ADOLESCENCIA Y VIOLENCIA DIGITAL

Carolina Álvarez Aceituno.
Abogada. LegalTech

Álvarez Aceituno
Abogados

ÍNDICE:

- Delitos de Violencia Digital que afectan a los adolescentes. El impacto social y tratamiento legal. Cómo funciona la Inteligencia Artificial en los dispositivos y nuestros hogares.
- Importancia de las Pruebas Digitales.

Álvarez Aceituno Abogados

LA VIOLENCIA DIGITAL. TRATAMIENTO TÉCNICO

La violencia digital es aquella agresión que se sufre a través de medios digitales o telemáticos. Esta es la distinción con otro tipo de violencia, el medio, pero no debemos olvidar que se trata de una agresión, cuyas consecuencias pueden suponer daños psicológicos importantes

https://www.youtube.com/watch?v=_dTUGgq615g

Álvarez Aceituno Abogados

REDES SOCIALES, ¿Por qué les gusta tanto?

- Pueden compartir de forma fácil e inmediata imágenes y vídeos (tanto permanentes, como temporales que solo duran unos minutos u horas visibles para el resto de miembros de la red).

- Es fácil añadir filtros, efectos, pegatinas (stickers), emojis, gifs y música a sus imágenes, vídeos y mensajes.

- Se puede etiquetar a distintas personas, y temáticas (#hashtags) en sus publicaciones.

- Les permiten reafirmar su popularidad social mediante el número de “me gusta” y seguidores que obtienen, comprobando así la aceptación que tienen frente a los demás.

Álvarez Aceituno Abogados

¿¿COMO LAS UTILIZAN??

PERFILES PÚBLICOS VS PRIVADOS

Por defecto, todas las cuentas en redes sociales se crean de manera pública, aunque hay menores que las convierten en privadas para limitar su exposición únicamente a sus contactos. Esta es la elección más segura, ya que nadie podrá seguir sus publicaciones a menos que el menor apruebe su solicitud.

¡PRECAUCIÓN! Aunque sus publicaciones solo lleguen a sus seguidores en privado, estos podrían hacerlas públicas. Siempre deben desconfiar a la hora de exponer sus datos personales.

Álvarez Aceituno Abogados

MUCHOS MENORES PREFIEREN EXPRESARSE CON IMÁGENES • Selfies, fotos de grupo, bailes, bromas… Las redes sociales permiten editar fotos y vídeos, aplicar filtros y efectos decorativos, e incorporar emoticonos, gifs animados y pegatinas (stickers) en los mensajes de texto.

• Cuando salen varias personas en una foto, o se mencionan en un mensaje, las etiquetan para que todas ellas puedan verlo. Sin embargo, a veces etiquetan a personas que no aparecen para llamar su atención.

• Cada vez pasan más tiempo en las redes sociales, hay una presión social por estar al día, responder al momento, o publicar imágenes perfectas. Por eso es conveniente hablar de las redes sociales en familia, reforzar su autoestima y pensamiento crítico.

Álvarez Aceituno Abogados

¡RECUERDA! Desde la distancia que les ofrece la pantalla, pueden tener cierta sensación de anonimato o seguridad, mostrándose más desinhibidos para compartir mensajes o imágenes de mayor riesgo, o menos respetuosos con los demás. Sin embargo, detrás de la pantalla siempre hay otra persona, y todo lo que se hace en Internet perdura.

Álvarez Aceituno Abogados

¿Cómo se financia una red social?

- Publicidad personalizada: cada usuario ve anuncios que encajan con sus intereses, siendo anuncios más dirigidos, relevantes y con mayores probabilidades de éxito.
- Segmentación de perfiles: pueden vender el acceso a los datos de sus usuarios para realizar acciones de marketing, estudios de mercado, electorales, etc.
- Publicidad encubierta: a menudo se comparten imágenes o vídeos de personas particulares o influencers, con intención comercial, pero sin identificar como publicidad.

Álvarez Aceituno Abogados

QUE RIESGOS PUEDEN AFECTAR A LOS MENORES

• Suplantación de identidad: otra persona podría utilizar sus imágenes y datos personales para crear un perfil falso, y actuar en su nombre.

• Grooming: conocer demasiados detalles de su vida privada, facilita que un adulto pueda hacerse pasar por un menor que comparte sus intereses, y se gane su confianza. De este modo puede manipularle y pedirle imágenes o vídeos íntimos con los que chantajearle.

• Ciberacoso: el acoso escolar puede reproducirse en el entorno digital, a través de comentarios y publicaciones negativas o humillantes hacia una persona. Dar me gusta, compartir las burlas o simplemente no denunciarlas es convertirse en cómplices.

• Uso excesivo: sin unos límites de tiempo equilibrados, pueden aparecer síntomas de dependencia que perjudiquen su desarrollo físico, social y educativo.

Álvarez Aceituno Abogados

Algunos consejos para la correcta utilización:

- Establecer el perfil como privado.
- Limitar la visibilidad de sus publicaciones solo a sus contactos.
- Limitar la recepción de mensajes y comentarios solo a sus contactos.
- Limitar las búsquedas dentro y fuera de la red social.
- Evitar la recepción de publicidad personalizada.

Álvarez Aceituno Abogados

Principales recomendaciones I

1. Utilizar **contraseñas seguras** y no compartirlas.

2. **Proteger** nuestro smartphone, tablets… con **patrones de seguridad**.

3. **Revisar los permisos que solicitan las aplicaciones** que instalamos en nuestro smartphone.

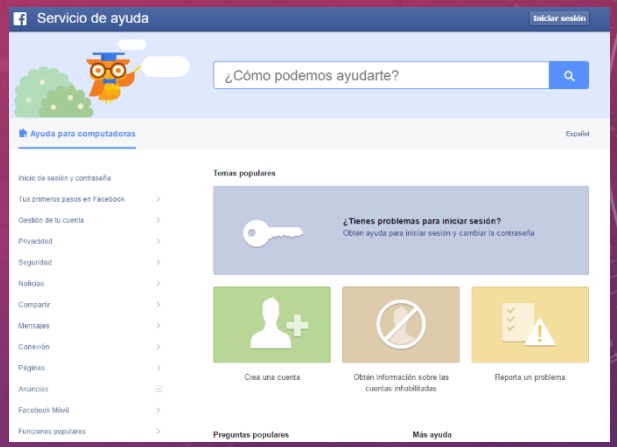
Álvarez Aceituno Abogados

Principales recomendaciones II

4. Informarse sobre las **condiciones y políticas de privacidad** antes de crear un perfil en una red social.

5. Configurar adecuadamente las **opciones de privacidad** del perfil de la red social.

6. **Revisar periódicamente** las opciones de privacidad.



Álvarez Aceituno Abogados

Principales recomendaciones

7. **Conectarse a páginas seguras** para **transacciones importantes** o informaciones sensibles.

8. **Valorar** cuando tener activado **servicios** como la **geolocalización**.

