CEIP MIGUEL DELIBES (Burgos)

PLAN DE SEGURIDAD Y CONFIANZA DIGITAL

Junta de Castilla y León
Consejería de Educación

Ceip Miguel Delibes
Caminamos juntos

CoDiCe TIC Excelente

INDICE Pág

1. INTRODUCCIÓN Y OBJETIVOS

Introducción

La Comisión Europea puso en marcha en marzo de 2010 «la estrategia Europa 2020», que contiene entre otras iniciativas la creación de la Agenda Digital Europea cuya finalidad es conseguir que la Unión Europea sea en 2020 una potencia tecnológica y digital, a la vez que se garantice la confianza y seguridad en el uso de las Tecnologías de la Información y la Comunicación (TIC). Dentro de este marco europeo, el Consejo de Ministros de 15 de febrero de 2013 aprobó la creación de la Agenda Digital para España con más de 100 líneas de actuación estructuradas en torno a seis grandes objetivos, uno de los cuales consiste en reforzar la confianza en el ámbito digital.

La Ley Orgánica 8/2013, de 9 de diciembre, para la mejora de la calidad educativa indica en su preámbulo que las TIC serán una pieza fundamental para producir el cambio metodológico que lleve a conseguir el objetivo de mejora de la calidad educativa. Asimismo, establece que el uso responsable y ordenado de estas nuevas tecnologías por parte del alumnado debe estar presente en todo el sistema educativo. Las TIC serán también una herramienta clave en la formación del profesorado y en el aprendizaje de los ciudadanos a lo largo de la vida, al permitirles compatibilizar la formación con las obligaciones personales o laborales y, asimismo, lo serán en la gestión de los procesos.

En este sentido, la Consejería de Educación de la Junta de Castilla y León considera de especial importancia impulsar el desarrollo de las tecnologías de la información y la comunicación en el ámbito educativo de forma segura y responsable. A tal efecto, la Dirección General de Innovación Educativa y Formación del Profesorado, mediante Resolución de 17 de octubre de 2014, puso en marcha con carácter experimental, en el curso 2014-15, el proyecto denominado «Plan de Seguridad y Confianza Digital en el ámbito educativo», como elemento de coordinación, información, difusión y promoción del uso seguro de internet por parte de los miembros de la comunidad educativa.

Después de la experiencia satisfactoria del proyecto y vista la consecución de sus objetivos durante el curso 2014-15, se considera oportuno regular este proyecto mediante Orden con el fin de consolidarlo y seguir desarrollándolo en los cursos venideros. Por esta razón, 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.

Bajo este marco, nuestro Centro fomenta el uso seguro, crítico y responsable de las TICA entre todos los miembros de nuestra comunidad educativa, en especial del alumnado.

Objetivos generales

- Impulsar la alfabetización digital de todos los miembros de la comunidad educativa.
- Formar sobre el uso seguro de Internet.
- Informar sobre las situaciones de riesgo más habituales al navegar por Internet.

- Difundir el buen uso de las TICA mediante la organización de talleres, experiencias…
- Dinamizar el uso seguro de las TICA en el centro.

2. APLICACIÓN DEL PLAN EN EL CENTRO

2.1. ¿Qué es la seguridad?

La seguridad se puede definir como:

- Ausencia de peligro o riesgo.
- Sensación de total confianza que se tiene en algo o alguien.

La seguridad trasladada al ámbito digital se puede definir como la protección que desarrollamos de forma preventiva para evitar posibles peligros o riesgos que pueden darse en la red de redes "Internet".

En el centro educativo hay que tener en cuenta estos aspectos relacionados con la seguridad digital:

- Hay que tener en cuenta la seguridad digital de forma transversal en todos los ámbitos (e-mail, servidor de centro, aulas virtuales, webs,…) en los que se tiene acceso a Internet y que existe la posibilidad de correr algún riesgo.
- Fomentar en el alumnado la importancia de crear una actitud de protección ante los riesgos que se pueden dar en la red y el correcto uso de la seguridad digital.
- Establecer en las directrices de seguridad digital para desarrollar el correcto funcionamiento de TICA.

