRMINOS CLAVES

A continuación vamos a definir determinados conceptos fundamentales en el Protocolo para facilitar la comprensión del mismo, sin perjuicio de los términos que se contienen en el glosario. Las definiciones que se dan a continuación tratan de clarificar el documento y promover que sea interpretado correctamente; por tanto, no pretenden ser exhaustivas.

NATIVA/O DIGITAL

Son nativas digitales todas las personas nacidas en países con capacidad tecnológica en la década de los años 1980 y posteriores, cuando la tecnología digital ya se encontraba bastante desarrollada y al alcance de buena parte de la sociedad. Como la tecnología digital comenzó a expandirse con mucha velocidad a finales de los años 70, quienes nacieron en los 80 o más tarde han tenido a su alcance en el hogar, centros escolares y centros de ocio, ordenadores, teléfonos móviles, videojuegos, tablets, y por tanto la posibilidad de comunicarse de manera instantánea, de hacer descargas de películas, canciones, etc. Su acceso al uso de los dispositivos electrónico es muy intuitivo pero no tienen de manera intuitiva pautas de relaciones seguras que las proteja de los abusos de Internet.

INMIGRANTE DIGITAL

Inmigrantes digitales son todas las personas que han nacido entre los años 1940 y 1980, ya que aunque no han accedido a las TIC de manera intuitiva, se han incorporado a ese mundo bien como espectadoras y receptoras de las consecuencias del fenómeno, bien como parte activa; tanto en el ámbito privado, como en el laboral y social.

Sobre inmigrantes digitales recae buena parte de la responsabilidad de proteger a las mujeres frente a la Ciberdelincuencia de Género, bien en calidad de padres y madres, bien como profesionales.

CIBERDELINCUENCIA

En un principio se consideraba Ciberdelito o Delito Informático el dirigido contra los dispositivos informáticos, los datos y la información informatizada. Actualmente se entiende delito informático tanto esa modalidad estricta como el cometido a través del ordenador -móviles o similares- o la red, siendo muy relevantes los cometidos mediante las redes sociales.

CIBERDELINCUENCIA DE GÉNERO

Es Cibedelincuencia de Género la violencia de género que se lleva a cabo aprovechando

las TIC. Normalmente coexiste la violencia usando las TIC con la violencia por vías “tradicionales” o “analógicas”, pero la intensidad, la repercusión a nivel relacional y psicológico, las diferencias a nivel de protección y judicial, y las peculiaridades de la prueba electrónica, hacen que siempre sea necesario en la actualidad tener presente el enfoque específico de la Ciberdelincuencia de Género.

Como ejemplo, se refieren las siguientes conductas delictivas que puede sufrir una mujer dentro de una situación de Ciberdelincuencia de Género:

- Descubrimiento y revelación de secretos (robos datos, fotos/videos, cuentas, perfiles).
- Injurias, calumnias a través de TIC.
- Trato denigrante a través de TIC.
- Difusión de imágenes denigrantes o dañinas a través de TIC.
- Usurpación de identidad (e-mail, blogs).
- Uso fraudulento de tarjetas (carding, compras en Internet).
- Daños (equipos, empresas, actividad profesional).
- Grooming y delitos relativos a la corrupción y prostitución de menores.
- Inducción al abandono del domicilio a menores a través de Internet.
- Inducción al suicidio a través de Internet.
- Amenazas y coacciones informáticas.
- Sextorsión.
- Pornografía infantil con uso de las TIC.

A nivel de colectivo, también hay un delito que se está incrementando mediante las TIC: La apología de la discriminación y de la violencia de género.

PRUEBA ELECTRÓNICA

Prueba electrónica es la obtenida a partir de un dispositivo electrónico o medio digital que sirve para formar la convicción en torno a una afirmación o punto de debate relevante en un procedimiento judicial. Por ejemplo, una fotografía, un video, un sms, una conversación por whatsapp, una página web, un e-mail, una base datos, en cualquier soporte constituye una prueba electrónica.

Por tanto, son pruebas derivadas de las nuevas tecnologías de la información y la comunicación.

La licitud de estas pruebas dependerá de que se obtengan respetando el derecho a la intimidad de las personas pues las comunicaciones electrónicas están protegidas en la Constitución (artículo 18), así como en el ámbito civil por la Ley Orgánica sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, y en el ámbito penal por la Ley Orgánica del Código Penal. Cuando la persona que ha obtenido la prueba ha formado parte de la comunicación, o la comunicación se ha realizado por medios públicos de difusión (por ejemplo un blog), la prueba es lícita. Al igual que cuando se incorpora al proceso por autorización judicial. Por tanto, no se vulnera el derecho a la intimidad de la otra persona si se aporta a los procedimientos judiciales un mail recibido con insultos, o la grabación de una conversación por quién participa en ella, o mensajes recibidos o publicados a través de Internet, etc..

El componente electrónico de la prueba electrónica hace que sea especialmente importante presentarla ante los Tribunales de forma clara y comprensible para que personas sin conocimientos TIC puedan comprenderla. Por eso en ocasiones será conveniente contar con un asesoramiento tecnológico o con un peritaje en seguridad informática.

En ocasiones la víctima destruye la propia prueba electrónica, pero con el uso de determinadas técnicas puede ser recuperada.

5. ÁMBITO DE APLICACIÓN

5.-ÁMBITO DE APLICACIÓN

El presente Protocolo es de aplicación en el ámbito de la atención a mujeres -incluidas menores- víctimas de violencia de género llevada a cabo directamente por el IAM o mediante otras entidades o instituciones vinculadas al IAM con ocasión de convenios, concesión de subvenciones, o contratación.

A continuación se relaciona los de servicios respecto de los cuales es de aplicación el Protocolo:

– Información, Asistencia Jurídica, Asistencia Social, Atención Psicológica de los Centros Provinciales del IAM y Centros Municipales de Información a la Mujer (CMIM)

– Información, Asistencia Jurídica, Asistencia Social y Atención Psicológica a mujeres, hijos e hijas, en los recursos del Servicio integral de Atención y Acogida a víctimas de violencia de género (Centros de emergencia, Casas de Acogida y Pisos Tutelados).

– Programa de atención psicológica a hijas e hijos de mujeres víctimas de violencia de género.

– Programa de Atención Psicológica a las Mujeres Menores de Edad Víctimas de Violencia de Género

– Atención telefónica a través del 900200999 (Teléfono de Atención de la Mujer)

– Plataforma de asesoramiento On-Line.

– Servicio Andaluz de Defensa Legal para las mujeres en caso de Discriminación Laboral.

– Cualquier servicio de atención directa del IAM o concertado con el IAM.

- Programa de Atención Psicológica Grupal a Mujeres Víctimas de Violencia de Género

- Servicio de Información, Asistencia Legal y Atención Psicológica a las mujeres víctimas de Violencia Sexual y Abuso Sexual en Andalucía.

6. OBJETIVOS DEL PROTOCOLO

6.- OBJETIVOS DEL PROTOCOLO

6.1.- OBJETIVO GENERAL DEL PROTOCOLO

Incorporar en las actuaciones de los y las profesionales vinculadas al IAM que realizan atención directa, ya sea personal propio o a través de contratos, subvenciones o convenios con el IAM, pautas específicas de actuación ante la Ciberdelincuencia de Género.

6.2.- OBJETIVOS ESPECÍFICOS:

- Garantizar las labores activas de detección a través del personal técnico, muy especialmente respecto de la Ciberdelincuencia de Género y las mujeres adolescentes y jóvenes.

- Garantizar que la información que llega al IAM y a sus entidades colaboradoras queda registrada de forma que facilite el uso compartido y la coordinación, evitando pérdidas de información relativa a las Tecnologías de la Información y la Comunicación.

- Garantizar que por los y las profesionales se da una atención específica correspondiente a las necesidades de cada usuaria mediante la oportuna evaluación, incluyendo aspectos relativos a las Tecnologías de la Información y la Comunicación, y redes sociales.

- Garantizar que la intervención se llevará a cabo conforme a la Evaluación realizada, Planificación de la Atención y Seguimiento, y al Plan de Actuación Individual, en el que se concreta la coordinación entre cada área, servicios conveniados y otros servicios o instituciones, y que en todas las intervenciones se encontrará incorporado el fenómeno de la Ciberdelincuencia de Género y las necesidades específicas que generan.
- Garantizar que el expediente cumple con el requisito de haber recogido la información fundamental completa, incluida la Ciberdelincuencia de Género sufrida, el uso de las TIC que hace la mujer y los riesgos detectados, y las recomendaciones al respecto tanto la que sean de aplicación directa por la mujer como las que tengan carácter de medida de protección y requiera la adopción judicial.

- Garantizar que la evaluación sobre la violencia y/o daño detectado, así como recomendaciones de pautas de seguridad y medidas de protección, incluidas las relativas a las Tecnologías de la Información y Comunicación, y la evolución detectada durante la intervención con ocasión de la Evaluación, Planificación de las Intervenciones y Plan de Actuación Individual, quedan de manera

comprensible a disposición de la usuaria mediante la entrega de informes y la entrega de copia de su expediente, pudiendo elegir la usuaria una de las dos vías, o ambas, si así lo solicita.

7. PAUTAS COMUNES DE ACTUACIÓN

7.- PAUTAS COMUNES DE ACTUACIÓN

Cumpliendo con los principios de actuación del IAM, la intervención técnica en situaciones de violencia de género se regirá por los siguientes criterios:

7.1.- RECEPCIÓN DE LA DEMANDA Y DETECCIÓN DE DEMANDAS IMPLÍCITAS.

Se tendrán en cuenta la demanda manifestada por la mujer así como la que se detecte durante el trascurso de la intervención y que con frecuencia será difícil para la mujer expresar. La posible demanda implícita se abordará con la usuaria si se observa que está con capacidad en ese momento para ello.

Se tendrá también en cuenta si la mujer ha acudido por iniciativa propia, sugerencia de una persona cercana, o por haber sido derivada, con el consentimiento de la mujer, desde:
Teléfono 900200999.
Centros Municipales de Información a la Mujer.
Servicios Sociales Comunitarios.
Centros de Salud Públicos o privados.
Cuerpos y Fuerzas de Seguridad, incluido el Grupo de Delitos Tecnológicos.
Juzgados y Fiscalía.
Servicios de Atención a Víctimas de Andalucía (SAVAs)
Centros educativos.
Universidad.
Centros Laborales.
Profesionales.

7.2.- ATENCIÓN ESPECIALIZADA, INTERDISCIPLINARIA E INTEGRAL.

La atención se llevará a cabo por profesionales que previamente hayan recibido capacitación por el Instituto Andaluz de la Mujer para actuar con especialización, y por tanto habrán recibido formación, herramientas y pautas específicas para la intervención ante la violencia de género, incluida la Ciberdelincuencia de Género.

La intervención será multidisciplinar, abarcando conocimientos del ámbito social, psicológico y jurídico, y también prácticos relativos a TIC y redes sociales. Estos conocimientos se usarán de manera coordinada para llevar a cabo una intervención integral que responda a las

necesidades sociales, psicológicas y jurídicas de la mujer, incluidas las derivadas del uso de la TIC.

7.3.- ATENCIÓN ADECUADA.

En todo caso la atención debe llevarse a cabo de manera cordial y cercana, potenciando un clima de comprensión, apoyo y confianza.

El o la profesional que realiza la intervención debe presentarse, así como al servicio que está prestando.

Se interactuará con las usuarias con un lenguaje acorde con el nivel socio-cultural de la mujer y su edad. Además, con las nativas digitales especialmente las adolescentes, y con mujeres inmigrantes digitales que refieran una situación de Ciberdelincuencia de Género, se usará el lenguaje propio de las TIC y las redes sociales.

Para facilitar esa labor forma parte de este Protocolo un Glosario de términos propios de las TIC y las redes sociales.

Se evitarán mensajes que inculpen a la usuaria (“cómo es posible que te haya pasado esto a ti con la formación que tienes....”).

Se tendrá especial cuidado en no manifestar sorpresa ni rechazo ante situaciones generadas por el uso de las TIC, y se potenciarán los mensajes de cercanía hacia las nativas digitales, aunque sus dinámicas relacionales estén muy alejadas de las que practique ordinariamente el personal técnico.

Si la mujer precisa una intervención por crisis de ansiedad se intentará calmarla y dejar para un momento posterior la recogida de información de su parte, y la entrega de información por parte del personal técnico. Intervendrá el Área de psicología y se valorará la necesidad de atención del Centro Sanitario.

Si sufre bloqueos emocionales o lapsus de memoria será derivada al Área Psicológica. Igualmente se derivará al área Psicológica si refiere agresión o abuso sexual, o situación de sextorsión.

Es muy importante dejar constancia documental de la crisis sufrida, bloqueos emocionales, afectaciones en la memoria, y de cualquier otra circunstancia relativa al estado de la víctima, así como a su capacidad para expresarse y recibir información.

7.4.- ATENCIÓN PERSONALIZADA Y PLANIFICADA

La atención se puede llevar a cabo mediante comunicación personal, por teléfono y por escrito. En cualquier caso el personal técnico deberá adecuar la intervención a las circunstancias y características personales de la usuaria. Cuando el contacto de la mujer es exclusivamente por teléfono o por escrito, las intervenciones se verán limitadas a la información que se obtenga por esa vía, y a la información que puede realizarse por esa vía. En todo caso, se abordará la Ciberdelincuencia de Género.

En la atención se tendrán en cuenta las necesidades derivadas de minoría de edad, vulnerabilidad, extranjería, diversidad en cuanto a la capacidad mental, física o sensorial, y cualquier otra relevante. Puesto que esas características y necesidades específicas no podrán ser por lo general identificadas de manera completa en una primera entrevista, sino que requerirán de un análisis profundo, y, además, pueden alterarse con el tiempo y la sucesión de nuevos hechos, se llevará a cabo una **EVALUACIÓN CONTINUADA** a través del siguiente circuito de intervenciones técnicas:

1.- Información inicial y general.

La lleva a cabo el Área de Información. Para realizarla se escuchará a la mujer, se identificarán las distintas formas de Violencia de Género -incluida la Ciberdelincuencia de Género- que refiera en ese momento (el desvelamiento suele ser progresivo), se identificará la demanda explícita de apoyo que realiza y, en su caso, la implícita, se tendrá en cuenta el estado que muestre la usuaria al momento de la intervención y la gravedad de lo relatado. En la valoración se incluirán la derivación que corresponda, la información que se ha ofrecido a la mujer, y cómo se ha mostrado ante la misma (si se observa que la comprende, que está bloqueada, que tiene confusión). En todo momento durante la interacción con la usuaria se tendrá en cuenta el estado de la mujer y se evitará una segunda victimización.

Esta intervención conllevará generalmente la entrada de la mujer en el circuito específico de atención por violencia de género del IAM y aunque tiene un carácter inicial, es de suma importancia para que la usuaria se sienta correctamente acogida así como para orientar las sucesivas intervenciones. También es sumamente importante que la informadora o el informador

presente de manera completa y ajustada al IAM, los servicios a favor de la usuaria, hijos e hijas, y sus derechos.

2.- Evaluación y Diagnóstico.

Con objeto de dar la atención personalizada que requiera cada usuaria, el Área Social, Psicológica y Jurídica deberán realizar una evaluación que culminará con un **diagnóstico de la situación.** Esta evaluación crea el primer enmarque detallado de la intervención, pues explicitará, desde las competencias de cada Área, el estado y necesidades de la usuaria, hijos e hijas, y los objetivos concretos del trabajo de cada Área.

En la evaluación de cada Área se abordará la posible situación de Violencia de Género, así como la Ciberdelincuencia de Género, analizando las características que tenga en cada caso, los derechos de la mujer que se detecten comprometidos con ese tipo de acciones, las necesidades específicas de la mujer, y la conceptuación y atribución causal que la mujer hace respecto de la violencia de género, pues es algo que puede repercutir en la persistencia de su demanda de apoyo, en el resultado de la terapia, del asesoramiento jurídico y del apoyo social.

En las sucesivas atenciones se harán **evaluaciones continuadas** para trabajar en la consecución de esos objetivos, abordando posibles nuevas incidencias y evolución del estado de la mujer, así como la aparición de nuevas necesidades. Los cambios pueden ser tan relevantes como para que se lleve a cabo un nuevo diagnóstico con una modificación sustancial de la intervención, o se realicen modificaciones parciales.

3.- Planificación de la Atención y Seguimientos.

Como consecuencia y complemento de la evaluación y del diagnóstico de cada Área, se elaborará una **Planificación de la Atención y Seguimiento respecto de las Áreas Social, Jurídica y Psicológica, y Diagnóstico Integral.**

Tras cada sesión se valorará lo detectado en la sesión y la conveniencia de mantener los mismos objetivos y planificación.

Si lo requiere el estado de la usuaria, podría volverse a una planificación anterior. Se tendrá especialmente en cuenta en los casos de Ciberdelincuencia de Género en los que puede desencadenarse una serie de ataques hacia la mujer mucho después del ataque original, incluso por numerosas personas desconocidas, lo que puede generar mucha inestabilidad en su estado y en sus necesidades (por ejemplo, tras un año de aparente tranquilidad, con los objetivos

cumplidos en el Área Jurídica y Psicológica, la usuaria descubre que ha sufrido una usurpación de identidad y precisa nueva atención psicológica por ello, así como jurídica).

4.- Plan de Actuación Individual.

Con ocasión del Diagnóstico Integral, de la evaluación continuada, y de las atenciones y seguimientos que se planifiquen, se elaborará en conjunto por el Área Jurídica, Psicológica y Social un Plan de Actuación Individual específico para cada usuaria.

Dependiendo de las necesidades de cada mujer, se designará entre el personal técnico el Área que asumirá la responsabilidad de coordinar la realización y ejecución de dicho Plan, en el plazo máximo de 15 días desde la primera intervención. El personal técnico implicado decidirá teniendo en cuenta las circunstancias concretas de cada situación y usuaria, el plazo para las revisiones del Plan de Actuación Individual, sin perjuicio de que cualquier cambio relevante detectado por una de las Áreas implicadas sea motivo de cambio en el Plan de Actuación, previa coordinación con las demás Áreas. En todo caso, el Plan de Actuación se revisará por todas las Áreas implicadas lo más tarde cada tres meses.

En las revisiones del Plan se decidirá sobre si procede mantenerlo en vigor, modificarlo dadas las necesidades del momento detectadas mediante la evaluación continuada, o dejarlo en suspenso.

Dentro del Plan de Actuación Individual habrá una parte dedicada a Seguimiento, en la cual cada Área volcará información relevante en SIAM sobre el seguimiento que está practicando que deba ser tenida en cuenta por las demás Áreas al llevar a cabo su intervención o que pueda resultarles útil. De manera que el o la profesional que vaya a intervenir pueda ponerse al día respecto de las actuaciones de las demás Áreas con rapidez consultando ese apartado.

