Contenido Unidad

[Protección contra contenido inapropiado]

Project: B-SAFE
Number: 2018-1CZ01-KA204-048148
Name of author: bit cz training
Last processing date: 24.6.2020

Funded by the
Erasmus+ Programme
of the European Union

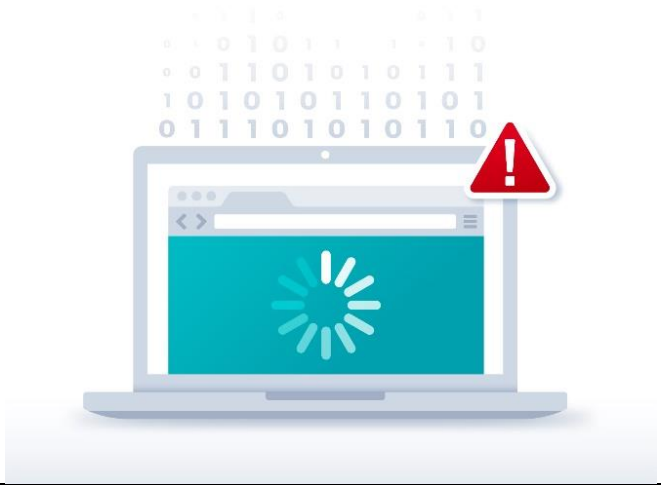
"The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein."

Co-funded by the
Erasmus+ Programme
of the European Union

Protección contra contenido inapropiado

Introducción

Internet, en esta era digital, nos ofrece la posibilidad de explorar un mundo virtual sin las limitaciones del mundo real. El contenido en Internet no se divide por edades o áreas apropiadas para el desarrollo. ¡Y ese es el problema! Algunos contenidos pueden ser ilegales, inapropiados, ofensivos o inadecuados para algunos grupos de edad. Sin supervisión y orientación, cualquier persona, incluso un niño pequeño, puede encontrar contenido perturbador, explícito o inapropiado. Muchos sitios web perturbadores no son "ilegales", lo que significa que nadie los supervisa y administra. Ver accidentalmente contenido en línea inapropiado puede tener un efecto traumático, especialmente en sus hijos. El ejemplo de contenido inapropiado podría ser: promover el odio basado en la raza, religión, discapacidad, preferencia sexual, extremismo violento, contenido sexual explícito, violencia real o simulada. Como padre, debe proteger y guiar a sus hijos durante sus primeros pasos en Internet y educarlos para que se conviertan en usuarios de Internet responsables e independientes.



Relevancia práctica: ¿para qué necesitas estos conocimientos y habilidades?

Después de aprender esta unidad de contenido, sabrá qué es contenido inapropiado, qué incluye y cómo protegerse contra él.
Además, aprenderá sobre métodos para difundir contenido inapropiado y sobre el impacto en la vida cotidiana.

Descripción general de los objetivos y competencias de aprendizaje

En OA_ Protección contra contenido inapropiado _O1 conocerá todos los aspectos importantes que están ocultos bajo contenido inapropiado y cómo protegerse contra él.
En OA_ Protección contra contenido inapropiado _O2, verá cómo el contenido inapropiado afecta a niños y adultos, así como a su vida privada y a su trabajo.
En OA_ Protección contra contenido inapropiado _O3, verá fuentes y medidas de Internet útiles para proporcionar información sobre contenido inapropiado y cómo comportarse de manera segura en Internet.

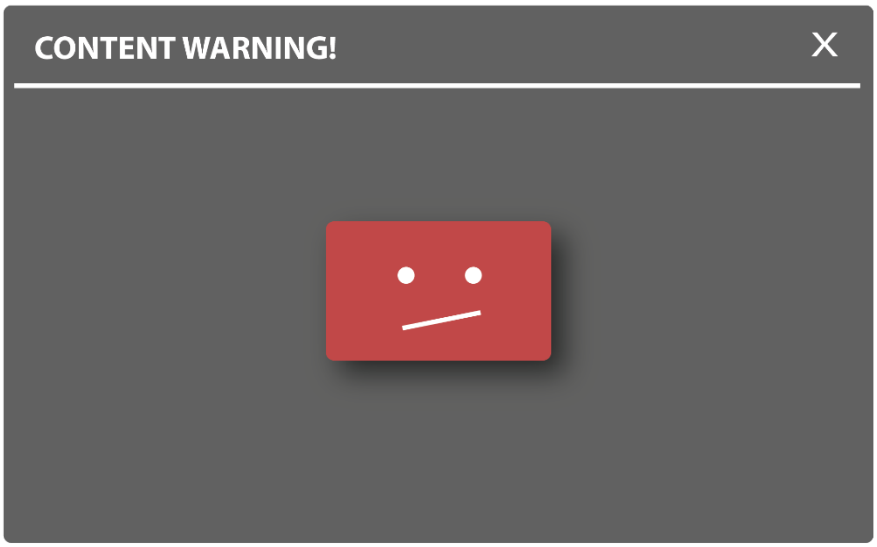
Objetivos de Aprendizaje (OA)	Objetivos específicos (OE)

