Ciber Corresponsales

plataforma de infancia españa

GOBIERNO DE ESPAÑA · MINISTERIO DE SANIDAD Y POLITICA SOCIAL

POR SOLIDARIDAD OTROS FINES DE INTERÉS SOCIAL

APUNTES PARA LA FORMACIÓN

Seguridad online

CONTENIDOS

>> Políticas, medidas y procedimientos de seguridad en Cibercorresponsales.

>> Los contenidos nocivos e ilícitos.

>> La protección de datos personales.

>> Los contactos indeseados y la suplantación de identidad.

>> La protección de los derechos de autor.

>> Las prácticas dañinas o ilícitas.

>> Consejos para la navegación segura en Internet.

AUTOR

OSCAR BELMONTE

Unicef Comité Español

Objetivos de este módulo

>> Que conozcan las políticas y medidas de seguridad de Cibercorresponsales.

>> Que conozcan el marco legal básico para la moderación de contenidos.

>> Que conozcan el marco legal básico para la dinamización de la participación en la comunidad virtual.

>> Que conozcan el marco legal básico referente a la protección de datos personales.

>> Que conozcan las medidas de protección de frente a los contactos indeseados y la suplantación de identidad.

>> Que conozcan y estén sensibilizados de los principales riesgos en Internet para la infancia.

Políticas, medidas y procedimientos de seguridad en Cibercorresponsales

Las medidas de seguridad de Cibercorresponsales están recogidas en el Documento de Seguridad que está publicado en la comunidad virtual y es accesible a los dinamizadores/as. Ese documento es periódicamente revisado y modificado como consecuencia de los trabajos permanentes de mejora de la seguridad, de calidad, de las auditorías de seguridad o de la investigación de incidentes. Cada vez que se publique una nueva versión se notificará a todos y todas los dinamizadores/as. No debe confundirse ese documento con el presente manual, más centrado en proporcionar un marco general para la contextualización de los problemas de seguridad propios de Internet en lo referente a comunidades virtuales adolescentes.

El documento de seguridad que puede encontrarse en la web está estructurado en políticas, medidas y procedimientos. Las políticas son epígrafes genéricos que tratan de abordar de forma global una problemática o de hacer frente a una amenaza potencial. Actualmente las **políticas de seguridad** de Cibercorresponsales son:

- Acceso, registro y protección de datos personales
- Protección frente al contenido nocivo e ilícito
- Contra el spam
- Protección y conservación del contenido y derechos de autoría
- Frente a la suplantación de personalidad
- Frente a los contactos indeseados
- Frente a compras y descargas
- Frente a acciones ilícitas o dañinas en la comunidad virtual

Las medidas detallan la forma de hacer frente a un riesgo y contribuyen en mayor o menor medida a la seguridad de la comunidad de Cibercorresponsales. La seguridad de un sistema de información nunca radica en una medida de seguridad aislada sino en un **conjunto de medidas interdependientes**.

Los procedimientos establecen la forma de hacer determinadas cosas de una forma segura; por ejemplo, registrar usuarios y usuarias, dimanizadores, editar datos personales, etc. Los procedimientos descritos en el documento de seguridad son de obligado cumpli-miento. Si consideras que un procedimiento no se adapta a tus necesidades o es mejorable, comuníca-noslo, no te lo saltes. Recuerda que debes **comunicar** siempre cualquier incidencia de seguridad, así como cualquier mejora o sugerencia que consideres oportuna.

Los contenidos nocivos o ilicitos

Al enfrentarnos a la moderación de los contenidos debemos distinguir entre:

- **contenidos ilícitos,** aquellos no están permitidos legalmente.
- **contenidos nocivos**, son aquellos que aunque están permitidos legalmente, se consideran dañinos para el desarrollo de las personas menores de edad.
- **contenidos falsos**.

La noción de contenido ilícito y nocivo en Internet no es muy uniforme, ya que hay que atender a conceptos éticos y jurídicos que pueden ser variables para cada territorio o para cada persona.
Con respecto a los contenidos ilícitos, aunque existen diferencias en las relación a la normativa legal de cada país, existe un cierto consenso internacional en relación a ciertas conductas entre las cuales destacan la apología al terrorismo, la pornografía infantil, la provocación o incitación al odio de una raza, etnia o grupo, la difamación en Internet claramente maliciosa y la distribución de material que viola la dignidad humana. La publicación de este tipo de contenidos está estrictamente prohibida y en estos casos caben muy pocas consideraciones en torno a la libertad de expresión.
Salvo casos tan fragrantes, la realidad es que frecuentemente la consideración de un contenido como ilícito dependerá en muchos casos de la resolución un **conflicto entre la libertad de expresión y otros derechos**. Estos conflictos suelen ser de difícil interpretación y resolución en términos legales. A conti-nuación vamos a intentar acercarnos a las bases legales relacionadas con la publicación de contenidos.

LA LIBERTAD DE EXPRESIÓN

La Declaración de Derechos Humanos afirma en su artículo 19 que:
"Todo individuo tiene derecho a la libertad de opinión y expresión, este derecho incluye el no ser molestado a causa de sus opiniones; el de investigar y recibir informaciones y opiniones; y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión."

El Comité de Derechos Humanos ha recordado en diversas ocasiones que los niños y niñas gozan de todos los derechos civiles y lamenta que continúen prevaleciendo prácticas donde no se reconocen estos derechos basándose en que los niños al no haber alcanzado la madurez no tienen la necesaria capacidad o competencia para ejercerlos. Al incorporar claramente los derechos civiles a la Convención de los Derechos del Niño se hace una declaración indiscutible de su derecho y capacidad para gozar plenamente de estas libertades fundamentales. La Convención de los Derechos del Niño estable en su artículo 13 que:
"El niño tendrá derecho a la libertad de expresión; ese derecho incluirán la libertad de buscar, recibir y difundir informaciones e ideas de todo tipo, sin consideración de fronteras, ya sea oralmente, por escrito o impresas, en forma artística o por cualquier otro medio elegido por el niño."

A su vez, el Comité de los Derechos del Niño también se ha expresado repetidamente preocupado por la insuficiente atención que se presta a la promoción de los derechos y libertades civiles del niño:
"En cuanto al derecho del niño a expresar sus opiniones (art. 12) y el derecho a la libertad de expresión (art. 13), al Comité le preocupan las actitudes dominantes en la familia, la escuela y otras instituciones así como en la sociedad, que obstaculizan el disfrute de esos derechos."

Tal y como nos recomienda el Comité debemos impedir que en nuestras decisiones al frente de nuestro grupo de cibercorresponsales prime el hecho de pensar que los niños y niñas no tienen la madurez necesaria para el ejercicio del derecho de expresión frente a su propio **derecho de expresarse**.
Hay que tener en cuenta que el derecho a la libertad de expresión está íntimamente ligado con el derecho a expresar libremente su opinión y a que esta sea te-

nida en cuenta art. 12, con el derecho a la libertad de pensamiento, de conciencia y de religión art. 14, con el derecho a la libertad de asociación art. 15, con el derecho a la protección de la vida privada art. 16 y con el derecho de acceso a la información art. 17.

