Programa ineco RURALTIC

Fecha 20/11/2024

Población:
Carrizo – León

Presentación del programa INECO Social

Conferencia de Jordi Romeu y Jesús Hernado.

¿Qué es?

Ingeniería y consultoría de referencia en el ámbito de la movilidad sostenible y la transformación digital dependiente del MITMA

Más de 50 años diseñando **soluciones integrales, innovadoras y tecnológicas** que han permitido avanzar hacia un nuevo modelo de movilidad más sostenible y más segura. Soluciones que contribuyen de manera directa en la mejora de la calidad de vida de millones de personas.

- ✓ Comprometidos con la **sociedad** y la transformación digital
- ✓ Valor de Ineco: 5.000 profesionales.
- ✓ Conocimiento al servicio de Rural TIC

https://www.ineco.com/webineco/ o simplemente teclea en Google nuestro nombre

¿Quiénes somos?

Jordi Romeu Crespo

Ingeniero en Electrónica
Ingeniero en Telecomunicaciones
MBA, MPRL
Director de Obra Señalización Ferroviaria y Telecomunicaciones Fijas
ADIF-AV LAV León-Asturias

¿por qué estamos aquí?
Compartir experiencia y conocimiento práctico en el uso de las nuevas tecnologías y redes sociales, habiéndome trasladado de la gran ciudad a un entorno rural

Estos somos nosotros y vosotros ¿quién sois?

¿Quiénes somos?

Jesús Hernando

Formación académica

ANALISTA INFORMÁTICO DEL MINISTERIO DE JUSTICIA

¿por qué estamos aquí?

Quiero ayudar a dar el paso que nos da “respeto”

Estos somos nosotros y vosotros ¿quién sois?

Introducción

Como todos sabemos hoy en día el uso de internet está cada vez más extendido entre nuestros niños y adolescentes. No sólo como medio de ocio si no como medio de estudio.

Esto nos genera cierta inseguridad al no tener a veces claro cómo actuar y lo que debemos hacer ante determinadas situaciones.

En este taller vamos a hablar de pautas a seguir, de "peligros", de cómo interactuar con los que están al otro lado, de conceptos quizás desconocidos para algunos de vosotros y también de las ventajas que tiene su uso. Así mismo, también nsmitir a nuestros hi

Queremos esto

no esto

Conceptos

¿Qué conceptos debemos conocer para evitar situaciones de riesgo en las Redes Sociales e internet?

Estos son algunos ejemplos de los más conocidos

- Ciberbullying: acoso de un niñ@ o adolescente a otro a través de internet o dispositivos móviles, Tablets, etc. Entendemos por acoso cuando es molestado, amenazado, ridiculizado, humillado, abusado etc..
- Sexting: es la acción de filmarse o sacarse fotos con contenido sexual, pornográfico o erótico y enviar esas imágenes o videos a otra persona.
- Grooming: es el acoso sexual de una persona adulta a un niñ@ o adolescente por medio de internet

Uso incontrolado

¿Qué riesgos puede tener el uso incontrolado de las redes sociales e internet?

Puede producir:

- Aislamiento social
- Adicción
- Bajo rendimiento
- Trastornos obsesivos compulsivos

Como podemos prevenirlo:

- Pactando el tiempo de uso (no más de 1,5-2horas a diario)
- Poniendo el ordenador en un espacio común
- Fomentando actividades sociales
- Potenciando actividades deportivas o culturales (lectura, cine,..)
- Favoreciendo el dialogo y la comunicación en la familia

Qué no y que sí debemos hacer

¿Qué debemos evitar nosotros los adultos?

A veces los adultos no nos damos cuenta y realizamos acciones o enviamos mensajes a nuestros hijos que no son acertados. A continuación, os mostramos unos ejemplos:

- La sobrexposición o Sharenting, se da cuando por parte los progenitores cuando comparten fotos de menores sin la cara tapada, ubicaciones, fotos del nombre del colegio etc..
- No debemos enviar el mensaje de que "internet" o las "redes sociales" son malas ya que puede provocar el efecto contrario al deseado
- No les prohibamos su uso, es mejor controlar lo que hacen desde casa que se conecten desde cualquier sitio o a través del dispositivo de un amigo y realmente no sepamos que hacen.

Qué no y que sí debemos hacer

¿Qué sí debemos hacer?

