Plan de Seguridad y Confianza Digital

C/ Dr. González Álvarez, 11 - 24350 - Veguellina de Órbigo (León) - tel. 987 37 41 13

Junta de Castilla y León
Consejería de Educación

Equipo TIC 24/25

IES RÍO ÓRBIGO

1. Introducción y objetivos

1.1. Introducción

La Comisión Europea lanzó en marzo de 2010 la «estrategia Europa 2020», que incluye, entre otras iniciativas, la creación de la Agenda Digital Europea, con el objetivo de convertir a la Unión Europea en una potencia tecnológica y digital para 2020, al mismo tiempo que se garantiza la confianza y seguridad en el uso de las Tecnologías de la Información y la Comunicación (TIC). En el marco de esta estrategia, el Consejo de Ministros aprobó el 15 de febrero de 2013 la creación de la Agenda Digital para España, que incluye más de 100 acciones organizadas en torno a seis grandes objetivos, uno de los cuales es reforzar la confianza en el entorno digital.

La Ley Orgánica 8/2013, de 9 de diciembre, para la mejora de la calidad educativa, menciona en su preámbulo que las TIC serán fundamentales para impulsar el cambio metodológico necesario para mejorar la calidad educativa. Además, establece que el uso responsable y ordenado de estas tecnologías por parte del alumnado debe ser parte integral de todo el sistema educativo. Las TIC también se consideran herramientas clave para la formación continua del profesorado y para el aprendizaje a lo largo de la vida de los ciudadanos, ya que permiten compatibilizar la formación con otras obligaciones personales o laborales, además de ser esenciales para la gestión de los procesos educativos.

En este contexto, la Consejería de Educación de la Junta de Castilla y León considera fundamental promover el desarrollo de las TIC en el ámbito educativo de manera segura y responsable. Con ese fin, la Dirección General de Innovación Educativa y Formación del Profesorado, a través de la Resolución del 17 de octubre de 2014, lanzó el proyecto piloto denominado «Plan de Seguridad y Confianza Digital en el ámbito educativo» durante el curso 2014-15, con el objetivo de coordinar, informar, difundir y promover el uso seguro de internet entre los miembros de la comunidad educativa.

Tras el éxito de este proyecto y la consecución de sus objetivos durante el curso 2014-15, se decidió regularlo mediante una orden para consolidarlo y seguir desarrollándolo en los próximos años. Así, el 14 de octubre de 2015 se publicó la ORDEN EDU/834/2015, que regula el «Plan de Seguridad y Confianza Digital en el ámbito educativo» en la Comunidad de Castilla y León.

En este marco, nuestro Centro promueve el uso seguro, crítico y responsable de las Tecnologías de la Información y la Comunicación (TICA) entre todos los miembros de nuestra comunidad educativa, especialmente entre el alumnado.

1.2. Objetivos

- Fomentar la educación digital entre todos los integrantes de la comunidad educativa.
- Enseñar cómo utilizar Internet de forma segura.
- Informar sobre los riesgos más comunes al navegar por la red.
- Promover el uso adecuado de las TIC a través de la organización de talleres y actividades.
- Impulsar el uso responsable y seguro de las TIC dentro del centro educativo.

2. Aplicación del plan en el centro

2.1. ¿Qué es la seguridad?

La seguridad se puede entender como:

- La ausencia de peligro o riesgo.
- La sensación de total confianza en algo o alguien.

Cuando hablamos de seguridad en el ámbito digital, nos referimos a las medidas preventivas que adoptamos para evitar los posibles peligros o riesgos en la red, es decir, en Internet.

En el contexto educativo, es importante considerar los siguientes aspectos relacionados con la seguridad digital:

- Se debe abordar la seguridad digital de manera integral en todos los ámbitos que impliquen acceso a Internet (como el correo electrónico, los servidores del centro, las aulas virtuales, las páginas web, etc.), donde podrían existir riesgos.
- Es fundamental fomentar en el alumnado una actitud protectora frente a los riesgos que pueden presentarse en la red, así como promover el uso adecuado de la seguridad digital.
- Establecer directrices claras de seguridad digital para garantizar un funcionamiento correcto y seguro de las Tecnologías de la Información y la Comunicación (TIC).