Cuando solamente se precise intervención de un Área además de la actuación previa del Área de Información, el Plan de Actuación Individual será elaborado exclusivamente por dicha Área, y coincidirá con la Planificación de Atenciones y Seguimientos.

7.5.- ATENCIÓN DOCUMENTADA, COORDINADA Y ACCESIBLE PARA LA USUARIA.

Todas las intervenciones se documentarán durante la intervención y tras finalizar la misma, conforme a las pautas que se establecen posteriormente. En el plazo de 3 días cada profesional que haya realizado una atención registrará en el sistema de información informatizado

del Instituto Andaluz de la Mujer, SIAM, la información referida a la misma. El o la profesional que atienda en persona por primera vez a la mujer, que por lo general será la informadora o informador, le dará de alta como usuaria, previo cumplimentar por su parte la correspondiente autorización de la Ley Orgánica de Protección de Datos.

La información obtenida de la mujer, así como los hechos sucedidos en presencia del o la profesional (por ejemplo estar recibiendo whatsapps que impresionan a la mujer), el estado que muestre la mujer, la evaluación o evaluaciones, la Planificación de las Intervenciones y Seguimientos, y el Plan de Actuación Individual, quedarán registrados en el expediente en SIAM.

La Ciberdelincuencia de Género se recogerá de manera descriptiva, indicando las estrategias concretas utilizadas para esta violencia que se hayan manifestado por la mujer o detectado directamente por el o la profesional.

Se incorporará también en el SIAM documentación relativa a la situación personal, familiar, social, jurídica, médica, farmacológica y psicológica de la mujer, que ésta aporte; así como documentos específicos en relación a la ciberdelincuencia de género (pantallazos de whatasapps, mails....).

Si se han visto comprometidas imágenes de la mujer, se dejará constancia de ello en el SIAM, describiendo el contenido de la imagen (imagen de la usuaria en la que....), pero sin incorporar la imagen al SIAM.

Se realizará una recogida exacta de la información dada por la mujer, incorporando las expresiones literales más significativas, incluidos los términos técnicos y los propios de las Redes Sociales, para hacer visible la violencia de género incluso en su dimensión de Ciberdelincuencia de Género.

El SIAM recogerá como parte relevante de la información: La Valoración Inicial, la Evaluación y Diagnóstico del Área Social, Psicológica y Jurídica, Planificación de Intervenciones y Seguimientos realizados por cada una de esas, Plan de Actuación Individual (que se llevará a cabo de manera coordinada por todas las Áreas implicadas) y los **Informes** que se realicen.

Respecto de la Ciberdelincuencia de Género, los informes se harán usando terminología propia de las TICs que sea necesaria, pero también describiendo en lenguaje común lo que significa a nivel de estrategias llevadas a cabo por el actor y de consecuencias para las víctimas.

8. INTERVENCIÓN DEL ÁREA DE INFORMACIÓN

8.- INTERVENCIÓN DEL ÁREA DE INFORMACIÓN

Este apartado es de aplicación para los y las informadoras de los Centros Provinciales del Instituto Andaluz de la Mujer así como para las técnicas o técnicos, encargados de dar, salvo circunstancias excepcionales, la primera información en los servicios subvencionados que atienden la violencia de género, como los CMIMs.

Las tareas de la técnica o técnico encargado del área de Información son las recogidas en el protocolo de actuación general del Instituto Andaluz de la Mujer, sin perjuicio de lo señalado en el presente protocolo de Ciberdelincuencia, es por ello que se incluirá en el procedimiento de información las siguientes actuaciones:

– En cuanto a la apertura del expediente en SIAM en el que se irán anotando los datos de la usuaria así como la información que aporte espontáneamente, incluida la Ciberdelincuencia de Género.

- Aportar a la mujer unas pautas básicas de seguridad informática, conforme a la ficha Nº 4.

- Analizar con la mujer la documentación que debe ir recopilando y resguardar en un lugar seguro, así como de la documentación que es conveniente mostrar y/o aportar en las entrevistas con otras áreas, incluida la prueba electrónica, conforme a la Ficha Nº 5.

– Hacer constar en el expediente SIAM los hechos sucedidos en presencia del o la profesional (por ejemplo estar recibiendo whatsapps que impresionan a la mujer), el estado de la usuaria y la derivación que se realiza.

9. INTERVECIÓN DEL ÁREA SOCIAL

9.- INTERVENCIÓN DEL ÁREA SOCIAL

Este apartado es de aplicación para todo el personal técnico del Área Social de los Centros Provinciales del Instituto Andaluz de la Mujer así como por las trabajadoras y trabajadores sociales encargados de llevar a cabo la intervención social, en los servicios conveniados.

Las tareas de la técnica o técnico encargado del área social son las recogidas en el protocolo de actuación general del Instituto Andaluz de la Mujer, sin perjuicio de lo señalado en el presente protocolo de Ciberdelincuencia, es por ello que se incluirá en el procedimiento de intervención del área social las siguientes actuaciones:

– Recoger e incorporar en el expediente SIAM lo relativo al uso de las TICs por parte de la mujer, así como situaciones de ciberdelincuencia de género que la mujer haya manifestado verbalmente, documentalmente, o que haya percibido directamente el o la profesional.

– En las entrevistas se incluirán contenidos específicos para la detección de la Ciberdelincuencia de Género conforme a la Ficha 6.

– En el supuesto de que la mujer solicite acogida, será el trabajador o trabajadora social la persona encargada de informarle básicamente sobre la importancia de seguir pautas de seguridad para evitar la localización a través del uso o con ocasión del uso de dispositivos electrónicos conforme a la Ficha Nº 7.

– Recordar a la usuaria pautas de seguridad informática (Ficha 3) y sobre recopilación de prueba electrónica (Ficha 4).

10. INTERVECIÓN DEL ÁREA PSICOLÓGICA

10.- INTERVENCIÓN DEL ÁREA PSICOLÓGICA

Este apartado es de aplicación para todo el personal técnico del Área Psicológica de los Centros Provinciales del Instituto Andaluz de la Mujer así como por las psicólogas y psicólogos encargados de llevar a cabo la intervención psicológica, en los servicios que se prestan desde el IAM mediante convenios.

Las tareas de los y las profesionales del área de psicología son las recogidas en el protocolo de actuación general del Instituto Andaluz de la Mujer, sin perjuicio de lo señalado en el presente protocolo de Ciberdelincuencia, es por ello que se incluirá en el procedimiento de intervención del área de psicología las siguientes actuaciones:

- Recoger en el relato de las usuarias lo relacionado a la Ciberdelincuencia de Género, dejando constancia de las dificultades que pueda presentar la mujer para situar temporalmente los hechos, incluidas las evidencias tecnológicas (por ejemplo, whatsapp enviado a tercera persona sobre los hechos).

– Anotar en SIAM el relato y demás hechos sucedidos en presencia de la o el profesional (por ejemplo estar recibiendo whatsapps que impresionan a la mujer), el estado de la usuaria, y la intervención realizada.

– Incorporar en el expediente SIAM los aspectos relativos al uso de las TICs por parte de la mujer y las redes sociales; así como situaciones de Ciberdelincuencia de Género que la mujer haya manifestado verbalmente, documentalmente, o que haya percibido directamente el o la profesional.

– En las entrevistas se ahondará sobre la Ciberdelincuencia de Género que se haya detectado previamente, y se indagará sobre la posible realización de hechos nuevos o no desvelados anteriormente, conforme a la Ficha Nº 6.

– En cuanto al impacto en la vida relacional de la usuaria de la Ciberdelincuencia de Género, la psicóloga o psicólogo se coordinará con la trabajadora o trabajador social. Esta o este profesional habrá previamente o estará analizando las redes sociales de apoyo que tiene la víctima. También habrá evaluado o estará evaluando el impacto de las acciones o estrategias de Ciberdelincuencia de Género sobre su reputación social, vida social, familiar y/o laboral. Dicha evaluación será tenida en cuenta para contrastar los resultados de la propia evaluación psicológica.

– Dentro de la Evaluación y Diagnóstico que realiza el Área Psicológica se incluye, a tenor de lo expresado por la mujer, las entrevistas a terceras personas, la documentación en su caso aportada, y lo observado y analizado con respecto a la ciberdelincuencia:

a) Descripción de hechos documentados, especialmente a través de las TIC (por ejemplo, acoso a través del mail, o de las redes sociales, violencia psicológica verbal que la víctima ha grabado etc.) o percibidos directamente por el o la técnica.

b) Recoger entre las características personales de la mujer la existencia de ciber-adicción.

c) Las consecuencias de la difusión del abuso a través de las TICs.

d) El riesgo que se percibe por el o la profesional de reiteración de conductas que pueden perjudicar psicológicamente a la mujer, así como del riesgo de sufrir una concatenación de ataques a través de Internet, o difusión de información u otro uso dañino de las TICs y las redes sociales, partiendo de su propio relato y la valoración efectuada sobre el mismo; y las consecuencias previsibles que esa reiteración tendría en la mujer.

e) La conveniencia, necesidad, o incluso el carácter urgente, de la adopción de pautas y medidas de protección, tanto de naturaleza civil, como penal. También se valorará la conveniencia de seguir pautas de seguridad informática, por la mujer, y, en su caso, los y las adolescentes, en coordinación con el Área Jurídica y, si se considera necesario, la Social, conforme a las Fichas 8 y 9.

f) En cuanto a la Ciberdelincuencia de Género, se analizarán necesidades específicas (recuperación de imagen social, superación de adicción a conexión, necesidades de protección ante posible concatenación de delitos...).

g) Pronóstico para el supuesto de que cese la exposición a la violencia y/o abuso, o a circunstancias aversivas derivadas del abuso inicial (como la redifusión por Internet de imágenes íntimas), y para el caso de que no cese a corto plazo; objetivos de la terapia y derivación a terapia de grupo, en su caso.

h) Si considera que se requiere atención específica de algún área en concreto, además de las recogidas en el protocolo general del IAM se prestará especial atención:

- Respecto a una mujer menor de edad, cuando se considere conveniente que la terapia que reciba sea o pase a ser de grupo, se explicará en un lenguaje que pueda comprender en qué consiste la terapia de grupo específica para este colectivo, con especial abordaje de la Ciberdelincuencia de Género.

- En casos de Ciberdelincuencia de Género o uso puntual de las TICs dentro de una dinámica tradicional de violencia de género, se abordarán estrategias de concienciación respecto de la Ciberdelincuencia de Género, de motivación para el uso de pautas de seguridad de la información en las Redes Sociales y en el uso en general de las TICs – Ficha Nº 4 -, así como estrategias terapéuticas para paliar los efectos del control y de las crisis de reputación a través de las TICs, la mejora de la imagen, la identidad, y, en su caso, de la sexualidad, que tan dañadas suelen verse tras la exposición a la Ciberdelincuencia de Género. Se valorará también la posible existencia de Ciberadicción y, en su caso, se dará atención al respecto siempre y cuando no se considere que precisa una atención previa específica por la adicción.

- Respecto del apoyo psicológico para la afrontación de los procedimientos jurídicos, se incorporará en los casos de uso de las TICs como herramienta de violencia de género estrategias de fortalecimiento ante la posible, aunque controlada, exposición gráfica de la intimidad en los

procedimientos, ante oleadas de mensajes recriminatorios, exposición pública a través de las TICs de los propios procedimientos, etc...

- Si se detecta durante la evaluación, o en cualquier otro momento, que la mujer padece un Trastorno Mental Grave del que no recibe tratamiento, o respecto del cual no se encuentra estabilizada, el psicólogo o psicóloga la derivará a la Unidad de Salud Mental para que valoren la intensidad de la psicopatología y la posibilidad de seguimiento. Una vez iniciado el tratamiento psicológico o psiquiátrico y estabilizada su situación, podría recibir asesoramiento psicológico o terapia grupal relativa a la Violencia de Género, incluida la Ciberdelincuencia de Género.

11. INTERVENCIÓN DEL ÁREA JURÍDICA

11.- INTERVENCION DEL ÁREA JURÍDICA

Este apartado es de aplicación para las y los profesionales del Área Jurídica de los Centros Provinciales del Instituto Andaluz de la Mujer así como por las asesoras y asesores jurídicos que llevan a cabo ese tipo de asesoramiento en los servicios contratados.

Las tareas del personal técnico encargado del área jurídica son las recogidas en el protocolo de actuación general del Instituto Andaluz de la Mujer, sin perjuicio de lo señalado en el presente protocolo de Ciberdelincuencia, es por ello que se incluirá en el procedimiento de intervención del área jurídica las siguientes actuaciones:

- Recoger en el expediente de SIAM el relato de las usuarias en cada entrevista relativo a violencia de género con el mayor detalle posible, incluida la Ciberdelincuencia de Género. Para ello se partirá de lo que ya conste en el expediente del SIAM para evitar repeticiones innecesarias, y actualizar la información.

- Anotar además los hechos, en su caso, sucedidos en presencia de la o el profesional (por ejemplo estar recibiendo whatsapps que impresionan a la mujer), así como el estado de la usuaria, la documentación que aporta la usuaria, y la intervención realizada.

- Recoger e incorporar en el expediente en SIAM los aspectos jurídicos, incluido lo relativo al uso de las TICs por parte de la mujer y las redes sociales; así como situaciones de Ciberdelincuencia de Género que la mujer haya manifestado verbalmente, documentalmente, o que haya percibido directamente el o la profesional, sirviendo como orientación la Ficha Nº 6.

- Dentro del asesoramiento jurídico se destaca: asesoramiento sobre procedimientos de familia (divorcios, medidas respecto de menores, medidas provisionales o provisionalísimas, ejecuciones, procedimientos de patria potestad y entre ellos los relacionados con las TIC así como con la evaluación y atención psicológica a menores....), penales (por violencia en la pareja, acoso en el ámbito escolar, acoso en el ámbito laboral, explotación sexual....), y, en relación especialmente a la Ciberdelincuencia de Género, procedimientos derivados de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, 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. Usará como orientación las Fichas 8 a 20.

- Recabar la máxima documentación posible a aportar en los procedimientos en apoyo de las

pretensiones de la usuaria, informando a la mujer sobre la recopilación y custodia de la prueba electrónica conforme a las Fichas Nº 5 y 8.

- Facilitar asesoramiento si la mujer quisiera ampliar la denuncia. Se explicará la importancia de que en la denuncia se detallen las estrategias o acciones de Ciberdelincuencia de Género que se hayan desarrollado, aunque en todas o partes de ellas se haya recibido el ataque de manera anónima; para ello tendrá que explicarse los motivos por los que se sospecha de un autor en concreto.

- Reflexionar con la mujer y elaborar las medidas de protección penales o civiles que se desean solicitar, con especial atención a las relativas a las TIC, conforme a la Ficha Nº 8.

- Recordar a la usuaria pautas de seguridad informática (Ficha 3) y sobre recopilación de prueba electrónica (Ficha 4), primeros consejos para preservarla (Ficha 18), e informar sobre la posibilidad de aportar informes periciales informáticos (Ficha 20).

12. INTERVENCIÓN EN ENTIDADES CONVENIADAS

12.- INTERVENCIÓN EN ENTIDADES CONVENIADAS

12.1.- PAUTAS GENERALES

Las entidades colaboradoras desarrollan un importante papel en la atención integral y protección a las mujeres, adolescentes y niñas víctimas de violencia de género, incluida la Ciberdelincuencia de Género. También tienen un papel relevante en la atención y protección a sus hijos e hijas, y en la prevención de la trasmisión generacional de la Violencia de Género.

En su actuación, dentro de las competencias de cada entidad, **se regirán por las pautas comunes explicitadas en el protocolo de actuación general del Instituto Andaluz de la Mujer.** Así, cada entidad colaboradora realizará labores activas de detección de la demanda de la mujer, incluyendo las demandas derivadas de la Ciberdelincuencia de Género; dará una atención adecuada, con un lenguaje acorde con el nivel socio-cultural de la mujer y su inmersión en las TIC y redes sociales; dará una atención personalizada y planificada, basada en la evaluación continuada, sin perjuicio de las limitaciones que los servicios de atención de urgencia u on-line tienen al respecto; y toda la atención estará documentada, se llevará a cabo con coordinación, y será accesible para las usuarias mediante la entrega de copia íntegra de su expediente así como mediante la entrega de informes.

Por tanto, aplicarán como pautas comunes de su intervención, las referidas en el presente Protocolo en el apartado 7; sin perjuicio de señalar a continuación otras de manera específica para casa servicio.

12.2.- Teléfono 900200999

Este servicio atiende tanto llamadas en situación de urgencias, como llamadas para asesoramiento y ayuda en la toma de decisiones; en estos últimos supuestos las llamadas suelen realizarse sin dar los datos.

Sin perjuicio de las pautas conveniadas previamente, en todo lo que no sea contrario con el presente Protocolo, son de aplicación las siguientes pautas:

– Las pautas comunes de actuación del presente Protocolo, en la medida en la que no excedan el formato de intervención del servicio.
– Detectar la violencia que se desprende de las manifestaciones de la mujer, incluida la

Ciberdelincuencia de Género, y hacer una valoración de la gravedad, teniendo en cuenta también el estado de la mujer, y las características de la persona que identifica como el agresor.
– Informar sobre sus derechos, así como sobre pautas básicas de seguridad informática (ciberconsejos) y prueba electrónica, conforme a las Fichas Nº 4 y 5.
– Remitir a la página web del IAM para acceder directamente a las referidas fichas.
– Dejar constancia documental de la intervención, incluida la Ciberdelincuencia de Género.

12.3.- ASESORAMIENTO JURÍDICO ON-LINE

El asesoramiento jurídico on-line está pensado en materia de Violencia de Género para facilitar que incluso mujeres que aún no quieren desvelar que se encuentran en esa situación puedan recibir información quedando en todo momento asegurada la confidencialidad puesto que no se registran datos personales. También permite que sean terceras personas las que se informen.

Durante el desarrollo de la labor de asesoramiento jurídico on-line es necesario:

– Hacer visible desde el propio formulario de consulta, la existencia, en general, de Violencia de Género en todos los ámbitos, y también de Ciberdelincuencia de Género.
– Si la mujer no ha expresado directamente una situación de Ciberdelincuencia de Género pero sí de Violencia de Género, incorporar en la respuesta: ejemplos de situaciones de control e intrusismo, desprestigio, acoso, uso de imágenes para hacer daño, a través de las TIC, y remisión a la página web del instituto para acceder a los Ciberconsejos, Ficha Nº 4.
– Si la mujer ha referido expresamente una situación de Ciberdelincuencia de Género, además del asesoramiento jurídico que corresponda, se incorporará información sobre pautas básicas de seguridad informática, conforme a la Ficha Nº 4, y sobre prueba electrónica, conforme a la Ficha Nº 5.
– Tener en cuenta en todo momento que la comunicación por mail debe ser clara y completa, no solo porque eso es imprescindible para que el asesoramiento sea efectivo, sino también porque la mujer puede decidir usar esos mails en procedimientos judiciales, siendo una prueba relevante de su estado y situación, y un elemento clave para entender su comportamiento.