OA_ Protección contra contenido inapropiado_01: conoce la caracterización de contenido inapropiado.	OE_ Usted conoce la caracterización de contenido inapropiado. 01_01: puede nombrar los tipos de contenido inapropiado. OE_ Usted conoce la caracterización de contenido inapropiado. 01_02: puede nombrar los métodos para difundir contenido inapropiado y obtener información confidencial. OE_ Usted conoce la caracterización de contenido inapropiado_01_03: puede nombrar las formas de calificar y revisar la idoneidad del contenido. OE_ Usted conoce la caracterización de contenido inapropiado_01_04: puede reconocer contenido no seguro en Internet.
OA_ Protección contra contenido inapropiado_02: conoce las amenazas de abuso de información confidencial y su impacto.	OE_ Usted conoce las amenazas de abusar de la información confidencial y su impacto. 02_01: puede describir el impacto de difundir contenido inapropiado en los niños. OE_ Conoce las amenazas de abusar de la información confidencial y su impacto. 02_02: puede describir el impacto de difundir contenido inapropiado en su vida privada y en su trabajo. OE_ Conoces las amenazas de abusar de información confidencial y su impacto. 02_02: Puedes caracterizar los grupos objetivo que podrían ser víctimas de apuntar a contenido inapropiado.
OA_ Protección contra contenido inapropiado_03: sabe cómo protegerse contra contenido inapropiado.	OE_01: Puede administrar y denunciar abuso, spam o contenido inapropiado en el sitio web de redes sociales. OE_02: Puede encontrar los contactos y las fuentes útiles para ayudar a mantenerse a salvo y protegerse del abuso. OE_03: Puede explicar cómo bloquear páginas con contenido inapropiado. OE_04: Puede nombrar los enfoques técnicos para evitar la captura de información confidencial. OE_05: Puede nombrar las razones por las cuales cierta información personal no debe publicarse en línea. OE_06: Puede comprender la medida legislativa de la UE contra la difusión de contenido inapropiado.

Co-funded by the
Erasmus+ Programme
of the European Union

1. ¿Qué es contenido inapropiado?

Contenido inapropiado es un término utilizado para capturar un número amplio y cada vez mayor de diferentes tipos de contenido problemático en línea.



El contenido generalmente inapropiado es cualquier cosa que viole los derechos del niño según lo definido por la Convención sobre los Derechos del Niño y todo lo que viole los derechos humanos según lo definido por la Carta de Derechos y Libertades Fundamentales, en particular el derecho a la vida, la privacidad, la información, protección y el derecho a participar en la sociedad, a ser protegidos del abuso y la violencia. Puede ser cualquier cosa, desde discursos de odio hasta imágenes de autolesiones o sitios web pro-ana. El contenido inapropiado puede incluir los siguientes temas:

- Pornografía
- Violencia, comportamiento extremista
- Productos peligrosos
- Racismo u odio
- Websites proanorexia
- Websites con contenido extremista

Para mostrar las características de estos subtemas, los veremos en detalle:

Pornografía

La pornografía se define como una descripción o imagen explícita destinada a estimular los sentimientos sexuales. Sin embargo, la pornografía puede ser obscena o no serlo, siempre que se argumente que la obra tiene valor literario, artístico, político o científico. Pero la falta de consenso dificulta los intentos objetivos de definir la pornografía con una sola definición.

Definición
Las definiciones de pornografía varían cada cierto tiempo y de un lugar a otro: algo definido como pornográfico hace unos años ahora puede considerarse erótico. La pornografía en Internet es cualquier pornografía a la que se pueda acceder a través de Internet, principalmente a través de sitios web, intercambio de archivos entre pares o grupos de noticias Usenet. La disponibilidad de acceso público generalizado a la red global a fines de la década de 1990 condujo al crecimiento de la pornografía en Internet.

Aquí hay algunos ejemplos de pornografía en Internet:

1. Representaciones de desnudos en los que el sujeto está desnudo o con ropa mínima, o donde la ropa no sería aceptable en un contexto público apropiado.
2. Representaciones, animaciones o ilustraciones de actos sexuales o poses sexualmente sugestivas.
3. Contenido que representa actos sexuales y fetiches.
4. Contenido que es lascivo o vulgar.
5. Contenido que representa, describe o fomenta la zoofilia.
6. Aplicaciones que promueven entretenimiento relacionado con el sexo, servicios de acompañantes u otros servicios que pueden interpretarse como actos sexuales a cambio de una compensación.

Violencia, comportamiento extremista

La violencia no es de dominio único de los videojuegos o películas. Internet también le da mucho espacio, especialmente portales para compartir videos, donde aparecen videos brutales de acción en vivo, así como ataques reales o eventos reales con un final trágico. Incluso hay portales especializados que se centran en recopilar enlaces a videos y fotos brutales. Es difícil evitar que se presente contenido violento en Internet, ya que la mayoría de las veces no hay violación de ninguna ley.

El contenido violento común en Internet se refiere a representaciones gráficas o descripciones de violencia realista o amenazas violentas a cualquier persona o animal. También podemos encontrarnos con aplicaciones que incluyan manifestaciones de violencia. Estas aplicaciones pueden promover la autolesión, el suicidio, los trastornos alimentarios o, a primera vista, juegos inofensivos u otros actos en los que pueden producirse lesiones graves o la muerte.

En casos extremos, puede encontrarse con contenido relacionado con el terrorismo, como contenido que promueva actos terroristas, incite a la violencia o celebre ataques terroristas.

Recuerda
El contenido relacionado con el terrorismo o la violencia también puede tener un propósito educativo, documental, científico o artístico. Para ese tipo de propósito, es necesario considerar cuidadosamente el uso del contenido y explicar consistentemente la nocividad de ese comportamiento.

Productos peligrosos

Mucha gente no se da cuenta de que Internet es un medio que puede ofrecer y facilitar la venta de explosivos, armas de fuego, municiones o ciertos accesorios de armas de fuego. Otras posibilidades incluyen componentes que sirven para la fabricación de explosivos, armas de fuego, municiones, accesorios restringidos para armas de fuego u otras armas e instrucciones sobre cómo convertir un arma de fuego en un arma automática o similar.

Darknet market o cryptomarket es un sitio web comercial ilegal en un sitio web especial no público llamado Darknet (Red Oscura), al que solo se puede acceder con software, configuraciones o autorización específicos. Funciona principalmente como un mercado negro para la venta o intermediación de transacciones que involucran drogas, armas cibernéticas, armas, dinero falso, datos de tarjetas de crédito robados, documentos falsificados, drogas ilícitas, esteroides y otros bienes ilegales, pero también bienes legales.