2.2. Cuándo aplicarla

Existen diferentes momentos en los que se debe aplicar la seguridad digital en el centro, según el momento en que se necesite. Estos momentos son:

- **Antes**: De forma preventiva, para evitar posibles ataques o amenazas que puedan llegar a través de la red. Para esto, se utiliza software como antivirus y cortafuegos, que son necesarios para bloquear dichas amenazas.
- **Durante**: De manera reactiva, verificando que las herramientas que protegen la red del centro estén funcionando correctamente y evitando intrusiones.
- **Después**: De forma restaurativa, estableciendo protocolos para actuar frente a una amenaza que ya haya ocurrido.

El coordinador TIC revisa el incidente e intenta solucionarlo utilizando un software que restaure el sistema. Si esta medida no funciona, se contacta al servicio técnico de informática del centro.

Todas las acciones realizadas en el mantenimiento de los equipos serán registradas y comunicadas al equipo directivo.

2.3. ¿Dónde?

Los ámbitos en los que se debe aplicar la protección para garantizar la seguridad digital en el centro educativo son los siguientes:

- **Hardware**: En los equipos informáticos, asegurándose de que estén actualizados según las necesidades, para que los programas funcionen correctamente (como ampliaciones de memoria RAM, entre otras). También es importante conectar correctamente los dispositivos a las conexiones físicas adecuadas de Internet y mantener en buen estado los armarios de Swift y los módems.
- **Software**: Instalando programas informáticos actualizados (como antivirus y protección para USBs) que aseguren la protección de los equipos informáticos.
- **Usuarios**: Capacitando a las personas (profesores y alumnos) que utilizan los equipos informáticos para que adopten comportamientos seguros en el entorno digital y sean conscientes de los riesgos que pueden surgir si no se aplican adecuadamente las estrategias de seguridad digital.

2.4. Estrategias de seguridad digital utilizadas

2.4.1. Copias de seguridad

El centro dispone de copias de seguridad del servidor principal, lo que permite recuperar los datos en caso de sufrir un ataque digital. Esta información puede ser restaurada en cualquier momento, ya que se guarda en dispositivos de la dirección provincial. Las acciones se llevarán a cabo según lo establecido, garantizando la protección de los datos y la seguridad física.

2.4.2. Antivirus

Los ordenadores cuentan software de protección instalado por el Centro de Atención al Usuario en el ámbito educativo de la Junta de Castilla y León.

2.4.3. DNS

Los servidores DNS son utilizados por todos los ordenadores del centro para evitar posibles riesgos. Tanto el Centro de Atención al Usuario (CAU) como el Sistema Integrado de Gestión e Información Educativa (SIGIE) de la Junta de Castilla y León y de la Dirección Provincial de Educación de León, disponen de la red mapeada con todas las DNS.

2.4.4. Correo corporativo

El personal docente y el alumnado del centro emplean el correo electrónico corporativo (@educa.jcyl.es) para acceder de manera segura a los datos que puedan enviarse a través de la red.

2.4.5. Página WEB

La web del centro se encuentra alojada en una web oficial asociada al dominio educa.jcyl.es.

2.4.6. Red Wifi

La red wifi disponible en el centro pertenece a la red de Escuelas Conectadas. De gestión por parte de la Junta de Castilla y León, los protocolos de seguridad se corresponden con el acceso de cualquier usuario con cuenta educa.

Para posibles casos de riesgo en la protección de datos, será el CAU Educativo el responsable de asegurar que la red se encuentra convenientemente asegurada.

2.4.7. Estrategias recomendables

El profesorado del centro organiza actividades de formación en las que se promueven estrategias para un uso responsable de la red, alertando sobre los posibles riesgos, ayudando a prevenirlos y promoviendo los beneficios del uso de las TIC.

Se informa a toda la comunidad educativa sobre la importancia de cumplir con las obligaciones legales (uso adecuado de la red, talleres, circulares informativas, etc.) en relación con la seguridad digital.

2.4.8. Contraseñas

A los equipos informáticos se accede con usuario y contraseña de la cuenta educa.

La instalación de software en los dispositivos digitales se hace desde el centro de software, aplicación controlada por el CAU Educativo donde se alojan los principales programas para la instalación segura. En caso de necesitar la instalación de un programa que no esté en ese repositorio, se llama al CAU para que lo instalen de forma remota, si es posible.

Al finalizar el curso, se eliminará la información de los equipos utilizados por el alumnado y profesorado, en un proceso controlado por el CAU Educativo.

2.4.9. Evaluación de la Seguridad

Se establecen estrategias para evaluar los riesgos que puede sufrir el centro.