12.4.- Servicios de Atención Jurídica, Asistencia Social y Atención Psicológica en los Centros de emergencia del Servicio integral de Atención y Acogida a víctimas de violencia de género.

Sin perjuicio de las pautas comunes establecidas en el protocolo de actuación general del

IAM y de las conveniadas para este servicio -incluido el Plan de Acción Anual del Servicio Integral, que no sean contrarias a lo establecido en este texto, se destacan las siguientes pautas:

1.- En cuanto a la información a la mujer:

Dentro de la información que se le aporte a la mujer se encontrará la relativa a los derechos ante el Instituto Andaluz de la Mujer, presentándose el servicio de acogimiento como parte de los Recursos a su favor en los cuales se aplican dichos derechos, conforme a la Ficha Nº 4.

2.- En cuanto a la Atención Social:

Se llevará a cabo una atención, evaluación, diagnóstico, documentación y emisión de informes, conforme a lo establecido para la Intervención del Área Social en el presente Protocolo y en el de actuación general del IAM.

3.- En cuanto a la intervención Psicológica:

Se llevará a cabo una atención psicológica individual, evaluación diagnóstico, documentación y emisión de informes, conforme a lo establecido para el Área Psicológica en el presente Protocolo y en el de actuación general del IAM, incorporando lo observado directamente por los y las profesionales durante la estancia. Además se incorpora la atención, evaluación, diagnóstico e informes, respecto de los y las menores, siguiendo las pautas previstas en el apartado 12.5, si bien la atención psicológica en los Centros de Emergencia será individual.

4.- En cuanto a la intervención Jurídica.

Se llevará a cabo una atención, evaluación diagnóstico, documentación y emisión de informes, conforme a lo establecido para el Área Jurídica en el presente Protocolo y en el de actuación general del IAM.

5.- En cuanto a los Contratos Reguladores de Estancias, Reglamento de Régimen Interno y Fichas de Ingreso.

La documentación se implementará haciendo visible la Ciberdelincuencia de Género, abordando pactos que garanticen la seguridad de la mujer y de las demás usuarias, y el uso seguro de Internet y las redes sociales; evitando, tanto respecto de la mujer como respecto de menores a su cargo, la localización a través de geolocalizadores, de otras aplicaciones, de las Redes Sociales, de la difusión de imágenes, o de cualquier dispositivo electrónico. Se aplicará lo previsto en la Ficha Nº 7.

12.5.- Servicio de Atención Jurídica, Asistencia Social y Atención Psicológica a mujeres, hijos e hijas, en las Casas de Acogida y Pisos Tutelados del Servicio integral de Atención y Acogida a víctimas de violencia de género.

Sin perjuicio de las pautas comunes establecidas en este Protocolo, en el de actuación general del IAM, y de las conveniadas para estos servicios -incluido el Plan de Acción Anual de las Casa de Acogida y Pisos Tutelados-, que no sean contrarias a lo establecido en este texto, se destacan las siguientes pautas:

1.- En cuanto a la atención psicológica a la mujer y menores:

Mujer:

– Se llevará a cabo una Evaluación psicológica del estado de la mujer, y se valorará si procede terapia de grupo.
– La evaluación psicológica abarcará las cuestiones detalladas en este Protocolo dentro de la intervención del Área Psicológica, y se le entregará por escrito a la mujer, preservando los datos de localización. Se incorporará como elemento relevante para la Evaluación y Diagnóstico, lo observado directamente por el personal técnico durante la estancia, que será valorado por el o la psicóloga.

– Dentro del asesoramiento psicológico y de las terapias grupales, se abordará la Ciberdelincuencia de Género, estrategias de concienciación al respecto, estrategias de motivación para el uso de pautas de seguridad de la información, en las redes sociales y en el uso en general de las TIC, conforme a la Ficha Nº 4; así como estrategias terapéuticas para paliar los efectos del control y de las crisis de reputación a través de las TIC, la mejora de la imagen, la identidad, y, en su caso, de la sexualidad.

Menores:

- Cuando se detecte la necesidad de recibir terapia, y/o lo demande la madre, con autorización expresa de ésta se procederá a una evaluación de su estado. Si se considera necesario iniciar una terapia de grupo o individual, se llevará a cabo.

- Con carácter previo a las entrevistas con menores se efectuará una con la madre para recoger información, explicarle la intervención que se puede llevar a cabo, y recibir por escrito la

autorización para intervenir y el consentimiento de la Ley de Protección de Datos. Es importante explicar a la mujer que aunque la responsabilidad última en la protección de sus hijos e hijas es de la Administración de Justicia, se trabajará de la forma más coordinada y documentada posible, para que la valoración e intervención que se efectúe por el servicio pueda ser presentada en los procedimientos judiciales y sirva para hacer llegar a las y los operadores jurídicos lo detectados por el personal técnico especializado que haya valorado y/o dado terapia a la o el menor.

- Se hará una primera valoración sobre las consecuencias de la Violencia de Género, incluida la Ciberdelincuencia de Género, sobre la o el menor, mediante al menos cuatro sesiones de al menos una hora cada una. La valoración se llevará a cabo conforme a lo previsto en este Protocolo para la Evaluación del Área Psicológica pero se incorporará como elemento relevante para la Evaluación y Diagnóstico, lo observado directamente por el personal técnico, durante la estancia que será valorado por el o la psicóloga.

- Si tras esa primera valoración el o la profesional considera necesario iniciar la terapia para la salud psicológica y desarrollo de la o el menor, la misma se desarrollará.

- En todo caso, se entregará a la progenitora un informe tras las sesiones de primera Evaluación, con el Diagnóstico y la recomendación que se haga por el o la profesional.

- Ya se valore la conveniencia de que reciba la o el menor terapia de grupo o individual, sin perjuicio de los objetivos conveniados para una y otra, dentro de ella se abordará dentro de sus capacidades, la Ciberdelincuencia de Género, estrategias de concienciación al respecto, estrategias de motivación para el uso de pautas de conforme a la Ficha Nº 4; así como estrategias terapéuticas para paliar los efectos del control, y otras formas de violencia psicológica o situaciones de riesgo a través de las TIC.

- Cada cuatro sesiones con el o la menor se llevará a cabo una sesión con la madre, en la que se informará del desarrollo de la intervención, y se le orientará para facilitar el desarrollo terapéutico. También se le entregará un informe de seguimiento. En cada informe, incluido el primero, se incluirán las recomendaciones de la o el profesional para la mejora del estado de la o el menor, y, en concreto, sus recomendaciones en cuanto al contacto con el agresor o con otras personas (por ejemplo familiares o amistades del agresor).

- En la medida de lo posible durante las sesiones con la o el menor se recogerá literalmente su relato. Tras las sesiones se completará esa recogida, si es necesario, y se anotará el estado

observado de la menor, los objetivos alcanzados, los nuevos objetivos, las conclusiones y recomendaciones de la o el profesional.

- En la Evaluación Continuada y Diagnóstico las y los menores se abarcarán las mismas cuestiones que se detallan en el presente Protocolo para la Evaluación Continuada y Diagnóstico del Área Psicológica de los Centros Provinciales respecto de las mujeres, si bien con las adaptaciones necesarias en cada caso derivadas de la edad y capacidad de las menores.

- Además se añadirán como instrumento de evaluación pruebas psicológicas acordes a la edad de la menor.

- Se abordará con las y los menores, en la medida en la que su capacidad lo permita, la importancia de llevar a cabo unas pautas sanas de comunicación también en el uso de los dispositivos electrónicos e Internet, conforme a la Ficha 4, adaptando el elenco de recomendaciones a su capacidad.

- Se abordará con la madre la importancia de proteger a las menores de comunicación invasiva, abusiva o violenta a través de las TIC, conforme a la Ficha Nº 4.

2.- En cuanto a la Atención de Social:

– Tanto en la intervención individual como grupal del personal de Trabajo Social y Auxiliar Social, se abordará la Ciberdelincuencia de Género y pautas básicas de seguridad informática.

– Se desarrollarán grupos de concienciación respecto de los riesgos de Internet y la Ciberdelincuencia de Género.

3.- En cuanto a la Atención Jurídica:

En la atención jurídica se incluirá información sobre prueba electrónica, así como respecto de la protección de datos, medidas civiles, penales y de seguridad informática, y aportaciones de imágenes a los procedimientos, conforme a las Fichas Nº 4, 5, 8 y 9.

4.- En cuanto a los Contratos Reguladores de Estancias, Reglamento de Régimen Interno y Fichas de Ingreso.

La documentación se implementará haciendo visible la Ciberdelincuencia de Género, abordando pactos que garanticen la seguridad de la mujer y de las demás usuarias, y el uso seguro de Internet y las redes sociales; evitando, tanto respecto de la mujer como respecto de menores a su cargo, la localización a través de geolocalizadores, de otras aplicaciones, de las Redes Sociales, de la difusión de imágenes, o de cualquier dispositivo electrónico. Se aplicará lo previsto en la Ficha Nº 7.

12.7.- Servicio de Atención Psicológica Grupal a mujeres víctimas de Violencia de Género Programa de Atención Psicológica Grupal a Mujeres Víctimas de Violencia de Género.

Este servicio se da actualmente mediante convenios específicos que abarcan:
– La terapia grupal a mujeres atendidas en los Centros Provinciales.
– La terapia grupal a mujeres de municipios de Andalucía Occidental.
– La terapia grupal a mujeres de municipios de Andalucía Oriental.

Sin perjuicio de las pautas comunes establecidas en este Protocolo, en el de actuación general del IAM, y de las conveniadas para estos servicios - incluido el protocolo para la intervención psicológica grupal con mujeres víctimas de violencia de género en Andalucía y la guía de buenas prácticas, que no sean contrarias a lo establecido en este texto, se destacan las siguientes pautas:

- Se iniciará la intervención de la atención psicológica grupal tras derivación con informe de Evaluación y Diagnóstico del personal técnico del Centro Provincial. Si la mujer ha recibido previamente asesoramiento psicológico por dicho Centro, en el informe se detallará además de lo detectado, la terapia realizada, y recomendaciones. Si ha recibido terapia individual por otra entidad o institución, se solicitará, con consentimiento expreso de la mujer, informe. Igualmente si la terapia ha sido recibida por parte de una o un profesional privado. Lo mismo se llevará a cabo si la terapia previa recibida ha sido grupal.

- Dentro de la terapia grupal, ya sea en la denominada “Grupos de Reflexión”, o “Talleres de Autoestima”, o “Grupo Terapéutico” o cualquier otro grupo terapéutico, se abordará la Ciberdelincuencia de Género, estrategias de concienciación al respecto, estrategias de motivación para el uso de pautas de seguridad de la información, en las redes sociales y en el uso en general de las TIC, conforme a la Ficha Nº 4; así como estrategias terapéuticas para paliar los efectos del control y de las crisis de reputación a través de las TIC, la mejora de la imagen, la identidad, y, en su caso, de la sexualidad.

- En la intervención se cumplirá las pautas comunes de actuación que recoge este Protocolo, así como, las específicas del Área Jurídica y del Área Psicológica, salvo las relativas a coordinación interna entre las técnicas y técnicos de los Centros Provinciales.

- Toda la intervención será recogida en el expediente en SIAM, y la mujer tendrá derecho a recibir copia íntegra del mismo, así como informes conforme a lo establecido en el Protocolo para las Áreas Jurídicas y Psicológicas. En todo caso, y sin perjuicio al derecho a obtener informe y copia íntegra de su expediente en cualquier fase de la terapia, a la mujer se le entregará al finalizar la terapia de grupo un informe que como mínimo resumirá los motivos por los que fue derivada a la terapia de grupo, lo detectado por el o la profesional durante la terapia de grupo, la duración de dicha terapia, la asistencia de la mujer, los objetivos de la terapia, la evolución de la mujer, y recomendaciones.

12.8.- Programa de atención psicológica a hijas e hijos de mujeres víctimas de violencia de género, tanto en el ámbito municipal como en el de los Centros Provinciales.

El servicio de Asistencia Psicológica a hijos e hijas de víctimas de Violencia de Género cumple una función imprescindible ya que por un lado sirve para indagar sobre la situación de los y las menores dentro de una dinámica de Violencia de Género, valorar las consecuencias sobre su salud y desarrollo, y recomendar las pautas necesarias para su recuperación.

- Se indagará la posible comunicación inapropiada del padre y los o las menores mediante las TIC.
- Se abordará con los niños y niñas, en la medida en la que su capacidad lo permita, la importancia de llevar a cabo unas pautas sanas de comunicación también en el uso de los dispositivos electrónicos e internet, conforme a la Ficha 4, adaptando el elenco de recomendaciones a su capacidad.

- Se abordará con la madre la importancia de proteger a las y los menores de comunicación invasiva, abusiva o violenta a través de las TIC, conforme a la Ficha Nº 4.

12.9.- Programa de Atención Psicológica a las Mujeres Menores de Edad Víctimas de Violencia de Género

En este servicio tiene una especial incidencia la Ciberdelincuencia de Género, dadas las edades de las usuarias. Será necesario, sin perjuicio de las pautas específicas ya conveniadas

que no sean contrarias a lo establecido en este texto, y de las comunes que recoge este Protocolo y el Protocolo de actuación general del IAM, se destacan las siguientes pautas:

- Se hará una primera valoración sobre las consecuencias de la Violencia de Género, incluida la Ciberdelincuencia de Género sobre la menor.

- Ya se valore la conveniencia de que reciba la menor terapia de grupo, sin perjuicio de los objetivos conveniados para una y otra, dentro de ella se abordará la Ciberdelincuencia de Género, estrategias de concienciación al respecto, estrategias de motivación para el uso de pautas de seguridad de la información, en las redes sociales y en el uso en general de las TIC, conforme a la Ficha Nº 4; así como estrategias terapéuticas para paliar los efectos del control y de las crisis de reputación a través de las TIC, la mejora de la imagen, la identidad, y, en su caso, de la sexualidad. Se valorará también la posible existencia de Ciberadicción y la conveniencia de que reciba la mujer una terapia específica para ello complementaria o alternativa.

- Se abordará con las menores, en la medida en la que su capacidad lo permita, la importancia de llevar a cabo unas pautas sanas de comunicación también en el uso de los dispositivos electrónicos e Internet, conforme a la Ficha 4, adaptando el elenco de recomendaciones a su capacidad.

- Se abordará con la madre y padre, o con las y los tutores, la importancia de proteger a las menores de comunicación invasiva, abusiva o violenta a través de las TIC, conforme a la Ficha Nº 4.

12.10.- Servicio de Información, Asistencia Legal y Atención Psicológica a las mujeres víctimas de Violencia Sexual y Abuso Sexual en Andalucía.

Sin perjuicio de las pautas comunes y de las conveniadas para este servicio en concreto que no sean contrarias a lo establecido en este texto, se destacan las siguientes:

- Dentro de la Violencia y Abuso sexual será abordados los casos de Sextorsión a través de las TIC, que se remitan por el Centro Provincial, tanto consumado como no.

12.11.- Servicio Andaluz de Defensa Legal para las mujeres en caso de discriminación laboral.

El Servicio Andaluz de Defensa Legal es relevante no sólo por la defensa de los intereses

de las mujeres que sufren discriminación laboral, sino porque en ocasiones la discriminación laboral forma parte de una situación más amplia de acoso laboral y/o acoso sexual, o de otra todavía más compleja cuando la mujer ha mantenido una relación sentimental con un superior o compañero, y la misma es o ha sido abusiva o violenta, o así está siendo la dinámica tras la ruptura.

Por tanto, además de las labores específicas de ejercicio de los derechos de la usuaria, es necesario desarrollar otras de detección de posible situación de Violencia de Género en el ámbito laboral, incluida la Ciberdelincuencia de Género. Respecto de la posible Ciberdelincuencia de Género, se incorporará en las entrevistas con la mujer preguntas específicas conforme a la Ficha Nº 6.

En cuanto a la prueba, se tendrá en cuenta la importancia de la prueba electrónica, informando al respecto a la usuaria, conforme a la Ficha Nº 5.

GLOSARIO

GLOSARIO

A continuación relacionamos palabras y términos compuestos que pueden salir con cierta facilidad al abordar la Ciberdelincuencia de Género o al atender a mujeres nativas digitales.

"A"

Archivo.- Unidad de información almacenada en el disco con un nombre específico. Puede contener datos en código máquina, necesarios para la ejecución de un programa, o información común y corriente procesada por la o el usuario. Tienen una extensión consistente en tres caracteres que lo identifican en su tipo o lo relación con un programa determinado.

ARP (Address Resolution Protocol, Protocolo de Resolución de Direcciones).- Un protocolo de resolución de direcciones electrónicas en números IP que corre en redes locales. Parte del conjunto de protocolos TCP/IP.

Attachment (adjunto).- Se llama así a un archivo de datos (por ejemplo una planilla de cálculo o una carta de procesador de textos) que se envía junto con un mensaje de correo electrónico.

Autentificación.- Procedimiento de comprobación de identidad de un usuario o usuaria. Mediante el mismo se garantiza que la persona que accede a un sistema de ordenador es quién dice ser. Por lo general los sistemas de autentificación se basan en el cifrado mediante clave o contraseña, privada y secreta, que solamente conoce la persona.

Autopornografía.- Material pornográfico producido por la propia persona en él representada.

Avatar.- Originariamente figura humana de un dios en la mitología hindú. Es una identidad ficticia en la que se hace una representación física (cara y cuerpo) de una persona conectada al mundo virtual de Internet. Muchas personas construyen su personalidad digital y luego se encuentran en servers determinados (por ejemplo, en Chats) para jugar o charlar con otras personas.

"B"

Backbone (columna vertebral).- Conexión de alta velocidad que une computadoras encargadas de hacer circular grandes volúmenes de información. Los backbones conectan ciudades o países y constituyen la estructura fundamental de las redes de comunicación. Las Redes WAN y los ISPs utilizan backbones para interconectarse.

Banner.- Aviso publicitario que ocupa parte de una página Web, en general ubicado en la parte superior, al centro. Haciendo un click sobre él, se puede llegar al sitio del anunciante. De este modo, los banners en general se cobran en base a los click-throughs que se obtienen.