Racismo u odio

La promoción o la incitación al odio contra personas o grupos por motivos de raza u origen étnico, religión, discapacidad, edad, nacionalidad, condición de veterano, orientación sexual, género, identidad de género o cualquier otra característica también es un tipo común de contenido inapropiado asociado. con discriminación o marginación sistémica. Las afirmaciones que se pretenden son demostrar que estos individuos o grupos son inhumanos, inferiores o dignos de ser odiados. Estas actividades incluyen características negativas (por ejemplo, maliciosas, corruptas, malignas, etc.), declaraciones de que el grupo es una amenaza o un discurso que intenta alentar a otros a creer que las personas deben ser odiadas o discriminadas por ser miembros de algún grupo..

Internet ofrece espacio ilimitado para publicar casi cualquier contenido, texto, vídeo, foto o música. Además, cualquier persona, ya sea un individuo o un grupo de personas, una organización o una empresa, puede obtener su presencia en Internet a través de un blog, sitio web o perfil social. A pesar de todos los esfuerzos para regular el contenido inapropiado, la gente siempre encuentra nuevas oportunidades y formas de conseguirlo en Internet. Las formas comunes de propagación incluyen:

Páginas web proanorexia

Los sitios, blogs, foros y grupos de redes sociales de proanorexia son la voz de un movimiento que entiende la anorexia como un estilo de vida, no como una enfermedad. Los anoréxicos no ven nada malo en su estilo de vida, pero perciben la resistencia de su entorno, por lo que se reúnen y se apoyan. Al mejorar su propia experiencia y comportamiento patológico en sitios web y redes sociales, aseguran una sensación de retroalimentación realmente positiva. Las opiniones sobre los sitios proanorexia varían: la primera parte sostiene que la proanorexia existe como un entorno seguro para que las personas anoréxicas hablen de su enfermedad y, por lo tanto, apoyen a quienes optan por la recuperación; la segunda parte utiliza los sitios proanorexia para respaldar su opinión de que la anorexia nerviosa no es una enfermedad, sino un estilo de vida que deben respetar los médicos y la familia.

Páginas web con contenido extremista

Los sitios web con contenido extremista a menudo parecen inocentes a primera vista: brindan información atractiva, como eventos históricos, pero los hechos están distorsionados y se refieren a otras fuentes de información ya manipuladas por una percepción modificada del mundo. Del mismo modo, los extremistas hacen uso, por ejemplo, de presentaciones de grupos musicales, en cuyos textos publicados en el sitio web suele haber contenido extremista oculto.

Redes sociales

Al igual que en los periódicos o la televisión, en Internet no está permitido distribuir contenido ilegal, como pornografía infantil o violencia. A pesar de todos los esfuerzos por regularlo, este contenido aparece en Internet. Además, Internet proporciona un espacio para la distribución de contenido legal, pero inapropiado, como simple pornografía o contenido violento que puede interferir con el desarrollo saludable de los niños.
Para la comunicación en línea, es cada vez más común enviar voluntariamente mensajes sexualmente sugerentes e imágenes o videos íntimos. Y con el boom de las redes sociales, es aún más fácil distribuir dicho contenido..

A veces es muy difícil distinguir qué contenido es inapropiado y cuál no.

La pornografía se confunde a menudo con el término “erotismo”.

¿Cuál es la diferencia?

Lo que constituye pornografía y erotismo varía dependiendo de los grupos y también de los individuos. También es probable que varíe con el tiempo: lo que se consideraba pornográfico, quizás a principios del siglo XX, ahora puede considerarse erótico.
El criterio utilizado para distinguir entre lo erótico y lo pornográfico está muy impregnado de valores personales morales, estéticos y religiosos. Aunque muchas personas consideran que estas dos orientaciones de la sexualidad humana se superponen, existe una diferencia significativa entre ellas. Lo erótico, a diferencia de la pornografía, no apela exclusivamente a nuestros sentidos o apetitos carnales, sino que también compromete nuestro sentido estético, nuestro juicio sobre cómo la figura ilustra un ideal de belleza humana. Lo erótico es más una cuestión artística y estética; la pornografía está más orientada a la satisfacción instintiva de las necesidades sexuales.

Clasificación de la pornografía en términos de psicología:

- suave = todo lo erótico, desde un acto artístico hasta una insinuación de acto sexual
- duro = representación directa del acto sexual, incluidos detalles de los genitales, su irritación, erección, penetración y eyaculación
- desviado = descripción directa de las desviaciones y prácticas sexuales que no ocurren en una vida sexual común y generalmente aceptada en una cultura determinada (sociedad): infantil, sadomasoquista, etc.

Pornografía vs pornografía infantil
No toda representación del cuerpo desnudo es pornografía. Para que este sea el caso, debe ser un trabajo (fotográfico, informático, escrito u otro) cuyo propósito sea inducir o aumentar la excitación sexual (la pornografía no es, por ejemplo, la representación de órganos genitales en un libro de texto de biología). Por tanto, la determinación de si la pornografía ya se basa en el sentimiento moral predominante. La pornografía infantil es aquella que representa o utiliza de otra manera a un niño o una persona que parece ser un niño. Actualmente, estos incluyen imágenes de niños que representan las posiciones de las relaciones sexuales reales o fingidas (en casos extremos, es posible que ni siquiera sean directamente visibles los órganos genitales expuestos) o imágenes de niños desnudos en posiciones que desafían la presentación de los órganos genitales. Las leyes europeas y nacionales prohíben la producción, distribución, importación, recepción o posesión de cualquier imagen de pornografía infantil. Una violación de las leyes de pornografía infantil es un delito grave, y los infractores condenados se enfrentan a multas y sanciones severas.

1.Aplica conocimiento

Ejercicio de OPCIÓN MÚLTIPLE

Objetivo asociado: FO_ Conoces la caracterización del contenido inapropiado.01_01: Puedes nombrar los tipos de contenido inapropiado.

Situación: ¿Qué temas podemos considerar como contenido inapropiado?
Tarea: Elija las opciones correctas siguiendo el principio de opción múltiple: más respuestas podrían ser verdaderas.