9. No publicar excesiva información personal: “**piensa antes de publicar**”.

Álvarez Aceituno Abogados

CONTRASEÑAS (PASSWORDS)

- **Una contraseña segura es tu primera línea de defensa contra cualquier intruso**

- **Por ello se convierte en uno de los mayores puntos críticos en nuestra seguridad en la Red.**

Álvarez Aceituno Abogados

CONTRASEÑAS (PASSWORDS)

- **No reveles jamás tu contraseña a nadie.**
- **No utilices la misma contraseña para sitios web distintos**
- **Crea contraseñas que sean fáciles de recordar pero que resulten difíciles de adivinar a los demás.**

Álvarez Aceituno Abogados

CONTRASEÑAS (PASSWORDS)

Por ejemplo, imaginemos una frase como “**T**erminé **d**e **e**studiar **e**n **e**l **c**olegio **e**n **2004**”

y usa las iniciales de cada palabra de este modo:

“Tdeeece2004”

Refranes, Canciones, Versos de Poemas, …

Álvarez Aceituno Abogados

CONTRASEÑAS (PASSWORDS)

- **Crea contraseñas que tengan al menos 8 caracteres**

- **Incluye números, mayúsculas y símbolos**

  RODMA SOLUTIONS → R0DM4 $07UT10N$

- **Usar un gestor de contraseñas**

  RoboForm (para Windows solamente)

  Lastpass (para Windows y Mac)

Álvarez Aceituno Abogados

CONTRASEÑAS (PASSWORDS)

- **Tener en cuenta los ataques de *phishing***

  Aunque parezca proceder de un sitio legítimo (entidades bancarias, correos, supermercados, etc…), ***hacer click en un vínculo*** que te pida iniciar sesión, cambiar la contraseña o proporcionar cualquier tipo de información personal, ***puede ser la "puerta"*** para que un ciberdelincuente se apodere de nuestros datos.

Álvarez Aceituno Abogados

CONTRASEÑAS (PASSWORDS)

- **Estudia la posibilidad de usar una contraseña también en el teléfono móvil y un antivirus, como por ejemplo el Conan Mobile (gratuito)**

Álvarez Aceituno Abogados

RECOMENDACIONES AL UTILIZAR UNA WIFI “GRATUITA”

- Debemos ***usar un Firewall*** (programa que bloquea acceso externo no autorizado a nuestras computadoras). Hay muchos *firewalls* gratuitos, como por ejemplo :

  ZoneAlarm

  Comodo Personal Firewall

  Si no queréis uno podéis usar el que viene incluido con su Windows

Álvarez Aceituno Abogados

RECOMENDACIONES AL UTILIZAR UNA WIFI “GRATUITA”

- ***Apagar el wifi cuando no lo estemos usando***, jamás conectarnos a una red pública y dejar nuestro dispositivo encendido y conectado vía wifi, siempre nos desconectaremos (*smartphones, tablets,* etc.) o apagaremos (ordenadores portátiles, etc.).

Álvarez Aceituno Abogados

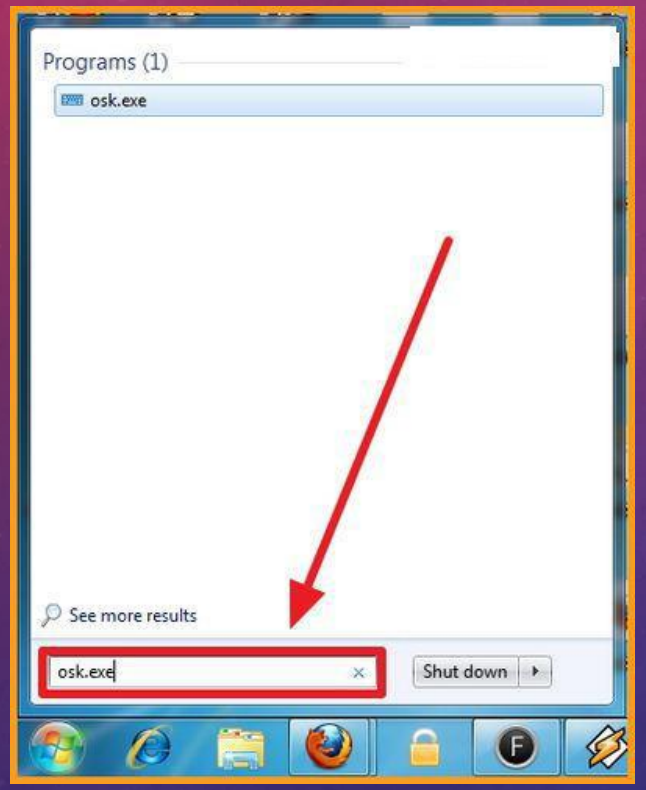
RECOMENDACIONES AL UTILIZAR UNA WIFI “GRATUITA”

- **No “trasmitir” información que no nos interese que otros vean, como transacciones** bancarias, accesos a webs o servicios que pudieran verse comprometidos.

- Cuando escribamos nuestras contraseñas o información “sensible”, utilicemos el **teclado “virtual” en pantalla.**

Álvarez Aceituno Abogados

RECOMENDACIONES AL UTILIZAR UNA WIFI “GRATUITA”



Álvarez Aceituno Abogados

RECOMENDACIONES AL UTILIZAR UNA WIFI “GRATUITA”

- Si no nos queda más remedio que realizar una transacción conectados a una wifi pública, **al menos asegurémonos que la página donde estamos haciendo la operación use el protocolo SSL.**
- Busca el icono con forma de candado a la izquierda de la URL del sitio en la barra de dirección para ver si el sitio usa **SSL**.

Álvarez Aceituno Abogados

RECOMENDACIONES AL UTILIZAR UNA WIFI “GRATUITA”

SSL es un protocolo que proporciona un túnel encriptado entre tu ordenador y el sitio que estás viendo. Los sitios pueden usar SSL para evitar que terceros interfieran con la información que viaja por el túnel.

Álvarez Aceituno Abogados

IDENTIDAD DIGITAL.-

CREANDO UNA BUENA IDENTIDAD DIGITAL Cada publicación, ya sea una imagen, un vídeo o un comentario, genera un impacto en las personas que lo ven. En conjunto van a construir una imagen pública que los menores deben cuidar, siendo conscientes de su repercusión en el futuro.