Bitcoin.- Bitcoin es una moneda, como el euro o el dólar estadounidense, que sirve para intercambiar bienes y servicios. Sin embargo, a diferencia de otras monedas, Bitcoin es una divisa electrónica que presenta novedosas características y destaca por su eficiencia, seguridad y facilidad de intercambio.

Bluedating o widating o wireless dating.- Es una forma de citas que se hacen mediante el Bluetooth del móvil. Los suscriptores del servicio introducen detalles para crear una imagen de sí mismo, y sobre su pareja ideal, como lo harían para otros servicios de citas en línea. Cuando su teléfono móvil está en la proximidad de la de otro abonado o abonada (un radio de unos 10 metros) reciben una alerta y pueden chatear a través del bluetooth (bluechat).

Blueplace.- Lugar donde encontrar otros usuarios o usuarias de un servicio de bluedating.

Bookmark (señalador o favoritos).- La sección de menú de un navegador donde se pueden almacenar los sitios preferidos, para luego volver a ellos simplemente eligiéndolos con un simple click desde un menú.

Bottleneck (cuello de botella).- Embotellamiento de paquetes de datos (información) que circulan por una conexión; causa demoras en la comunicación.

Bots.- Abreviatura de robots. Son programas muy particulares, inteligentes y autónomos que navegan por el ciberespacio esquivando maniobras para detenerlos. Los bots son sumamente ingeniosos y capaces de reaccionar según la situación. No necesariamente son benignos: sólo obedecen las órdenes de sus creadores. Muy utilizados para causar caos en los Chats.

Browser/Web browser (navegador o visualizador).- Programa que permite leer documentos en la Web y seguir enlaces (links) de documento en documento de hipertexto. Los navegadores hacen peticiones de archivos (páginas y otros) a los servers de Web según la elección del usuario o usuaria y luego muestran en el monitor el resultado de la petición en forma multimedial.

Buscador (Search Engine, mal llamado motor de búsqueda).- Es una herramienta que permite ubicar contenidos en la Red, buscando a través de palabras clave. Se organizan en buscadores

por palabra o índices (como Lycos o Infoseek) y buscadores temáticos o Directories (como Yahoo!). Dentro de estas dos categorías
básicas existen cientos de buscadores diferentes, cada uno con distintas habilidades o entornos de búsqueda.

"C"

Cablemódem.- Dispositivo que permite conectar una computadora a Internet a través de la conexión de coaxial de la televisión por cable. No es realmente un módem ya que no debe modular/demodular porque el sistema es puramente digital. Se perfila como una de las posibilidades de conexión que resolverían la problemática del limitado ancho de banda que se puede obtener a través de una conexión telefónica.

Caché.- Almacenamiento intermedio o temporario de información. Por ejemplo, un navegador posee un caché donde almacena las últimas páginas visitadas por el usuario o usuaria y, si alguna se solicita nuevamente, el navegador mostrará la que tiene acumulada en lugar de volver a buscarla en Internet. El término se utiliza para denominar todo depósito intermedio de datos solicitados con mayor frecuencia.

Cadena de Mensajes.- También se le conoce como cadena de correo electrónico, o cadena de mail. Es un sistema de propagación rápida de mensajes utilizando el correo electrónico y solicitando al usuario o usuaria que los recibe que lo remita a sus contactos. En muchos casos son mails engañosos y, además, se usa en ocasiones como forma de colapsar la bandeja de entrada de una persona concreta. por ejemplo, el ex marido de una empresaria, introduce su mail en varias cadenas de mail, con objeto de llenar su bandeja de entrada con este tipo de mensajes y dificultarle el acceso a los mails de trabajo.

Cam.- Ver Webcam.

Capper.- Persona -por lo general hombre- que se dedica a sacar capturas comprometidas de emisiones de webcam de otras personas -por lo general mujeres-, que suelen ser compartidas en redes sociales con otros cappers y en ocasiones usadas para la sextorsión.

CGI (Common Gateway Interface, Interfaz Común de Intercomunicación).- Conjunto de medios y formatos para permitir y unificar la comunicación entre la Web y otros sistemas externos, como las bases de datos. Similar al ActiveX.

Chat.- Sistema de conversación en línea que permite que varias personas de todo el mundo conversen en tiempo real a través de sus teclados. Existen varios sistemas de chat, uno de los más difundidos es el IRC.

Chaturbarse (o chatturbarse).- En inglés "chaturbate", significa masturbarse durante una sesión de chat, normalmente de videochat.

Ciberbullying o ciberacoso.- Hostigamiento producido por una o un menor hacia otra u otro menor, en forma de insultos, vejaciones, amenazas, chantaje, etc., utilizando para ello un canal tecnológico.

Las chicas cuando sufren ciberbullying suele haber un componente de género, con alguna relación en ocasiones con el sexting, la sextorsión, o existencia de relaciones de seudonoviazgo previas.

Click-stream.- Rastro que un usuario o usuaria deja de su paso por las distintas páginas web que visita. El nombre deriva del “click” del ratón.

Click-throughs.- Sistema de medición que almacena la cantidad de veces que un o una cliente potencial hace click en un banner de publicidad y visita el sitio de la persona o empresa anunciante. Utilizado como métrica para la venta de espacios de publicidad en los sitios Web.

Client side CGI script.- Script CGI que se ejecuta/corre en el o la cliente.

Cliente(Client).- Computadora o programa que se conecta a servidores para obtener información. Un o una cliente sólo obtiene datos, no puede ofrecerlos a otros u otras clientes sin depositarlos en un servidor. La mayoría de las computadoras que las personas utilizan para conectarse y navegar por Internet son clientes.

Cliente/Servidor (Client/Server).- Sistema de organización de interconexión de computadoras según el cual funciona Internet, así como otros tantos sistemas de redes. Se basa en la separación de las computadoras miembros en dos categorías: las que actúan como servidores (oferentes de información) y otras que actúan como clientes (receptores de información).

Comunidad virtual.- Conjunto de personas vinculadas por características o intereses comunes, cuyas relaciones e interacciones tienen lugar en un espacio virtual, no físico.

Conexión Segura.- Se conoce como conexión segura al uso de métodos de encriptación que impiden que la información intercambiada entre un ordenador y el servidor a que se conecta pueda ser interceptada o manipulada. De esta forma, por un lado se garantiza la confidencialidad y por otro la integridad.

Cookies (galletitas).- Pequeños archivos con datos que algunos sitios Web depositan en forma automática en las computadoras de los visitantes. Lo hacen con el objetivo de almacenar allí información sobre las personas y sus preferencias. Por ejemplo, la primera vez que un o una navegante visita un site y completa algún formulario con sus datos y perfil, el sistema podrá enviarle una cookie al asignarle una identificación. Cuando la o el usuario retorne, el sitio Web pedirá a la computadora cliente la cookie y, a través de ella, lo reconocerá.

Cracker (pirata informático).- Persona que se especializa en violar medidas de seguridad de una computadora o red de computadoras, venciendo claves de acceso y defensas para obtener información que cree valiosa.

Cross-platform (multi-plataforma).- Programa o dispositivo que puede utilizarse sin inconvenientes en distintas plataformas de hardware y sistemas operativos. Un programa en lenguaje Java posee esta característica.

Cuenta.- Conjunto de información que permite el acceso a una red social a través de la identificación del usuario o usuaria.

Cybermoney (ciberdinero).- Formas de pago virtuales alternativas que se están desarrollando en Internet. En este momento, la falta de mecanismos de pago que garanticen el intercambio de dinero es la principal barrera para el desarrollo del comercio electrónico. Actualmente, existen distintas alternativas en experimentación como CyberCash, Cybercoin y los mecanismos para el pago de sumas muy pequeñas, llamados micropagos.

Cyberspace (ciberespacio).- Es la denominación del espacio virtual (no físico) donde las personas se reúnen en Internet. También denomina a la cultura, usos y costumbres de la comunidad electrónica. Término inventado por el escritor de ciencia ficción William Gibson, en su obra Neuromancer.

"D"

Default (acción por omisión).- Opción que un programa asume si no se especifica lo contrario.

También llamado “valores predeterminados”.

Dial-in.- Conexión a Internet que se establece a través de un módem y una línea telefónica. A cada usuario o usuaria se le asigna un número IP dinámico, es decir, un número otorgado sólo durante la comunicación. Para establecer la conexión se utiliza algún estándar adecuado, como por ejemplo el PPP, SLIP o CSLIP.

Dial-up.- Término actualmente utilizado como sinónimo de dial-in. Anteriormente definía una conexión a Internet donde no se asignaba número IP.

Dirección electrónica (electronic address).- Serie de caracteres que identifican unívocamente un servidor (por ejemplo, hotmail.com), una persona (contacto@hotmail.com) o un recurso (un sitio Web como http://www.hotmail.com) en Internet. Se componen de varias partes de longitud variable. Las direcciones son convertidas por los DNS en los números IP correspondientes para que puedan viajar por la Red.
Directory.- Buscador organizado por temas.

DirectPC.- Nueva forma de conexión a Internet, basada en el uso de una antena satelital conectada a la computadora durante las 24 horas. Se perfila como una de las posibilidades de comunicación que resolverían la problemática del limitado ancho de banda que se puede obtener en una conexión telefónica.

DNS (Domain Name System/Server, servidor de nombres de dominios).- Sistema de computadoras que se encarga de convertir (resolver) las direcciones electrónicas de Internet (como http://www.hotmail.com) en la dirección IP correspondiente y viceversa. Componen la base del funcionamiento de las direcciones electrónicas en Internet y están organizados jerárquicamente. Ver Internic, ARP.

Download o bajar.- Es el proceso de bajar (traer) un archivo desde algún lugar en la Red al ordenador de un usuario o usuaria.

Driver.- Significa «controlador». Es el software adicional necesario para controlar la comunicación entre el sistema y un cierto dispositivo físico, tal como un monitor o una impresora.

Dynamic IP (IP dinámico).- Se dice así cuando el número IP de una computadora conectada a un proveedor de servicio vía dial-in es otorgado en el momento de la conexión en lugar de ser un

número fijo.

"E"

E-mail (electronic mail o correo electrónico).- Servicio de Internet que permite el envío de mensajes privados (semejantes al correo común) entre usuarios y usuarias. Basado en el SMTP. Más rápido, económico y versátil que ningún otro medio de comunicación actual. También utilizado como medio de debate grupal en las mailing lists.

Emoticons (o Smilies).- Conjunto de caracteres gráficos que sirven para demostrar estados de ánimo en un medio escrito como el e-mail. Por ejemplo, los símbolos :-), vistos de costado, muestran una cara sonriente y pueden significar chiste, broma, o buenos deseos.

Enlaces (links).- Conexiones que posee un documento de la Web (escrito en HTML). Un enlace puede apuntar a referencias en el mismo documento, en otro documento en el mismo site; también a otro site, a un gráfico, video o sonido.

Encriptación (Encryption).- Método para convertir los caracteres de un texto de modo que no sea posible entenderlo si no se lo lee con la clave correspondiente. Utilizado para proteger la integridad de información secreta en caso de que sea interceptada. Uno de los métodos más conocidos y seguros de encriptación es el PGP.

Entorno gráfico.- Sistema operativo en el que la información que aparece en pantalla aparece representada en forma gráfica, como es el caso de Windows.

Escáner.- Dispositivo Periférico que copia información impresa mediante un sistema óptico de lectura. Permite convertir imágenes, por ejemplo de fotografías, en imágenes tratables y almacenables por la computadora. El proceso de conversión se denomina digitalización. El término inglés scanner significa explorar o rastrear.

Evento.- Acontecimiento creado como una publicación o mensaje que se anuncia a otros usuarios o usuarias de la red social para que participen.

Estado..- Información de la situación, circunstancia o disposición del usuario o usuaria de una red social. Esta información puede ser compartida por el propio usuario/a, o por la plataforma de comunicación de manera automática, indicando su disponibilidad o actividad en ese momento.

Exhibicionismo digital o exhibicionismo online.- Exhibicionismo sexual realizado mediante las TIC, como Internet y los teléfonos móviles.

Extranet.- Utilización de la tecnología de Internet para conectar la red local (LAN) de una organización con otras redes (por ejemplo, proveedores y clientes).

"F"

Farming, farm server.- Servidor externo que se alquila para alojar información y ponerla a disposición de los las navegantes de la Red. Sinónimo de Hosting.

Flash (hacer un), o flashing.- Mostrar por unos segundos alguna parte íntima del cuerpo durante una emisión de webcam. Un flashing está con frecuencia en el origen de una situación de sextorsión o de bulling. Por ejemplo, estuvo en el origen del caso de Amanda Todd, que acabó suicidándose por el acoso sufrido.
Finger.- Comando que permite obtener información sobre una persona en la Red (por ejemplo, dirección de e-mail, dirección postal, hobbies), buscando ciertos datos que ésta pudo dejar en un formulario de consulta.

Firewall (pared a prueba de fuego).- Conjunto de programas de protección y dispositivos especiales que ponen barreras al acceso exterior a una determinada red privada. Es utilizado para proteger los recursos de una organización de consultas externas no autorizadas.

Firmware.- Son pequeños programas que por lo general vienen en un chip en el hardware, como es el caso de la ROM BIOS.

Flame (llamarada).- Ataque personal insultante. Mensaje de correo electrónico ofensivo.

Flirtexting.- En sentido estricto es flirtear mediante SMSs, pero por extensión se aplica también al flirteo usando teléfonos o dispositivos portátiles. La frontera con el sexting es difusa, ya que se suele empezar con mensajes y luego se pasa al envío de fotos o vídeos.

Formateo.- Proceso por el que se adapta la superficie magnética de un disco para aceptar la información bajo un sistema operativo determinado. En el proceso de formateado se colocan las marcas lógicas que permitirán localizar la información en el disco y las marcas de sincronismo además de comprobar la superficie del disco.

Frame-relay.- Tecnología de transporte de datos por paquetes muy utilizada en las conexiones por líneas dedicadas.

Freeware.- Política de distribución gratuita de programas. Utilizada para gran parte del software de Internet. En general, estos programas son creados por un estudiante o alguna organización (usualmente una Universidad) con el único objetivo de que mucha gente en el mundo pueda disfrutarlos. No son necesariamente sencillos: muchos de ellos son complejos y han llevado cientos de horas de desarrollo. Ejemplos de freeware son el sistema operativo Linux (un Unix) o el PGP (Pretty Good Privacy, un software de encriptación), que se distribuyen de este modo.

FTP (File Transfer Protocol, Protocolo de Transferencia de Archivos).- Es un servicio de Internet que permite transferir archivos (upload o subir- y download o bajar) entre computadoras conectadas a Internet. Este es el método por el cual la mayoría del software de Internet es distribuido.

Full-Duplex.- Característica de un medio de comunicación por el que se pueden enviar y recibir datos simultáneamente.

Gateway.- Dispositivo de comunicación entre dos o más redes locales (LANs) y remotas, usualmente capaz de convertir distintos protocolos, actuando de traductor para permitir la comunicación. Como término genérico, es utilizado para denominar a todo instrumento capaz de convertir o transformar datos que circulan entre dos medios o tecnologías.

GF.- Abreviatura de girlfriend (novia), usada con frecuentemente en webs dedicadas a recopilar fotos privadas de exparejas sin el consentimiento de éstas, incluso en páginas claramente de pornovengativo.

Grooming.- Conjunto de estrategias que una persona adulta, por lo general un hombre, desarrolla para ganarse la confianza de un o una menor, generalmente una niña o chica adolescente, a través de Internet con el fin último de obtener concesiones de índole sexual.

Grupo.-Servicio que proporcionan las redes sociales para la configuración de colectivos de usuarios y usuarias con un interés u objetivo común. Los grupos permiten crear espacios donde las y los miembros pueden compartir información y contenidos de forma privada o abierta.

Gusano Informático.- Es un programa de ordenador malicioso diseñado con la finalidad de

replicarse así mismo y reenviarse de un equipo a otro de forma automática, utilizando para ello funciones del sistema operativo que controlan que por lo general son invisibles a los usuarios y usuarias. Al cabo de unos días los gusanos llegan al disco duro para empezar a destruir el sistema operativo del ordenador, el cual normalmente presenta estos síntomas:

- Empieza a funcionar mal el ratón.
- Las tareas ordinarias están ralentizan.
- Se bloquean los sitios web.
- Errores en el servidor.
- Fallan programas.

"H"

Hacker.- Experto o experta técnica en algún tema relacionado con comunicaciones o seguridad informática. Los y las hackers suelen dedicarse a demostrar fallos en los sistemas de protección de una red de computadoras y son muy respetados por la comunidad técnica de Internet, a diferencia de las y los crackers, que se dedican a aprovecharse de las vulnerabilidades.
Hardware.- Componente físico de la computadora, como el monitor, la impresora o el disco rígido. El hardware por sí mismo no hace que una máquina funcione. Es necesario, además, instalar un Software adecuado.

Hashtag (Etiqueta).- Es una cadena de caracteres formada por una o varias palabras concatenadas y precedidas por una almohadilla o gato (#). Es, por lo tanto, una etiqueta precedida de un carácter especial con el fin de que tanto el sistema como el usuario o la usuaria la identifiquen de forma rápida.

Se usa en servicios web tales como Twitter, FriendFeed, identi.ca, facebook, Google+, Instagram o en mensajería basada en protocolos IRC para señalar un tema sobre el que gira cierta conversación. Indica un mismo tema sobre el que cualquier usuario o usuaria puede hacer un aporte u opinión personal con solo escribir dicho hashtag en el mensaje. Por ejemplo #sumatuvoz.

Cualquier usuaria o usuario podrá buscar la cadena #sumatuvoz y este mensaje estará presente en los resultados de la búsqueda junto con otros mensajes con el mismo hashtag. El uso masivo de un mismo hashtag determina un trending topic.

Hipermedia.- Combinación de hipertexto y multimedia. Uno de los grandes atractivos de la Web.

Hipertexto.- En lugar de leer un texto en forma continua, ciertos términos están unidos a otros mediante relaciones (enlaces o links) que tienen entre ellos. El hipertexto permite saltar de un punto a otro en un texto, y a través de los enlaces (con un simple click sobre las palabras subrayadas y en negrita), permite que los y las navegantes busquen información de su interés en la Red, guiándose por un camino distinto de razonamiento. Algunos programas muy difundidos, como la Ayuda de Windows o las enciclopedias en CD-ROM, están organizadas como hipertextos.

Home page (página principal o de entrada).- Página de información de la Web, escrita en HTML. En general, el término hace referencia a la página principal o de acceso inicial de un site.

Host.- Sinónimo de servidor.

Hostname (nombre de un host).- Denominación otorgada por el administrador a una computadora. El hostname es parte de la dirección electrónica de esa computadora, y debe ser único para cada máquina conectada a Internet.