- Arte con imágenes eróticas
- Páginas wec con racismo u odio
- Películas de acción generalistas
- Venta de productos peligrosos
- Película documental de guerra con violencia extrema

Co-funded by the
Erasmus+ Programme
of the European Union

2. ¿Cómo reconocer las páginas web con contenido inapropiado?

Ya existen varias instituciones que supervisan la disposición del contenido en línea. Es bueno poder distinguir la calidad y credibilidad de la información y saber cómo lidiar con material amenazante.

Common Sense Media

Common Sense Media es una empresa de clasificación de películas, series, libros, aplicaciones y otros contenidos que recomienda la edad adecuada para ese contenido. También ofrece a los usuarios la oportunidad de evaluar.

Kids-In-Mind

Kids-In-Mind describe lo que los niños verán en una película, pero no recomienda para qué grupo de edad es adecuado.

Other options

IMDb Movie Database proporciona información útil. En los detalles de la película, busque la Guía para padres y haga clic en el enlace “Ver aviso de contenido”. Serás dirigido a la página de información detallada. También puede encontrar recomendaciones de edad según las reglas específicas de cada país.

También hay varias formas de determinar si un contenido es adecuado para su hijo. Muchas plataformas utilizan un tipo de clasificación para asesorar sobre el nivel de violencia y contenido explícito que contiene un medio.

Estas son solo algunas cosas que puede tener en cuenta para ayudarlo a tomar una decisión informada sobre si una aplicación, sitio web o contenido es adecuado:

Clasificaciones de videos musicales en línea

Las calificaciones aparecen en las dos mayores plataformas para compartir videos: VEVO y YouTube. En YouTube, verá la etiqueta "Calificación de socio" en el vídeo debajo del video que mostrará si el vídeo es adecuado para personas de 12, 15 o 18 años (PG 12, 15 o 18). En VEVO, verá el símbolo de calificación en la esquina superior izquierda del reproductor de vídeo cuando se cargue el vídeo. También puede hacer clic en la "i" para obtener más información sobre la calificación.

Puntuaciones PEGI de juegos online

La información de juegos paneuropea o PEGI se utiliza para asesorar sobre qué videojuegos son adecuados para adolescentes mayores o más jóvenes o solo para adultos debido al tipo de contenido que tienen. Las clasificaciones PEGI se introdujeron en 2003 y van desde PEGI (se recomienda supervisión de los padres), PEGI 3, PEGI 7, PEGI 12, PEGI 16 y PEGI 18. El número se relaciona con la edad para la que es apropiado el juego. Por tanto, si un juego tiene una calificación PEGI 7, es adecuado para niños de 7 años en adelante. Estas calificaciones se pueden hacer cumplir legalmente, por lo que es ilegal vender un juego PEGI 18 a un niño. Además, estas calificaciones no se relacionan con el nivel de dificultad del juego, solo con el nivel de contenido apropiado.

Co-funded by the
Erasmus+ Programme
of the European Union

Plataformas bajo demanda

En plataformas como Netflix, BBC iPlayer y Amazon Prime, verá clasificaciones de edad en todo el contenido que ofrecen. Estos pueden diferir de las plataformas, pero la calificación siempre indicará si algo es para una audiencia "madura" o especificará si el contenido "contiene lenguaje inapropiado".

Plataformas de redes sociales con restricción por edad

La mayoría de los términos y condiciones de las plataformas de redes sociales aconsejan que los niños deben tener 13 años o más para usar las plataformas. El motivo de esta edad mínima no tiene que ver con el hecho de que el contenido de la plataforma solo es apto para mayores de 13 años, sino con la COPPA (Ley de Privacidad Infantil en Línea), que es una ley estadounidense aprobada para proteger la privacidad de los menores de 13 años.

Comprender la clasificación por edades de las apps

Tanto Google Play Store como la tienda de aplicaciones de Apple usan calificaciones de aplicaciones para resaltar el nivel de contenido sexual, malas palabras, temas para adultos y abuso de sustancias que puede contener una aplicación..

Abreviaturas de accesibilidad que puede encontrar en Internet (fuente: Clasificación de la Asociación de imágenes en movimiento):

1.G: película para niños, completamente seguro
2.PG: Los padres deben considerar dejar que los niños vean
3.PG-13: Niños menores de 13 años solo con los padres
4.R: Menores de 17 años solo con compañía
5.NC-17: no apropiado para menores de 18 años

Recuerda

Los controles parentales, la configuración de privacidad y varias clasificaciones son herramientas útiles para ayudar a minimizar los riesgos que pueden enfrentar sus hijos, pero no son 100% efectivos. Es muy importante enseñarle a su hijo habilidades como el pensamiento crítico y la resiliencia, para que sepa qué hacer si se encuentra con un riesgo. Anímelos siempre a que hablen con usted sobre cualquier cosa que les moleste en Internet.

Tan pronto como su hijo comience a usar Internet, debe comenzar a hablar sobre lo que podría encontrar allí. Ayúdelos a comprender que a veces pueden encontrarse con cosas que preferirían no ver o que usted preferiría que no vieran. Trate de mantener estas conversaciones con regularidad.

Las medidas recomendadas de cómo evitar el contenido inapropiado:

- Explique los límites de edad y los sitios inapropiados para cada edad.
- Hable con otros padres y la escuela
- Acuerde las reglas básicas
- Esté tranquilo y sea tranquilizador
- Verificación de edad en sitios comerciales de pornografía

- Fomentar el pensamiento crítico
- Habla sobre lo que es falso y lo que es real
- Hablar sobre formas positivas de usar la tecnología

Recuerda Es importante mantener la conversación y estar interesado en lo que hace su hijo en línea.

2.Aplica conocimiento

Ejercicio de OPCIÓN MÚLTIPLE

Objetivo asociado: FO_ Conoce la caracterización de contenido inapropiado.01_02: Puedes nombrar los métodos para difundir contenido inapropiado y obtener información sensible.