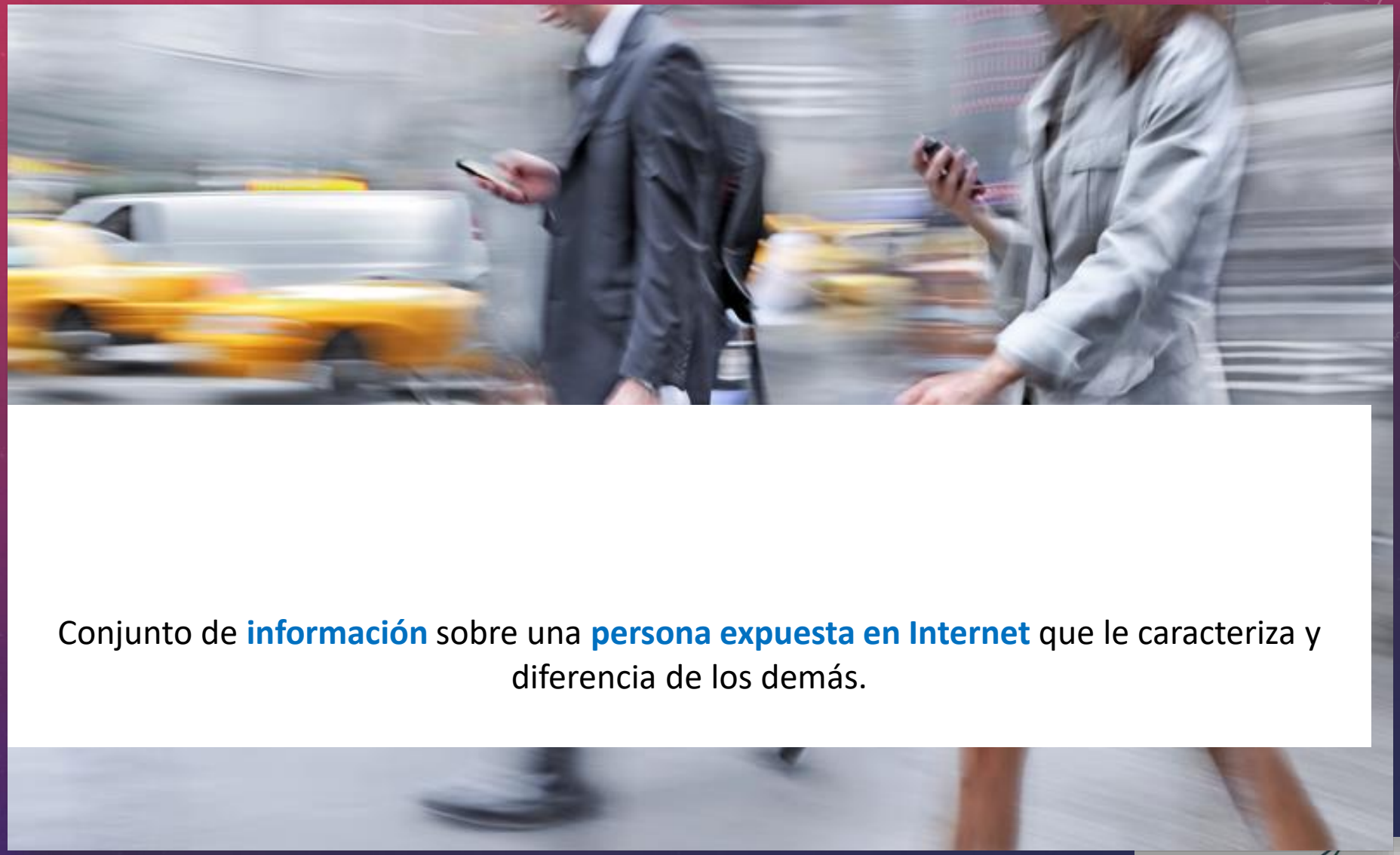
Publicar con responsabilidad, respetándose a sí mismos y a los demás, es la clave.

Antes de compartir una foto de otra persona, han de pedirle permiso. Si luego cambia de idea, han de respetar su decisión y eliminarla.

Álvarez Aceituno Abogados

Implica conocer las peculiaridades del medio de comunicación que utilizamos

Álvarez Aceituno Abogados

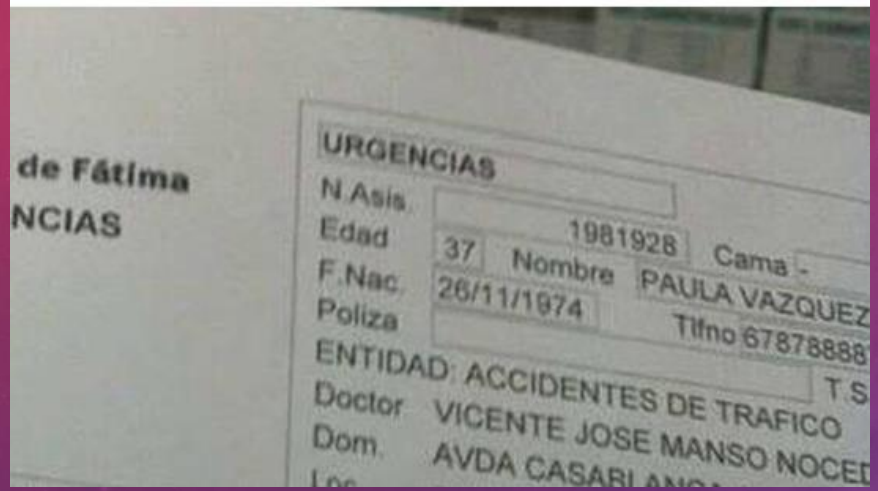


Conjunto de **información** sobre una **persona expuesta en Internet** que le caracteriza y diferencia de los demás.

Álvarez Aceituno Abogados

La presentadora ferrolana es una activa tuitera, con meteduras de pata tan célebres como la publicación de su teléfono en un tuit

A. / SANTIAGO
ía 26/11/2012 - 01.13h



SOCIEDAD

Detienen a un ladrón que se dejó abierto su Facebook en la casa que entró a robar

EP / MINNEAPOLIS | Día 26/06/2014 - 12.52h

Álvarez Aceituno Abogados

¿Qué pasa si alguien vulnera nuestra privacidad? ¿Puede ser un delito?

- **Reenviar por WhatsApp una foto o vídeo** de un compañero que alguien te ha enviado **sin su consentimiento**.
- **Acceder a la cuenta de Twitter** de un compañero que se ha dejado la **sesión abierta**.

Detectan un agujero de seguridad en 12 millones de routers

Imagen alegórica de la vulnerabilidad 'Misfortune Cookie'. (CHECKPOINT)

- Esta vulnerabilidad podría ser usada para tomar el control de los routers que no estén especialmente protegidos, como los de los hogares o las pymes.

Descubren un fallo en Facebook que permitía acceder a cualquier cuenta

Un 'hacker' de 22 años ha descubierto cómo pudo ver datos y mensajes privados de usuarios debido a una vulnerabilidad en la versión beta de la red social.

Detectan un fallo de seguridad en WhatsApp para iPhone que permite acceder a los chats ajenos

Descubren un fallo de seguridad que podría afectar al 95 por ciento de los usuarios de Android

Esta vulnerabilidad del sistema operativo de Google permitiría a un tercero tomar el control del móvil a través de un simple mensaje multimedia

Alvarez Aceituno Abogados

¿Qué pasaría si alguien te buscara por Internet?

Álvarez Aceituno Abogados

LA VIOLENCIA DIGITAL. LA INTELIGENCIA ARTIFICIAL EN EL HOGAR Y LOS DISPOSITIVOS

https://www.bbvaopenmind.com/tecnologia/inteligencia-artificial/10-ejemplos-de-que-ya-dependes-de-la-ia-en-tu-vida-diaria/

https://www.elespanol.com/ciencia/tecnologia/20181024/inteligencia-artificial-crea-hogares-comodos-seguros/347715787_0.html

Álvarez Aceituno Abogados

IA en nuestra vida cotidiana: ejemplos…

¿Quién… elige los resultados de tus búsquedas? - Google

¿Quién… elige tus lecturas favoritas? - Amazon

¿Quién… elige tus películas y tu música? – Netflix y Spotify

¿Quién… elige tus vacaciones? - eDreams

¿Quién… te busca casa? – Idealista

¿Quién… te concede la hipoteca? – Marvin (Bankia) y otros

¿Quién… te busca trabajo? - LinkedIn

¿Quién… te busca pareja? - Meetic

¿Quién… influencia (o incluso decide) tu voto? - Facebook

Álvarez Aceituno Abogados

IA: ¿Dónde están los límites técnico-jurídicos?...

