Protege a los menores de contenidos inadecuados en la Deep Web o Internet profunda

FAMILIAS | 29-JUN-2020

0 comentarios

En Internet existen espacios digitales menos conocidos, donde los usuarios/as pueden acceder y navegar manteniendo mayor privacidad. Una característica que ha permitido que en algunas de estas redes proliferen con mayor facilidad servicios que ofrecen contenidos ilegales, a los que los menores están accediendo, según hemos podido detectar desde INCIBE. Por lo que queremos explicarte qué es la *Deep Web* y la *Dark Web*, cuáles son sus riesgos y ayudarte a identificar si tus hijos/as están accediendo y cómo debes actuar.

Internet es mucho más grande de lo que vemos a simple vista, y existen otras zonas de la Red que se mantienen ocultas al usuario/a convencional. Es lo que se conoce como *Deep Web* o Internet profunda, y responde a la necesidad de mantener mayor privacidad y anonimato, imprescindible para la protección de los datos que se alojan en ella. El problema es que este espacio también facilita el desarrollo de actividades ilícitas que se encuentran escondidas en esta zona menos controlable y conocida.

¿Qué es la *Deep Web* y la *Dark Web*?

Cuando utilizamos Internet accedemos a los contenidos que ofrecen las distintas empresas, instituciones, personas, etc. Todas ellas intentan dar a conocer sus productos, ideas o servicios al resto de usuarios. A estos contenidos es posible acceder con los principales navegadores web, bajo los estándares y protocolos habituales. Hablamos de servicios como Google, o redes sociales como Facebook o Instagram.

Además, hay otra parte de la Red que no se encuentra al alcance de los buscadores, al tratarse de páginas privadas o que no permiten la indexación. Esta parte de Internet es la ***Deep Web*** (https://www.osi.es/es/actualidad/blog/2019/11/27/navegadores-y-deep-web-profundicemos-en-el-tema) o Internet profunda, y aquí se alojan muchos de los datos necesarios para el funcionamiento de los servicios que utilizamos a diario, que deben estar protegidos. Todo lo que se encuentre en la ***Deep Web*** no tiene por qué tener propósitos oscuros o cuestiones ilegales. Esta Red se configura mediante capas cifradas, como si se tratara de una cebolla, permitiendo un alto nivel de privacidad en las comunicaciones.

Pero aprovechando esta característica, dentro de la *Deep Web* existe una pequeña porción de esta red a la que es aún más difícil acceder, denominada *Dark Web*, la parte más oscura de Internet. Para acceder es necesario utilizar navegadores específicos, entre los que destaca TOR por ser el más conocido, aunque no es el único. En este espacio se concentran servicios y páginas que ofrecen contenidos ilegales o poco recomendables. Esto no quiere decir que no podamos encontrar esos productos o servicios en otras zonas de Internet, pero en la *Dark Web* proliferan más y es más difícil controlarlos, ya que una de sus características de diseño es el anonimato.

Desde la **Línea de Ayuda en Ciberseguridad de INCIBE, 017 (https://www.is4k.es/ayuda)**, se tiene constancia de que los menores conocen este entorno y están accediendo principalmente en busca de contenidos pornográficos, pero también con otros fines. Muchos padres y madres no son conscientes o no tienen conocimientos suficientes para identificar este tipo de sitios, por lo que queremos ayudarte a reconocerlos y saber cómo actuar.

¿Qué tipo de contenidos se encuentran en la Internet profunda?

Dentro de la *Deep Web* es posible encontrar todo tipo de información, desde una inocente página web personal hasta sitios con contenido poco apropiado para menores. Como hemos dicho, no toda la *Deep Web* es inadecuada o ilegal, la mayor parte está destinada a almacenar y administrar datos que necesitan una mayor protección, pero hay más probabilidades de acceder a contenidos peligrosos.

Existen páginas web que son auténticos mercados de productos ilegales. Así, se puede encontrar documentación falsa, como pasaportes, documentos de identidad y servicios de cibercriminales que ofertan accesos a cuentas de redes sociales, empresas o bancos. También se venden armas, todo tipo de drogas o incluso se mueve el tráfico de órganos. Uno de los mayores riesgos, sin duda, es la distribución y consumo de pornografía infantil, así como contenidos acerca de actos violentos o servicios de sicarios a sueldo.