- El coordinador TIC revisa frecuentemente los equipos informáticos para comprobar que no han sufrido ataques, virus, u otros aspectos que tienen que ver con la seguridad digital.
- La instalación y mantenimiento de los programas de gestión (GECE, IES2000, etc.) se realizará desde el SIGIE de la Dirección Provincial de León. No se permitirá la alteración de la configuración de la red de centro ya que se realizó con criterios comunes a todos los centros ya que puede tener incidencia importante en los procesos educativos y formativos del profesorado.
- La evaluación en la seguridad de las redes wifi se realiza de forma remota por el CAU Educativo.

2.4.10. Estrategias a largo recorrido

Se establece una comisión TIC en el centro, formada por miembros con experiencia en las TIC, con el objetivo de mejorar de manera continua y actual todos los aspectos relacionados con las TIC y la seguridad digital.

Además, los equipos directivos podrán contar con el apoyo, asesoramiento e información proporcionada por el Área de Programas Educativos y el CAU Educativo sobre las operaciones tecnológicas que se puedan llevar a cabo con los equipos del centro.

3. Actuaciones de formación para la comunidad educativa

3.1. Alumnado

Objetivos

- Ofrecer formación e información sobre diversos temas relacionados con el uso seguro, crítico y responsable de Internet.
- Capacitar en aspectos vinculados a la seguridad y confianza digital, gestión de riesgos en Internet y administración de la seguridad en dispositivos móviles, considerando estos aspectos como elementos clave para la innovación y calidad.
- Promover el debate sobre la relevancia de las redes sociales y su papel fundamental.

Actividades

- Siempre que sea posible, el Departamento de Orientación promoverá la realización de charlas para alumnos en colaboración con la policía y Guardia Civil.
- Celebración del Día de Internet Segura. En el mes de febrero, que sirva para concienciar sobre el uso seguro de las TIC.

3.2. Profesorado

Objetivos

- Dinamizar el uso seguro de las TIC en el alumnado.
- Capacitar en diversos aspectos relacionados con la seguridad y confianza digital, manejo de riesgos en Internet y gestión de la seguridad en dispositivos móviles, considerándolos como factores clave para la innovación y la calidad.

Actividades

- Realización de actividades de concienciación desde las materias, en especial desde el Departamento de Tecnología.
- Elaboración junto a los alumnos de actividades relacionadas con el día de internet segura.

3.3. Familias

Objetivos

- Proporcionar información sobre diversos temas relacionados con el uso seguro, crítico y responsable de Internet, en la web del centro.
- Fomentar la reflexión y la sensibilización sobre el rol fundamental que las familias deben tener en la relación de sus hijos con las nuevas tecnologías.
- Promover el debate sobre la influencia y el impacto de las redes sociales en la vida de sus hijos.

Actividades

- Información para las familias sobre el uso seguro de Internet, que tienen disponible en la web del centro.
- Asesoramiento en cuanto a seguridad de cuentas educa, gestión de contraseñas y uso seguro de Stilus y otras herramientas.

4. Actuaciones de prevención y actuación ante el ciberbullying

4.1. Introducción

El uso de Internet se ha extendido en la sociedad debido a las numerosas ventajas que ofrece en diversas áreas de nuestra vida. Esto también se aplica a los niños y niñas, quienes utilizan las nuevas tecnologías de forma natural. Internet les brinda un amplio abanico de oportunidades para el entretenimiento, la cultura, el aprendizaje y el conocimiento en general. Además, actúa como un espacio de socialización que contribuye a su desarrollo personal.

Sin embargo, este entorno también presenta algunas amenazas. Es nuestra responsabilidad trabajar para minimizar los riesgos, ya que, en general, los beneficios son mucho mayores, y por ello, el uso de Internet es una apuesta innegociable. Uno de los problemas que afectan a la sociedad en general y al entorno educativo en particular es el ciberacoso.

El ciberacoso es un fenómeno de gran importancia debido a su alta prevalencia, la gravedad de sus consecuencias y las dificultades que presenta para prevenirlo y abordarlo. Cuando ocurre entre niños, niñas y adolescentes, los efectos pueden ser devastadores, especialmente en un entorno donde se utilizan Internet y la telefonía móvil.

Aunque no siempre se manifieste en el ámbito escolar, es crucial que la comunidad educativa se involucre en su prevención y eliminación, para así promover el uso adecuado de Internet y las nuevas tecnologías, favoreciendo el bienestar del alumnado. Entre los factores que dificultan su manejo están el anonimato, la inmediatez, el efecto en cadena, la alta disponibilidad y la diversidad de canales y métodos utilizados para llevarlo a cabo.