ABC REDES

España ▾ Internacional Economía ▾ Sociedad Madrid ▾ Familia ▾ Opinión ▾ Deportes ▾ Gente ▾ Cultura ▾ Ciencia Historia Viajar ▾

ABC TECNOLOGÍA REDES Móviles Electrónica Redes Videojuegos

No te creas lo que ves: no es Mark Zuckerberg, «fake» creado con inteligencia artificial

- A estos vídeos manipulados se los conoce como «deepfake» por las técnicas que se utilizan para desa un resultado extremadamente realista

Publicidad

C/ de

Ed Vel ie

ABC TECNOLOGÍA

@abc_tecnologia

Actualizado: 16/06/2019 01:29h

1

Álvarez Aceituno Abogados

VIVIMOS CADA VEZ MÁS DIGITALIZADOS Y DEBIDO A ELLO LAS MEDIDAS DE SEGURIDAD SE HACEN CADA VEZ MÁS NECESARIAS.

Limitar horarios de uso

Dónde utilizar los dispositivos

Criterio de edades para la utilización

Acompañamiento de los adultos

Reglas del juego de utilización

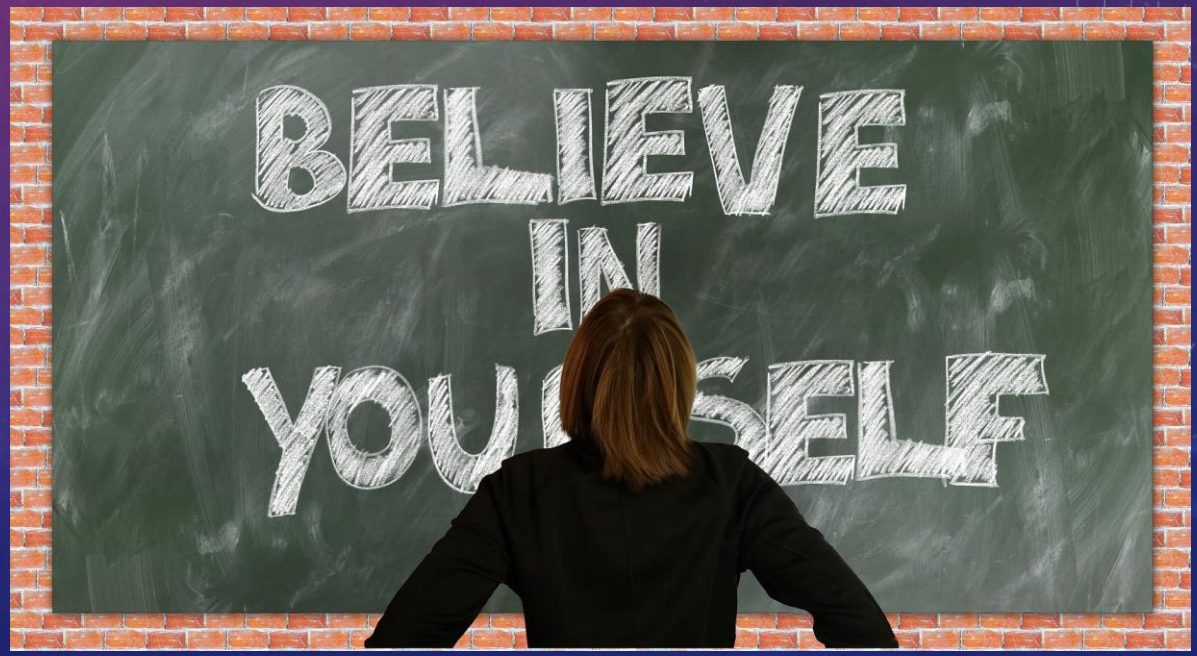
Dispositivos guardados y apagados por la noche

Máximo importe facturas

Educación familiar en sentimientos y emociones

RECOMENDACIONES

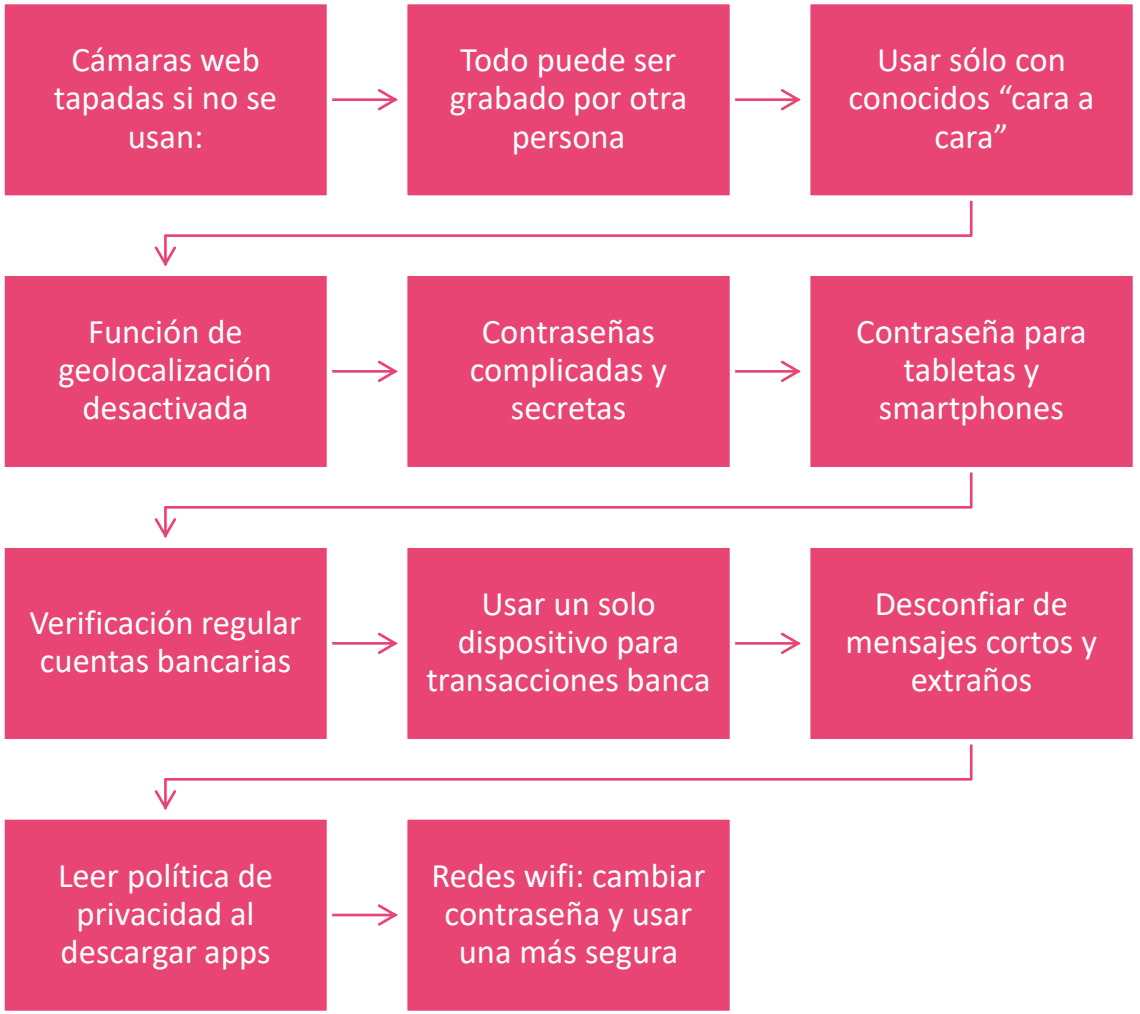
- Educación en derecho y respeto a la víctima
- Educación en aspectos técnicos
- Concepto de delito
- Niveles adecuados de comunicación intrafamiliar
- Derecho a la intimidad de los menores
- Riesgos publicación y envío fotografías
- Autorización menores para publicar fotos
- Riesgos citas a ciegas