HTML (HyperText Markup Language, Lenguaje de Marcado de Hipertextos).- Lenguaje que define textos, subgrupo del SGML, destinado a simplificar la escritura de documentos estándar. Es la base estructural en la que están diseñadas las páginas de la World Wide Web. Su definición está a cargo del Web Consortium.

HTTP (HyperText Transfer Protocol, Protocolo de Transferencia de Hipertexto).- Es el mecanismo de intercambio de información que constituye la base funcional de la World Wide Web.

Hyperdocuments (Hiperdocumentos).- Documento que tiene estructura de hipertexto, pero contiene además referencias a objetos multimediales (como sonidos, imágenes, videos).

Hyperlink.- Enlace entre dos nodos de un hipertexto.

"I"

IMO (In My Opinión, En Mi Opinión).- Una de las siglas utilizadas en los mensajes de Internet. También IMHO (In My Humble Opinion, En Mi Humilde Opinión).

Impressions (visualizaciones).- Unidad de medida que verifica cuántas veces una o un navegante ve un determinado banner de publicidad.

Ingeniería Social.- Es la práctica de obtener información confidencial a través de la manipulación de usuarios y usuarias aprovechando las reaccionar predecibles en ciertas situaciones -por ejemplo proporcionar detalles financieros a un aparente funcionario de un banco- en lugar de tener que encontrar agujeros de seguridad en los sistemas informáticos. Se usa comúnmente el teléfono o Internet para engañar a la gente, fingiendo ser, por ejemplo, una empleado de algún banco, un compañero de trabajo, una técnico o un cliente. Por Internet se envían solicitudes de renovación de permisos de acceso a páginas web, o memos falsos que solicitan respuestas e incluso las famosas cadenas. De esta forma se consigue que la víctima llegue a revelar información sensible.

Interface (Interfaz).- Cara visible de los programas. Interactúa con los y las usuarios. La interface abarca las pantallas y su diseño, el lenguaje usado, los botones y los mensajes de error, entre otros aspectos de la comunicación computadora/persona.

Internet Adress.- Sinónimo de número IP. Número asignado que identifica a un server en Internet. Está compuesto por dos o tres partes: número de red, número opcional de sub-red y número de host. Ver direcciones electrónicas, DNS.

Internet.- Red mundial de ordenadores cuya comunicación se realiza a través del protocoloTCP/IP

Intranet.- Utilización de la tecnología de Internet dentro de la red local (LAN) y/o red de área amplia (WAN) de una organización. Permite crear un sitio público donde se centraliza el acceso a la información de la compañía. Bien utilizada, una intranet permite optimizar el acceso a los recursos de una organización, organizar los datos existentes en las PCs de cada individuo y extender la tarea colaborativa entre los miembros de equipos de trabajo. Cuando una Intranet extiende sus fronteras mas allá de los límites de la organización, para permitir la intercomunicación con los sistemas de otras compañías, se la llama Extranet. IP

Número o dirección (IP address).- Dirección numérica asignada a un dispositivo de hardware (computadora, router, etc.) conectado a Internet, bajo el protocolo IP. La dirección se compone de cuatro números, y cada uno de ellos puede ser de 0 a 255, por ejemplo 200.78.67.192. Esto permite contar con hasta 256 elevado a la 4 números para asignar a las computadoras: cerca de 4 mil millones. Las direcciones IP se agrupan en clases. Para convertir una dirección IP en una dirección electrónica humana (por ejemplo, http://www.hotmail.com) se utilizan los DNS.

IRC (Internet Relay Chat).- Uno de los sistemas más populares de charlas interactivas (chats) de

múltiples usuarios vía Internet. Permite que miles de personas de todo el mundo se reúnan a "conversar" simultáneamente en forma escrita.

"L"

LAN (Local Area Network, Red de Area Local).- Red de computadoras interconectadas, distribuida en la superficie de una sola oficina o edificio. También llamadas redes privadas de datos. Su principal característica es la velocidad de conexión. Ver WAN y MAN.

Línea dedicada (Leased line).-Forma de conexión a Internet (con acceso las 24 horas) a través de un cable hasta un proveedor de Internet. Esta conexión puede ser utilizada por varias personas en forma simultánea.

List serv.- Software robot usado para la administración de un servidor de mailing list. Ampliamente utilizado.

Log.- Archivo que registra movimientos y actividades de un determinado programa (log file). Utilizado como mecanismo de control y estadística. Por ejemplo, el log de un Web server permite conocer el perfil de los visitantes a un sitio Web.

Login.- Proceso de seguridad que exige que un usuario o usuaria se identifique con un nombre (user-ID) y una clave, para poder acceder a una computadora o a un recurso.

"M"

Mail Robot (autoresponder).- Programa que responde e-mail en forma automática, enviando al instante información. Simplifica la tarea de administrar un correo. Los programas utilizados para administrar mailing lists son un tipo de mail robots.

Mailing List (listas de interés).- Modo de distribución de e-mail grupal. Mecanismos de debate grupales entre distintas personas interesadas en un determinado tema. Similares en concepto a los newsgroups, pero no es necesario utilizar un servidor especial ya que los mensajes son recibidos por el o la usuaria como correo electrónico.

Malware.- Es un término que proviene de la expresión inglesa malicious software (software malicioso), también se le conoce como badware, código maligno o software malintencionado. Es

un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario o propietaria. El término malware es muy utilizado por profesionales de la informática para referirse a una variedad de software hostil, intrusivo o molesto.

Un software se considera malware en función de los efectos que intencionadamente (la intención es de su creador, generalmente hasta ahora, hombres) provoque en un computador. El término malware incluye virus, gusanos, troyanos, la mayor parte de los rootkits, scareware, spyware, adware intrusivo, crimeware y otros softwares maliciosos. Malware no es lo mismo que software defectuoso, porque aunque éste causa daños o pueda causarlos, no es esa la intención de la persona que lo creó. Ahora bien, un software defectuoso puede ser instalado intencionadamente para causar daño en un dispositivo. En ese caso, la persona que ha actuado con esa intención habría cometido un ilícito valiéndose intencionadamente de un software defectuoso.

MAN (Metropolitan Area Network, Red de Area Metropolitana).- Red que resulta de varias redes locales (LANs) interconectadas por un enlace de mayor velocidad o backbone (por ejemplo de fibra óptica) en varias zonas. Es el tipo de estructura de red que se utiliza, por ejemplo, en un campus Universitario, donde se conectan los diversos edificios, casas de estudiantes, bibliotecas y centros de investigación. Una MAN ocupa un área geográfica más extensa que una LAN, pero más limitada que una WAN.

MIME (Multipurpose Internet Mail Extensions, Extensiones Multipropósito para e-mail).- Formato específico de codificación para la transferencia de correo electrónico y attachments entre dos computadoras; contiene cualquier tipo de datos. Más moderno que el UUEncoding; aunque menos difundido.

Mirror pic o mirror picture.- Autofoto sacada frente a un espejo. Es una práctica muy habitual en el sexting.

Módem (Modulador/Demodulador).- Dispositivo que se utiliza para transferir datos entre ordenadores a través de una línea telefónica. Unifica la información para que pueda ser transmitida entre dos medios distintos como un teléfono y una computadora. La velocidad del módem se mide en una unidad llamada baudios (bits por segundo), por ejemplo, 28.800 baudios. Cuanto más rápido es el módem, más datos pueden viajar por él en menos tiempo.

Mudd (Multi user Dungeons & Dragons, castillos multi-usuarios).- Conjunto de juegos virtuales de texto para jugar a través de Internet. Originados en las universidades y basados en los

llamados juegos de rol (role-playing games). Consisten en “universos” virtuales con cientos de partes, definidos por programadores, donde los y las participantes deben resolver acertijos y enigmas, muchas veces con la ayuda de otras y otros jugadores.

Multimedia.- Combinación de varias tecnologías de presentación de información (imágenes, sonido, animación, video, texto) con la intención de captar tantos sentidos humanos como sea posible. Previamente a la existencia de la multimedia, el intercambio de información con las computadoras estaba limitado al texto. Luego, con el nacimiento de las interfaces de usuario gráficas y los desarrollos en video y sonido, la multimedia permitió convertir el modo de comunicación entre personas y dispositivos aumentando la variedad de información disponible. El uso de la multimedia fue la razón principal por la que la World Wide Web facilitó la difusión masiva de Internet.

Muro.- Espacio del usuario o de la usuaria de una red social que comparte con el resto de sus contactos, donde estos pueden publicar sus comentarios u opiniones.

"N"

Navegador.- Ver Browser/Web browser.

Navegar.- Recorrer la Web, sin destino fijo, siguiendo enlaces o direcciones.

Netiquette.- Reglas de usos y buenas costumbres de Internet. Surgieron como una serie de políticas informales de “buen comportamiento”, y se difunden de usuaria/o en usuaria/o. Un ejemplo de estas reglas es no escribir mensajes de correo electrónico todo en letras MAYUSCULAS, ya que equivale a ¡GRITAR!.

Newsgroups (grupos de debate).- Mecanismos de debate grupales entre personas de todo el mundo interesadas en un determinado tema. Permiten crear mensajes públicos, que las y los usuarios pueden crear, leer y contestar. Son distribuidos diariamente por toda Internet. También es el área en la que se agrupan los mensajes públicos según su temática. Similares en concepto, aunque no en funcionamiento, a las mailing lists.

Nickname (Nick, sobrenombre o alias).- Nombre de fantasía que un usuario o usuaria de Internet utiliza, por ejemplo, para participar de un Chat.

NNTP (Network News Transfer Protocol, Protocolo deTransferencia de Noticias de la Red).- Protocolo normado de Internet utilizado para el intercambio y transferencia de Newsgroups entre servidores.

"O"

Off-line (fuera de línea).- Estado de comunicación diferida, no en tiempo real.

On-line (en línea).- En línea, similar a en estado de comunicación activa en Internet..

Overhead.- Desperdicio de ancho de banda, causado por la información adicional (de control, secuencia, etc.) que debe viajar además de los datos en los paquetes de un medio de comunicación. Afecta el Throughput de una conexión.

"P"

Página (page o Webpage).- Unidad que muestra información en la Web. Una página puede tener cualquier longitud, si bien equivale por lo general a la cantidad de texto que ocupan dos pantallas y media. Las páginas se diseñan en un lenguaje llamado HTML, y contienen enlaces a otros documentos. Un conjunto de páginas relacionadas componen un Site.

Password (clave o contraseña).- Palabra utilizada para validar el acceso de un usuario a una computadora servidor.
Perfil.- Datos personales y rasgos propios que caracterizan a un usuario o usuaria dentro de una red social, como su nombre, fotografía, lugar de residencia o preferencias. El perfil representa su identidad virtual.

PGP (Pretty Good Privacy, Muy Buena Privacidad).- Software de encriptación freeware muy utilizado, desarrollado por Paul Zimmerman. Se basa en un método de clave pública y clave privada, y es óptimo en cuanto a seguridad. Su eficacia es tal que los servicios de inteligencia de varios países ya lo han prohibido. Más datos en http://www.pgp.com/.

Pharming.- La palabra Pharming deriva del término farm (granja en inglés), y está muy relacionada con el término phishing (técnica de ingeniería social que se define a continuación).

Es una técnica que trata de obtener información confidencial de los usuarios o usuarias

redirigiendo las peticiones que realiza a través del navegador a sitios web que está controlados por los delincuentes, los cuales simulan la apariencia de los Servidores de Internet. Suele llevarse a cabo manipulando el ordenador del usuario o usuaria, o los servidores de nombres de dominio (DNS) en internet. De esta forma, una o un usuario que introduzca un determinado nombre de dominio que haya sido redirigido, accederá en su explorador de Internet a la página web que el atacante haya especificado para ese nombre de dominio, y entregará su información a los delincuentes..

Una vez que la persona atacantes, que hasta ahora generalmente es un hombre, ha conseguido acceso a un servidor DNS o varios servidores (granja de servidores o DNS), se dice que ha hecho un pharming.

Es una práctica que se usa con frecuencia frente a víctimas desconocidas de las que se pretende conseguir por ejemplo los datos bancarios, pero también se usa como forma de Ciberdelincuencia de Género, bien por usar esas técnicas para obtener datos bancarios, bien para obtener otra información confidencial en el contexto de una relación abusiva por motivos de género. Por ejemplo, tras negarse una mujer a mantener relaciones sexuales con un compañero de trabajo, éste accede mediante Pharming -o encargo a otra persona que acceda- en su ordenador para localizar sus claves bancarias y hacer disposiciones que le perjudican.

Phising.- El término phishing proviene de la palabra inglesa "fishing" (pesca),y hace alusión al intento de hacer que los usuarios o usuarias "muerdan el anzuelo". A la persona que lleva a cabo esta práctica delictiva se le denomina phisher.

Es una técnica de ingeniería social que trata de obtener información confidencial de usuarias o usuarios simulando la identidad de entidades prestadoras de servicios en Internet. La o el ciberdelincuente -phisher- suplanta ser una persona o empresa de confianza de la usuaria o usuario, simulando una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o utilizando también llamadas telefónicas.

En principio es una técnica que surgió para usarse contra un grupo indiferenciado de personas, como los y las clientes de un banco. Pero también es posible, y cada vez se da más, que la o el delincuente, que suele ser hasta ahora hombre, se dirija contra una persona en concreto. Así, hay casos de Ciberdelincuencia de Género en los que la mujer sufre un Phising. Cuando el phising tiene un objetivo específico, se le denomina spear phishing (pesca con arpón).
Ping (Unix).- Herramienta que permite averiguar si existe un camino (comunicación) de TCP/IP

entre dos computadoras de cualquier parte de Internet.

Plug & Play.- Tecnología que permite agregar dispositivos a una computadora (por ejemplo, CD-ROMs o
placas de sonido) que se conectan y configuran automáticamente.

Plug-in (agregado).- Programa que extiende las habilidades de un navegador, permitiéndole mayor funcionalidad. Por ejemplo, se puede agregar un plug-in que permita ver videos, jugar un juego grupal o
realizar una teleconferencia.

Porno vengativo (en inglés "revenge porn").- Imagen de sexting publicada en Internet por una ex-pareja o ex-amante como venganza o castigo. Es una de las estrategias de Ciberdelincuencia de Género.

Port (puerto).- Conexión lógica y/o física de una computadora, que permite comunicarse con otros dispositivos externos (por ejemplo, una impresora) o con otras computadoras. Los servicios de Internet (como el e-mail o la Web) utilizan ports lógicos para establecer comunicaciones entre una computadora cliente y un servidor.

Post..- Entrada, mensaje o publicación en una red social que puede consistir en un texto, opinión, comentario, enlace o archivo compartido.

Postmaster.- La persona que administra un servidor de Internet. Cuando se desea efectuar una consulta se envía un e-mail al postmaster, quien responderá la consulta.

Programa.- Sinónimo de software. Conjunto de instrucciones que se ejecutan en la memoria de una computadora para lograr algún objetivo. Creados por equipos de personas (en lenguajes especiales de programación.

Protocolo.- Conjunto de reglas formuladas para controlar el intercambio de datos entre dos entidades comunicadas. Pueden ser normados (definidos por un organismo capacitado, como la CCITT o la ISO) o de facto (creados por una compañía y adoptados por el resto del mercado).

Provider (Proveedor, ISP o Intermediario).- Empresa que actúa de mediadora entre una o un usuario de Internet y la Red en sí misma. Ofrece el servicio de conexión dial-in o dedicado, y

brinda servicios adicionales como el Web hosting.

"R"

Red (network).- Dos o más computadoras conectadas para cumplir una función, como compartir periféricos (impresoras), información (datos) o para comunicarse (correo electrónico). Existen varios tipos de redes: según su estructura jerárquica se catalogan en redes cliente/servidor, con computadoras que ofrecen información y otras que solo consultan información, y las peer-to-peer, donde todas las computadoras ofrecen y consultan información simultáneamente. A su vez, según el área geográfica que cubran, las redes se organizan en LANs (locales), MANs (metropolitanas) o WANs (área amplia).

Request (pedido).- Solicitud de información o datos que una computadora cliente efectúa a un servidor.

Router (ruteador).- Dispositivo de conexión y distribución de datos en una red. Es el encargado de guiar los paquetes de información que viajan por Internet hacia su destino. Ver TCP/IP, LAN.

"S"

Seguidor..- Llamado *follower* en la terminología de Twitter. Usuario o usuaria de esta red social que se suscribe a los mensajes o publicaciones (tweets) de otros usuarios/as, bien por admiración, como en el caso de las y los seguidores de deportistas o actores; por simpatizar con sus ideas; por mantenerse informado de sus actividades en Twitter; o, simplemente, por amistad.

Server (servidor de información).- Computadora que pone sus recursos (datos, impresoras, accesos) al servicio de otras a través de una red.

SET (Secure Electronic Transactions, Transacciones Electrónicas Seguras).- Un estándar para pagos electrónicos encriptados que está siendo desarrollado por Mastercard, Visa y otras empresas. Similar al SSL.

Sexting.- Envío de contenidos de tipo sexual —\principalmente fotografías o vídeos—\ producidos generalmente por quién los remite, a otra persona por medio de teléfonos móviles u otros dispositivos tecnológicos. Relacionado con el sexting se encuentra el llamado “sex-casting”: la grabación de contenidos sexuales a través de la webcam y difusión de los mismos por email,

redes sociales o cualquier canal que permitan las nuevas tecnologías. En los últimos tiempos todo esto además se ve acompañado por el hecho de que se está produciendo una sexualización precoz de la infancia, en buena parte mediante este tipo de prácticas.

Aunque no todas las prácticas de sexting acaban generando consecuencias negativas para la o las personas implicadas, con frecuencia son el origen de conductas de sextorsión.

Sextorsión, sex+extorsión.- Este neologismo tiene su origen en el inglés y consiste en hacer chantaje a una persona, generalmente una mujer, para mantener relaciones sexuales con el chantajista u otra persona, para producir pornografía, u otras acciones de contenido sexual. Para llevar a cabo ese chantaje se usa la amenaza de difundir una imagen desnuda, o sexual de ella, a través de móviles o Internet. Normalmente esa imagen se han obtenido porque la víctima la ha compartido a través del sexting. Otras veces se ha obtenido mediante la amenaza de causar algún mal a ella o a personas de su entorno.

Este delito tiene un gran impacto sobre las víctimas que se enfrentan a una terrible realidad: con un clic de ratón el chantajista podría hacer un daño irreparable a su vida, ya que las imágenes digitales son sencillas de guardar, manipular y distribuir.

Las menores son un colectivo de alto riesgo de sufrir sextorsión. Muchas veces, en el marco de un caso de grooming donde el adulto acosador sexual, una vez obtenida la primera imagen sensible, pretende que la menor acceda a sus peticiones. En otras ocasiones, las adolescentes son protagonistas dentro de una relación de "noviazgo" de prácticas de sexting que acaban siendo usadas para forzarlas a mantener relaciones sexuales.