2.2. Cuándo aplicarla

Existen distintos momentos donde hay que aplicar la seguridad digital en el centro según el momento en el que haya que aplicarla. Los momentos son:

- Antes: De modo preventivo para evitar los posibles ataques o amenazas que puedan llegar a través de la red. Para ello se cuenta con software (antivirus, cortafuegos) necesarios para evitar las amenazas.
- Durante: De modo reactivo, comprobando el correcto funcionamiento de las herramientas que evitan la intrusión en la red del centro.
- Después: De forma restaurativo, donde se establecen unos protocolos de actuación para actuar ante una amenaza ya ocurrida.
  El coordinador Tic revisa la incidencia e intenta repararla pasando un software para restaurar el problema. Si la medida no es efectiva se avisa al servicio técnico de informática con la que cuenta el centro.
  Todas las operaciones que se realicen en el mantenimiento de los equipos serán registradas y serán puestas en conocimiento del equipo directivo.

2.3. ¿Dónde?

Los lugares donde hay que aplicar la protección para conseguir la seguridad digital en el centro educativo es:

- Hardware: En los equipos informáticos, manteniéndolos actualizados en función de las necesidades para que los programas puedan funcionar correctamente (ampliaciones de memoria ram, …). También conectando correctamente los dispositivos a las conexiones físicas correctas de Internet. Manteniendo los armarios de Swift y módem correctamente.
- Software: Instalando programas informáticos (antivirus, vacunas de usb,…) actualizados para la protección de los equipos informáticos.
- Usuarios: Formando a las personas (profesores y alumnado) que utilizan los equipos informáticos para que desarrollen unas actitudes de seguridad digital y sensibilidad ante las posibles amenazas que pueden suceder si no se utilizan correctamente las estrategias de seguridad digital.

2.4 Estrategias de seguridad digital utilizadas

Copias de seguridad.

El centro cuenta con copias de seguridad de los diferentes ordenadores de aula y equipos directivos que permiten recuperar datos que pueden ser atacados por algún ataque digital.
Dicha información se puede recuperar en cualquier momento ya que es guardada en dispositivos físicos (Pendriver) y de forma virtual (Onedrive de la Junta Castilla y León)
Se actuará conforme a lo establecido, proporcionando protección de los datos y seguridad física. El almacenamiento se realizará con cifrado y con copias de seguridad en dispositivos de almacenamiento extraíble.
Sobre el manejo de datos existe el protocolo de fotocopiar en un papel especial y concreto que incluirá un sello de confidencial.

Antivirus.

Los ordenadores cuentan software de protección ofrecido por Microsoft Security Essentials y Panda Security USB Vaccine.

DNS.

Los servidores DNS son utilizados por todos los ordenadores del centro para evitar posibles riesgos. En la zona privada del equipo directivo se utilizan las DNS corporativas 10.151.126.17 y 10.151.126.21.

Correo corporativo.

El personal docente y alumnado del centro utilizan el correo corporativo (@educa.jcyl.es) para realizar un acceso seguro a los datos que se puedan enviar a través de la red.

Página WEB

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

Red Wifi.

La red wifi con la que se cuenta en el centro se encuentra localizada en las aulas desde las que se da acceso con contraseñas a los dispositivos digitales que cuenta con el alumnado.
Dichos dispositivos de emisión de wifi serán sustituidos por los dispositivos que Escuelas conectadas (EE.CC.) dotarán en un futuro.

Estrategias recomendables.

El profesorado del centro establece actividades de formación donde se promueven estrategias para realizar un uso adecuado de la red, avisando de los posibles riesgos, ayudando a evitarlos y fomentando los beneficios del uso de las TICA.
Se informa a toda la comunidad educativa de la importancia de respetar las obligaciones legales (uso adecuado de la red, talleres, circulares informativas…) ante la seguridad digital.

Contraseñas.

Los equipos informáticos tienen contraseñas que se encuentran en poder del equipo directivo y del coordinador TIC.
La instalación de software en los dispositivos digitales necesita de la autorización del coordinador TIC para que puedan ser instalados en los equipos. De esta forma se evita la instalación de programas que puedan violar la seguridad digital del centro.
Generaremos hábitos y contraseñas seguras, para minimizar y evaluar nuestros propios riesgos y peligros.
AL finalizar el curso se borrará la información de los equipos que manejan los alumnos y el profesorado.
El equipo directivo y coordinador TIC tendrá que conocer y custodiar todas las claves y registrarlas en el documento de Red de Centro. Cambiándolas por lo una vez al año.

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 (Escuela, GECE 2000, Colegios, etc.) se realizará desde el SIGIE de la Dirección Provincial de Burgos.
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

Estrategias a largo recorrido.