Situación: ¿Sobre qué se discute en las páginas web proanorexia?
Tarea: Elija las opciones correctas siguiendo el principio de opción múltiple: solo una respuesta es verdadera.

- publicación de materiales obscenos
- recopilación enlaces a videos y fotos brutales
- promoción de autolesiones, suicidios o juegos brutales
- conversaciones sobre anorexia

3. ¿Qué es contenido inapropiado para mis hijos?

Sin orientación, los jóvenes tienen acceso a un mundo prácticamente ilimitado, por lo que los padres deben ser conscientes de los riesgos. Internet está abierto a cualquier persona para publicar y crear contenido, por lo que a veces sus hijos pueden ver cosas que desearían no haber visto o acceder a sitios inapropiados para su edad. Lo inapropiado puede significar diferentes cosas para diferentes personas, desde malas palabras hasta imágenes o vídeos pornográficos, y lo que es inapropiado para su hijo también cambiará a medida que crezca y se desarrolle.
Hay una variedad de cosas en línea que podrían molestar a los niños y afectar lo que debería ser una experiencia en línea saludable. Es importante recordar que el contenido inapropiado en línea incluye contenido pornográfico, pero también podría incluir otro contenido como el odio racial, los trastornos a favor de la alimentación o los sitios de juegos de apuestas.

Co-funded by the
Erasmus+ Programme
of the European Union

¿Qué contenido es inapropiado para un niño?

El contenido inapropiado incluye, en la mayoría de los casos, información o imágenes que molestan al niño o información que podría llevar o tentar a su hijo a comportarse ilegalmente o ser peligroso. Esto podría ser:

1.Material pornográfico
2.Contenido con vocabulario inapropiado
3.Páginas web que fomentan el vandalismo, la delincuencia, el terrorismo, el racismo, los trastornos alimentarios, las autolesiones o incluso el suicidio
4.Imágenes, videos o juegos que muestran imágenes de violencia o crueldad hacia otras personas o animales.
5.Páginas web de juego
6.Salas de chat no moderadas: en las que nadie supervisa la conversación y no se bloquean los comentarios inadecuados.
7.Sexismo o sitios que retratan a las mujeres en roles muy tradicionales que no reflejan los valores y expectativas contemporáneos.

Generalmente casi todas las personas se ven afectadas por el contenido inapropiado y podemos dividirlas en varias categorías para definir los temas específicos de la protección:
1.Preescolar (0 – 5 años)
2.Niños en edad escolar (6-11 años)
3.Jóvenes en edad escolar (12-15 años)
4.Juventud (15-18 años)
5.Adultos

Preescolar

Cada vez más niños en edad preescolar usan las computadoras, teléfonos inteligentes o tabletas de sus padres para jugar, usar aplicaciones y ver sus programas de televisión favoritos. Hay cosas sencillas que se puede hacer para asegurarse de que estén usando Internet de forma segura. Es necesario construir una buena relación con el contenido correcto explorando juntos, instalando los controles parentales, usando las contraseñas para no permitir la admisión y estableciendo los límites / reglas para estar en línea.

Niños en edad escolar

Se ha demostrado que el uso temprano de la tecnología digital mejora las habilidades lingüísticas y promueve el desarrollo social y la creatividad de los niños. Pero no está exento de riesgos para los niños pequeños, que pueden encontrar contenido inapropiado o comenzar a copiar lo que hacen los niños mayores en línea. Puede utilizar los mismos temas que para los niños en edad preescolar y para complementarlo utilizando el modo avión (no permitir comunicarse con otras personas a través de su dispositivo), hablar con los niños mayores sobre lo que están haciendo en línea y lo que muestran a los niños más pequeños y para monitorear las clasificaciones de edad lo que es adecuado para esa edad.

Jóvenes en edad escolar

Los alumnos de primaria son el grupo más riesgoso en cuanto al aumento masivo del uso de la tecnología moderna sin la instrucción y el control pertinentes, la ingenuidad fácilmente abusiva, el desafío a la autoridad y la búsqueda de su propia identidad, que, si no es satisfactoria en el mundo real, se encuentra con el mundo virtual. Es común para un grupo de edad determinado que su vida virtual esté sujeta a un control parental mínimo, superficial o nulo, a menudo siendo más ágiles con la informática que los propios padres, quienes a menudo perciben la tecnología como hostil y permiten que los niños la usen para relajarse por sí mismos. Por tanto, una gran proporción de usuarios jóvenes ha desarrollado la sensación de que pueden hacer cualquier cosa que les guste en el mundo virtual sin el sentido de responsabilidad y respeto de los demás usuarios.

Juventud

Los estudiantes de escuelas secundarias y escuelas vocacionales son específicos por su uso más profundo de las tecnologías modernas, especialmente Internet y las redes sociales y los peligros que surgen de ellas.. Su hijo debe establecer la configuración de privacidad en la mayoría de los sitios de redes sociales para que solo los amigos cercanos puedan buscarlos, etiquetarlos en una fotografía o compartir lo que han publicado. Hágales saber que todo lo que publiquen, envíen por correo electrónico o escriban, podría permanecer en línea para siempre. Recuérdeles que solo deben hacer cosas en línea que no les importaría que usted, su maestro o un futuro empleador vean. Haz que piensen en crear una huella digital positiva. Recuérdeles lo importante que es no ceder a la presión de los compañeros para enviar comentarios o imágenes inapropiados. Para ese grupo objetivo lo más importante es su confianza. Tiene que estar interesado en sus necesidades, hablar con ellos y ser más un amigo que un padre. Comparta su contenido con ellos y trate de motivarlos a compartir su contenido con usted.

