DECALOGO CIBERSEGURIDAD

IES Eulogio Florentino Sanz

Curso 2022-2023

Junta de Castilla y León
Consejería de Educación

PROFESORES DEL IES QUE HAN REALIZADO ESTE DECÁLOGO DE NORMAS DE CIBERSEGURIDAD

Daniel Piñero Fernandez
Diana Arroyo Calzada
Jorge Tabanera Serra
Eva María Tudela Calvo
Javier Fernandez Abad
María Mateo Rodriguez
Agustín Carpizo Vallejo
Francisco Gracia Sotos

Decálogo de normas de Ciberseguridad
Tecnología y Digitalización – Música – Inglés – Filosofía – Robótica.

Código del centro: 05000427
Denominación: IES Eulogio Florentino Sanz
Domicilio: Avenida de Emilio Romero, 22
Localidad: Arévalo Código postal: 05200 Provincia: Ávila
Teléfono: 920300221 Fax: 920303458
Correo electrónico: 05000427@educa.jcyl.es
Página web: http://ieseulogioflorentinosanz.centros.educa.jcyl.es

Enseñanzas que imparten: Educación Secundaria Obligatoria, Bachillerato y Formación Profesional

Nuestro agradecimiento a la **GUARDIA CIVIL** de la Comandancia de Avila y al **INCIBE,** por habernos prestado contenidos para la realización de este documento.

En la dirección **seguridadescolar@policia.es** se pueden concertar charlas para los alumnos y alumnas e informarles de como utilizar internet con responsabilidad y seguridad.

Contenido

I. Introducción

Tener a los alumnos y alumnas bien informados en cuanto al consumo y/o difusión de contenidos en las redes, influye directamente en el uso correcto y responsable de la tecnología. La digitalización también permite mejorar este aprovechamiento gracias a la automatización de los procesos, facilitando la gestión, administración y seguridad, así como reduciendo tiempos y costes de producción en el desarrollo de los proyectos, pero hay que indicar los riesgos que hay o puede haber por el hecho de utilizarlos ya que es un entorno que no está exento de peligros y abusos. Este es nuestro objetivo, el objetivo de este Decálogo.

"Todos los niños y las niñas sin excepción, tienen el derecho a ser protegidos de todas las formas de violencia y al desarrollo de todo su potencial de aprendizaje en un ambiente seguro"

Niño buscando en Internet contenidos

Artículo 19 de la Convención de Naciones Unidas sobre los Derechos del Niño

Internet es una zona llena de oportunidades, intercambio de información o comunicaciones con nuestros amigos, realizar proyectos del instituto, adquirir información en empresas de prestigio o que nos aporten. Crear blog, páginas, donde compartir experiencias o descubrimientos con nuestro círculo más próximo. Pero …..

Internet y las nuevas tecnologías entrañan riesgos que debemos de conocer para combatirlas y no participar en ellos.

Un uso excesivo produce ciberdependencia, es decir, cuesta trabajo desconectarse de internet o de la red.

Mucho tiempo conectado o delante de una pantalla, bien de ordenador o del teléfono, produce dolor de cabeza, de espalda, insomnio, afecta a nuestro peso, es perjudicial para la vista y sobre todo y más importante: abusando de su uso vamos a perder un tiempo valioso con los estudios, para la práctica del deporte, con nuestros amigos y lo más enriquecedor ….. vamos a perder experiencias positivas en la vida o con las personas que más queremos.