Se crea una comisión TICA en el centro compuesta por unos miembros que mantienen un vinculo con las TIC para ir mejorando de forma progresiva y actual todos los aspectos relacionados con TICA y con la seguridad digital.

Se podrá contar con el apoyo, el asesoramiento y la información a los equipos directivos desde el Área de Programas Educativos sobre operaciones tecnológicas que se puedan realizar con los equipos del centro.

3. ACTUACIONES DE FORMACIÓN PARA LA COMUNIDAD EDUCATIVA

3.1. Alumnado

Objetivos

- Formar e informar sobre diferentes temas de interés relacionados con el uso seguro, crítico y responsable de Internet.
- Formar sobre diferentes aspectos relativos a la seguridad y confianza digital, gestión de peligros en Internet y administración de la seguridad en dispositivos móviles como elementos de innovación y calidad.
- Debatir sobre el importante papel que juegan las redes sociales.

Actividades

- **Realización de charlas para alumnos de 4º, 5º y 6º, en colaboración con la policía municipal de Burgos**.
  - 4º EPO- "Consejos para navegar en la red"
  - 5º EPO- "Riesgos en internet"
  - 6º EPO- "Uso de las redes sociales" y "Ciberacoso"
- **Realización de talleres para alumnos de 3º, 4º, 5º y 6º**
  La impartición de estos talleres se llevará a cabo por el profesorado del centro con el apoyo del material elaborado por la Consejería de Educación y seleccionado por el profesorado. (Anexo I)
  http://www.educa.jcyl.es/plandeseguridad/es
  http://apeburgos.es/tic/Plan_Seguridad_Burgos/
- **Realización y exposición de vídeos relacionados con el tema.**
- **Celebración del Día de Internet Segura**.
  En el mes de febrero, que sirva para concienciar sobre el uso seguro de las TICA.

3.2. Profesorado

Objetivos:

- Dinamizar el uso seguro de las TICA en el alumnado.

- Formar sobre diferentes aspectos relativos a la seguridad y confianza digital, gestión de peligros en Internet y administración de la seguridad en dispositivos móviles como elementos de innovación y calidad.

Actividades

- **Realización de talleres para el profesorado, en las sesiones del seminario de Red XXI y la participación de charlas ofrecidas por la policía.**
- **Elaboración junto a los alumnos de videos de internet segura.**

3.3. Familias

Objetivos:

- Informar sobre diferentes temas de interés relacionados con el uso seguro, crítico y responsable de Internet.
- Reflexionar y sensibilizar acerca del importante papel que pueden y deben jugar las familias en cuanto a la relación de sus hijos con las nuevas tecnologías.
- Debatir sobre el importante papel que juegan las redes sociales en sus hijos.

Actividades

- **Realización de talleres para las familias sobre el uso seguro de Internet.**
  Para la realización de estos talleres se utilizará el material elaborado por la Consejería de Educación. (ANEXO I)

4. ACTUACIONES DE PREVENCIÓN Y ACTUACIÓN ANTE EL CIBERBULLYING

4.1. Introducción

El uso de Internet se ha generalizado en la sociedad por las múltiples ventajas que nos aporta en las más diversas facetas de nuestra vida. No es diferente en el caso de niños, niñas quienes, además, utilizan las nuevas tecnologías de manera natural. Internet les ofrece un universo de oportunidades para el ocio, la cultura, el aprendizaje... para el conocimiento en general. Es también un entorno de socialización que, como tal, contribuye a su desarrollo personal.

No obstante, tal entorno viene acompañado de algunas amenazas. Es nuestra labor trabajar por maximizar los beneficios y reducir al máximo los efectos negativos que pueder producirse porque, en todo caso, el saldo es muy positivo y, por lo tanto, la apuesta irrenunciable. Entre los problemas que afectan a la sociedad en general y al entorno educativo en particular se encuentra el ciberbullying.

Se trata de un fenómeno de gran relevancia por su prevalencia, la gravedad de sus consecuencias y las dificultades que presenta para su prevención y abordaje. Cuando se produce entre niños, niñas y adolescentes, los efectos pueden ser devastadores, puesto que se derivan del uso no adecuado de tecnologías tan poderosas y cotidianas como Internet y la telefonía móvil.

Independientemente de que se manifieste o no en el contexto escolar, la comunidad educativa debe conocer cuál es la mejor forma de detectarlo, afrontarlo y erradicarlo, para poder así contribuir al uso adecuado de Internet para favorecer el desarrollo óptimo del alumnado. Esta no es tarea fácil debido a las singulares características del acoso por medio de las nuevas tecnologías: anonimato, inmediatez, efecto en cadena, alta disponibilidad y diversidad de canales y procedimientos, entre otros.