Adultos

El contenido para adultos también puede verse afectado por contenido inapropiado en línea. Muchos sitios web contienen virus. Estos se colocan con mayor frecuencia en páginas con contenido inapropiado. En la mayoría de los casos, se trata de una descarga por error de un virus informático propagado a través de sitios de contenido pornográfico. Estos sitios son muy atractivos para los ciberdelincuentes porque tienen una gran cantidad de usuarios. Además, a menudo se muestran reacios a informar sobre un ciberataque o una infección en su dispositivo porque se sienten avergonzados si se descubre que proceden de sitios pornográficos. Las enfermedades digitales más comunes que los usuarios pueden descargar visitando sitios web con contenido inapropiado en su dispositivo incluyen troyanos, clickjacking, tinder bots, cat-phishing, ransomware, gusanos, pornware o spyware.

Aplica conocimiento

Ejercicio de OPCIÓN MÚLTIPLE

Co-funded by the
Erasmus+ Programme
of the European Union

Objetivo asociado: FO_Conoce las amenazas de abuso de información sensible y su impacto.02_02: Puede caracterizar a los grupos objetivo que podrían ser víctimas de apuntar a contenido inapropiado.

Situación: ¿Qué grupo de personas es más vulnerable frente al contenido inapropiado?
Tarea: Elija las opciones correctas siguiendo el principio de opción múltiple: solo una respuesta es verdadera.

- Personas mayores
- niños entre 12 y 18 años
- todos los niños menores de 15 años
- todos los jóvenes mayores de 15 años

4. ¿Cómo puedo proteger a mis hijos y a mí mismo del contenido inapropiado?

Herramientas como los controles parentales pueden ayudar a proteger a sus hijos del acceso a contenido inapropiado, pero no puede verificar todo lo que ven en Internet. Debe ayudarlos a evitar el contenido inadecuado y afrontarlo si lo ven. El primer paso es hablar con ellos al respecto.

La mayoría de estos sitios web perturbadores no son "ilegales", lo que significa que permanecerán en línea y que los padres deben controlarlos y administrarlos. No se sentiría seguro al permitir que su hijo deambule sin rumbo fijo por una gran ciudad, solo y en medio de la noche, así que recuerde que Internet es como una gran ciudad, llena de cosas buenas y malas y un lugar donde un niño necesita ser supervisado.

¿Qué puedo hacer cuando reconozco los sitios web con contenido inadecuado?

- Informar al administrador correspondiente directamente en la aplicación (navegador web, redes sociales, etc.)
- Informar a la policía u otras instituciones relevantes
- Para utilizar las herramientas de software para bloquear el contenido inapropiado (control parental)
- Hablar con los niños sobre ese tema.

Es posible informar al administrador de la aplicación sobre el contenido inadecuado en aplicaciones comunes (Google, Facebook, etc.). Por lo general, puede encontrar el botón en la configuración de la aplicación.

Co-funded by the
Erasmus+ Programme
of the European Union

También puede informar a la policía sobre el contenido inapropiado mediante la especificación detallada de la fuente.

Los controles parentales son opciones de software o dispositivos específicos que permiten a los padres monitorear el uso de Internet de sus hijos. Evitan que los niños accedan a contenido inapropiado o inadecuado en línea. Se pueden implementar dentro de su proveedor de servicios de Internet, motores de búsqueda, sitios de transmisión de video y más.

Las herramientas más frecuentes de control parental en Internet son:

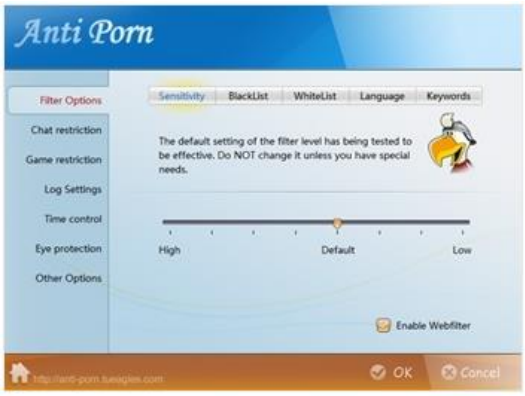
- Configure los controles parentales para su red en el router
- Utilice las aplicaciones que monitorean el tiempo que pasa en Internet el niño
- Restringir el acceso a Internet en mi wifi
- Ponga el control parental en los navegadores web

If you are trying to avoid visiting problematic sites from your computer not only for children, but also for employees - some topics can distract them from work - typically those with pornography, extremist issues, , you can use several types of protection methods.

¿Qué programa, filtro o complemento es mejor para restringir el acceso a estos sitios inapropiados?

Anti Porn

Uno de los programas más conocidos y utilizados para prohibir las visitas de pornografía a la web. Esto se debe principalmente a su fácil maniobrabilidad y fácil ajuste. La aplicación reconoce y marca automáticamente el contenido como erótico e inmediatamente prohíbe el acceso a ese lado. También tiene una base de datos de varios miles de sitios web maliciosos, que se actualiza periódicamente.

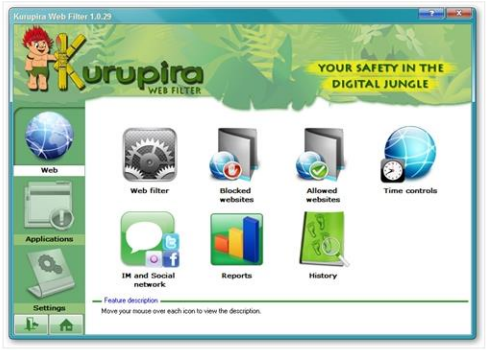


K9 Web Protection

Otro programa de filtrado para protegerse de las trampas de Internet. Puede funcionar tanto un protector de malware como un filtro de contenido inapropiado. Es gratuito y se puede utilizar tanto en Windows como en Mac OS X. Además, este programa es fácil de configurar y utilizar. Los sitios maliciosos se clasifican por tipo de contenido pornográfico, de redes sociales, violento, etc.