Sistema Operativo.- Conjunto de programas que se encarga de coordinar el funcionamiento de una computadora, cumpliendo la función de interface entre los programas de aplicación, circuitos y dispositivos de una computadora. Algunos de los más conocidos son el DOS, el Windows, el UNIX.

Sistemas Abiertos.- Conjunto de computadoras de distintas marcas interconectadas, que utilizan el mismo protocolo normado de comunicación. El protocolo estándar más difundido es el TCP/IP.

Site (sitio).- En general, se lo utiliza para definir un conjunto coherente y unificado de páginas y objetos intercomunicados, almacenados en un servidor. Formalmente es un servicio ofrecido por un server en un determinado port. Esta definición no siempre hace corresponder a un solo site con

un server; por ejemplo: varios servers pueden responder a un mismo site, como los ocho servers que componen el buscador Yahoo! y también es posible que un solo server atienda simultáneamente varios sites, como sucede en los servers de los proveedores de Web hosting.

SMTP (Simple Mail Transfer Protocol, Protocolo Simple de Transferencia de Correo).- Protocolo estándar de Internet para intercambiar mensajes de e-mail.

Snail mail (correo caracol).- Modo en que el correo postal común es conocido en Internet. Juego de palabras por su lentitud comparada con la inmediatez del e-mail.

Software.- Componentes intangibles (programas) de las computadoras. Complemento del hardware. El software más importante de una computadora es el Sistema Operativo.

Solicitud de amistad.- Mensaje enviado a otro usuario o usuaria como petición para pertenecer a su lista de contactos, y viceversa. Una vez recibida la solicitud, el usuario o usuaria puede aceptar y agregar un nuevo contacto para compartir con él o ella su contenido e información.

Spam.- Mensaje electrónico no solicitado enviado a muchas personas.

Spiders (arañas).- Complejos programas autónomos que recorren la Web siguiendo enlace tras enlace en cada página; almacena estas últimas para que más tarde sean catalogadas en las enormes bases de datos de los índices de búsqueda.

Spoofing.- Suplantación de la identidad de una o un tercero a través de Internet. Aunque puede producirse en diferentes entornos uno de los más habituales es en el envío masivo de Spam.

SSL (Secure Socket Layer, Capa de Seguridad).- Estándar para transacciones electrónicas encriptadas que está siendo ampliamente utilizado para hacer negocios vía la Red. Ver *SET*.

Streaming (Transferencia Continua).- Sistema de envío continuo de información, que permite, por ejemplo, ver un video a medida que se baja de la Red.

Sysop (System operator, operador del sistema).- Persona encargada de la administración y el mantenimiento de un host. Ver *Postmaster y Webmaster.*

"T"

Tag (etiqueta).- Código marcador de estructura de lenguaje HTML utilizado para estructurar las páginas de la Web.

TCP (Transmission Control Protocol, Protocolo de Control de Transmisión).- Conjunto de protocolos de comunicación que se encargan de la seguridad y la integridad de los paquetes de datos que viajan por Internet. Complemento del IP en el TCP/IP.

TCP/IP (Transmission Control Protocol/Internet Protocol, Protocolo de Control de Transmisión/Protocolo Internet).- Conjunto de casi 100 programas de comunicación de datos usados para organizar computadoras en redes. Norma de comunicación en Internet, compuesta por dos partes: el TCP/IP. El IP desarma los envíos en paquetes y los rutea, mientras que el TCP se encarga de la seguridad de la conexión, comprueba que los datos lleguen todos, completos, y que compongan finalmente el envío original.

Teleconferencia.- Sistema que permite conversar con una o varias personas simultáneamente, viendo su imagen en movimiento (video) además de la voz.

Telnet (Unix).- Programa que permite el acceso remoto a un host. Utilizado para conectarse y controlar computadoras ubicadas en cualquier parte del planeta.

Thread, threaded messages (hilación, mensajes hilados).- Mensajes de correo electrónico, (de un newsgroup o una lista de interés), relacionados al mismo tema, o que son respuestas a un mismo asunto.

Throughput.- Rendimiento final de una conexión. Volumen de datos que una conexión brinda como resultante de la suma de su capacidad y la resta de los overheads que reducen su rendimiento. Ver Red.

Toothing.- Práctica consistente en utilizar las capacidades Bluetooth de teléfonos móviles, PDAs u otros dispositivos portátiles para ligar con personas desconocidas.

Trending topic.- Tema popular en un momento determinado, en relación al número de publicaciones o mensajes (tweets) que se hacen sobre él en Twitter.

Tweet..- Mensaje o publicación de 140 caracteres que se escribe y envía a las y los usuarios seguidores mediante la red social de microblogging Twitter. También existe el Retweet (RT) que

es, sencillamente, el reenvío de un tweet.

"U"

Unix.- Sistema operativo diseñado por los Laboratorios Bell y refinado en Berkley entre otros lugares, que soporta operaciones multiusuario, multitasking y estándares abiertos. Ampliamente difundido en Internet, es utilizado para ejecutar en los Servidores.

Upgrade.- Actualización de un programa.

Upload (subir).- Proceso de enviar un archivo desde su computadora a otro sistema dentro de la red. Vea Download, FTP.

URL (Uniform Resource Locator, Localizador Uniforme de Recursos).- Dirección electrónica. Puntero dentro de páginas HTML que especifican el protocolo de transmisión y la dirección de un recurso para poder acceder a él en un server de Web remoto.

User Account..- Cuenta de usuaria o usuario. Similar a user ID.

User ID.- Identificación de usuario en una computadora. Relacionado con una clave de acceso o password.

Usuaria/o.- Persona o entidad que utiliza y forma parte de una red social. El usuario o usuaria puede acceder a la red social con su propio nombre o mediante un alias, aunque con la revolución de la Web 2.0 se aprecia un cambio en el que las usuarias y los usuarios se identifican con nombres reales. En la red social de microblogging Twitter, la cuenta y perfil adoptan el nombre real, pero sus miembros identifican sus actividades en la red mediante un nombre de usuario o usuaria que puede ser diferente, similar o idéntico a su nombre real, y que, además, añade delante de éste el símbolo @.

"V"

Virus.- Pequeños programas de computadora que tienen la capacidad de autoduplicarse y parasitar en otros programas. Una vez que se difunden, los virus se activan bajo determinadas circunstancias y, en general, provocan algún daño o molestia. Ver Worm.

"W"

W3C (World Wide Web Consortium).- Organización que desarrolla estándares para guiar la expansión de la Web. Organizado por el CERN y el MIT y apadrinado por varias empresas. Su Website es http://www.w3.org/. Ver Sistemas Abiertos.

WAN (Wide Area Network, Red de área amplia).- Resultante de la interconexión de varias redes locales localizadas en diferentes sitios (distintas ciudades o países), comunicadas a través de conexiones públicas (líneas dedicadas). La conexión puede ser física directa (un cable) o a través de un satélite, por ejemplo. La conexión es más lenta que una LAN. Ver MAN, RED.

Web..- La World Wide Web (WWW) o Red informática mundial, generalmente conocida como la web, es un sistema de distribución de documentos de hipertexto o hipermedios interconectados y accesibles vía Internet. Con un navegador web, una persona puede visualizar sitios web compuestos de páginas web que pueden contener texto, imágenes, vídeos u otros contenidos multimedia, y navegar a través de esas páginas usando hiperenlaces.

Las páginas web estáticas son básicamente informativas y están enfocadas principalmente a mostrar una información permanente, donde el navegante se limita a obtener dicha información sin poder interactuar con la página visitada, con lo que tiene un papel pasivo.

Webcam.- Una webcam o cámara web es una pequeña cámara digital conectada a un ordenador, que puede capturar imágenes y transmitirlas a través de Internet, ya sea a una página web o a otros ordenadores de forma privada.

Las cámaras web necesitan un ordenador para transmitir las imágenes. Sin embargo, existen otras cámaras autónomas que tan sólo necesitan un punto de acceso a la red informática, bien sea Ethernet o inalámbrico. Para diferenciarlas de las cámaras web se las denomina cámaras de red.

Las webcams están diseñadas para enviar vídeos en vivo y grabados así como capturas de imagen a través de la red a una/uno o más usuarios y usuarias.
Webcast.- Emisión de vídeo por Internet mediante una webcam.

Webmaster.- Administrador o administradora y/o autor o autora de un sitio Web. Ver Postmaster.

WebTV.- Dispositivo que cruza entre una PC simple y un televisor. Tiene como objetivo abaratar los costos de acceso a la Red y simplificar su uso. Si bien fue lanzado en diciembre de 1996, hasta ahora ha tenido poca difusión.

***Web 2.0*.-** El término Web 2.0 comprende aquellos sitios web que facilitan el compartir información, y permiten a los usuarios y usuarias interactuar y colaborar entre sí como creadores de contenido en una comunidad virtual. Las web 2.0 se diferencia de los sitios web estáticos porque en éstos las usuarias y los usuarios se limitan a la observación pasiva de los contenidos que se han creado para ellos. Ejemplos de la Web 2.0 son los servicios de red social, los servicios de alojamiento de videos, las wikis y blogs.

White Pages (páginas blancas).- Listado de direcciones electrónicas de usuarias y usuarios de Internet.

Whiteboard (pizarrón blanco).- Programa especial para trabajo en grupo que permite que varias personas trabajen a la vez en un proyecto. Aunque las personas no estén físicamente en un mismo lugar, pueden trabajar a la vez desde cualquier punto del planeta a través de Internet. Ver Groupware.

Workstation (estación de trabajo).- Puesto de trabajo o computadora de una usuaria o un usuario. Similar al concepto de Cliente. También se llama así a pequeños servidores con gran capacidad gráfica, como los de Silicon Graphics.

World Wide Web o W3 o WWW.- Conjunto de servidores que proveen información organizada en sites, cada uno con cierta cantidad de páginas relacionadas. La Web es una forma novedosa de organizar toda la información existente en Internet a través de un mecanismo de acceso común de fácil uso, con la ayuda del hipertexto y la multimedia. El hipertexto permite una gran flexibilidad en la organización de la información, al vincular textos disponibles en todo el mundo. La multimedia aporta color, sonido y movimiento a esta experiencia. El contenido de la Web se escribe en lenguaje HTML y puede utilizarse con intuitiva facilidad mediante un programa llamado navegador. Se convirtió en el servicio más popular de la Red y se emplea cotidianamente para los usos más diversos: desde leer un diario de otro continente hasta participar de un juego grupal.

ANEXO FICHAS

FICHA Nº 1. REQUISITOS DEL DEBER DE INFORMACIÓN EN LA RECOGIDA DE DATOS CONFORME A LA LOPD:

- El deber de información de los derechos de la LOPD deberá realizarse de manera que permita acreditar su cumplimiento.

- Cuando se utilicen cuestionarios o impresos para la recogida de datos, figurará la información de los derechos A.R.C.O claramente legible

- Cláusula que proponemos ***para el cumplimiento deber de información LOPD:***

"Los datos de carácter personal que nos falicite quedarán registrados en un Fichero de titularidad del INSTITUTO ANDALUZ DE LA MUJER con la finalidad de prestar el conjunto de servicios que son de competencia de esta Agencia Administrativa según la LEY y su Reglamento. En cualquier momento puede ejercitar sus derechos de Acceso, Rectificación, Oposición o Cancelación sobre sus datos personales dirigiéndose a este Centro por escrito a la siguiente dirección… En cualquier momento este consentimiento puede ser revocado".

FICHA Nº 2. ATENCIÓN A MENORES DE EDAD

- Las y los menores de 14 años deberán ser informadas de sus derechos y recursos a su favor con lenguaje comprensible y adaptado a su estado evolutivo, y, en general, en presencia de quién tenga su tutela, que será quien firme la autorización. Si es mayor de 14 años se podrá informar directamente al menor sin la presencia de una o un progenitor ni de una o un tutor, comprobando especialmente que entiende lo que se le explica.

- (*) No hay que informar a las y los progenitores en caso de ser los contrarios en algún proceso judicial, ya que cuando existe un conflicto de intereses el derecho a la defensa y a la tutela judicial efectiva prevalece al derecho de información del contrario del que se traten datos personales. Esta indicación afecta a recogida de datos tanto a mayores como menores de edad.

- Se puede atender a los y las menores sin firma del consentimiento para el uso de sus datos por parte de progenitor, en casos en los que la menor o el menor así lo demanda y se prevea necesario, conforme a los previsto en el Art. 10 del Reglamento nº 1720/2007 por el que se aprueba el Reglamento de Desarrollo de la
LOPD, apartado 3º. Según dicha norma *"Los datos de carácter personal podrán tratarse sin necesidad del consentimiento del interesado cuando: a) Se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de las competencias que les atribuya una norma con rango de Ley (*) o norma de Derecho comunitario"...*

(*) Ley 10/1988, de 29 de diciembre, de Presupuesto de la Comunidad Autónoma de Andalucía para 1989 (BOJA nº106, de 30/12/88)

TITULO VI De los organismos Autónomos

Artículo Trigésimo. Instituto Andaluz de la Mujer
1.Se crea el Instituto Andaluz de la Mujer como Organismo autónomo de carácter administrativo, dependiente de la Consejería de la Presidencia.

2.El Instituto Andaluz de la Mujer tendrá como fin promover las condiciones para que sea real y efectiva la igualdad del hombre y la mujer andaluces, haciendo posible la participación y presencia de la mujer en la vida política, económica, cultural y social, y superando cualquier discriminación laboral, cultural, económica o política de la mujer."

- Las menores o los menores que puedan ser víctimas de violencia de género serán atendidos por parte del personal técnico del Área Psicológica. En esa atención valorarán la necesidad de recibir atención psicológica.

- Si el o la menor precisa atención psicológica de Urgencia previsiblemente con ocasión de una situación de violencia de género, la misma se le dará por el personal técnico del Área de Psicología, o de las entidades conveniadas con el IAM para realizar dicho servicio, aún sin consentimiento de las y los progenitores. Pero para realizar una intervención no urgente sino programada en profundidad como terapia se precisará el consentimiento de ambos progenitores, salvo que solamente corresponda a uno de ellos el ejercicio de la patria potestad.

En los casos en los que sea preciso el consentimiento de ambos progenitores y solamente uno de ellos de consentimiento, o se prevea que no lo hará, se emitirá informe por parte del psicólogo o la psicóloga valorando la situación de la menor para que la madre pueda instar judicialmente la autorización para que la o el menor reciba el tratamiento. Si se considera que el o la menor puede sufrir un daño relevante debido al retraso en el tratamiento, se emitirá informe por parte del personal del Área Psicológica, en coordinación con el Área Jurídica, a Fiscalía, solicitando que se desarrolle el procedimiento necesario para que la terapia se lleve a cabo a la mayor brevedad.

FICHA Nº 3. FUNCIONES DEL I.A.M. Y DERECHOS DE LA MUJER ANTE EL IAM.

Según la Ley de creación del I.A.M. 10/1988, de 29 diciembre, y más en concreto según el Art. 4.ñ) del Reglamento del IAM, Decreto 1/1989, de 10 de Enero*, se puede realizar la recogida de datos para la canalización de denuncias formuladas por mujeres en casos concretos de discriminación de hecho o de derecho por razón de sexo.* En su apartado O) se indica con carácter general que entre sus fines está realizar *cualquier actividad requerida para el logro de los fines expuestos de acuerdo con la legislación aplicable a los Entes Institucionales de la Comunidad Autónoma*

Derechos de la mujer ante el IAM.

- Derecho a recibir información y asesoramiento jurídico adecuado a su situación personal prestados por personal técnico especializado, en lenguaje comprensible, y a que se evalúe su situación jurídica, a través de los servicios que se presten desde el IAM o por entidades colaboradoras del IAM.

- Derecho a que se les ofrezca por personal técnico especializado información social comprensible sobre las ayudas de carácter social y, si lo solicitan, a la gestión de esas ayudas; así como a que se evalúe su situación a nivel social.

- Derecho a recibir, por personal técnico especializado, atención psicológica, así como sus hijos e hijas, tanto individual como de grupo, teniendo en cuenta lo que sea conveniente a nivel terapéutico; así como a que se evalúe su estado psicológico, el de sus hijos e hijas.

- Derecho a recibir copia de todo su expediente así como a que se le entregue informe sobre la situación de violencia de género (incluida la Ciberdelincuencia de Género) detectada, así como la intervención realizada, evaluación, diagnóstico, pronóstico y recomendaciones.

- Derecho a que se preserve en todo momento su intimidad y la privacidad de sus datos personales, así como los de sus descendientes y los de otras personas que estén a su cargo.

- Derecho a la atención y acogida en los centros especializados, junto con sus hijos e hijas, cuando necesiten protección, y a que se les otorgue atención integral por profesionales especializadas o especializados.

- Derecho a que se pongan en funcionamiento mecanismos de atención integral por el o la profesional que realice la primera atención, remitiendo los datos necesarios al resto de instituciones competentes y realizando el seguimiento del caso, en el ámbito de actuación que le corresponda.

FICHA Nº 4. PAUTAS BÁSICAS DE SEGURIDAD INFORMÁTICA: CIBERCONSEJOS

Actualmente los dispositivos electrónicos y nuestras comunicaciones son atacados con frecuencia, tanto los de uso personal, como los profesionales. En no pocas ocasiones la persona que realiza el ataque es un hombre con el que la mujer ha mantenido o mantiene una relación de pareja, laboral, en el entorno educativo, o social. En otras ocasiones es un hombre desconocido para la mujer, pero su motivación también tiene que ver controlar, humillar o usar a la mujer como objeto.

Por eso en situaciones conflictivas de crisis de pareja, relaciones laborales, educativas, o sociales, así como en situaciones de Violencia de Género, es especialmente importante que se sigan pautas de seguridad informática, para evitar que llegue a producirse Ciberdelincuencia de Género, o, si ya se ha producido, evitar que se repita y paliar las consecuencias. Entre ellas destacamos las siguientes:

1.- ¡Cuidado con el uso de tu móvil y los selfies!
No es necesario ni conveniente compartir tu vida privada y los datos de tu vida diaria de manera exhaustiva, ni con muchas personas.

Piensa dos veces antes de hacer un selfie comprometido y antes de enviarlo. Puede terminar circulando por la red.

Evita que otras personas tengan acceso a los datos y las comunicaciones de tu móvil, con el uso de contraseña seguras y…. secretas.