4.2. ¿Qué es el ciberbullying?

Es el uso de las TIC (Internet, telefonía móvil, videojuegos conectados on-line...) para ejercer el acoso psicológico entre iguales. Esto implica que puede ser ejercido, padecido y presenciado desde cualquier lugar y en cualquier momento. El hecho de que el ciberbullying se desarrolle on-line o usando el teléfono móvil conlleva una invasión del espacio personal de la víctima, incluido el hogar

4.3. ¿Cómo se manifiesta?

Contar con claves que faciliten la detección de situaciones de ciberbullying es uno de los pilares fundamentales de la intervención frente a este tipo de problemas que caracterizan, entre otras cosas, por agravarse de forma significativa mientras se prolongan en el tiempo. Por tanto, **detectar lo antes posible** el problema significará abordarlo en la fase más incipiente y, por tan tanto, con menores consecuencias para los implicados.

Sin embargo, conocer lo que es ciberbullying no es suficiente para asegurar la detección de los posibles casos que puedan estar aconteciendo en nuestro entorno. Otra característica del ciberbullying es la **ley del silencio**. Es necesario contar con **indicadores** que nos ayuden a contrarrestar esta ley del silencio y que nos permitan descubrir aquellas situaciones que podrían suponer un riesgo de ciberbullying.

Las **formas** que adopta son **muy variadas** y solo se encuentran limitadas por la pericia tecnológica y la imaginación de los/as menores acosadores/as. Veamos algunos ejemplos concretos:

- Colgar en Internet una imagen comprometida (real o trucada) o datos que pueden perjudicar o avergonzar a la víctima y darlo a conocer en su entorno de relaciones.
- Dar de alta a la víctima, con foto incluida, en un sitio web donde se elige a la persona más fea, a la más repelente... y cargarle de “votos” para que aparezca en los primeros lugares.

- Crear un perfil o espacio falso en nombre de la vict , donde esta comparta intimidades, realice demandas explícitas de contactos sexuales, etc.
- Dejar comentarios ofensivos en foros o participar agresivamente en chats haciéndose pasar por la víctima, de modo que las reacciones adversas vayan dirigidas a quien ha sufrido la usurpación de personalidad.
- Dar de alta en determinados sitios la dirección de correo electrónico de la persona acosada para que sea víctima de spam, de contactos con desconocidos, etc.
- Robar su clave de correo electrónico para leer los mensajes que le llegan a su buzón, violando su intimidad, e impedir que su legítimo propietario lo consulte.
- Provocar a la víctima en servicios web que disponen de una persona que vigila o modera lo que allí sucede (chats, juegos on-line, comunidades virtuales...) para conseguir una reacción violenta que, una vez denunciada, suponga la exclusión de quien no es sino una víctima.
- Poner en circulación rumores acerca de un comportamiento reprochable, ofensivo o desleal por parte de la víctima, de modo que sean otras personas quienes, sin poner en duda lo que leen, ejerzan acciones de represalia o acoso.
- Enviar menajes amenazantes por e-mail o SMS.
- Perseguir y acechar a la víctima en los lugares de Internet en los que se relaciona de manera habitual, provocándole estrés.

4.4. Ciberbullying : un fenómeno en crecimiento

Alta disponibilidad
Las nuevas tecnologías (Internet, móvil...) están cada vez más presentes en la vida de los menores. Ello facilita que el acoso se pueda perpetrar desde cualquier lugar y momento, sin necesidad de que abusón y víctima coincidan ni en el espacio ni en el tiempo.

Importancia en aumento
El "ciberespacio" tiene cada vez más peso en la socialización de nuestros menores. Por ello, un acoso en este "mundo" puede llegar a ser tan traumático o más que una situación de abuso en el centro escolar.

Menor percepción del daño causado
Cuando el abuso se produce de la manera tradicional, víctima y acosador se conocen, están cerca o incluso cara a cara, de manera que tanto el que abusa como el grupo de testigos asisten de manera directa a las consecuencias del acoso. En los casos de ciberbullying esto no es así, por lo que la remisión de la actitud acosadora o la intervención defensiva de los testigos es improbable.