También debemos tener en cuenta que el derecho a la libertad de expresión incluye en su propia definición:
- el derecho de no ser molestado o molestada a causa de sus opiniones;
- el derecho de investigar y recibir informaciones y opiniones;
- el derecho de difundirlas

Deberíamos impedir las conductas que tiendan a molestar a los cibercorresponsales a causa de sus opiniones en el seno de la comunidad virtual o real. Y favorecer el derecho de los jóvenes a investigar y recibir informaciones y a difundirlas a través del medio de expresión que consideren oportuno.

Todo lo expuesto no quita para que el ejercicio del derecho a la libertad de expresión esté sujeto a ciertas restricciones, que según establece la propia Convención para los Derechos del Niño serán únicamente las que la ley prevea y sean necesarias:

- para el respeto de los derechos o reputación de los demás;
- o para la protección de la seguridad nacional o el orden público o para proteger la salud o moral públicas.

El artículo 20 de la Constitución establece los límites a las libertades informativas en los derechos a la personalidad, que protegen el ámbito privado de una persona. Éstos son el honor, la intimidad y la propia imagen, y están regulados en el artículo 18.1 y en la Ley de protección civil del derecho al honor y la propia imagen (Ley Orgánica 1/82)

EL DERECHO AL HONOR

El honor es el aprecio y estima que una persona tiene en la sociedad en la que vive. Son titulares del derecho al honor todas las personas físicas. Sin embargo el Tribunal Constitucional ha reconocido 2 excepciones:

- el honor también puede ser importante para determinadas personas jurídicas (empresas, organizaciones, etc…)
- el derecho al honor protege también a los miembros de un pueblo o una etnia

Se produce una colisión entre el derecho al honor y las libertades informativas:
"Cuando se imputan hechos o se manifiestan juicios de valor que lesionan la dignidad de una persona con menoscabo de su fama o un atentado contra su propia autoestima."
Ley orgánica 1/82 sobre la protección civil al derecho al honor, a la intimidad y a la propia imagen
Uno de los criterios más importantes para resolver una colisión entre el derecho al honor y las libertades información es la veracidad. La **veracidad** debe entenderse como la diligencia del periodista. Basta que el o la periodista actúe con diligencia en la comprobación de los hechos para atribuir la veracidad de la información.

INJURIAS

Consiste en acciones y expresiones que lesionan la **dignidad** de una persona, causando un daño en su fama o a su propia estima. Para que exista se necesitan una serie de **elementos**:

1. Debe existir un insulto o un elemento objetivo que consista en un contenido **ofensivo**. La injuria puede cometerse de palabra, por escrito o por medio de caricaturas o gestos. Lo relevante es que la manifestación injuriosa tenga un claro contenido ofensivo o denigratorio para otra persona que socialmente considera que lo desacredita. La acción ha de tener un contenido objetivamente ofensivo según la opinión generalizada. Esto es un problema porque la opinión generalizada cambia constantemente.

2. La **intención** específica de ultrajar. Existe ánimo de injuriar cuando hay intención específica de promover el rechazo social hacia una persona. Es la intención de "meterse con alguien". Si hay ánimo de injuria no hay ejercicio legítimo de las libertades informativas. No existe ánimo de injuriar cuando:

- se explican unos hechos o se valoran unas actitudes con el propósito de criticar o censurar

constructivamente un comportamiento ajeno (ánimo narrativo o de crítica).
- una expresión deshonrosa pero dentro de un espíritu de amistad o broma no constituye injurias.

3. La injuria debe hacerse **públicamente**. La injuria debe llegar a conocimiento de la persona injuriada. Un insulto o menosprecio sin repercusión social no es considerado como delito. La injuria (y también la calumnia) se consideran hechas con publicidad cuando se propagan por medio de la imprenta, la radiodifusión o Internet.
En principio cuando una injuria se dirige a particulares, no se puede aplicar la excepción por veracidad. Por ejemplo, resaltar los defectos físicos de una persona, su raza, sexo o religión; por más que sea verdad, no es relevante.

DIFAMACIÓN

La difamación consiste en publicar una **información falsa** con ánimo de dañar el honor, la dignidad o la reputación de una persona.

CALUMNIAS

La calumnia es otro delito contra el honor y consiste en afirmar que alguien ha cometido un delito siendo consciente de su falsedad. Requisitos para que exista delito de calumnias:
- Afirmación falsa de la comisión de un delito. El hecho que se imputa debe ser concreto y la persona debe ser determinable de forma inequívoca. La falsedad de la información denota la intención especial de hacer daño en el honor de una persona.
- La excepción por veracidad es plenamente aplicable a las calumnias. No existe calumnia si puede probarse, ante un tribunal, los hechos de los que se acusa.

EL DERECHO A LA INTIMIDAD

El derecho a la intimidad personal y familiar es el reducto más privado de una persona. Es un ámbito que está reservado al conocimiento de los demás y muy protegido. Este derecho lo tienen todas las personas físicas, no las personas jurídicas (empresas, organizaciones, etc.).

El derecho a la intimidad pretende que una persona pueda **controlar el acceso y la divulgación** de información sobre su **vida privada**. La legitimidad de las intromisiones en la intimidad de las personas depende fundamentalmente del consentimiento del titular. Si hay **consentimiento** del titular no hay violación del derecho a la intimidad. Ese consentimiento tiene que ser expreso y puede ser revocable en cualquier momento. En estos casos, no es importante si la información es veraz o no. El derecho a la intimidad se vulnera por la simple imputación de un hecho que forma parte de la esfera íntima y más personal de un ser humano. La ley contempla 3 casos:
1. Obtención de la información sin consentimiento. Colocar aparatos de escuchar, de filmación, de dispositivos ópticos o cualquier otro medio para grabar o reproducir la vida íntima de las personas sin su permiso.
2. Divulgación de la información. Dar a conocer hechos de la vida privada de una persona o revelar el contenido de cartas, memorias, etc. u otros escritos personales de carácter íntimo.
3. Quebramiento de la confianza. Revelación de datos privados de una persona o familia, conocidos a través de la actividad profesional u oficial de quien los revela. Se trata de una desviación de la información del fin para el que se ha dado.

EL DERECHO A LA PROPIA IMAGEN

Es un derecho complementario al derecho a la intimidad. Este derecho garantiza la protección de lo que se consideran las **cualidades definitorias de una persona: imagen física, voz y nombre**.
Este derecho lo tienen todas las personas físicas independientemente de su consideración.
Se considera intromisión ilegítima en el derecho a la propia imagen captar, reproducir o publicar por fotografía, video o cualquier otro procedimiento, la imagen de una persona en lugares o momentos de su vida privada o incluso fuera de ella. La intromisión ilegítima se produce con que se da una de estas circunstancias: captar, reproducir o publicar. Este supuesto tiene una serie de **excepciones**:
- Si se trata de una persona que ejerce un cargo público o de notoriedad y la imagen se capta durante un acto público o lugares abiertos al público

■ Si se trata de caricaturas de esas personas de acuerdo con el uso social
■ Si en la información gráfica sobre un suceso o acontecimiento público, la imagen de una persona aparece como meramente accesoria.

El más complejo es el primero de los supuestos. Espacio abierto al público no tiene unas reglas generales, se estudia caso a caso. Ejemplos:
■ Fotos de unos famosos tomadas en una reserva de Kenya: no era intromisión porque el lugar era público y las fotos no eran comprometidas.
■ Fotos de una actriz tomadas mientras hacía topless: hay intromisión porque era una playa alejada del gran público y eso denotaba la intención de aislarse y por eso no era un lugar público.