4.2. ¿Qué es el ciberbullying?

El ciberacoso es el uso de las TIC (Internet, telefonía móvil, videojuegos conectados en línea, etc.) para llevar a cabo un acoso psicológico entre iguales. Esto significa que puede ocurrir, ser sufrido o presenciado en cualquier lugar y en cualquier momento.

El hecho de que el ciberbullying se lleve a cabo en línea o a través del teléfono móvil implica una invasión del espacio personal de la víctima, afectando incluso su hogar.

4.3. Cómo se manifiesta

Contar con claves que ayuden a detectar situaciones de ciberbullying es esencial para intervenir eficazmente frente a este tipo de problemas, los cuales tienden a empeorar significativamente a medida que se prolongan en el tiempo. Por lo tanto, identificar el problema lo antes posible permite abordarlo en sus primeras etapas y, en consecuencia, con menores consecuencias para las personas involucradas.

Sin embargo, saber qué es el ciberbullying no es suficiente para garantizar que podamos detectar todos los posibles casos que puedan ocurrir en nuestro entorno.

Otra característica del ciberbullying es la "ley del silencio". Por ello, es crucial contar con indicadores que nos ayuden a contrarrestar esta ley del silencio y a identificar situaciones que podrían representar un riesgo de ciberbullying. Las formas que adopta son muy diversas y solo están limitadas por las habilidades tecnológicas y la creatividad de los menores acosadores. A continuación, se presentarán algunos ejemplos concretos:

- Subir a internet una imagen comprometedora (real o manipulada) o información que pueda dañar o avergonzar a la víctima y difundirla en su círculo social.
- Registrarse en un sitio web donde se elige a la persona más fea o desagradable, utilizando la foto de la víctima y asignándole votos para que aparezca en las primeras posiciones.
- Crear un perfil o espacio falso a nombre de la víctima, donde se compartan intimidades o se hagan solicitudes explícitas de contactos sexuales, entre otras cosas.

- Dejar comentarios ofensivos en foros o participar de manera agresiva en chats haciéndose pasar por la víctima, para que las reacciones negativas se dirijan a quien ha sufrido la suplantación de identidad.
- Registrarse en sitios web con la dirección de correo electrónico de la víctima, exponiéndola a spam, contactos indeseados, etc.
- Robar la contraseña del correo electrónico de la víctima para leer los mensajes que recibe, invadiendo su privacidad e impidiendo que el propietario legítimo acceda a su cuenta.
- Provocar a la víctima en servicios web que tienen moderadores (como chats, juegos online, comunidades virtuales...) para conseguir que reaccione violentamente, lo que, al ser denunciado, cause su exclusión del servicio.
- Difundir rumores sobre un comportamiento inadecuado, ofensivo o desleal por parte de la víctima, de modo que otros crean en ellos y actúen en represalia o acosen a la persona afectada.
- Enviar mensajes amenazantes por correo electrónico o SMS.
- Acechar y seguir a la víctima en los sitios web en los que se relaciona habitualmente, provocándole estrés y malestar.

4.4. Ciberbullying: fenómeno en crecimiento

Alta disponibilidad

Las nuevas tecnologías (Internet, móvil, etc.) están cada vez más integradas en la vida de los menores. Esto facilita que el acoso pueda ocurrir en cualquier lugar y en cualquier momento, sin que el acosador y la víctima necesiten coincidir ni en el espacio ni en el tiempo.

Importancia en aumento

El ciberespacio juega un papel cada vez más importante en la socialización de nuestros menores. Por esta razón, el acoso en este entorno digital puede ser tan traumático, o incluso más, que un caso de abuso en el ámbito escolar.

Menor percepción del daño causado

Cuando el abuso ocurre de manera tradicional, la víctima y el acosador se conocen y están cerca, incluso cara a cara, lo que permite que tanto el abusador como los testigos presencien directamente las consecuencias del acoso. Sin embargo, en los casos de ciberbullying esto no sucede, lo que hace que sea menos probable que la actitud acosadora disminuya o que los testigos intervengan para defender a la víctima.

Mayor número de candidatos

La víctima no necesariamente tiene que ser un compañero de clase o un vecino. Puede ser cualquier persona a la que se pueda llegar a través de Internet, el móvil o los videojuegos. Quien lleva a cabo el abuso no tiene que ser fuerte, valiente, contar con el apoyo del grupo o estar respaldado por otros.

En este contexto, que requiere tan pocas condiciones de las partes involucradas, las posibilidades de que se dé el acoso son muchas.