Mayor número de candidatos
La víctima no tiene por qué ser un compañero de clase o una vecina. Puede ser cualquier persona a la que lleguemos por medio de Internet, el móvil o los videojuegos. Quien abusa no tiene por qué ser fuerte, valiente, contar con el beneplácito del grupo o estar protegido por terceros. En este contexto, que exige tan pocas condiciones a las partes intervinientes, las posibilidades son múltiples.

Sensación de impunidad
Detrás del ordenador o del móvil, quien acosa tiene sensación de anonimato, lo que no es del todo cierto. Además, aunque descubran su identidad, no es frecuente que haya de los responsables escolares, su madre o su padre.

Adopción de roles y actitudes aceptada
En ocasiones, el abuso se produce como un juego en el que quien acosa no es consciente del daño que ocasiona. Otras veces, ocurre que ni siquiera se plantea las consecuencias de su acción, ya que ésta se atribuye a un personaje o rol que es interpretado en la Red. Esto hace más difícil que el acosador se reconozca en su papel y lo abandone.

Características propicias de Internet
El fácil agrupamiento de hostigadores -sean conocidos o no- a quienes se puede pedir colaboración de manera rápida, así como la cómoda reproducción y distribución de contenidos audiovisuales son otros factores que, en ciertos casos, resultan determinantes para que surja o se consolide 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 medidas para prevenir los casos de acoso.

- Fomentar el juego y trabajo cooperativo.
- Educar en derechos a los niños/as.
- Propiciar en nuestro alumnado la identificación y superación de estereotipos y prejuicios para promover relaciones basadas en el respeto.
- Desarrollar en nuestros alumnos habilidades y valores de empatía, asertividad, solidaridad y respeto mutuo.
- Identificar situaciones de violencia.
- Identificar sus emociones y saber expresarlas a los demás.
- Buscar y solicitar ayuda. No ocultar lo que sucede. Aprender que la denuncia es un paso necesario para superar las experiencias injustas y evitar delitos.
- Trabajar mediante charlas, debates, talleres… el uso responsable y seguro en la Red. (Plan TICA).

4.6. Recomendaciones para los alumnos/as

Para que nuestros niños y niñas estén seguros en la red hay una serie de recomendaciones que debemos transmitirles y analizar con ellos/as. No debemos olvidar además de este trabajo de toma de conciencia sobre los riesgos y precauciones en el uso de las diferentes TIC, hay que sumar la construcción de una socialización que rechace cualquier actitud de violencia hacia ellos/as y hacia otras personas.

Datos personales y seguridad

- Sé muy cuidadoso con los datos personales: nombre, teléfono, dirección, fotografías, centro escolar... No los proporciones. Cuanto menos sepan de uno/a, mejor. Reflexiona sobre lo que expones abiertamente en chats o incluso en las salas privadas, ya que pueden ser pistas que otros utilicen para obtener tus datos. Usa siempre apodos y nombre figurados. No pienses que estás del todo seguro/a al otro lado de la pantalla.
- Siempre que utilices un dispositivo público o compartido cierra bien la sesión: correo, aula virtual, página de educacyl… de manera que otras personas no puedan acceder a tus contraseñas o utilizar tus páginas personales.
- Genera contraseñas seguras, diferentes para cada actividad y cámbialas con frecuencia. Para ser seguras, las contraseñas deben contener mayúsculas, minúsculas y números.
- Instala un código de acceso en la Tablet.
- Si tu dispositivo dispone de webcam, para que no puedan acceder otras personas, cuando no la estés utilizando, puedes taparla con un celo, pegatina, etc.
- Instala antivirus en tu ordenador, aunque este no sustituye la prudencia y navegación responsable.

La Red

- Presta especial atención a la netiqueta (reglas de comportamiento en Internet como saludar, usar emoticonos para expresar estados de ánimo, no escribir en mayúsculas...). Además, hay que considerar que los/as interlocutores/as pueden tener otra cultura, otro contexto social o malinterpretar nuestras palabras. Si se produce un malentendido, trata de aclararlo con cortesía.
- No hagas en la Red lo que no harías a la cara.
- Nunca debes responder a una provocación y mucho menos si eres presa de la furia. Es mejor calmarse antes. Si contar hasta diez no te vale, haz algo que te entretenga durante unos minutos antes de volver a sentarte delante del ordenador. Responder suele ser la mayor alegría que le puedes dar al ciberabusón y un paso hacia el agravamiento del problema. Advierte a quien abusa de que está cometiendo un delito.
- No agregues a nadie que no conozcas en a vida real.
- Si te molestan, abandona la conexión y pide ayuda.
- No te dejes engañar en las redes. No descargues archivos de procedencia desconocida, piensa bien antes de abrir un correo electrónico de alguien que no conoces, desconfía de extraños que te presentan ofertas increíbles y regalos.
- Cuando la amenaza o el acoso persiste, es recomendable guardar pruebas de lo sucedido (aunque no tenga validez legal, guarda o imprime el mensaje o lo que aparezca en pantalla), cerrar la conexión y pedir ayuda a una persona adulta.
- En previsión de que hayan podido publicar on-line informaciones sobre ti, puedes utilizar Google para buscar tus datos (nombre, apodo...) y ver si hay algo en la Red que hace referencia a tu persona.