FOTOGRAFIAR A MENORES DE EDAD

La publicación de fotografías de menores de edad pasa en primer lugar por el **consentimiento** del niño o la niña cuando tiene capacidad para otorgarlo (lo que según el Tribunal Supremo sucede en líneas generales a partir de los catorce años) y si no la tiene, la **autorización** de su familia o tutores legales.
Por otro lado, se considera intromisión ilegítima en el derecho al honor, a la intimidad personal y familiar y a la propia imagen del menor, cualquier utilización de su imagen o su nombre en los medios de comunicación que pueda implicar menoscabo de su **honra** o reputación, o que sea contraria a sus intereses incluso si consta el consentimiento de la persona menor de edad o de sus representantes legales.

Además de tener el consentimiento de los menores o sus padres es necesario cautelar que las imágenes publicadas respeten a los retratados, procurando que los muestren en acciones constructivas y dignificantes.

LOS CONTENIDOS NOCIVOS

Son contenidos nocivos los que, a pesar de ser legales, pueden perjudicar el desarrollo de los niños, niñas y adolescentes y no están permitidos en cibercorresponsales como: la pornografía entre adultos, la violencia, el consumo de drogas o el fomento de trastornos alimentarios como la anorexia y la bulimia.
El concepto "nocivo" varía en función de las diferencias culturales y las diferencias individuales de los usuarios (edad, madurez intelectual, cultura, ideología, creencia religiosa, etc.). Estas variables deberán ser manejadas por los educadores y educadoras y aplicadas en cada caso.

LOS CONTENIDOS FALSOS

Necesitamos aprender las claves para buscar información concisa y necesitan adquirir las habilidades necesarias para ser **críticos** ante la información que encuentran en Internet. Debemos guiar a las y los cibercorresponsales, ayudarles a comprender la información que encuentran y a distinguir entre los hechos, las opiniones, los rumores y las mentiras. También es importante tener en cuenta que a veces la información que se ofrece es parcial o responde a una ideología muy concreta.

Debemos invitarles constantemente a indicar las fuentes consultadas y a contrastar entre diversas fuentes.

LA RESPONSABILIDAD DE LOS COMENTARIOS EN EL BLOG

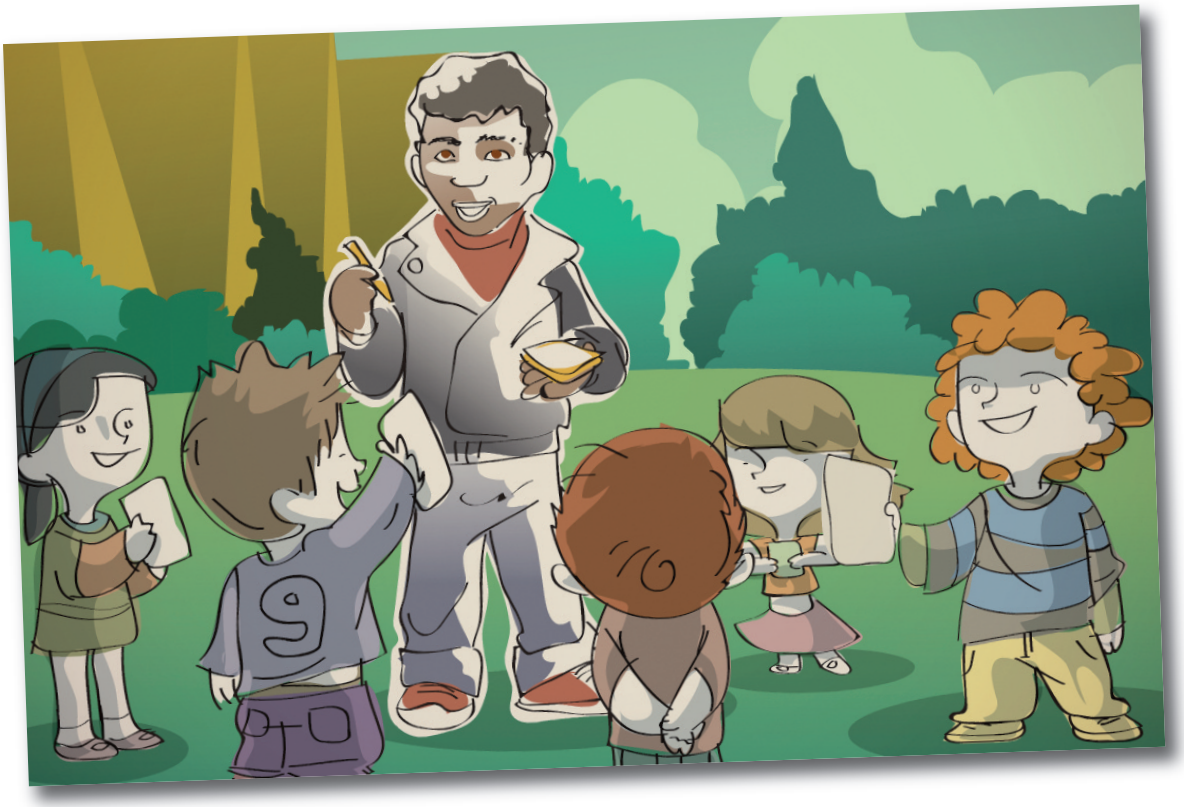
El problema al que nos enfrentamos es global, la información y la comunicación no son ya tarea exclusiva de las y los periodistas y medios profesionales. Cada día se crean miles de blogs, las y los internautas publican otros tantos vídeos en YouTube, millones de comentarios, entradas en páginas de ela-boración colaborativa como la Wikipedia. Un estudio de International Data Corporation (IDC) asegura que hasta el 70% de los contenidos publicados en Internet han sido **creados por las y los usuarios**.
En la elaboración de la programación televisiva o las páginas de un periódico intervienen varios filtros que deciden qué se publica y qué no. Pero en Internet el funcionamiento es distinto, los medios han abierto la puerta a los contenidos elaborados por sus usuarios y ususarias y publican comentarios, textos y vídeos ajenos a la redacción. La responsabilidad por las infracciones que puedan cometerse en esos contenidos -delitos contra el honor o derechos de autor, nor-

malmente- quedó fijada hace tiempo en una ley, pero su aplicación está generando más dudas de las esperadas.

La ley dice que el medio sólo será legalmente responsable cuando **tenga "conocimiento** efectivo de que la actividad o la información almacenada es ilícita" y no haya actuado con "diligencia para retirar los datos o hacer imposible el acceso a ellos". No obstante, en algunos casos los jueces no han llegado a un acuerdo al aplicar la norma y han hecho recaer la responsabilidad sobre quien **aloja** los contenidos, no sobre su **autor** real. Así ha sido en dos de los casos que más repercusión han tenido en los últimos meses: el caso de la General de Autores contra la Asociación de Internautas y el caso de la Frikipedia, en ambos casos por alojar contenidos que atentan contra el honor de la SGAE o sus representantes. En estos fallos inculpatorios para los alojadores de contenidos subyacen dos cuestiones:

■ Los jueces aplican la doctrina tradicional, conforme a la cual **el medio es responsable** de todos los contenidos, sobre todo si son anónimos, basándose en el funcionamiento de los periódicos. Pero en Internet no es así, no hay un jefe de rotativa que filtra el contenido sino que todo funciona de forma automática. La normativa española sobre el tema, es la LSSI, que establece que "sólo hay responsabilidad cuando el proveedor tiene conocimiento de un contenido ilícito, declarado como tal por la autoridad competente, y se haya notificado esa resolución". Los fallos de estas sentencias están recurridos y se está a la espera de una sentencia del Supremo que cree jurisprudencia. La Asociación de Internautas está impulsando una petición para que las autoridades europeas, de las que salió la directiva que inspira la legislación española, interpreten definitivamente esta cuestión.