2.- Custodia con precaución la información que tengas en los dispositivos de almacenamiento externos que utilicemos, tales como pendrives, CD, DVD, disco duro externo, entre otros.
Es muy fácil acceder a ellos si los dejamos simplemente encima de la mesa, o guardado en un cajón. En situaciones de crisis o en situaciones evidentes de Violencia de Género, hay que tener en cuenta la posibilidad de que se lleven a cabo actos de Ciberdelincuencia de Género, como acceder a los datos personales, difundirlos, etc. Por ello, NO OLVIDES ALEJAR LA INFORMACIÓN PERSONAL Y SENSIBLE DEL POSIBLE AGRESOR. Elige un lugar seguro para su custodia, como, por ejemplo, el domicilio de un familiar en quién confíes plenamente.

Por ello es conveniente cifrar o proteger con alguna contraseña la información.

3.- Haz copias de seguridad.

Por si acaso falla tu seguridad, es importante que diariamente hagas backups o copias de seguridad. Es muy útil que tus datos relevantes estén en otro disco, alejado del posible agresor, o en servicios en la nube.

En cuanto a tu software, también puede ser atacado y es importante que hagas una copia de respaldo.

Si el contenido de tu comunicación por mail o redes sociales puede ser relevante como prueba, o por otro motivo, haz copias de seguridad del mismo.

Tanto respecto del software como respecto del contenido de tu comunicación por mail o redes sociales puedes encontrar en Internet tutoriales para llevarlo a cabo. Recuerda que es importante que las copias de seguridad estén cifradas y con contraseña. Lógicamente no deben conocer tus contraseñas nadie más que tú.

4.- Cuidado con los adjuntos en tu correo.

Si no conoces al remitente, no lo abras. Si conoces al remitente pero tiene aspecto sospechoso, no lo abras antes de confirmar el envío.

NO ABRAS UN CORREO DE DESCONOCIDO SIN ANTIVIRUS QUE LO ANALICE. ANALIZA TODOS LOS ARCHIVOS ADJUNTOS.

5.- Actualiza el software de tu sistema periódicamente.

Es importante tener nuestras aplicaciones y sistema operativo actualizados porque muchas de estas suelen deberse a vulnerabilidades encontradas. De esta forma si instalamos las actualizaciones no seremos vulnerables a esos fallos de seguridad encontrados – si están arregladas.

6.- Convierte tus contraseñas en seguras.

Para ello te aconsejamos:

• No uses contraseñas obvias: fechas importantes, apodos, número personales, etc.

Las contraseñas deben tener las siguientes características:

Uso de números, letras mayúsculas y minúsculas, símbolos y como mínimo 8 caracteres.

• Cambia la contraseña: por lo menos una vez cada 3 meses en todas tus cuentas,

¡Y DE INMEDIATO SI ESTÁS EN UNA SITUACIÓN DE CIBERDELINCIENCIA O EN RIESGO DE

SUFRIRLA!

• Utiliza diferentes contraseñas: para cada cuenta que crees.

• No apuntes tu contraseña en un papel.
¡No le des la contraseña a tu pareja!

7.- Usa antivirus y aplicaciones anti-malware.
Salvo que seas una especialista en seguridad informática, tus dispositivos serán más seguros si tienen antivirus activos que si no lo tienen.

Acuérdate: puedes recibir virus de tu expareja, compañero de trabajo, de estudios....

Usa al menos uno gratuito, por ejemplo, buscando en Internet por el concepto “antivirus gratuito”.

8.- Cierra las sesiones al terminar.
Si abres Facebook, Gmail o cualquier otro servicio, acostúmbrate a cerrar la sesión antes de levantarte de la silla para irte. Y no solamente si estás en un lugar público, también cuando lo haces desde el ordenador de una persona de tu confianza. Cada vez que te levantes del ordenador, cierra la sesión.

9.- Activa el Firewall de tu sistema.
Activa el cortafuegos que viene con tu sistema operativo para bloquear los accesos no autorizados.

10.- Lee cuidadosamente los correos bancarios, institucionales o de empresa, que piden información persona (por ejemplo un banco) porque pueden ser fraudes informáticos.

11.- Desconéctate de Internet cuando no lo necesites
Apaga tu punto de acceso a Internet cuando no lo utilices. Esto permitirá que no puedan conectarse un intruso a tus equipos por la red si lo hubiera.

12.- Protege tu red WiFi frente a intrusos
Una red WiFi abierta es algo peligroso, porque pueden realizar intrusiones en tus sistemas si consiguen acceder a tu red.

13.- Controla la privacidad de tus redes

En tus perfiles tal vez haya información personal que pueda usarse en tu contra (por ejemplo, para adivinar contraseñas o para engañarte emocionalmente).

Rechaza solicitudes de amistad sospechosas y configura bien la privacidad de Facebook y otras redes sociales.

14.- No compartas la "cuenta de usuario" con nadie, ni siquiera con tu pareja, tus hijas o hijos.

Si más de una persona va a usar un PC, crea diferentes cuentas, cada una protegida por una contraseña fuerte u otro sistema de identificación.

Si tienes hijas o hijos menores, haz que estén informados sobre los riesgos de Internet, y espera a que además de estar informados tengan madurez suficiente para gestionar las relaciones múltiples a través de Internet, antes de dejar de supervisar su cuenta, y sus comunicaciones.

Si compartes tu móvil puedes instalar App Lock para poner contraseñas a las aplicaciones, implementando una barrera más de seguridad e imposibilitando el acceso a terceras personas que conozcan tu contraseña de desbloqueo del móvil pero no de las aplicaciones protegidas.

15.- Bloquea tu móvil inteligente y tus ordenadores.

Están llenos de tus propias vivencias, de tu memoria. No es aconsejable que una persona, ni siquiera de tu confianza, pueda acceder a ellas sin tu consentimiento en cada ocasión.

16.- Enseña a tus hijos e hijas a usar Internet y los dispositivos electrónicos con seguridad.

Fórmate y ayúdales a formarse constantemente en Informática para no ser absorbidos por la ola tecnológica que avanza tan rápidamente.

17.- Si has tenido o tienes una relación muy controladora, es conveniente que un técnico o una técnica en seguridad informática valore el estado de tus dispositivos, por si tienes actualizado geolocalizadores, aplicaciones espías, etc.

FICHA Nº 5. PRUEBA ELECTRÓNICA

Cada vez es más importante en los procedimientos judiciales la prueba electrónica. Por eso, cuando se sufren ciberataques además de reflexionar sobre medidas para frenar los mismos, o medidas para proteger a la mujer, será necesario valorar la necesidad de recoger la prueba electrónica. ¡Cuidado, no suele ser una buena decisión eliminar los whatsapps, o mails…. o el móvil!

Puede ser muy útil para el posible procedimiento judicial y, en definitiva, para hacer visible la Ciberdelincuencia de Género y frenar al agresor, recopilar la siguiente prueba electrónica o relacionada con prueba electrónica:

- Capturas de pantalla de Facebook, Tuenti, Twitter y otras Redes.
- Mensajes de texto o sms.
- Conversaciones o chats de Wathsapp con contrario, o con testigos etc.
- Correos electrónicos.
- Grabaciones.
- Dispositivos, móviles antiguos, discos duros, pendrives, etc.
- Las comunicaciones entre el agresor y los hijos e hijas a través de Internet y las redes sociales, ya que con frecuencia se les usa para seguir controlando o dañando a la madre.
- Evidencias de intrusismo (como existencia de aplicaciones espía). Para ello probablemente tendrás que contar con la participación de un técnico o técnica de seguridad, al que es conveniente que le encargues la evaluación de los dispositivos y emisión de informe con ratificación en juicio.
- Testigos presenciales o de referencia de las fuentes de prueba. Además, es importante que identifiques a las personas que han podido participar en esa prueba electrónica (por ejemplo, una amiga a la que le enviaste un whatsapp contándole lo sucedido, o una fotografía con señales), ya que pueden intervenir como
testigo.

Además, te aconsejamos que tengas en cuenta lo siguiente:

- No se recomienda borrar las conversaciones de Chat, Redes sociales, mensajes de texto sms, o conversaciones de Wathsapp que nos puedan servir como prueba, mejor consultar con un técnico o técnica, puesto que:

Pueden recuperarse si no se han sobreescrito

Pueden recuperarse si no se han borrado permanentemente del sistema.

Pueden recuperarse si no están dañadas

Y en esos casos, al recuperarlas, se podrá proceder a autentificarlas por un Técnico Informático Forense para poder aportar dichas conversaciones al proceso judicial.

- No está limitado el soporte por cual se puede aportar una prueba a un procedimiento.

El diseño legal es muy amplio. Primero el Art. 299. 2 de la Ley de Enjuiciamiento Civil distingue dos grandes tipos de prueba tecnológica:

- Medios audiovisuales
- Instrumentos de Archivo o almacenamiento de datos (por ejemplo pendrives, cd, memoria disco duro...)

Pero a continuación el **art. 299** completa con su apartado tercero una amplitud de posibilidades, dado que expresa literalmente “cuando por cualquier otro medio no previsto expresamente en los apartados anteriores de este artículo pudiera obtenerse certeza sobre hechos relevantes, el tribunal a instancia de parte, lo admitirá como prueba, adoptando las medidas que en cada caso resulten necesarias”

Por tanto la Ley contempla amplias posibilidades de dar cabida a otros tipos de instrumentos o soportes tecnológicos que puedan ser utilizados como medio de prueba en un proceso para acreditar hechos relevantes. Se desarrolla además en los **artículos 382 a 384 L.E.C.**

- Pueden aportarse vídeos, y también pueden impugnarse.

Es muy frecuente hoy día la aportación de videos entre las partes, de los que, si están manipulados o se recortan fotogramas o partes del mismo, pueden derivarse consecuencias perniciosas para la defensa jurídica de la afectada/o.

Si constan hechos relevantes en la grabación audiovisual que afecten a la parte, y que se ha podido obtener con una cámara digital, ordenador, teléfono móvil y otros dispositivos, se pueden aportar al procedimiento con “los dictámenes (1) y pruebas instrumentales (2)” que considere pertinentes, **Art. 382.2 Ley de Enjuiciamiento Civil.**

(1) Sobre el Dictamen Pericial (informático) se habla más detalladamente en la Ficha nº 20.

(2) Medios instrumentales -acompañar la prueba de vídeo con testigos, interrogatorio de partes, o

documentos, por ejemplo, si lo que se aporta es una grabación de voz sin imágenes, se puede aportar acompañándola una fotografía.

Igualmente, si quién los presenta es la parte contraria, y para evitar que no se presenten en su integridad y puedan manipularse para conseguir sacar de contexto la grabación, es esencial impugnar dicha prueba con un dictamen pericial que discuta su autenticidad, exactitud, e integridad del contenido de la reproducción, y la cadena de custodia que se ha seguido en el dispositivo de almacenamiento hasta que se aportó al Juzgado o Tribunal.

Ficha Nº 6. SIGNOS DE ALARMA. DETECCIÓN.

A través de las TIC se pueden desarrollar muchas formas de Ciberdelincuencia de Género. Es importante saber detectar los signos de alarma para actuar con rapidez ante el **Ciberacoso**, la **Suplantación de Identidad**, la **Sextorsión**, el robo de datos para perjudicar económica o emocionalmente, etc. A continuación referimos los siguientes signos de alarma:

- Vigilar y expurgar los comentarios que hacen en las redes sociales de la pareja.
- Revisar las publicaciones y fotos de los amigos o amigas y utilizarlas para hacer reproches o cuestionar sus relaciones.
- Publicar las fotos de la mujer o incluir mensajes cariñosos sin el consentimiento de ésta con el fin de que sus contactos conozcan que mantienen una relación.
- Buscar en el perfil pruebas de engaño sobre distintos temas o sobre una supuesta infidelidad.
- Presionar para que den de baja de la lista de contactos a personas que no son de su agrado.
- Exigir que le incluya en sus redes sociales de todo tipo.
- Indicar que lo “normal” es que la pareja comparta las credenciales o contraseñas de todas las redes o cuentas de email, etc. O buscar la manera de obtener sus contraseñas para controlar los perfiles y leer sus mensajes.
- Exigir que elimine fotos concretas de su perfil porque no le gusta cómo te ve o la ropa que llevas.
- Si publican fotos donde aparecen con otros hombres, hostigar para que le explique quiénes son y dónde los conoció.
- Insistir o exigir para que se actualice o aclare su situación sentimental en su perfil de Facebook.
- Presionar para que lea los correos en su presencia.
- Amenazar con publicar fotos o información íntima en las redes sociales con el propósito de chantaje.
- Insistir para que le envíe fotos o videos comprometidos.
- Insistir para mantener relaciones sexuales mediante la webcam.
- Insistir para que la mujer haga algo que no quiere –por ejemplo un contacto sexual indicando que si no lo hace enseñará las imágenes comprometidas, o las difundirá por Internet.
- Recibir en el móvil llamadas o mensajes de personas desconocidas que pueden tener una información falsa o personal de la mujer.
- Recibir en el mail mensajes de personas desconocidas que pueden tener unas expectativas que no se corresponden con la realidad, o tener información falsa, o información privada de la mujer.
- Recibir personas cercanas a la mujer información sobre ella o datos personales, como fotografías, sin su consentimiento.
- Recibir reproches de familiares, amistades o personas cercanas, por conductas que no se han

realizado, por ejemplo, por haber enviado mensajes que no se han enviado.

- Difundirse rumores falsos y ofensivos a través de las redes sociales.
- Ver publicada información personal o sensible.
- Personas desconocidas acuden a su domicilio o lugar de trabajo, intentando contactar con la mujer.
- El agresor refiere información que solamente puede tener si ha accedido a los archivos del ordenador de la mujer, a sus comunicaciones por whatsapp, mail, etc.

Ficha Nº 7. “EVITANDO SER LOCALIZADAS”

Para las mujeres que precisan ser acogidas es especialmente importante evitar ser localizadas por el agresor o personas del entorno de éste. En la era de las TIC evitar la localización requiere una especial atención, por eso antes de ser acogidas recomendamos que se informen sobre las siguientes pautas básicas, sin perjuicio de las que se establecerán de manera concreta con cada usuaria en el Centro de Emergencia, Casa de Acogida o Piso Tutelado:

- No subir a las redes sociales fotografías que puedan dar pistas sobre la localización, y pedir que no las suban otras personas.
- Configurar las redes sociales de una manera segura (por ejemplo, sin usar el nombre o al menos no de forma completa) y reflexionar con el personal técnico del Centro sobre los contenidos seguros y los que no, pactando el uso de las redes.
- Desactivar la webcam (basta con colocarle una tirita encima).
- Desactivar el GPS y todo tipo de geolocalizadores de todos los dispositivos.
- ¡Que los hijos e hijas apliquen las mismas medidas!

No sirven de nada las anteriores pautas si los hijos e hijas de la afectada tienen dispositivos electrónicos con conexión a Internet y usan las redes sociales sin aplicar medidas de seguridad y específicas para evitar la localización.

FICHA Nº 8: PRIVACIDAD, PROTECCIÓN Y ACCESO A LOS DATOS.

Hay datos de carácter personal que revelan directamente información que expone nuestra esfera más íntima. Datos que están siendo continuamente tratados tanto en ficheros de empresas como TAMBIÉN en ficheros domésticos.

Nuestra imagen, nuestra propia representación como personas está expuesta al exterior.

Son especialmente vulnerables las y los menores y las personas con discapacidad.

Para recabar datos personales de menores de catorce años de edad, se requiere el consentimiento de los padres/ madres o tutores/ tutoras, según la normativa de protección de datos que veremos en las fichas correlativas. Y alguna referencia a que pueden obtener los datos relativos a sus hijos e hijas menores.

¿QUÉ ES EL DERECHO A LA PROTECCIÓN DE DATOS DE CÁRACTER PERSONAL?

El Derecho Fundamental a la Protección de Datos. Es el derecho a que las y los terceros no puedan tratar ni ceder nuestros datos sin nuestro consentimiento.

El Tribunal Constitucional lo considera también un Derecho fundamental autónomo, es el derecho a tener el control sobre nuestros datos, a la autodeterminación informativa.

También se ha desarrollado en una Ley orgánica, la Ley Orgánica de Protección de Datos de Carácter Personal, 15/1999, y su Reglamento de Desarrollo, R .Decreto n º1720/2007. **Esta normativa tiene múltiples aplicaciones en materia de protección de los derechos a que los datos se traten correctamente, por lo que es especialmente útil para preservar los derechos de la mujer ante empresas o instituciones públicas, y en servidores de Internet**, estando su ámbito de aplicación en el art. 2 de dicha Ley, en adelante LOPD.

DATOS PERSONALES ESPECIALMENTE PROTEGIDOS SEGÚN LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL.

- Ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.
- Nadie puede ser obligado/a a declarar sobre su ideología religión o creencias.
- Datos sobre salud, presente pasada o futura, tanto física como mental. Datos sobre porcentaje de discapacidad o información genética.

PROTECCIÓN PENAL. Título X del Código Penal, “Delitos contra la Intimidad, el Derecho a la propia Imagen y la inviolabilidad del domicilio”. Título XI “Delitos contra el Honor” Entre otros, sin ánimo exhaustivo, mencionar que de los Artículos 197 del Código Penal al 201 regulan la revelación de secretos.

Art. 248. 2º C. Penal, delitos de estafa cometidos a través de las Tecnologías o usando datos privados. El Art. 264 Código Penal regula el delito de daños informáticos o en los datos.

Procesales: Petición de Medidas cautelares del Art. 13 LECRIM en relación con el 544 Bis y Ter.

PROTECCIÓN CIVIL DEL DERECHO AL HONOR, PROPIA IMAGEN E INTIMIDAD PERSONAL Y FAMILIAR.

La Constitución en su art.18.1 garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. Se trata de derechos de la personalidad catalogadas como derechos fundamentales. Este precepto ha sido regulado por la LO 1/1982, de 5 mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen, que tiene por objeto la protección civil frente a las intromisiones consideradas ilegítimas, entendiendo por tales, todas aquellas que no estuviera expresamente autorizada
por la ley o consentida por el titular del derecho.

DERECHO DE FAMILIA. No nos olvidemos de la incidencia de las TIC en los procesos de ruptura de la pareja o matrimoniales, y medidas sobre visitas, custodia, en los que pueden darse y en la práctica se darán numerosas cuestiones relativas a las TIC, como por ejemplo:

- Asesoramiento para pactos en Convenios Reguladores de separación o divorcio relativos a uso de las TIC por hijos/as menores, uso de Internet y móviles inteligentes a partir de cierta edad, unificación de criterios publicación de fotografías y vídeos de las o los menores en Internet y similares por parte de progenitores y familia extensa.
- Posibilidad de que las y los progenitores estén en desacuerdo sobre uso de las TIC por las y los menores, y procesos o peticiones del Art. 156 o del 158 Código Civil en relación con situaciones de abuso en Internet o Redes en los que difieran ambas partes.
- Situaciones de Ilicitud de la prueba, pruebas obtenidas violando el derecho fundamental a la intimidad, como por ejemplo, el espionaje de los correos electrónicos y su aportación por la parte contraria. Impugnación de dichas pruebas tanto por su ilicitud como por su eficacia.