ESQUEMA DE LO QUE DEBEMOS CONOCER:

1. Actualización regular sistema operativo
2. Actualización navegador y uso de extensiones
3. Instalación sistemas de filtrado de contenidos
4. Utilización de antivirus y firewall con licencia
5. Amenaza software malicioso
6. No confianza ciega en las aplicaciones instaladas
7. Instalación en smartphone o tablet:
8. Instalación ante permisos numerosos o innecesarios
9. Descarga sólo de sitios oficiales

BUENAS PRÁCTICAS:



ANOMALÍAS EN EL USO DE LOS MEDIOS TECNOLÓGICOS:

- Ciberacoso
- Grooming
- Sexting. Riesgos:
  - Pérdida privacidad
  - Antesala acoso sexual o grooming
  - Material de difusión de redes pornografía infantil
  - Reenvío imágenes alumnos mismo centro -> ciberbullying
- Violencia de género a través de las tic
- Acceso a contenidos ilegales o inadecuados

ALGUNOS DATOS SOBRE VIOLENCIA DE GÉNERO Y ADOLESCENTES.-

Censurar las fotos que cuelgas, mandarte mensajes insultantes, vigilar tu ubicación… todo esto no es amor, es **cibercontrol** y **violencia de género digital**.

Un 38,3% de las mujeres entre 16 y 24 años ha sufrido violencia psicológica de control por parte de su pareja. A esto se añade el uso masivo del móvil e Internet, lo que ha convertido la violencia de género digital en adolescentes en un gran tema de preocupación.

De hecho, según los datos de la **Delegación del Gobierno para la Violencia de Género**, más del 25% de las chicas en España reconocen haber sufrido algún tipo de control o violencia por esa vía.

Según explica Carmen Ruiz Repullo, socióloga cordobesa, en su investigación **'Voces tras los datos'**, existen tres aspectos que son la raíz de la violencia de género: **el machismo**, **la masculinidad hegemónica** y **el amor romántico**.

Las formas más comunes de violencia de género digital en adolescentes son:

Acosar o **controlar a la pareja con el móvil**.

Interferir en relaciones que tiene la pareja con otras personas en Internet.

Espiar el móvil de la pareja.

Censurar fotos que la pareja publica y comparte en redes sociales.

Controlar lo que hace la pareja en las **redes sociales**.

Exigir a la pareja que conocer dónde está en todo momento con la **geolocalización**.

Obligar a la pareja a que envíe **imágenes íntimas**.

Comprometer a la pareja para que te **facilite sus claves personales**.

Obligar a la pareja a que **muestre lo mensajes** de un chat con otra persona.

Mostrar enfado por no **tener siempre una respuesta inmediata online**.

NO TIENES DERECHO A

UTILIZAR EL MÓVIL
PARA CONTROLAR
CON QUIÉN ANDA,
DÓNDE ESTÁ
O CÓMO SE VISTE

MANDARLE MENSAJES DESPECTIVOS,
HIRIENTES
O QUE SUPONGAN
UN CHANTAJE

PEDIRLE SU CONTRASEÑA
O COTILLEAR SU MÓVIL.
NO ES CUESTIÓN
DE CONFIANZA,
ES UN ABUSO.

#JóvenesConRespeto
#NoLeControles

900 116 117
Línea de ayuda
EN CIBERSEGURIDAD

incibe_
is4k INTERNET SEGURA FORKIDS

Cofinanciado por la Unión Europea
Mecanismo «Conectar Europa»

GOBIERNO DE ESPAÑA MINISTERIO DE ECONOMÍA Y EMPRESA

incibe_

is4k INTERNET SEGURA FORKiDS

Cofinanciado por la Unión Europea
Mecanismo «Conectar Europa»

NO TIENES DERECHO A MANDARLE MENSAJES DESPECTIVOS, HIRIENTES O QUE SUPONGAN UN CHANTAJE

#JóvenesConRespeto
#NoLeControles

GOBIERNO DE ESPAÑA · MINISTERIO DE ECONOMÍA Y EMPRESA

incibe_

is4k INTERNET SEGURA FORKIDS

Cofinanciado por la Unión Europea
Mecanismo «Conectar Europa»

GOBIERNO DE ESPAÑA MINISTERIO DE ECONOMÍA Y EMPRESA
incibe_
is4k INTERNET SEGURA FORKiDS
Cofinanciado por la Unión Europea
Mecanismo «Conectar Europa»

STALKING:

- ART. 172.TER.- (…) el que acose a una persona llevando a cabo de forma insistente y reiterada, y sin estar legítimamente autorizado, alguna de las conductas siguientes y, de este modo, altere gravemente el desarrollo de su vida cotidiana:

- 1.ª La vigile, la persiga o busque su cercanía física.
- 2.ª Establezca o intente establecer contacto con ella a través de cualquier medio de comunicación, o por medio de terceras personas.
- 3.ª Mediante el uso indebido de sus datos personales, adquiera productos o mercancías, o contrate servicios, o haga que terceras personas se pongan en contacto con ella.
- 4.ª Atente contra su libertad o contra su patrimonio, o contra la libertad o patrimonio de otra persona próxima a ella.
- Si se trata de una persona especialmente vulnerable por razón de su edad, enfermedad o situación, se impondrá la pena de prisión de seis meses a dos años.

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

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

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

En la actualidad gran parte del stalking se ha desplazado a las redes sociales, (delito ciberintrusivo) donde el acechador vigilia, comenta o llega incluso a hackear la cuenta de la víctima con el fin de conocer cualquier cambio en su vida diaria.

El Stalker.-

- Stalker resentido: el fin principal de sus conductas de stalking es asustar y afligir a la víctima debido a un sentimiento de rencor y resentimiento hacia ella, por cualquiera que sea el motivo.
- Stalker depredador: En este caso el acechador espía a su víctima, generalmente con fines de índole sexual, hasta que encuentra el momento adecuado para atacarla.
- Stalker rechazado: este acosador acecha con intenciones vengativas o con el fin de retomar una relación (amorosa, laboral, amistosa, etc) que la víctima ha roto.
- Stalker pretendiente ineficaz: este tipo de acechador suele tener poca capacidad de comunicación y de relación con otras personas y entiende de forma equivocada el hecho de compartir gustos, actividades o aficiones con la víctima, hasta llegar al punto de obsesionarse con ella.
- Stalker deseoso de intimidad: La obsesión por una relación amorosa e íntima con la víctima es la principal motivación de este tipo de stalker, que ve en la otra persona el alma gemela que siempre ha buscado aunque no tenga una relación estrecha ni profunda con ella.

LAS CONDUCTAS QUE EN LA PÁGINA WEB PÁGINA WEB HTTP://WWW.VICTIMSOFCRIME.ORG EN «STALKING RESOURCE CENTER» SE DESCRIBEN, EN EL DERECHO ANGLOSAJÓN, COMO INTEGRANTES DEL DELITO DE STALKING SON LAS SIGUIENTES:

1.- Perseguir a la víctima y aparecer en cualquier lugar.