■ Los tribunales, ante la dificultad que supone identificar a cualquier internauta, adoptan una salida de compromiso consistente en la imputación de la responsabilidad a quienes alojan los contenidos. Algunos expertos reconocen que el tema del anonimato es el problemático y sugieren que para solucionarlo se tendría que establecer un régimen legal claro que obligue a todo el que tenga sistemas automáticos de publicación a conservar y proporcionar la IP de sus usuarios en caso de ser solicitada por la justicia. La **dirección IP** es una dirección única que cada ordenador tiene en Internet y mediante la cual puede identificarse, a través del operador de telecomunicaciones y mediante requerimiento judicial, a la persona con nombre y apellidos a la que pertenece un ordenador.



La protección de datos personales

Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernen y este derecho le atribuye la facultad de controlar sus datos.

Reconocen el derecho fundamental a la protección de datos de carácter personal:
- Constitución Española
- Ley Orgánica 15/1999 de Protección de Datos
- Carta De Derechos Fundamentales de la Unión Europea
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD).
- Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones (LGT).
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI).
- Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de Diciembre de Protección de Datos de Carácter Personal (B.O.E. Num. 17, 19 De Enero 2008).

A todo este marco normativo nos referimos cuando hablamos comúnmente de la **Ley de Protección de Datos**.
Las empresas y organismos públicos que tratan datos de carácter personal tanto en soporte electrónicos como en papel están obligados a garantizar el derecho fundamental a la Protección de datos. Nosotros/as, por supuesto, también.

QUIÉN SE RESPONSABILIZA DEL FICHERO

El responsable del fichero es la entidad que crea una base de datos o un archivo en papel y que decide sobre la finalidad, el contenido y el uso del tratamiento de los datos personales. En nuestro caso, la Plataforma de Infancia es responsable del fichero de cibercorresponsales.

No debéis mantener otras bases de datos o ficheros en papel de las y los participantes en el programa al margen de la base de datos oficial del programa. En el caso de que creéis una base de datos propia seriáis los únicos responsables del cumplimiento de la Ley de Protección de Datos en relación a esos ficheros.

QUIÉN ES EL ENCARGADO

Asociada a la figura del responsable, está la figura del encargado, que es la entidad u organismo que trata los datos por cuenta del responsable del fichero.

Es decir, vuestras organizaciones son las encargadas del tratamiento del fichero de cibercorresponsales.

La Ley de Protección de Datos establece que la realización de un tratamiento de datos por cuenta de terceros debe estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido. Este contrato fue firmado por vuestra organización como parte del documento de adhesión al programa de cibercorresponsales.

Este acuerdo establece, tal y como determina la Ley de Protección de Datos (LOPD), que:
- el encargado tratará los datos conforme a las instrucciones del responsable,
- que no los aplicará o utilizará con fin distinto al que figure en dicho contrato,
- que ni los comunicará, ni siquiera para su conservación, a otras personas.
- y también se especifican las medidas de seguridad a implementar.

Ambas organizaciones, encargada y responsable del tratamiento, pueden ser sancionadas de acuerdo a la ley si incumplen sus obligaciones. La Agencia de Protección de Datos se ocupa de velar por el cumplimiento de la normativa de protección de datos. La Agencia de Protección de Datos ejecuta su capacidad sancionadora sobre las organizaciones, no sobre las personas que trabajan o colaboran en ellas.

La Ley de Protección de Datos nos exige las siguientes obligaciones a los responsables del fichero de cibercorresponsales y a los encargados de su tratamiento; es decir a la Plataforma de Infancia y las organizaciones participantes en el programa de cibercorresponsales.

Notificar los ficheros ante el Registro General de Protección de Datos para que se proceda a su inscripción.

Esta gestión le corresponde a la Plataforma de Organizaciones de Infancia como responsable del fichero.

Informar a los titulares de los datos personales en la recogida de éstos.
Cualquier persona tiene derecho a saber si sus datos personales van a ser incluidos en un fichero y a conocer los tratamientos que se realizan con esos datos.

La Ley de Protección de Datos recoge la obligación que tienen los responsables de los ficheros y los responsables de los tratamientos de informar a los ciudadanos y ciudadanas de la incorporación de sus datos a un fichero, de la identidad y dirección del responsable, de la finalidad del fichero, de los destinatarios de la información, del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas, de las consecuencias de la obtención de los datos o de la negativa a suministrarlos, así como de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
La ley exime del deber de informar sobre algunos de estos aspectos cuando se deduzcan inequívocamente de la naturaleza de los propios datos personales y de las circunstancias en las que se produce la recogida.
En el caso de utilizar Internet como medio de recogida de los datos, también debe facilitarse esta información a los usuarios que registran sus datos y debe de hacerse de modo que la información sea siempre previa al tratamiento. Además es recomendable que el texto informativo resulte lo más claro y legible posible.

Obligaciones de la Ley de Protección de Datos

- **Notificar los ficheros ante el Registro General de Protección de Datos para que se proceda a su inscripción.**
- **Informar a los titulares de los datos personales en la recogida de éstos.**
- **Obtener el consentimiento para el tratamiento de los datos personales.**
- **Asegurarse de que los datos sean adecuados y veraces, obtenidos lícita y legítimamente y tratados de modo proporcional a la finalidad para la que fueron recabados.**
- **Garantizar el cumplimiento de los deberes de secreto y seguridad.**
- **Facilitar y garantizar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.**
- **Asegurar que en sus relaciones con terceros que le presten servicios, que comporten el acceso a datos personales, se cumpla lo dispuesto en la Ley de Protección de Datos.**
- **Cumplir, cuando proceda, con lo dispuesto en la legislación sectorial que le sea de aplicación.**
- **Garantizar que el envío de comunicaciones electrónicas masivas se realiza de acuerdo a la LSICE**

Toda esta información y consideraciones legales están incluidas en los cuestionarios de inscripción de los cibercorresponsales en papel y en la web.

Os recomendamos que no uséis impresos propios de recogida de los datos de los cibercorresponsales pues en tal caso vosotros seriáis los únicos responsables del cumplimiento de la Ley de Protección de Datos. Por favor, emplead siempre los formularios de inscripción suministrados por la Plataforma de Infancia.

Obtener el consentimiento para el tratamiento de los datos personales.
En el caso de los menores de edad se exige que la información se exprese en un lenguaje que sea fácilmente comprensible.

Como regla general, la Ley de Protección de Datos prohíbe pedir o tratar datos de menores de catorce años sin el consentimiento de sus padres. Si son mayores de **catorce años**, no se exige dicho consentimiento, salvo que sean actos que los menores de dieciocho años no puedan realizar sin permiso paterno. Si, además, se pretende recoger datos con información relativa a los miembros del grupo familiar o sus características, será necesario que los titulares de los mismos den su consentimiento.
Por tanto a la hora de pedir los datos de los participantes en el programa de cibercorresponsales hay que distinguir entre los mayores de catorce años y los menores de catorce.
Los mayores de catorce años pueden darnos directamente sus datos personales, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En ciertos casos de discapacidad intelectual o salud mental y en algunos casos de menores de edad en protección o reforma, por ejemplo, puede ocurrir que la Ley exija la asistencia de titulares de la patria potestad o tutela.