Podemos hacer infinidad de cosas para hacer entender a nuestros hijos que es un buen uso de internet y de las redes sociales. Estos son sólo algunos ejemplos:

- **Firmar una especie de contrato familiar**. Así construiremos un vínculo de confianza que los miembros de la familia deben de firmar y actualizar. De cumplirse las "cláusulas" recompensaremos al menor con algo pactado previamente.
- **Anticiparnos a la curiosidad de los menores** viendo con ellos documentales sobre los que poder charlar, ofreciendo respuestas y fomentando el conocimiento que invite a formular otras preguntas. Todo llega a su debido tiempo y cada nivel de comprensión y madurez debe ser abordado de manera distinta
- **Aportar datos y realidades para educar sin asustar**. Hay que alertarles de los peligros y animarlos a blindar su propia privacidad, esto será determinante para que, en su maduración, ganen confianza y conocimiento de las distintas herramientas de internet
- **Demostrar que confiamos en ellos** valorando su libertad y su espacio personal, dejando por ejemplo periodos en los que pueda buscar información

Qué no y que sí debemos hacer

En resumen

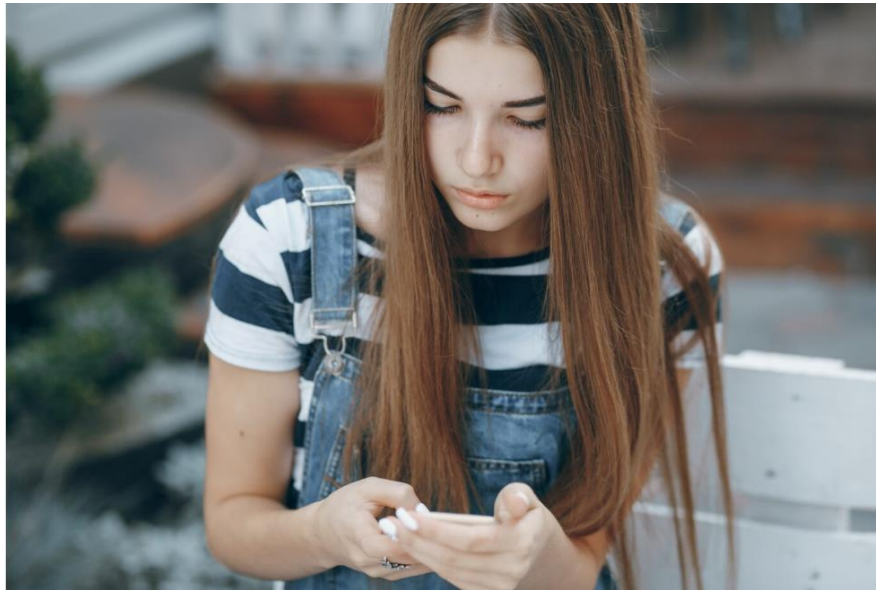
https://youtu.be/tJ1Qgvuqxb8 (32’’)

A qué debemos estar atentos

Debemos estar atentos al fomento de ideas o mensajes inadecuados, a las noticias falsas (o fake news), al contenido para adultos, al contenido sensible o a los retos virales que pueden poner en riesgo su integridad física. En definitiva, debemos estar atentos a todo.

Y como la realidad es que normalmente no podemos estar atentos al 100% por distintos motivos, lo mejor es establecer una relación de confianza donde se sientan seguros para contar cualquier cosa y educarles sobre como tienen que utilizar internet y las redes sociales y qué hacer si se encuentren en determinadas circunstancias.

Queremos un uso responsable



No podemos ser vigilantes el 100% del tiempo

Pasos que podemos seguir

Explicarles que

- Es la huella digital y qué consecuencias tiene
- La importancia de su privacidad
- Por qué debemos estar con ellos cuando den de alta su cuenta en una RRSS
- No deben publicar información personal
- No deben publicar fotos en las que se les vea al 100%
- Deben evitar mostrar su cara al 100%
- Deben ser respetuosos con los demás, detrás de un perfil/avatar siempre hay una persona
- Por qué es mejor usar un pseudónimo y no su nombre real
- Por qué no deben admitir como "amig@s" a personas que no conozcan
- Es el contenido sensible
- Es el contenido para adultos
- Qué hacer si se encuentran con este tipo de contenidos
- Qué hacer si son acosados o si se encuentran con alguna situación de acoso
- Es el sexting y porque no debe enviar ese tipo de fotos
- Es el grooming y que deben hacer para sentirse protegidos
- Que contenido consideras que es apto y por qué

Qué debemos hacer si…

- Son acosados o son testigos de un acoso:

  Lo primero que debemos es escucharlos y apoyarles, que comprendan que no es culpa suya y que no contesten a los instigadores. Por último, guarde las pruebas y busque ayuda.

  En el caso de que sean testigos de ese acoso lo primero que tienen que hacer es comunicárselo a la familia del acosado porque puede que no lo sepan.

- Encuentran contenido para adultos:

  Lo primero no debemos "asustarnos", no debemos sancionarles, debemos hablar con ellos de una manera natural, no juzgarles, que nos cuenten como han llegado ahí, porque les llamó la atención, que sensación les produjo, que pensaron, no debemos condenar el hecho, debemos explicarles que la sexualidad no es eso, que implica muchas más cosas. Que la pornografía que suele ser gratuita es violenta y machista, no hay respeto ni consentimiento. Hagamos que se sientan cómodos hablando de sexo.