Sensación de impunidad

Detrás del ordenador o del móvil, el acosador siente que está en el anonimato, aunque esto no sea completamente cierto. Además, incluso si se descubre su identidad, no es común que los responsables escolares, ni su madre ni su padre, intervengan de manera efectiva.

Adopción de roles y actitudes aceptadas

En ocasiones, el abuso se lleva a cabo como un juego en el que el acosador no es consciente del daño que está causando. Otras veces, ni siquiera considera las consecuencias de sus acciones, ya que se atribuye a un personaje o rol que interpreta en la Red. Esto dificulta que el acosador reconozca su comportamiento y decida abandonarlo.

Características propicias de internet

La facilidad para agrupar a los hostigadores, ya sean conocidos o no, y pedir su colaboración de forma rápida, junto con la sencilla reproducción y distribución de contenidos audiovisuales, son factores que, en algunos casos, juegan un papel clave en la aparición o consolidación de una situación de ciberacoso.

Miedo a la pérdida de permisos de uso

En ocasiones, quienes son acosados no piden ayuda porque temen que al confesarse “metidos en problemas” se les limite o retire el uso de Internet, el teléfono móvil o los videojuegos.

4.5. Medidas de prevención

Desde el Centro promovemos las siguientes acciones para prevenir los casos de acoso:

- Fomentar el trabajo y juego cooperativo.
- Educar a los niños y niñas en sus derechos.
- Fomentar la identificación y superación de estereotipos y prejuicios en el alumnado, promoviendo relaciones basadas en el respeto.

- Desarrollar habilidades y valores como la empatía, la asertividad, la solidaridad y el respeto mutuo.
- Identificar situaciones de violencia.
- Ayudar a los estudiantes a reconocer sus emociones y a expresarlas adecuadamente.
- Fomentar la búsqueda y solicitud de ayuda, evitando ocultar lo que ocurre, y enseñar que la denuncia es un paso fundamental para superar experiencias injustas y prevenir delitos.
- Trabajar a través de charlas, debates, talleres, etc., el uso responsable y seguro de Internet (Plan TIC).

4.6. Recomendaciones para los alumnos

Para garantizar la seguridad de nuestros niños y niñas en la red, es fundamental transmitirles una serie de recomendaciones y analizarlas con ellos. Además del trabajo para concienciarlos sobre los riesgos y precauciones en el uso de las diferentes TIC, también es crucial fomentar una socialización que rechace cualquier tipo de violencia hacia ellos y hacia los demás.

Datos personales y seguridad

- Ten mucho cuidado con la información personal: nombre, teléfono, dirección, centro escolar, etc. No la compartas. Cuanto menos sepan de ti, mejor. Piensa bien en lo que compartes en chats o incluso en salas privadas, ya que esto puede ser usado por otros para obtener tus datos. Utiliza siempre apodos o nombres ficticios. No te confíes de estar completamente seguro/a al otro lado de la pantalla.
- Si usas un dispositivo público o compartido, asegúrate de cerrar sesión correctamente en tu correo, aula virtual, página de Educacyl, etc., para que nadie pueda acceder a tus contraseñas ni utilizar tus cuentas personales.
- Crea contraseñas seguras, únicas para cada actividad, y cámbialas con regularidad. Para que sean seguras, deben contener letras mayúsculas, minúsculas y números.
- Coloca un código de acceso en tu Tablet, teléfono u ordenador.
- Si tu dispositivo tiene una webcam, tápala con un pedazo de cinta, pegatina, etc., cuando no la estés utilizando, para evitar que otros puedan acceder a ella.
- Instala un antivirus en tu ordenador, pero recuerda que no sustituye la prudencia y una navegación responsable.

La red

- No hagas en la Red lo que no harías en persona.
- Nunca respondas a una provocación, especialmente si estás enfadado/a. Es mejor calmarse primero. Si contar hasta diez no te ayuda, haz algo que te distraiga durante unos minutos antes de regresar al ordenador. Responder suele ser lo que más contenta al ciberacoso y solo empeora el problema. Advierte al acosador que está cometiendo un delito.
- No aceptes solicitudes de amistad de personas que no conoces en la vida real.
- Si te están molestando, sal de la conexión y busca ayuda.
- No te dejes engañar en las redes. No descargues archivos de fuentes desconocidas, piensa dos veces antes de abrir correos de personas que no conoces, y desconfía de ofertas increíbles o regalos de extraños.
- Si el acoso o amenaza persiste, guarda pruebas de lo sucedido (aunque no tengan valor legal, guarda o imprime los mensajes o lo que aparezca en pantalla), cierra la conexión y busca ayuda de un adulto.
- Si tienes dudas de que hayan publicado información sobre ti en línea, puedes usar Google para buscar tu nombre o apodo y ver si hay algo relacionado contigo en la Red.