2.- Enviar regalos no deseados, cartas, tarjetas, o correos electrónicos.

3.- Dañar su casa, automóvil u otros bienes.

4.- Controlar sus llamadas telefónicas o el uso del ordenador.

5.- Utilice la tecnología, como cámaras ocultas o sistemas de posicionamiento global (GPS), para seguir a donde vaya.

6.- Conduzca por o pasar el rato en su casa, escuela o trabajo.

7.- Amenaza con hacerle daño a usted, su familia, amigos o mascotas.

8.- Averiguar sobre la víctima mediante el uso de los registros públicos o los servicios de búsqueda en línea, la contratación de investigadores, pasando por su basura, o ponerse en contacto con amigos, familiares, vecinos o compañeros de trabajo.

9.- Publicar información o propagar rumores sobre usted en Internet, en un lugar público, o por el boca a boca.

10.- Otras acciones que controlen, la pista, o asustan.

CONVENIO DE BUDAPEST.- CIBERCRIMINALIDAD.- NOVIEMBRE DE 2001. RATIFICADO POR ESPAÑA 17 DE SEPTIEMBRE DE 2010.

Clasificación de delitos informáticos:

- Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos. Art 197, 264.2 CP
- Abuso de dispositivos para cometer delitos
- Robo o interceptación de datos de terceros
- Acceso de manera no legal

Delitos Informáticos. Art. 248 CP; 255; 256CP

- Alteración fraudulenta de datos, es decir borrado, falsificación, supresión, etc…

Delitos que tengan que ver con el contenido. Art. 186 y 189 CP

- Producción, oferta, difusión, etc de contenidos delictivos

Delitos contra la propiedad intelectual. Art. 270 y 276 CP

- Piratería en general

ESQUEMA DEL CONVENIO DE BUDAPEST:

El convenio se estructuras en tres ejes o bloques de materias.-

1.- En el primer eje se aborda el tema de los delitos informáticos, y tiene como objetivo establecer un catálogo de figuras dedicadas a penar las modalidades de criminalidad informática.

2.-En el segundo eje se abarcan las normas procesales: aquí se establecen los procedimientos para salvaguardar la evidencia digital, así como también las herramientas relacionadas con la manipulación de esta evidencia. El alcance de esta sección va más allá de los delitos definidos en el punto anterior, ya que aplica a cualquier delito cometido por un medio informático o cualquier tipo de evidencia en formato electrónico. Entre otras cosas determina la obtención y conservación de datos digitales para ser utilizados como pruebas.

3.- El último eje contiene las normas de cooperación internacional, que son reglas de cooperación para investigar cualquier delito que involucre evidencia digital, ya sean delitos tradicionales o informáticos. Incluye, entre otras, disposiciones acerca de la localización de sospechosos, recolección o envío de evidencia digital, e incluso lo referente a extradición.

ESPECIAL MENCIÓN DEL CONVENIO BUDAPEST A LAS EVIDENCIAS DIGITALES.-

- La **evidencia digital** es volátil e intangible, es decir, puede desaparecer o ser alterada muy rápido, por lo que las investigaciones que involucran este tipo de pruebas deben ser rápidas y precisas. Para esto, se requiere un proceso penal ágil y eficiente, con esfuerzo organizado por parte de los países. En este capítulo se establece la red 24×7, un punto de contacto que debe funcionar las 24 horas, los 7 días a la semana y asegurar una rápida asistencia entre las partes.

- Entre los deberes que debe realizar el país una vez adherido al convenio, se destacan por un lado, la designación de un punto de contacto para la red 24×7 (según define el artículo 35 del convenio) con el fin de proveer apoyo y cooperación de forma rápida y efectiva, y por el otro lado, un proceso de adecuación de normas y legislación al convenio de Budapest.

- PRUEBA DIGITAL EN EL PROCESO JUDICIAL ESPAÑOL.-
- Han de aportarse en su formato original.
- Indicar el dispositivo del que proceden.
- Ha de transcribirse el texto, y debe constar: cabecera de los mensajes o los propios mensajes consecutivos para acreditar la veracidad.
- Podemos solicitar certificación de los prestadores de servicios.
- Podemos protocolizar notarialmente el mensaje o la comunicación electrónica
- Solicitar un dictamen pericial (Art. 335 y SS LEC) acredita sobre todo lo autenticidad de la misma.

- # VALORACIÓN DE LA PRUEBA.-
- A).- Mensajería instantánea.- Se conservan en los dispositivos implicados en la transmisión, archivos de la nube o carpetas locales. Si hay duda de su alteración o manipulación hay que acudir a las copias de seguridad de los prestadores de servicios.
- B).- Mensaje por SMS.- Se acredita su veracidad con la certificación que ofrece la empresa prestadora del servicio.
- C).- Correo Electrónico.- Los servidores conservan copias de los mensajes. Los prestadores de servicios acreditan la existencia y la veracidad de la comunicación.-
- D).- Redes Sociales.- Pueden haber sido borrados, pero los prestadores de servicios conservan la mayoría de los contenidos publicados en sus redes. En todas las ocasiones requerirá autorización judicial si la prueba es sobre un tercero.

- NOTA.- Podemos solicitar a los prestadores de servicios que preserven información sensible de poder desaparecer para posteriormente ser utilizada, siempre con autorización judicial

Reformas legislativas Código Penal Incorporación del Concepto Género:

LEY ORGÁNICA 10/1995 DE 23 DE DICIEMBRE DEL CODIGO PENAL.-

1. Se incorpora el género como motivo de discriminación en la agravante 4ª del artículo 22 CP.

ARTICULO FUE MODIFICADO por la LO 5/2010, de 22 de junio, por la que se MODIFICA la LO 10/95 de 23 de noviembre del CP.

1. Incluir cometer el delito por razón de discriminación por razón de "identidad sexual".

NUEVAMENTE MODIFICADO por la actual reforma del CP por LO 1/2015:

La Agravante del art. 22.4CP queda redactada de la siguiente manera:

Cometer el delito por motivos racistas, antisemitas y otra clase de discriminación referente a la ideología, religión o creencias de la víctima, la etnia, raza o nación a la que pertenezca, su sexo, orientación o identidad sexual, razones de género, la enfermedad que padezca o su discapacidad".

Desaparece la falta de injurias leves en la violencia de género y se convierte en delito leve.

“En el ámbito de violencia de género, a fin de dotar de un nivel de protección más elevado a las víctimas, cuando las injurias o vejaciones se cometan sobre alguna de las personas a que se refiere el art. 173.2 CP, esta conducta será un delito leve de injurias o vejaciones injustas previsto y penado en el número 4 del art. 173 que sanciona el que causare injuria o vejación injusta de carácter leve, cuando el ofendido fuera una de las personas a las que se refiere el apartado 2 del artículo 173.”

Se añade al art. 468 CP, que regula los quebrantamientos, el apartado 3º.

Regula la manipulación de los dispositivos de telemáticos de seguimiento y control, también conocidos como “Pulsera electrónica”. Estaba planteando problemas de conceptualización jurídica.