- Encuentran contenido inadecuado o sensible:

  Como actos violentos, uso de sustancias, comportamientos autolesivos, grupos que fomentan el suicidio. Básicamente lo mismo que si encuentran contenido para adultos. Hablar con ellos con calma y naturalidad. La comunicación es

Qué debemos hacer si…

- Se creen todas las noticias que ven:

  Hoy en día las llamadas fake news o noticias falsas, circulan constantemente. Por lo que si vemos que se creen todo lo que ven, una vez más lo que debemos es hablar con ellos y enseñarles como esa noticia que ellos pensaban verdadera, no lo es. Para ello podemos utilizar páginas web como maldita.es, o newtral.es que es su parte derecha dispone de un apartado llamado "verificación" y este a su vez uno que pone "fake".

  Debemos fomentar que cuando lean una noticia no se queden sólo en el titular si no que profundicen y si aún, así no les "cuadra" pregunten si esa noticia es veraz

Control parental

Hoy en día existen muchas aplicaciones que nos permiten realizar un control parental tanto para Pc como para móvil, aquí les mostramos unas cuantas:

- **SafeDNS:** además de otras funciones relacionadas con la seguridad y la gestión de Internet, este filtro permite bloquear los recursos no deseados e inapropiados. ¿Cómo lo hace? En su base de datos tienen analizados 120 millones de dominios divididos en 57 categorías. Lo que les permite filtrar no sólo las webs sino banners, pop-ups, vídeo, audio…
- **K9 Protection:** este filtro cuenta con un bloqueo de páginas web donde establecen 5 niveles de bloqueo y uno adicional para personalizar las páginas que se bloquearán. Este bloqueo se hace por palabras clave, las cuáles se localizan gracias a la monitorización y escaseado de millones de webs.
- **FamilyTime:** dentro de todas las funciones que incluye como control parental esta app disponible para Android e IOS, está la de gestión de páginas web. Cuenta con un sistema que bloquea todas las webs que no están incluidas en una lista previamente configurada. También ofrecen un conjunto de filtros a elegir y diferentes niveles de seguridad con los que proteger de forma más exhaustiva a los menores.

Control parental

- **Planes de Protección Digital Gaptain:** no podían faltar en esta lista nuestros planes de protección que incluyen control parental con bloqueo de contenido inadecuado, además de formación, asesoramiento psico social, e incluso ciberseguridad para el hogar. Con la app Control parental no sólo se les puede proteger de información inapropiada, sino que cuenta con bloqueo de contactos, límite de tiempo de uso, localizador y muchas funciones más que te hará fácil el acompañamiento y la supervisión de su actividad digital…
- **Safesearch:** Permite bloquear contenido desde el navegador. ¿Cómo? Siguiendo estos pasos
  - Configuración > Cuentas > Familia y otros usuarios > Administrar la configuración de la familia en línea.
  - Haga clic en la cuenta Microsoft de su hijo y seleccione Filtros de contenido.
  - Escriba la URL del sitio o los sitios web que desea **bloquear**.

Pero llegará un día que estas apps ya no nos sirvan porque irán creciendo y teniendo accesos más fáciles, por eso la importancia de la educación en el buen uso de internet y las redes sociales.

Cómo saber por dónde navegan

Por último, podemos saber por dónde navegan de la siguiente forma, no a través del propio navegador, que puede ser borrado con facilidad, sino a través de My Activity de Google o el siguiente atajo en Windows: pulsamos Windows + R, pinchamos sobre **Ejecutar** en la ventaja que aparecerá, escribiremos el comando **cdm** y en el guion bajo que aparecerá en la ventana escribiremos **Ipconfig/displaynds**. Después pulsamos Enter y automáticamente veremos todo el historial, hasta en caso de borrado.

Y no lo olvidemos, los navegadores también alojan datos en nuestro disco duro. Ese posible contenido sensible puede encontrarse en esta ruta:

- En **Internet Explorer**/Edge: En C:\Users(nombre de usuario)\AppData\Local\Microsoft\Windows\History.
- En **Google Chrome**: En C:\Users(nombre de usuario)\AppData\Local\Google\Chrome\User Data\Default, el archivo History.
- En **Mozilla Firefox**: En C:\Users(nombre de usuario)\AppData\Roaming\Mozilla\Firefox\Profiles\, el archivo places.sqlite.

En cualquier caso, una vez detectemos posible contenido sensible, no debemos darle más importancia de la necesaria, sino **abordarlo como una cuestión educativa de la cual aprender juntos** y saciar así la curiosidad del menor.

¡GRACIAS POR VUESTRA ATENCIÓN!