Antes de compartir

- Todo lo que publiques en internet es fácil de localizar y puede difundirse rápidamente.
- No puedes garantizar que lo que envíes se mantendrá únicamente en el dispositivo de quien lo recibe.
- Ten cuidado con lo que compartes, ya que esto influye en la opinión que los demás puedan formarse sobre ti.
- Todo lo que subas a la red puede quedar allí de forma permanente. Recuerda que alguien podría haberlo descargado o capturado en pantalla.

No seas ciberacosador/a ni cómplice

- Evita usar las redes sociales para insultar, menospreciar o acosar a otros.
- No distribuyas contenido ofensivo bajo ninguna circunstancia.
- Respeta la privacidad y la intimidad de las demás personas.
- Si recibes una imagen ofensiva sobre alguien, elimínala de inmediato y solicita que no se comparta.
- Rechaza la difusión de mensajes que puedan ofender o perjudicar a otros.

- Bloquea a quienes se comporten de forma acosadora en el entorno digital.
- Denuncia cualquier conducta inapropiada o contenido de acoso que encuentres en las redes. Informar sobre estas situaciones es completamente confidencial y no requiere revelar tu identidad.

4.7. Cómo actuar si existe una sospecha de ciberbullying

- No restar importancia a las acciones de los agresores.
- Observar de manera constante y detallada el comportamiento del niño o la niña en todos los entornos.
- Comunicar lo sucedido al tutor y al equipo directivo utilizando una hoja de observación donde se detallen los hechos y los involucrados con la mayor precisión posible.
- Actuar con la mayor rapidez, aplicando las medidas previamente establecidas.
- Realizar intervenciones individuales con todas las personas implicadas: la víctima, los agresores y los testigos.
- Evitar la mediación, ya que esta situación implica un desequilibrio de poder entre las partes.
- No culpar ni a la víctima ni a los agresores, para evitar que aumente la intimidación o se generen sentimientos de resentimiento.
- Trabajar con todo el grupo para fomentar el rechazo generalizado hacia actitudes y comportamientos negativos.
- Respetar el derecho del niño o la niña a decidir con quién desea hablar sobre el problema.

5. Enlaces de interés

Instituciones

- Ministerio de Educación, Cultura y Deporte http://www.mecd.gob.es/
- Policía Nacional http://www.policia.es/org_central/judicial/udef/bit_alertas.html
- Instituto Nacional de Ciberseguridad https://www.incibe.es/
- Asociación de Internautas http://www.internautas.org/
- Agencia Española de Protección de Datos https://www.agpd.es/
- Asociación Española de Pediatría http://www.aeped.es
- Fundación CTIC http://www.fundacionctic.org/
- Asociación ACPI http://www.protegeles.com/
- Asociación Española de Usuarios de Internet http://aui.es/
- Family Online Safety Institute (FOSI) http://www.fosi.org/
- Portal de Sociedad de la Información de la Unión Europea http://ec.europa.eu/information_society
- International Association of Internet Hotlines (INHOPE) https://www.inhope.org
- Self-regulation for a Better Internet for Kids http://ec.europa.eu/information_society/activities/sip/index_en.htm
- Planm Avanza http://www.planavanza.es/
- Childnet International http://www.childnet-int.org/
- Observatorio de Sociedad de la Información en Castilla y León http://www.orsi.es

Otras páginas web

- Seguridad en la Red http://www.seguridadenlared.org/
- Protégeles: Línea de denuncia http://www.protegeles.com/
- Internet sin Acoso http://www.internetsinacoso.com/
- Tecnoadicciones http://www.tecnoadicciones.com/
- Portal del menor http://www.portaldelmenor.es/
- Ciberfamilias http://www.ciberfamilias.com
- Educared http://www.educared.net/
- Chaval.es http://chaval.red.es
- Safer Internet http://www.saferinternet.org/
- Pantallas Amigas http://www.pantallasamigas.net/
- El Programa Safer Internet de la Unión Europea http://ec.europa.eu/information_society/activities/sip/index_en.htm
- Ciberbullying http://www.ciberbullying.net/
- SafeKids http://www.safekids.com/