- Otras situaciones derivadas del cambio constante de las Tecnologías.

Todo ello sin perjuicio de procesos específicos de tipo legal que existan, o de otros cauces procesales que se vayan instaurando.

FICHA Nº 9: ALGUNAS PAUTAS INICIALES PARA PRESERVAR NUESTROS DATOS PERSONALES:

- Cambio periódico de claves o contraseñas en todas las comunicaciones, cuentas de correo electrónico, Redes sociales o aplicaciones.
- Creación de una cuenta de correo personal y nueva para contactar con Abogadas/os, psicólogas/os y otras/os profesionales que intervengan y que no haya riesgo de ser una cuenta de correo que tengan otras personas o de las que se pueda recuperar la contraseña.
- Posibles estrategias coordinadas con asesoramiento jurídico e informático o técnico.
- Control y protección de claves o credenciales y contraseñas para operar con compañías suministradoras de electricidad, agua, gas, seguros de hogar, tomar medidas para evitar que el contrario use dichas claves para causar un perjuicio económico, o bien con fines de control de las nuevas cuentas bancarias de la afectada, o su facturación y espionaje de otros datos por esta vía.
- No usar correos de la empresa o corporativos para enviar o tratar información sensible de carácter personal o privado.
- Protección de las aplicaciones del teléfono móvil –como las conversaciones de Whatsapp, galería de fotos, correo electrónico, Facebook, con contraseñas. Existen aplicaciones como AppsLock para ello.
- Otras medidas tecnológicas que preserven y guarden nuestra privacidad y vayan surgiendo. Para ello es importante el acceso a la formación.
- Adoptar medidas similares con respecto a los dispositivos y aplicaciones de nuestras hijas e hijos. Si ellas o ellos no preservan sus contraseñas, las comparten, o están al alcance de terceros fácilmente, se producen situaciones de vulnerabilidad de nuestros datos y privacidad de todo el grupo familiar.

FICHA Nº 10: SOBRE APORTACIÓN DE FOTOGRAFÍAS INTIMAS AL PROCESO JUDICIAL.

La incorporación de imágenes íntimas a los procedimientos judiciales suele ser algo que preocupa a las mujeres víctimas de Violencia de Género, especialmente en la modalidad de Ciberdelincuencia de Género. A continuación se refiere las normas de aplicación para conseguir que esa aportación en el Juzgado se lleve a cabo de manera reservada:

1.- La Constitución en su art.18.1 garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. Se trata de derechos de la personalidad catalogadas como derechos fundamentales. Este derecho ha sido regulado por la LO 1/1982, de 5 mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen, que tiene por objeto la protección civil frente a las intromisiones consideradas ilegítimas, entendiendo por tales, todas aquellas que no estuviera expresamente autorizada por la ley o consentida por el titular del derecho (art.2). Más en concreto, el art. 7 de la LO 1/1982 enumera las conductas que se consideran intromisiones ilegítimas entre las que destacan, por lo que aquí interesa, algunas muy concretas: la colocación en cualquier lugar de aparatos de escucha, de filmación de dispositivos ópticos o de cualquier otro medio apto para grabar o reproducir la vida óptima de las personas (aptdo.1); la captación, reproducción o publicación por fotografía, filme o cualquier otro procedimiento, de la imagen de una persona en lugares o momentos de su vida privada o fuera de ellos, salvo los casos previstos en el art.8.2 (aptdo.5).

2.- El artículo Art. 61 de la Ley Orgánica 1/24, de 28 de diciembre, sobre las medidas cautelares mantiene la posibilidad de adoptar, incluso de oficio, cualquier medida cautelar de protección que se considere necesaria.

3.- El Artículo 21 de Directivo 2012/29/UE, establece el derecho a la protección de la intimidad de las víctimas, indicando que "todos los estados miembros velarán porque durante el proceso penal las autoridades competentes puedan tomar las medidas adecuadas para proteger la intimidad, incluidas las características personales de las víctimas tenidas en cuenta en la evaluación individual contemplada en el artículo 22, así como las imágenes de las víctimas y de sus familiares."

Por ello, es aconsejable, si la víctima va a aportar imágenes íntimas a los procedimientos, que lo haga solicitando el carácter reservado de la misma, para que conste en el procedimiento en sobre cerrado, al que accederán exclusivamente las partes y el Tribunal.

FICHA Nº 11: DERECHO A LA INTIMIDAD EN EL TRABAJO.

El derecho a la intimidad de trabajadoras y trabajadores se reconoce en el Estatuto del Trabajador, art.18, donde al regular la inviolabilidad de la persona del trabajador/a en relación con los registros que puede practicar la o el empresario, señala que «se respetará al máximo la dignidad e intimidad del trabajador».

Sin embargo, los problemas más graves que se vienen produciendo en relación con la eventual vulneración del derecho a la intimidad de los trabajadores y las trabajadoras, tienen que ver con las facultades de dirección y control de la actividad laboral que el Estatuto del Trabajador en su art.20 reconoce a la o el empresario. En efecto, este artículo establece en su aptdo.3 que *«El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso».*

De ahí que debemos ser muy prudentes con los datos y contenidos que tratamos con medios informáticos de la empresa, y especialmente si da la casualidad de que la mujer es empleada de su agresor o en una empresa de éste.

FICHA Nº 12: LOS DERECHOS DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS:

- Los Artículos 15 a 17 LODP y 27 a 31 Reglamento, regulan los derechos de Acceso, Rectificación, Cancelación y Oposición, en adelante, los llamaremos los derechos A.R.C.O
- Derecho de Acceso.
- Derecho de Rectificación.
- Derecho de Cancelación
- Derecho de Oposición.

Otros derechos de la LOPD:

- Derecho a obtener una indemnización en caso de infracción en a que se vean afectados nuestros derechos ARCO.
- Derecho de información. La Agencia Española de Protección de Datos tiene un servicio gratuito de consultas telefónicas y en su Web.
- Derecho a la consulta en el Registro General de Protección de Datos. Se puede consultar pública y gratuitamente quién sea el titular de los ficheros para poder ejercer nuestros derechos ARCO frente al Responsable.
- Derecho a la impugnación de valoraciones.
- Derecho de ser excluidas/os de guías telefónicas
- Derecho a no recibir publicidad no deseada.

MENORES Y PROTECCIÓN DE DATOS:

Las y los menores de edad tienen los mismos derechos. Los y las menores de 14 años serán informados de los Derechos A.R.C.O representados por sus padres, madres o tutores y tutoras.

- No se puede recabar de las y los menores de edad datos que permitan obtener información de los demás miembros del grupo familiar, y esto debemos tenerlo en cuenta cuando se tratan datos de menores, por ejemplo, cuando se dan de alta en Tuenti o en otras Redes Sociales, debemos comprobar que se cumple esta
normativa y denunciar los abusos sobre privacidad en su caso.

- Hay que informar a las y los menores de sus derechos A.R.C.O, -lo cual se puede hacer directamente a partir de los 14 años- en términos comprensibles.

FICHA Nº 13: ¿CÓMO EJERCER LOS DERECHOS A.R.C.O?

- Los derechos que contempla la L.O.P.D. son independientes, es decir, se pueden ejercer todos o parte de ellos, de manera autónoma.

- Siempre debe poder permitirse su ejercicio de manera gratuita y sencilla.

- Basta realizar una comunicación del interesado o interesada titular de los datos a la persona responsable de los ficheros ya sea de titularidad pública o privada, si bien este derecho es independiente y no incompatible con los derechos de la Ley 30/1992 de 26 de noviembre sobre acceso a los datos incorporados a un expediente administrativo.
- El interesado o interesada, al dirigirse a la persona responsable de los ficheros para ejercer los derechos ARCO, debe acreditar su identidad con DNI o firma electrónica (sin perjuicio de aplicar también la normativa sobre comprobación de datos personales por parte de las Administraciones Públicas).

- La petición constará de un encabezamiento con los datos, nombre y apellidos de la titular o afectada o afectado, con una copia del DNI o firma electrónica, y la petición concreta de los datos, que pueden ser todos o parte de los que se traten por la persona responsable, a elección del interesado o interesada, indicando un domicilio a efectos de notificaciones o dirección para poder recibir la contestación. Terminar con la fecha y la firma.

FICHA Nº 14: USANDO LA LEY DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL PARA PROTEGENERNOS ANTE ABUSOS ECONÓMICOS:

- Solicitar a tenor de la LOPD que las claves de Internet de banca electrónica sean personales de cada titular, no el mismo para dos titulares de una cuenta bancaria, en su caso.

- Modificar por escrito la dirección donde recibir correspondencia de bancos y otras entidades. Por ejemplo, solicitar a la entidad bancaria la entrega en mano de la correspondencia o a una dirección postal no conocida por el contrario.

- Claves o credenciales y contraseñas para operar con compañías suministradoras de electricidad, agua, gas, tomar medidas para evitar que el contrario use dichas claves para domiciliar pagos en cuentas de la afectada de manera inconsentida.

- Realizar siempre estas peticiones por escrito y de manera que se pueda realizar luego la pertinente comprobación ante las entidades o empresas responsables de nuestros datos en estos casos.

FICHA Nº 15: ACCIONES LEGALES ANTE ABUSOS EN INTERNET. DISTINTAS OPCIONES.

Mediante una denuncia penal o querella de los hechos que en su caso sean constitutivos de algunos de los tipos previstos en el Código Penal. Por ejemplo, apoderarse de un vídeo privado y publicarlo, o amenazar con hacerlo, podría ser constitutivo de alguno de los tipos previstos en el Art. 197 Código Penal, que serían de aplicación preferente, solicitando al Juzgado la retirada de estos datos como medida cautelar al amparo del Art. 13 de la Ley de Enjuiciamiento Criminal solicitando que el Juzgado oficie al "Web Master" - (*) Web Master: Es la persona o empresa responsable de la gestión de una página Web y de los tratamientos de datos personales que se hagan en ella.

También se puede acudir a la normativa civil contenida en la Ley 5/1982, de Protección del derecho al Honor Intimidad personal y Familiar y Propia Imagen, solicitando medidas para restaurar estos derechos, incluso en favor de personas que hayan fallecido ya.

Igualmente la Ley 15/1999, esto es, la también ya mencionada Ley Orgánica de Protección de Datos de Carácter Personal, así como su Reglamento de desarrollo R.D 1720/2007, la que nos permitiría en su caso dirigirnos a Responsables de los distintos servicios, ya pertenezcan a ficheros públicos o privados, que existen en Internet. Para ello, usar los derechos A.R.C.O previstos en la Ficha nº 12 y 13, por ejemplo solicitar que se retire de una página web, blog, red social, Youtube, o que se impida el acceso ejerciendo los derechos de Oposición o cancelación de dichos datos personales dentro del ámbito de aplicación del art. 2 de la citada L.O.P.D. y concordantes.

Sin perjuicio de otros procesos específicos y órdenes jurisdiccionales como el Contencioso Administrativo en determinados casos.

FICHA Nº 16: OBLIGACIÓN DE CONSERVACION DE DATOS DE COMUNICACIONES ELECTRÓNICAS.

Existe la obligación de que los operadores públicos o privados conserven ciertos datos que permitan la investigación y localización de las comunicaciones o los equipos desde los que se realiza.

¿Cuánto tiempo se conservan estos datos? Estas obligaciones están reguladas en la **Ley 25/2007 de 18 de octubre sobre Conservación de Datos Relativos a las comunicaciones electrónicas y a las redes públicas decomunicaciones.** Según esta Ley, el plazo de conservación de datos genéricos según el art. 5 de dicha Ley es de 12 meses, en que se deben conservar los datos que permitan, entre otros, la identificación del número de teléfono de origen o destino, el IMEI, datos para la localización del equipo, o la etiqueta de localización geográfica en caso de servicio anónimo pre-pago.

Dicha Ley 25/2007, es plenamente compatible con lo dispuesto sobre conservación y bloqueo de datos en la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal.

FICHA Nº 17: ASESORAMIENTO SOBRE LA RE-DIFUSIÓN O RE-ENVÍO DE ALGUNOS VÍDEOS O CHATS, QUE NOS LLEGAN DE TERCERAS PERSONAS.

Difundir un vídeo vejando a una persona o agrediéndola, o comentarios ofensivos por redes sociales, retwittear estos contenidos, también puede constituir una infracción penal, aunque la o el que lo difunda no sea autor propiamente.

También es muy frecuente que por desconocimiento la propia víctima pueda llegar a cometer alguna infracción penal –retwittear contenidos ofensivos que han colgado otras personas o a veces incluso responder al agresor por este medio de manera, que le puede resultar contraproducente.

FICHA Nº 18: LA PRUEBA ELECTRÓNICA. PRIMEROS CONSEJOS PARA PRESERVARLA antes de su aportación procesal.

Vamos a enumerar algunos consejos para que las víctimas no intoxiquen las posibles pruebas desde la detección de una posible intrusión, robo de datos, acceso no autorizado, etc.

- En el momento de tener una posible prueba electrónica en un dispositivo móvil lo mejor es no utilizarlo. Debido a que el o la usuaria puede modificar o alterar las pruebas de tal manera que la prueba sea nula o imposible de obtenerla.

- Protegerlo en algún sitio controlado por la víctima para que no se produzca ninguna modificación, borrado o alteración de las pruebas por otras personas interesadas o no en esas posibles pruebas.

- Muchos móviles inteligentes tienen una memoria externa a través de una micro SD donde quedan registrados y guardados muchos archivos y datos. Seguramente en él se puede encontrar la prueba que posteriormente quiera analizar la víctima por ello es importante protegerlo y no perderlo.

- Las aplicaciones de chats normalmente al borrar una conversación o parcialmente una conversación mandan una instrucción al sistema para que éste lo sobre-escriba. Puede tardar horas, meses y años hasta que realmente se realice la escritura encima de esta conversación que contiene amenazas, insultos o algún tipo de prueba. Por eso es importarte dejar de usar la aplicación afectada o incluso el dispositivo en su totalidad.

- Los sistemas operativos tienen un registro de accesos y eventos que pueden ser una evidencia clara de accesos no autorizados por ello es importante no realizar modificaciones o alteraciones en el sistema que puedan comprometer estos registros.

- En el caso de recibir llamadas donde su contenido (voz) quiera ser una prueba documental debemos instalar una aplicación que grabe estas conversaciones (existen una gran cantidad de aplicaciones que realizan estas labores. Los archivos multimedia deben estar protegidos y guardados por ejemplo en la nube. Es importante no perder el móvil que realizo la acción para luego usar el registro de llamadas como prueba junto a la conversación presentada.

- Es importe que contacten con un o una experta en seguridad informática especialista en análisis

forenses de móviles para que pueda aconsejarle sobre la investigación y en su caso autenficación, ya que puede interesar realizar diferentes intervenciones.

Consejos específicos en la cadena de custodia en ordenadores personales:

- El primer consejo es que no se apague nunca el ordenador en el momento de que la o el usuario detecte una incidencia o una intrusión. Debido a que en la memoria RAM que tiene la característica de ser volátil (por ello no apagarse) puede encontrarse pruebas. Por ejemplo si está recibiendo una intrusión en su sistema informático no los apagues y rápidamente llame a la policía o a una técnica/o en seguridad informática.

- La información en un ordenador se guarda en el disco duro. Si desconoces cómo extraerlo para proceder a protegerlo es mejor no tocarlo hasta contactar con la o el perito o experta/o informática/o.

- De todas las evidencias informáticas se puede hacer una captura de pantalla (botón localizado normalmente en la barra superior del teclado a la derecha “ImpPnt PetSis”), por ejemplo, para dejar constancia de un insulto que recibió la víctima por correo, las redes sociales, etc.

FICHA Nº 19: APORTACIÓN PROCESAL, Y REPRODUCCIÓN EN JUICIO.

ART. 26 del Código Penal expresa que documento es:
«Todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria»·

A modo de ejemplo, y sin ánimo de ser un listado cerrado, hemos hablado de los distintos tipos que figuran en la Ficha nº 5.

Es conveniente su aportación en fase inicial del proceso para evitar impugnación por indefensión de la parte contraria, y en el proceso judicial cumplir los preceptos que regulan el momento de preclusión para presentarlos.

Procurar que el tipo de archivo de sonido, imagen, software usado, etc se conozca en el Juzgado para poder disponerlo y que se pueda proceder a la reproducción.

En todo momento el documento debe estar bajo la custodia del Secretario o Secretaria Judicial, el cual será el encargado, normalmente previa petición de alguna de las partes, de llevar a cabo las transcripciones y cotejos que sean necesarios.
Es importante pedir la reproducción en la Vista de la grabación o video, para lo cual debe pedirse la asistencia del Secretario o Secretaria Judicial.

FICHA Nº 20: LA APORTACIÓN DEL INFORME PERICIAL TÉCNICO EN CASOS DE CIBERDELINCUENCIA DE GÉNERO.

El Informe Pericial elaborado por un técnico o técnica de seguridad informática, debe aportarse siempre que vayan a volcarse al procedimiento los medios de prueba contemplados en la Ficha nº 5 y la nº 19.
El peritaje informático en líneas generales, consiste en:

- Obtener de manera lícita la prueba, y custodiarla.

- Realizar las operaciones periciales y técnicas necesarias confirmar el resultado y comprobar la indemnidad del proceso de llevar la fuente de prueba al soporte - pendrive, cd, dvd, software, disco externo, etc- que será considerado el “MEDIO DE PRUEBA”.

- Autentificar las conversaciones de chat, whatsapp, sms, y otras ya mencionadas en la Ficha nº 5.

- Emitir un Informe Pericial, y ratifica la información técnica que confirma que la prueba no ha sido alterada en el Juzgado.

Existe la posibilidad de nombrar Perito (en este caso con conocimientos en informática y en concreto en Seguridad Informática y de los datos) a cargo de la Justicia Gratuita, ya que figura regulado en la **Ley de Asistencia Jurídica Gratuita en su artículo 6.**

El artículo 339 de la Ley de Enjuiciamiento Civil, establece:

1. Si cualquiera de las partes fuese titular del derecho de asistencia jurídica gratuita, no tendrá que aportar con la demanda o la contestación el dictamen pericial, sino simplemente anunciarlo, a los efectos de que se proceda a la designación judicial de perito, conforme a lo que se establece en la Ley de Asistencia Jurídica Gratuita.

JUNTA DE ANDALUCIA
Instituto Andaluz de la Mujer
CONSEJERÍA DE IGUALDAD Y POLÍTICAS SOCIALES