Para los mayores de edad el consentimiento se obtiene al rellenar la ficha de inscripción y en caso de hacerlo a través de la web antes de rellenar el formulario de inscripción.

Las y los menores de 14 años requerirán siempre del consentimiento de familias o tutores. Debéis usar la ficha de inscripción específica y pedirles a vuestra madre, padre o tutores que firmen el consentimiento.

Debéis guardar las fichas de inscripción y todos los consentimientos en papel respetando las medidas de seguridad adecuadas para los ficheros no automatizados.

Asegurarse de que los datos sean adecuados y veraces, obtenidos lícita y legítimamente y tratados de modo proporcional a la finalidad para la que fueron recabados.

La Ley de Protección de Datos nos impide expresamente: *"Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de las personas que Ley ampara".*
El titular de los datos que se tratan tiene derecho gratuitamente a **solicitar y obtener información** de sus datos de carácter personal sometidos a tratamiento, y del origen de dichos datos así como las comunicaciones realizadas o que se prevén hacer de los mismos.
Los participantes podrán ejercer sus derechos de **acceso, rectificación o anulación** a través de la web mediante el uso de su usuario y contraseña pueden modificar inmediatamente sus datos o darse de baja.
También se les informa en la web de la forma de ejercer sus derechos de acceso, rectificación y anulación mediante el envío de comunicaciones electrónicas o postales a la Plataforma de Infancia.
Por otro lado, existe la obligación de contestar a cualquier solicitante aunque no figuren datos suyos y se debe hacer por medios que permitan acreditar el envío y la recepción de la notificación, es decir, por carta certificada con acuse de recibo.
Los datos nunca pueden ser borrados; siempre son bloqueados para su uso ya que la administración podría requerírnoslos en el futuro. Esta operación de bloqueo la realiza la aplicación de Cibercorresponsales automáticamente.

Garantizar el cumplimiento de los deberes de secreto y seguridad
La Ley de Protección de Datos condiciona estas medidas al estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.
La aplicación de las medidas de seguridad se ordena a garantizar la confidencialidad, integridad y disponibilidad de los datos. La seguridad constituye un instrumento esencial para garantizar el derecho fundamental a la protección de datos.

Las medidas de seguridad se aplican tanto a los ficheros como a los tratamientos.
Las medidas de seguridad deben aplicarse tanto por el responsable del fichero como por los encargados del tratamiento.
El reglamento de desarrollo de la Ley Orgánica de Protección de Datos fija tres niveles de seguridad atendiendo a la naturaleza de la información. Nuestros ficheros se encuentran registrados en el nivel básico, al que pertenecen todos los ficheros que contengan datos de carácter personal.

La descripción detallada de las políticas de seguridad así como la descripción de los procedimientos y medidas de seguridad podéis encontrarlas en el Documento de Seguridad.

Asegurar que en sus relaciones con terceros que le presten servicios, que comporten el acceso a datos personales, se cumpla lo dispuesto en la Ley de Protección de Datos.

Las organizaciones participantes en el programa Cibercorresponsales no pueden ceder los datos de los cibercorresponsales a terceros.

La Plataforma de Organizaciones de Infancia no cede los datos a ningún tercero salvo en el caso de la empresa de mantenimiento informático de la web para la finalidad expresa del mantenimiento técnico de las bases de datos y mantiene una autorización y contrato de cesión de datos para este fin.

Garantizar que el envío de comunicaciones electrónicas masivas se realiza de acuerdo a la LSICE
En el caso del envío de comunicaciones realizadas a través de correo electrónico o medios de comunicación electrónica equivalentes (como la mensajería privada de Cibercorresponsales) sólo podrán realizarse cuando hubieran sido solicitadas o expresamente autorizadas por las personas destinatarias de las mismas. También podrán realizarse cuando exista una relación contractual previa, siempre que se hubieran obtenido de forma lícita los datos de contacto del destinatario y se emplearan para el envío de comunicaciones referentes a productos o servicios de la propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente.

Es decir, siempre podremos enviar comunicaciones masivas a los cibercorresponsales que tengan que ver con la actividad del programa, tanto al correo electrónico que nos facilitaron al inscribirse como a su buzón de la web de cibercorresponsales.

En cualquier caso, el prestador debe ofrecer al destinatario la posibilidad de **oponerse** a su envío mediante un procedimiento sencillo y gratuito. Esta posibilidad de oponerse es automáticamente incluida en el pie de las comunicaciones que se envían desde la web de Cibercorresponsales.

Los derechos de autoría

Los derechos de autoría protegen los derechos de las y los autores sobre su obra. En España se conoce como propiedad intelectual.

Cualquier obra tiene **automáticamente** derechos de autoría, no hace falta hacer nada para protegerlas, el mero hecho de crearlas hace que estén protegidas bajo esta ley.
La mera posesión de un libro, manuscrito, pintura o cualquier otra copia o fonograma le otorga a su dueño o dueña el "derecho de autor".
Las y los autores suelen dejar una "nota" en la obra alegando su autoría, el típico símbolo de **copyright** © con el año y el nombre del autor o autores, eso asegura que esa obra no es de dominio público.
La violación de este derecho esta penada por la ley bajo demanda de quien ha elaborado la obra.
El o la titular de los derechos de autoría goza de **derechos exclusivos** respecto de:

- **Reproducir** la obra en copias.
- Preparar obras **derivadas** basadas en la obra.
- **Distribuir** copias de la obra al público vendiéndolas o haciendo otro tipo de transferencias de propiedad tales como alquilar, arrendar o prestar dichas copias.
- Presentar y **mostrar** la obra públicamente.

Las autoras de una obra colectiva son co-dueñas del derecho de autoría de dicha obra a menos que haya un acuerdo que indique lo contrario.
El derecho de autoría de cada contribución individual de una publicación periódica o en serie, o cualquier otra obra colectiva, existen a parte del derecho de autoría de una **obra colectiva** en su totalidad y están conferidos inicialmente al autor de cada contribución.
Las personas **menores de edad** pueden reclamar derecho de autoría, pero -al ser menores de edad- pueden existir leyes específicas que reglamenten cualquier transacción relacionada.
En la actualidad, y tal como establece la Ley de Propiedad Intelectual, puede decirse de modo general que, en el caso más simple y frecuente de un solo autor, los derechos de explotación de la obra duran **toda la vida del autor o autora y 70 años después** de su muerte o declaración del fallecimiento.

EXCEPCIONES A LOS DERECHOS DE AUTORÍA

Son aquellos casos en los que la creadora o el creador ve limitado su derecho exclusivo de explotar su obra en favor del interés social. La Ley reconoce, entre otros, los siguientes usos de obras protegidas sin autorización, sin perjuicio de que, en algunos casos, se le deba abonar una remuneración por dichos actos de explotación:

Parodia: no es necesario el consentimiento del autor o autora de una obra ya divulgada para parodiarla cuando la parodia:

- no implique riesgo de confusión con la obra original,
- no infiera un daño a la obra original y
- no cause daño al autor de la obra original.