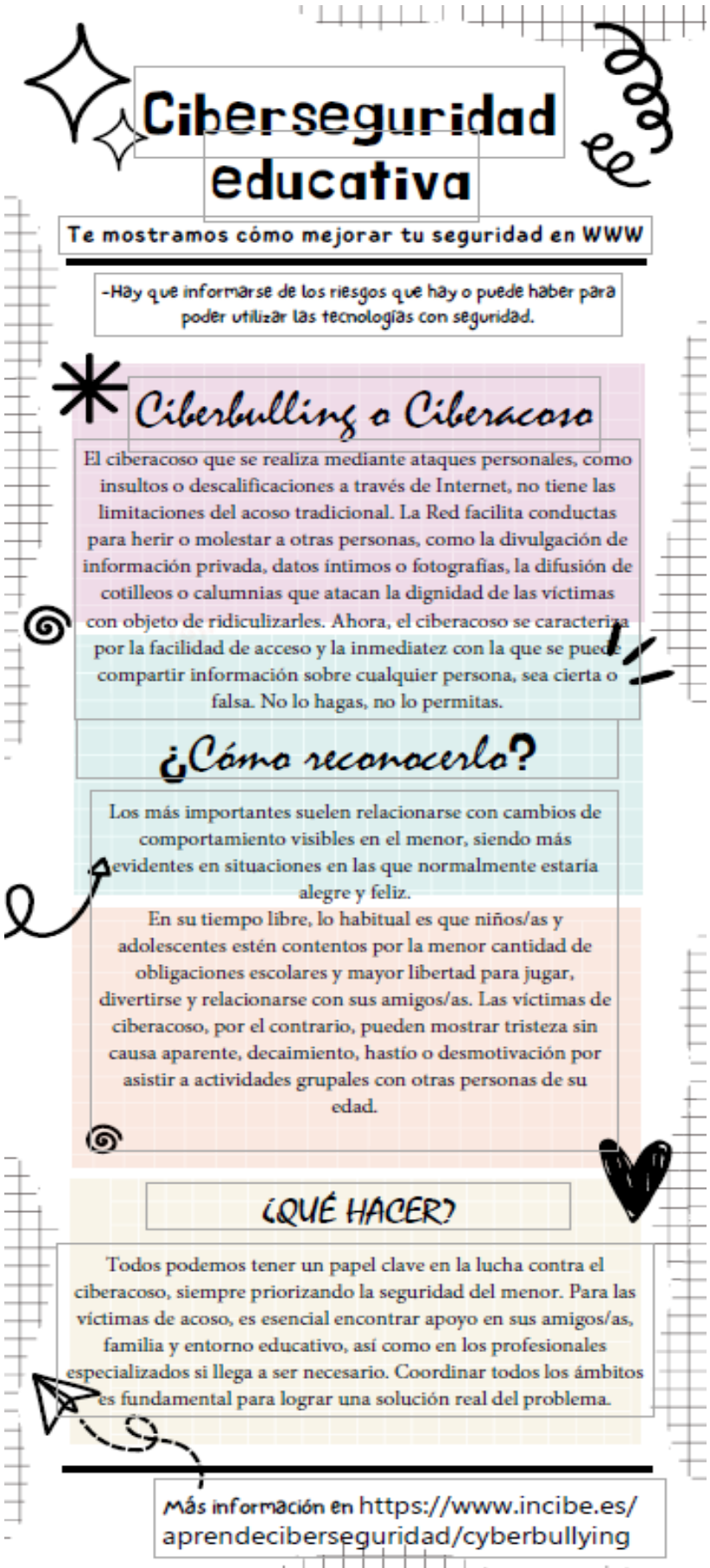
En este Decálogo, nos vamos a centrar, dentro de la multitud de casuística que se produce por un mal uso y abuso de Internet en el Ciberbulling o Ciberacoso, sexting o sexteo, grooming, phishing o ciberfraude. Todos ellos muy relacionados.

II. Objetivos

- Entender el concepto de **ciberbulling o ciberacoso.**
- Entender el concepto de **sexting o sexteo.**
- Entender el concepto de **grooming.**
- Entender el concepto de **phishing o ciberfraude.**

III. CIBERBULLING O CIBERACOSO ➔Acoso Virtual

Ciberacoso y Ciberbulling ➔ Hay que poner remedio inmediatamente. Son mensajes intimidantes, violentos o amenazantes a través de redes sociales, o por los móviles ➔ no hay que callarse. Hay que denunciarlo.
Hay que protegerte y proteger a aquellos que te rodean, no perder de vista internet y las tecnologías de la información y la comunicación tambien te abren a un mundo de oportunidades para usar tu creatividad, investigar, comunicarte, producir contenido, generar acciones, etc.....