COMPORTAMIENTOS A EVITAR EN LA UTILIZACIÓN DE MEDIOS DIGITALES:

1. Acosar o controlar a tu pareja usando el móvil
2. 2. Interferir en relaciones de tu pareja en Internet con otras personas
3. 3. Espiar el móvil de tu pareja
4. 4. Censurar fotos que tu pareja publica y comparte en redes sociales
5. 5. Controlar lo que hace tu pareja en las redes sociales
6. 6. Exigir a tu pareja que demuestre dónde está con su geolocalización
7. 7. Obligar a tu pareja a que te envíe imágenes íntimas
8. 8. Comprometer a tu pareja para que te facilite sus claves personales
9. 9. Obligar a tu pareja a que te muestre un chat con otra persona
10. 10. Mostrar enfado por no tener siempre una respuesta inmediata

RESPONSABILIDAD DE LOS PROGENITORES:

- Esta vendrá determinada por el juez. Puede ser:
  - Responsabilidad sólo de los padres o sólo del centro educativo.
  - Responsabilidad compartida entre ambos.

- El amparo legal de la responsabilidad de los progenitores será:
  - Art, 154 CC; Art. 1902CC y Art. 1903 CC.-
  - Art. 61 de la Ley de Responsabilidad Penal del menor atribuye responsabilidad Solidaria a los guardadores de hecho, incluido el centro educativo. La acción será ejercita por le Ministerio Fiscal, y habrá tantas piezas separadas por responsabilidad civil como hechos.

- Si los hechos cometidos son por un menor de 18 años, responden solidariamente con él de los daños y perjuicios causados sus padres, tutores, acogedores y guardadores legales o de hecho. El Juez moderará la responsabilidad de éstos según su intervención dolosa o no en los hechos.

Álvarez Aceituno Abogados

LEGISLACIÓN APLICABLE A LOS DELITOS CON MENORES:

- Los menores y los delitos en internet:
- Además de la ya mencionada de Ley Orgánica 5/2000 de 12 de enero que regula la responsabilidad de los menores, los mayores de 14 años pueden incurrir en los siguientes delitos aunque no lo hagan de manera consciente:
- Ataques al derecho a la intimidad: delito de descubrimiento y revelación de secretos mediante apoderamiento y difusión de datos reservados registrados en ficheros o soportes informáticos (artículos 197-201 del Código Penal).
- Amenazas y coacciones:
  - Amenazas realizadas por cualquier medio de comunicación (artículo 169 y siguientes del Código Penal).
  - Coacciones: artículo 172 del Código Penal.
  - Trato degradante: delito contra la integridad moral (artículo 173 del Código Penal).
- Calumnias e injurias:
  - Calumnia: delito hecho con conocimiento de su falsedad o temerario desprecio hacia la verdad (artículo 205 del Código Penal)
  - Injurias: acciones o expresiones que lesionan la dignidad de otra persona, menoscabando su fama atentando contra su propia estimación, delito contra el honor (artículo 208 del Código Penal).

Álvarez Aceituno Abogados

LEGISLACIÓN APLICABLE: CONTINUACIÓN:

- <u>Responsabilidad civil en los casos de acoso escolar:</u>
  - Se tomarán acciones de responsabilidad civil para reparar los daños físicos o morales en situaciones de acoso en el ámbito educativo (acciones de alumnos o por negligencia o inacción del centro educativo):
    - Artículo 1902 del Código Civil determina que "El que por acción u omisión causa daño a otro, interviniendo culpa o negligencia, está obligado a reparar el daño causado".
    - El artículo 1903 del CC regula la responsabilidad de los garantes de la integridad física de los menores y deben poner los medios para que los daños no se produzcan y, de producirse, responderán por las consecuencias de los mismos. Prescribe: "La obligación que impone el artículo 1902 es exigible no solo por los actos u omisiones propios, sino por los de aquellas personas de quienes se debe responder".
    - El art. 1903 determina las personas y entidades responsables en función de quien tenga la custodia del alumno /s acosador/es y establece que “Los padres son responsables de los daños causados por los hijos que se encuentren bajo su guarda”. Además: “Las personas o entidades que sean titulares de un Centro docente de enseñanza no superior responderán por los daños y perjuicios que causen sus alumnos menores de edad durante los períodos de tiempo en que los mismos se hallen bajo el control o vigilancia del profesorado del Centro, desarrollando actividades escolares o extraescolares y complementarias”
  - En el caso de que las personas mencionadas prueben que emplearon toda diligencia de un buen padre de familia para prevenir el daño, no existirá responsabilidad civil.

Álvarez Aceituno Abogados

DELITOS DE VIOLENCIA DIGITAL
PROCEDIMIENTO PARA MENORES DE 14 AÑOS Y RESPONSABILIDADES

- No hay ningún tipo específico relativo al ciberbullying u otro tipo de violencia ejercida en la red, por lo que los delitos se encuadrarán como delitos más genéricos tales como delito contra la integridad moral, delito contra la libertad y contra el honor.
- Las penas aplicables serán distintas en función de la edad de quien comete el delito
- Cuando el autor es menor de 18 años, se aplica la Ley Orgánica 5/2000 de 12 de enero, reguladora de la responsabilidad civil de los menores:
- Si es menor de 14 años, el artículo 3 de dicha ley dispone que "no se le exigirá responsabilidad con arreglo a la presente Ley, sino que se le aplicará lo dispuesto en las normas sobre protección de menores previstas en el Código Civil y demás disposiciones vigentes“
- Además, el artículo 61.3 de dicha LO establece que “Cuando el responsable de los hechos cometidos sea un menor de dieciocho años, responderán solidariamente con él de los daños y perjuicios causados sus padres, tutores, acogedores y guardadores legales o de hecho, por este orden. Cuando éstos no hubieren favorecido la conducta del menor con dolo o negligencia grave, su responsabilidad podrá ser moderada por el Juez según los casos”

Álvarez Aceituno Abogados

DELITOS DE VIOLENCIA DIGITAL PROCEDIMIENTO PARA MAYORES DE 14 AÑOS Y RESPONSABILIDADES

- Si el menor es mayor de 14 años el artículo 1 de Ley Orgánica 5/2000 de 12 de enero estipula que “Esta ley se aplicará para exigir la responsabilidad de las personas mayores de catorce años y menores de dieciocho por la comisión de hechos tipificados como delitos en el Código Penal o las leyes penales especiales”.

- En cuanto a las responsabilidades, serán las mismas que para las menores de 14 años: el artículo 61.3 de la LO establece que “Cuando el responsable de los hechos cometidos sea un menor de dieciocho años, responderán solidariamente con él de los daños y perjuicios causados sus padres, tutores, acogedores y guardadores legales o de hecho, por este orden. Cuando éstos no hubieren favorecido la conducta del menor con dolo o negligencia grave, su responsabilidad podrá ser moderada por el Juez según los casos”

Álvarez Aceituno Abogados

DELITOS DE VIOLENCIA DIGITAL

a) “Acoso”: el delito. Art. 173 C.P.

1. El que infligiera a otra persona un trato degradante, menoscabando gravemente su integridad moral, será castigado con la pena de prisión de seis meses a dos años.

b) Acoso sexual: Artículo 184. C.P.

1. El que solicitare favores de naturaleza sexual, para sí o para un tercero, en el ámbito de una relación laboral, docente o de prestación de servicios, continuada o habitual, y con tal comportamiento provocare a la víctima una situación objetiva y gravemente intimidatoria, hostil o humillante, será castigado, como autor de acoso sexual, con la pena de prisión de tres a cinco meses o multa de seis a 10 meses.