Utilización de las obras con ocasión de informaciones de actualidad y de las situadas en vías públicas: no es necesaria la autorización del autor de una obra protegida para reproducirla, distribuirla y comunicarla públicamente, cuando ésta pueda ser vista u oída en una información de actualidad. Esta utilización debe estar justificada por la finalidad informativa.

Tampoco es necesaria autorización para reproducir, distribuir y comunicar libremente por medio de pinturas, dibujos, fotografías y procedimientos audiovisuales **las obras situadas permanentemente en cualquier vía pública**.

Trabajos sobre temas de actualidad: los trabajos y artículos de actualidad difundidos por los medios de comunicación social podrán ser reproducidos, distribuidos y comunicados públicamente por otros de la misma clase sin autorización de sus autores o autoras, siempre que se citen, siempre que el trabajo hubiera aparecido con firma. No se podrá realizar esta reproducción si en el artículo consta la reserva de derechos.

Cita e Ilustración en la enseñanza: la inclusión en una obra propia de fragmentos de obras ajenas no necesita la autorización del autor de la obra citada o reseñada, siempre que se cumplan todas las condiciones detalladas a continuación:

■ que el fragmento que se incluya corresponda a una obra ya divulgada,
■ que su inclusión se realice a título de cita o reseña para su análisis, comentario o juicio crítico,
■ que se realice con fines docentes o de investigación,
■ que se indique la fuente y el nombre del autor de la obra utilizada.

En caso de oposición expresa del autor, dicha actividad no se entenderá amparada por este límite.

Obras de dominio público:
Las obras, después de expirar la protección de los derechos, pasan a dominio público. Esto significa que cualquier persona las puede reproducir, sin que haga falta pedir permiso a nadie ni pagar ningún derecho. Se puede licenciar una obra directamente bajo dominio público con la licencia de Creative Commons.

Copyleft:
Copyleft o "copia permitida" comprende a un grupo de derechos de autoría caracterizados por eliminar restricciones de distribución o modificación. Los trabajos así registrados se identifican con el símbolo © mirando a la izquierda. El objetivo es difundir más y mejor el conocimiento, eliminar sus barreras, dentro de una filosofía que se traduce en diversos tipos de licencias comerciales.

Creative Commons:
Creative Commons es una organización no gubernamental sin ánimo de lucro que desarrolla planes para ayudar a reducir las barreras legales de la creatividad, por medio de nueva legislación y nuevas tecnologías. Para ello, propone diferentes tipos de licencias copyleft bajo la idea de fomentar la cultura, la cooperación y el desarrollo de todas las obras a través de Internet (así como protegerlas). Estas licencias se aplican a los trabajos creativos (pero no a los de software, para estos esta el GNU o GLP).
Creativecommons.org ha desarrollado una aplicación Web (http://es.creativecommons.org/) que ayuda a la gente a brindar sus creaciones al dominio público o a reservarse los derechos de autoría, dejándolos libres para ciertas aplicaciones, en ciertas condiciones de uso. También han desarrollado buscadores para localizar contenidos con estas licencias. Las diferentes licencias Creative Commons se basan en combinar distintas propiedades. Estas propiedades son:
■ Attribution (by): Obliga a citar las fuentes de esos contenidos. El autor debe figurar en los créditos.
■ Noncommercial o NonCommercial (nc): Obliga a que el uso de los contenidos no pueda tener bonificación económica alguna para quien haga uso de esa licencia.
■ No Derivative Works or NoDerivs (nd): Obliga a que esa obra sea distribuida inalterada, sin cambios.
■ ShareAlike (sa): Obliga a que todas las obras derivadas se distribuyan siempre bajo la misma licencia del trabajo original.

Muchas de las licencias Creative Commons se identifican con el **acrónimo CC**, que hace referencia a su nombre.

Fotografiar contenido protegido:
El fotografiar una obra protegida por derecho de autoría es como reproducirla. Por consiguiente, antes de tomar una foto de cualquier obra protegida, se necesita pedir permiso al titular.
No siempre se necesita permiso de la persona autora o propietaria de este contenido, depende de varias cosas como el contenido en sí o el uso que se le vaya a dar a la fotografía. También hay que tener en cuenta si es de dominio público o si no se reproduce parte sustancial de la misma. En general, deben tenerse en cuenta las siguientes reglas:
■ Edificios: Están protegidos por derechos de autoría, pero si se encuentran en lugares visibles desde un lugar público se pueden fotografiar, publicar y distribuir sin permiso.
■ Obras protegidas en lugares públicos: igual que con los edificios, pero se aplica a obras tridimensionales (como esculturas, para otras tal vez se necesite pedir permiso) que estén permanentemente en un lugar público (no temporalmente).
■ Fotografías para prensa, reseñas o críticas: Siempre que su fin sea este y se cite al autor o autora y el título se puede fotografiar este tipo de contenido.
■ Obra protegida como fondo: En la mayoría de países no se necesita autorización si algo protegido no añade a la fotografía parte sustancial, si se queda como mero fondo, sin fin estético o comercial.

En caso de necesitar un permiso hay que pedírselo a la persona titular del derecho de autoría. Además, también puede ser necesaria la autorización de la persona propietaria o de alguien que le represente, si no se puede acceder directamente.
También la ley protege la **reputación** del autor y de la obra, un ejemplo muy claro es el de situar en una foto pornográfica una escultura religiosa, con lo cual se podría intentar un procedimiento judicial contra el autor.
Otro punto son las **ideas**. La ley protege fotografías, no ideas, puedes copiar tranquilamente la pose de una fotografía cambiando el modelo.
Por último quedan las **marcas**. Fotografiar algo con una marca (una persona con una camiseta de determinada marca por ejemplo) puede traer problemas.
A diferencia de la legislación sobre derecho de autoría, la legislación sobre marcas como tal no restringe el uso de una marca en una fotografía. Lo que sí prohíbe es el uso de una marca de forma que pueda inducir a confusión respecto de la afiliación del titular de la marca con la imagen. Si es probable que las y los consumidores crean erróneamente que el titular de la marca patrocina la fotografía, puede que se infrinja el derecho de marcas. Debido a este uso se asumirá que el autor está intentando apropiarse de una parte la reputación asociada con la marca, y probablemente los consumidores pensarán que las prendas de vestir están relacionadas con la marca.

Contactos indeseados y suplantación de identidad

Debemos conocer que los agresores sexuales utilizan las redes sociales y otros sitios de Internet para encontrar y conocer a niños, niñas y adolescentes. En ocasiones, esto puede acabar en abuso sexual, en persona o desde el ordenador y sin contacto físico real, por ej., enviándoles o intercambiando imágenes sexuales y/o convenciéndoles de que manden imágenes explícitas de ellos/as mismos/as.

La comunidad de cibercorresponsales es un espacio protegido frente a estas amenazas. Por este motivo la identidad real de las y los jóvenes se oculta y sólo es conocida por los dinamizadores/as de su grupo.
Los datos personales de los cibercorresponsales están claramente divididos en dos:
- Identidad virtual (pública y visible para todo el mundo): avatar, Lema, Nick
- Identidad real (privada y visible solo para ciertas personas): datos personales nombre y apellidos, dirección, correo electrónico, etc.