IV. SEXTING O SEXTEO

https://view.genial.ly/5fbd77b302156b0d0ec1fc65/presentation-que-pasa-si-haces-y-compartes-una-foto-sin-consentimiento

V. GROOMING

Recuerda:

- No des ningún dato personal ni de casa a ningún internauta desconocido.
- De vez en cuando, haz un barrido a quien tienes en tus redes y si hay alguien desconocido, indaga quien es. Si no lo sabes: borrale o bloqueale. Si es amigo o amiga ya te llamará, primero es tu SEGURIDAD.
- Existen internautas que se hacen pasar por personas que NO son lo que dicen ser, con el objetivo de acercarse a menores, para obtener imágenes o en casos extremos acordar citas, esto es **Grooming** y comienza con una conversción que puede parecer inocente y desisteresada.

- Respetar la edad recomendada en películas, videos, juegos, etc… El Fornite es un juego catalogado para mayores de 12 años. Es un juego adictivo desaconsejado por la UE y la OMS.

VI. PHISHING O CIBERFRAUDE.

El ***phishing*** es una técnica que consiste en el envío de un correo electrónico por parte de un ciberdelincuente a un usuario simulando ser una entidad legítima (red social, banco, institución pública, etc.) con el objetivo de robarle información privada, realizarle un cargo económico o infectar el dispositivo. Para ello, adjuntan archivos infectados o enlaces a páginas fraudulentas en el correo electrónico.

Normalmente, además, bloquean el teléfono de su víctima y toman el control de nuestra tarjeta SIM de tal manera que el Banco, al enviar un mensaje de verificación, es el delincuente el que efectua el control. Realiza compras de elementos electrónicos que luego vende en las redes a un precio muy inferior.

La empresa de ciberseguridad Clario nos comparte su último estudio, en el que parte de un listado de más de 30 parámetros que recopilan las grandes marcas, datos que principalmente provienen del uso de sus apps o plataformas. Esas mismas en las que **solemos hacer clic en "aceptar" sin leer la información sobre el uso que se le dará a los datos y cookies.**

- ¿Qué saben estas empresas de nosotros? La respuesta es: **TODO** (lo que quieran saber). Por ejemplo:
- Terminos que buscas, es decir, tú histórico de búsquedas.
- Los videos que ves en cualquier programa o aplicación.
- Visualizaciones y las interacciones con el contenido y los anuncios.
- Información sobre voz y audio cuando utilizas funciones de audio.
- Actividades de compra. Páginas que visitas, donde y asiduidad de tus compras.
- Usuarios con los que te comunicas o compartes contenidos.
- Actividad en sitios WEB y aplicaciones de terceros que utilizan nuestros servicios. Toda la actividad realizada en Internet, queda registrada con nuestra IP.
- Historial de navegación de Chrome que has sincronizado con tu cuenta google o cualquier aplicación.
- Ubicación con acceso a GPS, dirección IP, datos de los sensores, información de los elementos cercanos al telefono como wifi, bluetooch activados.
- Facebook recopila más del 70% de los datos de usuario.
- Google resume las ubicaciones por donde hemos estado y teniendo la “ubicación” desactivada.

¿Qué debes hacer ante un incidente?

Denunciar en cualquier puesto para que sea investigado por:

Dialogar con tus padres y educadores, con naturalidad, sobre el contenido no apropiado que encuentras y cómo te sientes ante él

Denuncia o reporta un contenido inapropiado. Líneas de denuncia anónima. Ejemplo: Google+; Consejos de Google

Unidades especializadas de investigación: Policía Nacional, Guardia Civil

Denunciar en cualquier puesto para que sea investigado por:

VII. Webgrafía:

- https://es.wikipedia.org/wiki/Ciberacoso
- https://en.wikipedia.org/wiki/Cyberbullying
- https://en.wikipedia.org/wiki/Sexting
- https://es.wiktionary.org/wiki/grooming
- https://es.wikipedia.org/wiki/Phishing
- https://es.wikipedia.org/wiki/Delito_informatico
- https://www.incibe.es/
- https://www.guardiacivil.es/es/institucional/actividades_escolares/index.html
- https://www.policia.es/_es/tupolicia_conocenos_infantil_portada.php
- http://www.ciberexperto.org/ (para padres y profesores)
- https://www.youtube.com/watch?v=DaHqVBPN9X8 (recomendado para todos y todas)
- https://www.youtube.com/watch?v=HfsMnKVfspY (recomendado para todos y todas)
- https://www.cuerpomente.com/psicologia/por-que-ninos-no-deben-jugar-fortnite-explicacion-psicologica_6919
- https://www.youtube.com/watch?v=SSjdJgINu2E
- https://www.osi.es/es/campanas/ingenieria-social (para padres y profesores)
- https://www.incibe.es
- https://www.is4k.es