2. Si el culpable de acoso sexual hubiera cometido el hecho prevaliéndose de una situación de superioridad laboral, docente o jerárquica, o con el anuncio expreso o tácito de causar a la víctima un mal relacionado con las legítimas expectativas que aquélla pueda tener en el ámbito de la indicada relación, la pena será de prisión de cinco a siete meses o multa de diez a catorce meses.

3. Cuando la víctima sea especialmente vulnerable, por razón de su edad, enfermedad o situación, la pena será de prisión de cinco a siete meses o multa de diez a catorce meses en los supuestos previstos en el apartado 1, y de prisión de seis meses a un año en los supuestos previstos en el apartado 2 de este artículo

Álvarez Aceituno Abogados

DELITOS DE VIOLENCIA DIGITAL

c) Delitos contra la intimidad:

“Revelación de secretos” – Art. 197 C.P.

197.2.: prisión de uno a cuatro años y multa de doce a veinticuatro meses “al que sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado”.

“Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores”.

“Cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o un incapaz, se impondrán las penas previstas en su mitad superior”.

Álvarez Aceituno Abogados

DELITOS DE VIOLENCIA DIGITAL

d) Delitos contra el honor:

“Injurias” recogida en los Artículos. 208 y siguientes del C.P.

“Injuria”: “acción o expresión que lesionan la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación”.

e) Delitos contra las personas:

En relación al tema que tratamos podemos considerar dos tipos:

– “lesiones” (Art. 147 C.P.)

– “vejaciones” (Art. 620 C.P.)

“Lesión”: aquella que menoscabe la integridad corporal o la salud física o mental a otro/a, y que será castigada como reo del delito de lesión.

“Vejaciones”: pena de multa de diez a veinte días los que causen a otro una amenaza, coacción, injuria o vejación injusta de carácter leve, salvo que el hecho sea constitutivo de delito.

Álvarez Aceituno Abogados

DELITOS DE VIOLENCIA DIGITAL

Otros delitos conexos que podrían relacionarse con los anteriores son:

– Calumnias.

– Estafa.

– Delitos de opinión.

– Tortura o daños contra la integridad moral.

– Inducción al suicidio.

– Usurpación de la identidad

En estos momentos, el anteproyecto de Código Penal pretende mediante la incorporación de nuevos tipos, llenar los vacíos detectados, para evitar dejar sin castigar aquellas actuaciones que no encontraban acomodo en los tipos existentes hasta el momento:

Álvarez Aceituno Abogados

DELITOS DE VIOLENCIA DIGITAL

– ACOSO a las mujeres a través del uso indebido de datos para atentar contra su libertad o patrimonio que será castigado con hasta dos años de cárcel.(Art. 172 ter C.P.))

– ACCESO SIN AUTORIZACIÓN, EN CONTRA DE LA VOLUNTAD DE QUIEN TENGA EL LEGÍTIMO DERECHO A EXCLUIRLO Y VULNERANDO LAS MEDIDAS DE SEGURIDAD EXISTENTES PARA IMPEDIR DICHO ACCESO a datos o programas informáticos contenidos en sistemas informáticos, que será castigado con una pena de hasta dos años de prisión.(Art. 197.3 C.P.)

– DIFUSIÓN DE IMÁGENES ÍNTIMAS, pues será castigado con hasta un año de prisión la difusión no autorizada de imágenes o grabaciones íntimas obtenidas con consentimiento de la víctima pero sin autorización para su difusión. (Art. 197.4 C.P.)

– Agravamiento de las penas establecidas en los apartados 1 a 4 bis del Art.197 en su mitad superior, cuando existan INTERESES LUCRATIVOS. En el caso de que el ACCESO ILÍCITO A LA INTIMIDAD AJENA, LLEVADO A CABO CON FINES LUCRATIVOS, AFECTASE A DATOS DE CARÁCTER PERSONAL QUE REVELEN LA IDEOLOGÍA, RELIGIÓN, CREENCIAS, SALUD, ORIGEN RACIAL O VIDA SEXUAL, O LA VÍCTIMA FUERE UN MENOR DE EDAD O UN INCAPAZ, la pena a imponer será la de prisión de cuatro a siete años.

Álvarez Aceituno Abogados

USO EXCESIVO DE LAS TIC:

Al igual que otros hábitos excesivos, se caracteriza por:

Intenso deseo, ansia o necesidad incontrolable de estar conectado cada vez durante más tiempo a Internet o a los videojuegos para sentir el mismo bienestar que antes. Este hecho se denomina tolerancia.

Aparición del llamado síndrome de abstinencia: el menor siente malestar e irritabilidad ante la ausencia de contacto o conexión con las TIC.

Negación del problema, cuando las personas allegadas como la familia, dándose cuenta del problema, advierten al menor y éste suele responder negando el problema que padece y poniéndose a la defensiva.

Dependencia de la acción placentera, que se une a la tolerancia y el síndrome de abstinencia. Cuando el menor necesita la gratificación instantánea y aprobación social por parte de otros usuarios de Internet con los que interactúa.

Pérdida o descuido de los intereses y las actividades habituales previas, tanto las escolares como las personales.

COMUNIDADES PELIGROSAS:

Las comunidades peligrosas suelen disfrazar su actividad de fondo a través de otras aparentemente inocentes. No suelen estar localizadas, sino más bien dispersas a través de diferentes redes sociales, foros y webs, y se configuran frecuentemente como grupos privados, por lo que resultan difíciles de controlar. Además, el contacto con ellas puede darse también a través de canales de mensajería instantánea, chats de juegos online, etc.

Los jóvenes más vulnerables ante las comunidades peligrosas en línea suelen presentar una serie de aspectos en su perfil que son tomados como referencia por los grupos con ánimo de captar a menores:

Suelen ser adolescentes introvertidos, con baja autoestima o enfadados frente a aquellos conflictos con familiares o compañeros que no son capaces de gestionar.

Se refugian en las redes sociales buscando reconocimiento o evitando, precisamente, la presión social que encuentran en la vida real. Esto, junto con el propio proceso natural de la adolescencia, interfiere en la toma de decisiones razonadas y éticas.

En ocasiones son jóvenes con escasas habilidades o un bajo criterio y capacidad emocional para reaccionar frente a las agresiones. La falta de sociabilidad, la timidez y la tendencia al conformismo ahondan en ello.

Para hacer frente a estas comunidades, las redes sociales cada vez más están incorporando mecanismos de control de eventos o grupos peligrosos. Al tiempo que se activan, también son burlados con cierta facilidad, mediante la suplantación de perfiles o la creación de otros ficticios cuya apariencia resulta normal e inocente.

MIS FUENTES DE INSPIRACIÓN.-

WWW.elderecho.es

www.madrid.org

www.pantallasamigas.net

www.interior.gob.es Plan Director CNP para la convivencia y mejora de la seguridad en los centros educativos y su entorno

www.incibe.es

www.is4K.es

https://www.aepd.es/

“LAS TECNOLOGÍAS NOS AYUDAN A MEJORAR NUESTRAS VIDAS. EDUCANDO EN EL RESPETO Y LA CONVIVENCIA , NO SERÁN ARMAS PELIGROSAS, SINO HERRAMIENTAS QUE NOS AYUDAN A EVOLUCIONAR.”

- Gracias por vuestra asistencia.
  - Carolina Álvarez Aceituno. Abogada.
  - Ca.alvarezaceituno@icam.es
  - www.alvarezaceitunoabogados.es

Álvarez Aceituno Abogados