Debemos indicarles a las y los cibercorresponsales esta división entre su identidad virtual, usada para relacionarse en el ciberespacio manteniendo su intimidad, y su identidad real.

ABRIR UNA CUENTA

Está prohibido abrir una cuenta de cibercorresponsal a un usuario que no conocemos personalmente. Siempre debe existir un conocimiento personal entre la o el joven participante y el dinamizador/a. Además la familia del joven debe conocer que está participando en el proyecto. Este conocimiento interpersonal es la principal medida de prevención

frente a la infiltración de adultos con intenciones maliciosas.

CERRAR CUENTAS INACTIVAS

Debemos estar pendientes de cerrar las cuentas de jóvenes que no estén participando en el proyecto.

PARA PROTEGER IDENTIDAD Y NO DIFUNDIR DATOS PERSONALES

Colgar información personal supone que las y los menores de edad estarán expuestos a la burla, el robo de identidad, al acoso y a los contactos no deseados con extraños. Serán menos vulnerables si antes de colgar su información se paran a pensar que:

- Sus datos personales identifican dónde viven y cómo se les puede contactar.
- Las imágenes sirven para encontrarles (por ej. el uniforme del colegio). Debemos evitar que las imágenes de los avatares revelen datos personales de los participantes.
- Que los nombres y las imágenes que ponen pueden sugerir que son mayores de lo que son.

Los niños y los adolescentes tienen que conocer y utilizar bien las herramientas que aparecen en las páginas de las redes para controlar su privacidad y su información para evitar los contactos o mensajes no deseados.

Debemos concienciar a los jóvenes de estos riesgos y ante la publicación de datos personales en espacios públicos como foros o blog debemos eliminar el contenido o pedirle al autor lo elimine. También debemos asegurarnos que entienden por qué es perjudicial esa información y por qué tienen que eliminarlo.

PERFILES FALSOS O FRAUDULENTOS

Los perfiles falsos o los que suplantan una identidad hacen referencia a los usuarios que se inventan un perfil en las redes sociales para hacerse pasar por otro, por ej., otro chico o chica por un dinamizador/a. A menudo, empieza haciéndose para divertirse, sin tener en cuenta las consecuencias. En otros, sin embargo, los perfiles falsos se crean deliberadamente para hacer daño u ofender a otra persona. En estos perfiles falsos o que se hacen pasar por otro, pueden incluso aparecer fotos del suplantado hechas con el teléfono móvil.

Para evitar la creación de perfiles falsos la creación de usuarios en la comunidad, el alta de nuevos cibercorresponsales solo podrá realizarla el educador o educadora de cada organización, que debe comprobar en la medida de lo posible que los datos aportados por el/la joven son veraces.

La forma más y eficaz de eliminar un perfil falso de una red social es pedirle al autor que lo elimine él, eso si sabe quién es el impostor. Antes de pedirle que elimine el perfil, asegúrese de que entienden por qué es perjudicial esa información y por qué tienen que eliminarlo.

PROTECCIÓN CON LA CONTRASEÑA

Explica a los cibercorresponsales que es fundamental protegerse con una contraseña para garantizar que su ordenador y los otros dispositivos digitales están seguros al acceder a la página de una red social.

Si utilizan un ordenador público o compartido, tienen que desactivar cualquier tipo de conexión automática (“recordar contraseña”) y tienen que comprobar siempre que desconectan al final de la sesión.

RECONOCER EL ‘GROOMING’

Aunque nuestra comunidad mantenga unos elevados estándares de seguridad debemos permanecer siempre alerta ya que existen muchas otras comunidades virtuales en Internet potencialmente peligrosas.
El ‘Grooming’, o ‘manipulación de los niños’, es un proceso durante el cual alguien entra en contacto con un niño o una niña con el fin de irle preparando y conociendo para abusar del menor sexualmente, desde la red o en persona.
Los agresores sexuales saben servirse de un amplio arsenal de técnicas para entrar en contacto con los menores, por ejemplo:

- ofrecen oportunidades para hacer de modelos, en especial a las chicas

■ prometen citas con ídolos de la música pop o con gente famosa
■ hacen ofertas de productos o
■ pagan a los chicos y chicas jóvenes por posar desnudos y realizar actos sexuales grabados por la cámara web.

Tened en cuenta que resulta dificilísimo para las jóvenes víctimas buscar ayuda o revelar el abuso al que están siendo sometidas en la red. Les da vergüenza, se sienten culpables, creen que pueden tener ellos la responsabilidad y tienen miedo de que no les crean o incluso de que se les acuse y se queden sin acceso a Internet.

LAS PRÁCTICAS DAÑINAS O ILÍCITAS

Casi cualquier práctica ilícita es susceptible de realizarse por Internet. Las denuncias por delitos de menores de edad con medios telemáticos crecieron de forma notable en 2007, un alza que puede deberse tanto a un efecto rebote por la difusión que se les da en ocasiones en los medios, como por la creciente conciencia social que ha incrementado el número de denuncias.
Asumiendo que es raro que alguno de las y los participantes en el programa pueda realizar una actividad ilícita en la comunidad de Cibercorresponsales, no debemos dejar de tener en cuenta esta posibilidad y frente a la sospecha de cualquier práctica ilícita debemos **comunicar** inmediatamente con las y los res-ponsables del programa en la plataforma de infancia.
Ante cualquier indicio de actividad ilegal se puede recurrir al Grupo de Delitos Telemáticos de la Guardia Civil, y para temas específicos que atenten contra los derechos de los menores. También los portales: www.protegeles.com, www.noalapornografiainfantil.com y www.asociacion-acpi.org ofrecen un sistema de **denuncias** on-line.

A continuación se relatan algunas de las prácticas ilícitas más frecuentes en Internet:
La mayoría de las prácticas ilícitas están vinculados a publicación de contenidos ilícitos y han sido abordados en ese apartado: revelación de secreto, apología de la discriminación, amenazas, injurias, calumnias, contra el derecho al honor o la intimidad, vulneración de derechos de propiedad intelectual, etc.
También debemos vigilar las informaciones en torno a las estafas en Internet, frecuentemente vinculadas a dialer (programas de pago que se instalan sin nuestro consentimiento), casinos on-line o subastas on-line y eliminar cualquier contenido que pueda estar vinculado a estas actividades.

EL ACOSO, LO MÁS HABITUAL

El acoso, ya sea sexual o de otro tipo, por medio de los sistemas de mensajería, conversación o videoconferencia, suele ser la situación de riesgo más habitual a la que se exponen los jóvenes en Internet. Ni que decir tiene que este tipo de comportamientos no pueden ser tolerados en la comunidad de Cibercorresponsales.
Identificar los mensajes que implican una actividad de acoso de los mensajes que simplemente tratan de molestar al destinatario puede ser complejo.
El siguiente documento nos puede ayudar a distinguirlos: PARRY AFTAB Guía práctica para madres y padres. Internet con los menores. Riesgos. Edex – Fundación Esplai. Apéndice IV Ciberbuying. Páginas 161-164.

EL ROBO DE IDENTIDAD

Consiste en obtener la contraseña de un usuario por medio de la sugestión o la amenaza para posteriormente cambiar la clave y hacerse con el control de su cuenta de correo o cuenta de algún otro servicio web. Posteriormente amenazan a los usuarios con enviar mensajes en su nombre o los extorsionan pidiendo dinero o favores a cambio de recuperar su contraseña.