Antes de compartir…

- Cualquier cosa que se cuelga en la red es fácil de encontrar y fácilmente se puede difundir.
- Nadie te puede asegurar que solo permanecerá en el dispositivo de la persona a quien se lo has enviado.
- Cuida lo que compartes ya que ayuda a que otras personas se creen una opinión de ti.
- Cualquier cosa que cuelgues en la red puede permanecer ahí para siempre. Piensa que alguien puede habérsela descargado o hecho una captura.

No seas ciberacosador/a ni cómplice

- No utilices las redes sociales para insultar, menospreciar o acosar a otras personas.
- No compartas material ofensivo con nadie.
- Respeta la intimidad y privacidad de los otros.
- Si te llega alguna imagen ofensiva de otra persona, bórrala y exige que no se reenvíe.
- Niégate a pasar mensajes que ofendan a otras personas.
- Bloquea la comunicación con personas ciberacosadoras.
- Denuncia las malas conductas o contenidos acosadores que detectes en las redes. Informar sobre estas actitudes es confidencial, no hace falta identificarse.

4.7. Cómo actuar si existe una sospecha de ciberbullying

- No minimizar la gravedad de los agresores.
- Observar de manera sistemática al niño/a en todos los espacios.
- Informar al tutor y al equipo directivo, mediante una hoja de observación, donde se recojan los hechos y los implicados con la mayor precisión posible.
- Intentar actuar lo más rápido posible, tomando las medidas acordadas.
- Hacer intervenciones individuales con las personas involucradas: las víctimas, los agresores y los observadores.
- No hacer mediación, porque se trata de una situación en la que existe un desequilibrio de poder.
- No culpabilizar ni a la víctima ni a los agresores ya que puede acrecentar la intimidación y provocar resentimiento.
- Intervenir con todo el grupo para que las actitudes y conductas negativas sean rechazadas por todos y todas.
- Respetar el derecho del niño/a a elegir la persona a quien desee contarle el problema.

En caso de detección de ciberacoso seguiremos el **PROCEDIMIENTO DE ACTUACIÓN ANTE SITUACIONES DE CONFLICTO PROVOCADAS POR LA UTILIZACIÓN INADECUADA DE LAS NUEVAS TECNOLOGÍAS (INTERNET, TELÉFONOS MÓVILES) Y ESPECIALMENTE EN CASOS DE CIBERACOSO, CIBERABUSO Y OTRAS SITUACIONES DE CIBERAGRESIÓN. Que está en nuestro Plan de convivencia**

Burgos, 31 de enero de 2020

COMISIÓN TICA

ANEXO I

MATERIAL SELECCIONADO DEL PORTAL DE EDUCACIÓN

http://www.educa.jcyl.es/plandeseguridad/es

http://apeburgos.es/tic/Plan_Seguridad_Burgos/

→ Aspectos legales del uso de Internet
A Descarga recursos de forma legal
A Usa legalmente tu correo electrónico

→ Búsquedas
B Buscadores infantiles
B Búsqueda efectiva
B Búsqueda segura
B Búsquedas en Internet

→ Navega seguro
C Navega en privado

→ Netiqueta
D Normas de comportamiento en la Red

→ Seguridad y confianza digital
E Aplicaciones móviles
E Contraseñas seguras
E Seguridad y dispositivos móviles

→Talleres con alumnos
- Taller navegación segura
- Buenas prácticas en Internet
- Día internacional de Internet segura

→Talleres con familias
- Aplicaciones móviles
- Control parental
- Navegación segura
- Uso seguro en internet
- Privacidad menores en Internet

TODOS ESTOS TALLERES SE ENCUENTRAN **EN EL ANEXO 8. del Plan TICA**

ANEXO II

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 pág. 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/