VIII. Consejillos:

- “Siempre que os metais en páginas de internet, procurar que la URL comience por http**s**, es decir, que tenga la “**s**” al final de la dirección”. Eso quiere decir que es una página segura.
- No hacer fotos subidas de tono o comprometidas (ni a los amigos o amigas, novios o novias) y subirlas a la RED (whatsapp, tiktok, instagram, facebook, telegram, etc…) y cuidado con enviar fotos a un grupo distinto en el que estais habitualmente.
- El teléfono NO es tuyo, es de tus padres (a su nombre está la línea, el contrato y es quien paga la factura), vosotros sois menores. Por lo que deben de saber que utilidad le das, para asesoraros sobre su uso correcto y responsable.
- En vuestros dispositivos, debereis de tener instalado un antivirus y los padres tener acceso al dispositivo. En caso de necesitar tener acceso a el, son a quienes primero van a preguntar. Apuntar IMEI, contraseña y modelo de móvil y que lo tengan los padres.
- Tambien es conveniente tener instalado APP de Geolocalización y hacer un grupo con los padres, EXCLUSIVAMENTE. Los padres son vuestros protectores y si sucede algo, son vuestros más fieles aliados. No se lo pongais dificil, facilitarles que os ayuden.
- Acoso tambien es:
    - Ignorar a alguien.
    - Meterse con él o ella.
    - Enviar un montón de whatsapp a esa persona.
- No hablar o whatsappear si estás con alguien, es de mala educación.
- Cuidado con la playstation: aisla de tu entorno.
- El móvil fuera de la habitación, sobre todo cuando duermes.
- El propietario red WIFI donde te conectes, tiene acceso a los números de teléfonos.
- Los padres estarán atentos con quien juegan en juegos online. Hay intrusos con perfiles falsos, aunque eso ya lo sabeis.
- El tener perfil en las redes sociales está prohibido para menores 14-16 años (art. 13 del Real Decreto 1720/2007, de 21 de diciembre).
- Cuidado con las autorizaciones de App´s, hay que leerlas.
- Redes ➔ El abuso provoca ansiedad, depresión, exclusión social.

IX. Redes o Plataformas más utilizadas.

Las redes más habituales donde se conectan nuestros chicos y chicas son:

- WeChat: servicio de mensajería de texto móvil.
- Twitter: servicio de microblogging.
- Tumblr: plataforma de microblogeo que permite a los usuarios compartir textos, imágenes, enlaces, audios, citas…
- Pinterest: plataforma para compartir imágenes.
- Reddit: sitio web de marcadores sociales y agregador de noticias.
- Snapchat: aplicación de mensajería efímera. Sus imágenes y mensajes son sólo accesibles durante un periodo de tiempo corto.
- Foursquare: servicio basado en la localización web aplicada a redes sociales. Permite localizar un dispositivo fijo o móvil en una ubicación geográfica.
- Youtube: sitio web dedicado a compartir vídeos.
- Flickr: sitio web que permite almacenar, ordenar, buscar, vender y compartir fotografías o vídeos en línea.
- Tik Tok: aplicación para crear y compartir vídeos cortos.

Para luchar contra todas estas redes, algunas de estas plataformas han creado alternativas dirigidas a los más pequeños.

- Es el caso de Youtube Kids, apta para niños de entre 2 y 8 años, o Messenger Kids.

Y por último:

"

Formación mejor que imposición

"

Esperamos que os ayude a tener cuidado y a utilizar todas estas herramientas y recursos en la generación de contenidos positivos para todas las personas.


¡Gracias!
Esperamos que toméis nota y tengáis cuidado al utilizar esta herramienta tan básica en nuestros tiempos.
El profesorado del
IES EULOGIO FLORENTINO SANZ.
10-02-2023
Firma
Fecha