Vigilar los mensajes que solicitan claves, atender las solicitudes de cambio de contraseñas y recomendar a los cibercorresponsales no revelar sus contraseñas son medidas de prevención frente a estas acciones que deben ser siempre investigadas y perseguidas.

EL PHISHING

Consiste en la simulación de páginas webs que simulan ser bancos, entidades de comercio electrónico o cualquier otro tipo de entidad y que pretenden engañar a los usuarios. A veces los autores de phi-

sing publican el botín de sus delitos (números de tarjeta, contraseñas o códigos) en comentarios a foros o blogs ajenos.

Si encontramos mensajes sin sentido aparente compuesto por series numéricas o alfanuméricas en nuestro blog o foro debemos eliminarlos.

EL HACKING

Los mensajes que hacen referencia a la violación de sistemas de seguridad y todas aquellas actividades realizadas por hackers obviamente tampoco están permitidos.

A continuación se describen otras prácticas, que si bien no son ilícitas, pueden dañar gravemente la convivencia y que deben ser prevenidas:

Promoción productos o servicios
Debemos eliminar toda aquella información que solo pretende hacerle publicidad a un negocio o llamar la atención sobre su sitio web.

Comercialización
Las actividades de comercialización de bienes o servicios con ánimo de lucro a través de la comunidad de cibercorresponsales no están permitidas.

Spam
Se llama spam, correo basura a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades que perjudican de alguna o varias maneras al receptor. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es la basada en el correo electrónico.
El correo electrónico no solicitado está terminantemente prohibido por la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE).
Otras tecnologías de Internet que han sido objeto de correo basura incluyen wikis, foros y blogs. Esta práctica de spam consiste en dejar un comentario en una entrada, que por lo general no tiene nada que ver con la misma sino que tiene links a sitios comerciales, o promociona algún producto.

LOS TROLLS

En la jerga de Internet, un troll (a veces trol) es un mensaje u otra forma de participación que busca intencionadamente provocar reacciones predecibles, especialmente por parte de usuarias y usuarios novatos, con fines diversos, desde el simple divertimento hasta interrumpir o desviar los hilos de las discusiones, o bien enfadando a sus participantes y enfrentándolos entre sí. El troll puede ser más o menos sofisticado, desde mensajes groseros, ofensivos o fuera de tema, a sutiles provocaciones o mentiras difíciles de detectar, con la intención en cualquier caso de confundir o provocar la reacción de los demás.
En general, la sabiduría popular aconseja a los usuarios **evitar alimentar a los trolls**, e ignorar las tentaciones de responder. Contestar a un troll lleva la discusión inevitablemente fuera del tema, para consternación de los espectadores, y proporciona al troll la ansiada atención. Mejores resultados suelen obtenerse cuando los usuarios adoptan el papel de moderador y despliegan comportamientos más constructivos evitando juicios y confrontaciones. Los trolls son excitados por los cazadores y frustrados por los indiferentes, y ninguna de estas dos emociones producen resultados positivos para el foro. Hay que tener en cuenta que los adolescentes pueden experimentar el "remordimiento del troll", un sentimiento de gran pesar tras perder su cuenta debido a sus acciones temerarias.

La ofensa
No debemos olvidar que las comunidades virtuales las forman personas reales y que se debe mantener un trato respetuoso hacia el resto de participantes.
El tono con que escribes puede hacer la diferencia. En la red normalmente no tienes gestos, ni entonación o timbre de voz, por lo cual debes vigilar que tus palabras no parezcan muy cortantes o duras. Ten en cuenta que temas controvertidos como la religión, la política o el sexo suelen ser muy susceptibles de ser ofensivos.

La publicación de datos personales
No permitas que se revelen datos personales en foros, blogs o espacios públicos. Siempre investiga quien los ha solicitado y porque e informa a los cibercorresponsales de los

Consejos para la navegación segura

Debemos tener en cuenta que cuando los jóvenes navegan fuera de la comunidad de Cibercorresponsales se enfrentan a nuevos riesgos y retos para su seguridad. Por otro lado muchos cibercorresponsales realizarán su actividad en sus casas o en otros lugares fuera de las instalaciones de nuestra organización. Existen numerosas páginas con consejos para los padres y madres sobre navegación segura referenciadas en el apartado de bibliografía.

Básicamente podemos recomendarles:

- Enseñe a sus hijos e hijas los riesgos de comunicarse en línea con desconocidos.
- Defina reglas familiares de Internet y póngalas a la vista de todo el mundo.
- Fomente la comunicación entre usted y sus hijas e hijos.
- Mantenga los equipos conectados a Internet en un área abierta y fuera de los dormitorios de las y los adolescentes.
- Asegúrese de que sus hijos e hijas no convierten el ordenador en su única amistad: no deben sustituir las relaciones interpersonales.
- Ayúdeles a distribuir su tiempo libre.

Estos mismos consejos debemos aplicárnoslos y tratar de seguir estas recomendaciones. Para elaborar unas reglas de uso de Internet acordes con nuestro grupo podemos basarnos en los siguientes documentos:

Consejos para padres y educadores sobre navegación segura
http://chaval.red.es/de11a13/padreseducadores/padreseducadores.shtml

Sitio de Microsoft sobre seguridad e infancia
http://www.microsoft.com/latam/athome/security/children/kidtips13-17.mspx

Contrato paterno filial para una navegación segura.
PARRY AFTAB Guía práctica para madres y padres.
Internet con los menores. Riesgos. Edex-Fundación Esplai.

Es importante llegar a estos consensos de forma participativa con las y los jóvenes teniendo en cuenta su opinión y contando con su colaboración.

Referencias y enlaces

Agencia Española de Protección De Datos. Guía del responsable de ficheros.

Agencia Española de Protección De Datos. Derechos de los niños y niñas y deberes de los padres y madres. Recomendaciones.

Agencia española de protección de datos: https://www.agpd.es/

Conceptos básicos y límites de los derechos de autor: http://www.cedro.org/limites.asp

Ley de la propiedad intelectual: http://www.sgae.es/resources/pdf/9/4/1159365773049.pdf

Creative Commons: http://es.creativecommons.org/

Nettiqueta. La buena educación en la red: http://es.wikipedia.org/wiki/Netiquette

La violencia contra los niños en el ciberespacio:
http://www.ecpat.net/EI/Publications/ICT/Cyberspace_SPA.pdf

Consejos para padres y educadores sobre navegación segura
http://www.iqua.net/Recomendaciones/Consejos_para_padres_y_educadores/?go=WWiW6aWP3cIUyUj7fiM3LUP2TCyKxjHYpx1BRAqqMzW5kPpV3BzlHkc0YA==

Guía Orange para padres sobre uso de teléfono móvil, Internet y televisión
http://www.chaval.es/docs/guia_de_padres.pdf

Sitio de Microsoft sobre seguridad e infancia
http://www.microsoft.com/latam/athome/security/children/kidtips13-17.mspx

PARRY AFTAB Guía práctica para madres y padres. Internet con los menores. Riesgos. Edex – Fundación Esplai.

Sitio web de Protégeles sobre seguridad en Internet dedicado a padres y educadores
http://ciberfamilias.com/index.htm

TeachToday ofrece a los profesores/as recursos para el uso responsable y seguro de las nuevas tecnologías de la comunicación: http://es.teachtoday.eu/