La falta de control de los contenidos que se alojan en la *Deep Web* y la *Dark Web* también conlleva la aparición de blogs, foros y tablones que promocionan formas de actuar nada saludables y peligrosas, como grupos que incitan y promueven la anorexia, la bulimia o la prostitución, incluso la autolesión o el suicidio. Además, las sectas o grupos organizados también utilizan esta parte de la Red para sus estrategias de captación y manipulación de personas vulnerables.

Además, la gran cantidad de contenidos que se oferta en estas redes alimenta a su vez la proliferación de todo tipo de malware y virus informáticos (https://www.osi.es/es/contra-virus), que ponen en peligro los equipos de aquellos usuarios/as que navegan por ellas. Muchos menores acceden a estos espacios sin los conocimientos mínimos para detectarlos.

En resumen, el anonimato de la comunicación en la *Deep Web* es por un lado un beneficio para quien navega con normalidad, pero también un campo abierto para quien desea realizar actividades fuera de la legalidad.

¿Cuáles son los riesgos?

Para cualquier persona esta parte de la Red puede suponer un riesgo, dado que no existe tanto control sobre qué nos podemos encontrar o quién ofrece esos servicios de contenido o información.

Para los menores, sin duda, es aún más peligroso por su vulnerabilidad para ser captados por personas malintencionadas o encontrar contenidos inadecuados. A menudo acceden a la *Deep Web* guiados por compañeros o amigos que les envían instrucciones mediante WhatsApp o Telegram, normalmente sin más información sobre lo que se van a encontrar. Estos son los principales aspectos de riesgo a tener en cuenta:

- Visualización de contenidos no apropiados para menores, que pueden resultarles complejos, perturbadores o derivar en consecuencias penales.
- Captación por parte de comunidades peligrosas, que pueden conducirles a conductas poco saludables o dañinas a nivel físico o emocional.
- Acceso a servicios ilegales que pueden conllevar riesgos físicos y/o consecuencias legales para el menor: mercado negro de sustancias y armas, contenidos pornográficos, órganos, etc.

Para los usuarios/as inexpertos puede parecer que existe cierta sensación de impunidad al utilizar estos espacios digitales supuestamente ocultos, pero esta mayor privacidad no es una garantía total, ya que depende de muchos factores. Fácilmente pueden ocurrir fallos que hacen que este anonimato no sea real y el usuario/a sea rastreado y localizado.

¿Mi hijo/a puede estar accediendo a la *Deep Web*?

Por supuesto es posible. Hay menores que acceden a esta red, por curiosidad, por influencia de su grupo de amigos o compañeros, por romper límites o con el objetivo de encontrar contenidos concretos, exponiéndose a muchos riesgos. Por ello, es importante tener unos conocimientos mínimos que nos permitan reconocer esta actividad.

Si supervisamos el uso de Internet en el ordenador, los navegadores y programas que utilizan esta Red pueden ser identificados a través de su icono con forma de cebolla y también a través de los nombres de dominio (la dirección que aparece en el buscador), que no son legibles y claramente difieren de las páginas web convencionales. A su vez, en ocasiones necesitan programas específicos que estarán instalados en el dispositivo, así como los propios archivos o contenidos que haya encontrado, que estarán almacenados y seguramente escondidos a primera vista.

Además, deben llamarnos la atención los cambios de actitud en el menor, que pueden ser una señal de alerta. La búsqueda de espacios privados para navegar o la insistencia exagerada para tener un dispositivo propio pueden darnos pistas sobre este tipo de uso. Otras conductas llamativas, como bajadas de ánimo, cambios de humor o problemas para conciliar el sueño, entre otros, pueden ser un síntoma de que algo no está bien y necesita nuestro apoyo.

¿Cómo actuar si detecto que está accediendo a la Internet profunda o la red TOR?

- Nuestra primera reacción debe ser moderada, recordando que existen diferentes usos de esta red y que no necesariamente el acceso a la *Deep Web* está relacionado con actividades ilegales. Es importante crear un clima de confianza con el menor para averiguar cuál es el objetivo real que le ha llevado a acceder.
- La principal amenaza es el uso que esté haciendo de esta parte de Internet. En cualquier caso, es necesario informar y concienciar al menor de los peligros de los contenidos que puede encontrar, adaptándonos a su nivel de madurez, pero siendo realistas y procurando que las explicaciones no alimenten el interés por estos contenidos.
- La instalación de un **software de control parental (https://www.is4k.es/de-utilidad/herramientas)** que permita bloquear el acceso a la *Deep Web* o la red TOR puede ser útil si se trata de preadolescentes o menores con pocos conocimientos informáticos. Debemos ser conscientes de que esta red está diseñada para saltarse protecciones y bloqueos, por lo que habrá que ser cuidadosos en la comprobación de la efectividad de estas aplicaciones o servicios.
- Para los menores con una gran curiosidad o habilidad por el entorno digital puede ser interesante animarlos a conocer el uso positivo de estos espacios, motivando su formación formal o informal en estos aspectos, a través de iniciativas como **CyberCamp (https://cybercamp.es/)** o **CyberOlympics (https://www.is4k.es/programas/cyberolympics)**.