Filtro Web Kurupira

Programa poco conocido y extendido, pero puede hacer muy bien su trabajo en un entorno agradable y orientado a principiantes. Además tiene la ventaja de que es también una licencia de aplicación gratuita. Para acceder al programa, debe ingresar una contraseña para que solo quienes la conozcan puedan establecer filtros.



iWebFilter

La aplicación contiene una amplia base de datos de páginas, palabras y contenidos problemáticos y, por supuesto, el usuario puede ampliarla. El bloqueo se puede configurar para ambos navegadores web, mensajería instantánea (IM) y clientes de correo electrónico y otras aplicaciones. También hay un horario de acceso a Internet, límite de transferencia de datos y registro detallado de eventos.

Co-funded by the
Erasmus+ Programme
of the European Union

En caso de encontrar contenido censurable, no debe seguir viéndolo, apague la pantalla o salga de ella. El adulto no debe reprender al niño por navegar en lugares inapropiados en Internet. No es por lo que se muestra en Internet. Si descubre que su hijo está viendo pornografía, violencia, etc. intencionalmente, debe pensar en la causa. Es necesario tener en cuenta la edad y el evento o buscar asesoramiento profesional, por ejemplo, en el centro de asesoramiento pedagógico-psicológico correspondiente.

Insafe e INHOPE trabajan juntos a través de una red de Centros de Internet más seguros (SIC) en toda Europa, que generalmente comprenden un centro de concienciación, una línea de ayuda, una línea directa y líneas de atención para jóvenes, dedicadas a la eliminación de contenido ilegal en línea), operan Centros de Internet más seguros (SIC) en 30 países europeos en la lucha por mantener la seguridad de los niños y los jóvenes en línea. A través de una gama de servicios, los SIC responden a los últimos problemas en línea, ayudando a promover las muchas oportunidades que ofrece el mundo en línea, al tiempo que abordan sus desafíos.

¿Cómo denunciar contenido inapropiado?
Si usted o su hijo encuentran contenido inapropiado que incite a la violencia o al odio, esto es lo que puede hacer:

- En caso de contenido ilegal (infracción de la ley), debe comunicarse principalmente con la policía.
- Póngase en contacto con las organizaciones / instituciones dedicadas a la seguridad en Internet (por ejemplo, SIC: https://www.betterinternetforkids.eu/web/portal/policy/insafe-inhope) para que le ayuden con la eliminación / bloqueo de contenido.
- Informar al administrador de la página / plataforma.
- Cambie la configuración en su ordenador.
- Póngase en contacto con los expertos para ayudar a su hijo con la situación traumática.
- Hable con su hijo.
- Mantenga la calma.

A continuación, se incluyen guías rápidas en vídeo de cómo hacerlo para establecer la configuración correcta en las plataformas más populares y otras cosas que puede hacer:

Facebook Privacy Checker
https://www.youtube.com/watch?v=wN3jz2Mv_ME&feature=emb_title

YouTube Restricted Mode
https://www.youtube.com/watch?v=XuXnatkASTQ&feature=emb_title

Co-funded by the
Erasmus+ Programme
of the European Union

Google SafeSearch
https://www.youtube.com/watch?v=LK-MIwjQz20&feature=emb_title

Seguridad y spyware

Algunos ordenadores, especialmente en lugares públicos (biblioteca, cafeterías, escuelas, etc.) pueden tener algún software de monitoreo que pueda capturar la pantalla y, por lo tanto, represente una amenaza para la información confidencial en la pantalla. Estas herramientas de vigilancia de PC pueden monitorear todo tipo de actividad en una computadora. El software antivirus y los firewalls no protegen completamente el sistema contra la mayoría de los programas espía y las amenazas a la privacidad. El software espía se incluye comúnmente con descargas de software, se adjunta a correos electrónicos o se transmite a través de redes, por lo que parece ser software legítimo, pero una vez instalado, puede ser casi imposible detectarlo y eliminarlo sin la ayuda de una herramienta de eliminación de software espía dedicada. La protección y la prevención de software espía son esenciales para defender la privacidad de las miradas indiscretas y los intrusos virtuales. Estas medidas también se pueden instalar en los ordenadores privados para protegerlo a usted y a sus hijos del contenido inapropiado al monitorear toda la actividad en línea. Los ejemplos de esas herramientas se pueden encontrar en el texto anterior.

A continuación, se ofrecen algunos consejos rápidos para identificar sitios y aplicaciones poco fiables:

- Compruebe que la URL de un sitio web sea la URL principal que utiliza normalmente para acceder a ese sitio.
- Tenga cuidado con los correos electrónicos de personas que no conoce. En caso de duda, no haga clic en enlaces ni abra archivos adjuntos en correos electrónicos.
- Compruebe que la marca sea precisa, que parezca igual en todas las plataformas, y que el logotipo no esté borroso.
- ¿Hay errores tipográficos en el sitio web o en los correos electrónicos que le solicitan que inicie sesión y actualice sus datos? Si es así, es probable que se trate de una estafa.
- Consulte su tienda de aplicaciones para ver reseñas de aplicaciones antes de descargarlas. Si hay muchos usuarios y buenas críticas, es poco probable que sea una estafa. Si no hay reseñas, investigue un poco más en línea; las estafas generalmente se identifican con bastante rapidez y las personas a menudo publican en línea sobre ellas.
- ¿Una aplicación le pide que ingrese mucha información personal o que proporcione sus datos de inicio de sesión para cualquier cuenta de redes sociales? Entonces, es probable que sea una estafa.

Información personal

La otra cuestión relacionada con el contenido inapropiado también debería ser la publicación de su información personal. Todo el mundo puede ver y descargar lo que publique en línea y utilizarlo en otro contexto o hacer un mal uso de la información.

Choo (2008) describió tres categorías de grupos organizados en el ciberespacio:

El tipo de información más importante que debemos guardar es la Información de Identificación Personal (PII).

Definición
Según la Administración de Servicios Generales de EE. UU., PII es "Información que se puede utilizar para distinguir o rastrear la identidad de una persona, ya sea sola o combinada con otra información personal o de identificación que esté vinculada o pueda vincularse a una persona específica".

Algunos ejemplos de PII son:

- Nombres: su nombre completo, su apellido de soltero y el apellido de soltera de su madre
- Números de identificación personal: su número de la Seguridad Social, número de licencia de conducción, número de pasaporte, número de identificación de paciente, número de identificación del contribuyente, número de cuenta de crédito o número de cuenta bancaria
- Direcciones: su dirección postal y dirección de correo electrónico
- Biometría: escaneos de retina, huellas dactilares, geometría facial o firmas de voz
- Matrículas de vehículos
- Números de teléfono
- Información sobre activos tecnológicos: direcciones de Control de Acceso a Medios (MAC) o de Protocolo de Internet (IP) que están vinculadas a un determinado individuo

¿Por qué debería mantener su información personal privada? Asegurar su información personal puede ayudarle a prevenir el robo de identidad, proteger su información financiera, evitar ser robado, proteger su empleabilidad y la reputación de su negocio, y mucho más.

Aquí hay algunos consejos para que pueda mantener sus cuentas seguras y mantener el control de su privacidad en línea. También puede leer más sobre cómo proteger su identidad.

1.Haga una verificación de privacidad revisando la configuración de todas sus cuentas de redes sociales.
2.Establezca contraseñas seguras y actualice las antiguas.
3.No comparta sus contraseñas.
4.Asegúrese de descargar e instalar nuevos sistemas operativos y de software en su teléfono, tablet u ordenador tan pronto como estén disponibles.
5.No agregue personas en las redes sociales que no haya conocido sin conexión.
6.Cuando los sitios web o las aplicaciones soliciten su información personal, verifique que sean legítimos.

La Comisión Europea adoptó una recomendación sobre medidas para abordar eficazmente el contenido ilegal en línea. Cuestiones como la incitación al terrorismo, el discurso de odio ilegal o el material de abuso sexual infantil, así como las infracciones de los derechos de Propiedad Intelectual y la protección del consumidor en línea, necesitan un enfoque coordinado fuerte en toda la UE. El enfoque está totalmente alineado y es coherente con la Directiva de derechos de autor, incluidos los aspectos ampliamente debatidos de la responsabilidad de las plataformas en línea. También es totalmente coherente con la revisión de la Directiva de medios audiovisuales.

Las plataformas en línea deben ser más responsables de la gestión del contenido. Es recomendable adoptar un enfoque común para detectar, eliminar y prevenir la reaparición de contenido en línea de manera rápida y proactiva:

- Procedimientos más claros de 'notificación y acción'
- Herramientas más eficientes y tecnologías proactivas.
- Garantías más fuertes para garantizar los derechos fundamentales.
- Atención especial a pequeñas empresas.
- Cooperación más estrecha con las autoridades.

Co-funded by the
Erasmus+ Programme
of the European Union

Aplica conocimiento

Ejercicio de OPCIÓN MÚLTIPLE

Objetivo asociado: O_ Conoce el papel del delito cibernético en Internet.03_05: puede nombrar la información personal que no debe publicarse en línea

Situación: ¿Cuáles son las formas básicas de evitar la difusión de contenido inapropiado?

Tarea: Elija las opciones correctas siguiendo el principio de opción múltiple: más respuestas podrían ser ciertas.

- No envíe su foto a nadie que no conozca.
- Mantenga las contraseñas en secreto y no las revele a un amigo cercano.
- No abra el archivo adjunto de un mensaje que proviene de una dirección desconocida.
- No visite ninguna red social.

Fuentes:

Internet matters.org: https://www.internetmatters.org/issues/inappropriate-content/learn-about-it/#age-ratings

CNET.com: https://download.cnet.com/Anti-Porn/3000-27064_4-10207334.html

K9 Web Protection: https://www.downloadsource.net/1771222/k9-web-protection/

Soft free download (Soft 32): https://kurupira-web-filter-and-parental-control.soft32.com/

Softpedia: https://www.softpedia.com/get/Internet/Other-Internet-Related/iWebFilter.shtml

Co-funded by the
Erasmus+ Programme
of the European Union

Afianza conocimiento

Resumen

Las formas de contenido censurable son ricas. Los más comunes incluyen:

- Pornografía
- Violencia, comportamiento extremista
- Productos peligrosos
- Racismo u odio
- Páginas web proanorexia
- Páginas web con contenido extremista

A menudo, el contenido es indeseable y dañino, pero puede no ser ilegal. Esto depende de cómo cargarlos, respectivamente, de cómo evitar su accesibilidad. Sin embargo, tanto el contenido nocivo ilegal como el legal pueden tener un impacto indeseable en quienes lo encuentran.

En general, es aconsejable contactar con la policía en caso de actos ilegales. Sin embargo, a veces es esencial, sobre todo, evitar rápidamente la distribución de dicho contenido, y es posible recurrir a otro lugar para ese propósito. Si encuentra pornografía ilegal o un sitio extremista, repórtelo a la policía.
En primer lugar, los niños (dependiendo de su edad) no deberían encontrar contenido peligroso en absoluto. Los filtros en el navegador de Internet pueden ser útiles (por ejemplo, es posible deshabilitar la visualización de una página que contiene el término "pornografía", etc.).

Los controles parentales son opciones específicas de software o dispositivo que permiten a los padres monitorear el uso de Internet de sus hijos. Evitan que los niños accedan a contenido inapropiado o inadecuado en línea. Se pueden implementar dentro de su proveedor de servicios de Internet, motores de búsqueda, sitios de transmisión de video y más. Las herramientas más frecuentes del control parental en Internet son:

- Configurar los controles parentales de su red en el router
- Utilizar las aplicaciones que monitorizan el tiempo que los niños pasan en Internet
- Restringir el acceso a Internet con Wi-Fi
- Poner control parental en los navegadores

La protección más importante contra el contenido inapropiado es el debate y el cuidado de nuestros hijos, saber lo que hacen y estar interesados en sus necesidades y pasatiempos. Podemos tener herramientas útiles para la protección como las leyes, los controles parentales, la configuración del software, las instituciones de apoyo, pero la clave es la confianza entre usted y el niño.