Siempre es práctico contar con personas cercanas a nosotros o profesionales con mayor conocimiento de estos espacios digitales, que puedan aportar una perspectiva profesional al menor sobre los riesgos y las posibles consecuencias.

La Línea de Ayuda en Ciberseguridad de INCIBE, 017 (https://www.is4k.es/ayuda), está a vuestra disposición para situaciones como esta, en la que los menores pueden creer estar suficiente formados o ser autónomos como para enfrentarse a estos espacios digitales por sí mismos, pero siguen necesitando nuestro acompañamiento, nuestro apoyo y nuestra madurez ante los riesgos a los que se exponen.

ACTUALIDAD (/SEARCH/NODE/ACTUALIDAD)
| COMUNIDADES PELIGROSAS (/SEARCH/NODE/COMUNIDADES PELIGROSAS)
| CONTENIDO INAPROPIADO (/SEARCH/NODE/CONTENIDO INAPROPIADO)
| RIESGOS (/SEARCH/NODE/RIESGOS)

Artículos relacionados

(/blog/como-es-la-relacion-de-las-familias-digitales-espanolas-con-la-red)

FAMILIAS | 28-MAYO-2020

¿Cómo es la relación de las familias digitales españolas con la Red?

(/blog/familia-cibersegura-v-la-importancia-de-fomentar-el-pensamiento-critico-en-nuestros-hijos)

FAMILIAS | 25-MAYO-2020

Familia cibersegura V: La importancia de fomentar el pensamiento crítico

(/blog/educa
i-es-el-mome
competencia

EDUCADOR

**Educanc
ciberseg
momen
en comp**

Añadir nuevo comentario

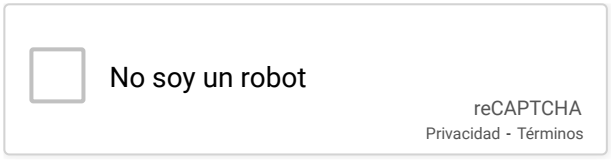
Su nombre

Comentario *

*** Campos obligatorios**

CAPTCHA

Esta pregunta es para comprobar que usted no es un robot y para evitar envíos automáticos de spam.



GUARDAR

Búsqueda en el blog

Público

- Cualquiera -

Etiquetas

- Cualquiera -

BUSCAR **LIMPIAR**

(https://www.is4k.es/necesitas-saber)

Boletines

SUSCRIBIRSE (HTTPS://WWW.IS4K.ES/NEWSLETTER/SUBSCRIPTIONS)

(https://www.is4k.es/ayuda) (https://www.is4

(https://www.incibe.es/sites/default/files/certificado_ens_incibe_31102019.pdf)

(https://www.incibe.es/sites/default/files/certificado_sgsi_11112019.pdf)

(https://www.incibe.es/sites/default/files/certificado_sgc_13122019.pdf)

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

(http://www.mineco.gob.es/portal/site/mineco/)

(http://www.incibe.es) • (http://www.red.es)

Cofinanciado por la Unión Europea
Mecanismo «Conectar Europa»

NIPO: 094-20-023-4

(https://www.twitter.com/is4k) (https://www.facebook.com/is4k.es)

(https://www.youtube.com/channel/UCBoX1urZFEt29_5XqB_5BTg)

(https://www.is4k.es/canales-rss)

AVISO LEGAL (HTTPS://WWW.INCIBE.ES/AVISO-LEGAL)

| POLÍTICA DE COOKIES (HTTPS://WWW.INCIBE.ES/POLITICA-COOKIES)

| ACCESIBILIDAD (HTTPS://WWW.INCIBE.ES/DECLARACION-DE-ACCESIBILIDAD)

| MAPA WEB (/SITEMAP)

| SOBRE NOSOTROS (HTTPS://WWW.IS4K.ES/SOBRE-NOSOTROS)

| CONTACTO (/CONTACTO) | ENCUESTA (/ENCUESTA) | AGENDA (/CALENDARIO)

| BOLETÍN (/NEWSLETTER/SUBSCRIPTIONS)