Digipadres

UNA INICIATIVA DE saferkidsonline by eset

¿Qué tan accesibles son las diferentes capas de Internet para los niños?

Los peligros asociados a la **Dark Web** se suelen debatir con bastante frecuencia. Pero a muchos padres todavía no les queda claro el funcionamiento de estos sitios web y los riesgos que representan.

Descubre en qué se diferencian la Surface, Deep y Dark Web y cómo pueden afectar a tus hijos.

¿Por qué es importante comprender cómo funcionan las diferentes capas de Internet?

Aunque uno pensaría que las peores cosas suceden en la Dark Web, muchas interacciones problemáticas pueden tener lugar en la capa más accesible, la Surface Web. Por ejemplo, un acosador a menudo no necesita nada más que las plataformas de aplicaciones de chat comúnmente disponibles para comunicarse con los niños. Por otra parte, el material que se publica sobre niños en las redes sociales puede terminar con facilidad en las bases de datos que se ofrecen en la Dark Web.

Conocer la relación entre la **Surface**, **Deep** y **Dark Web** te permitirá establecer los mecanismos de control y la comunicación correcta con tu hijo.

SURFACE WEB (red superficial)

Está conformada por sitios web de acceso público que los usuarios pueden encontrar mediante motores de búsqueda de Internet como **Google**, **DuckDuckGo** o **Bing**. Esta es la capa más accesible de Internet, donde se pueden ver páginas indexadas.

DEEP WEB (red profunda)

Es la capa de Internet que está disponible solo para ciertos grupos de personas, por ejemplo, libros de informes electrónicos, contenido educativo destinado a una clase específica, pero también las secciones pagas de los portales de noticias o sistemas internos de las empresas. Estos sitios y contenidos no son accesibles para usuarios aleatorios. Si un usuario quiere buscarlos u obtener acceso, **necesita software o herramientas especiales, o privilegios de acceso**, ya que estas páginas no están indexadas para aparecer en un motor de búsqueda.

DARK WEB (red oscura)

Esta capa no está indexada por los motores de búsqueda y se ejecuta en una infraestructura oculta que les proporciona anonimato a sus operadores y usuarios. Para conectarse a la Dark Web, un usuario **debe instalar un software especializado como TOR o el servicio I2P** (Invisible Internet Project).

Fuente: Manual de seguridad digital para maestros

Si bien una parte considerable de la **Deep Web** es legal y legítima, **gran parte de la Dark Web** consiste en productos o contenido ilegal. Según GoGuardian, los elementos que se encuentran en la Dark Web a menudo incluyen drogas, armas sin licencia, identificaciones falsas, herramientas de piratería, tarjetas de crédito robadas, contenido para adultos y muchos foros para cosas que no tienen un lugar en la red normal. También hay software que permite acceder en forma remota a las computadoras de otras personas.

Sin embargo, **no todo en la Dark Web es ilegal**. Por ejemplo, hay una gran comunidad de lectores, aunque el material puede ser cualquier cosa, desde libros educativos y de ficción hasta publicaciones con ideologías extremistas.

Otro servicio inusual es una alternativa anónima a Airbnb, que encontró **Ondrej Kubovič**, especialista en **concientización de seguridad de ESET**. "*A diferencia de Airbnb, este servicio no requiere verificación de identidad ni obliga a sus usuarios a compartir grandes cantidades de datos. Simplemente se crea una identidad con un apodo, bajo el cual se va construyendo gradualmente una reputación, y se gestiona el alojamiento de manera más independiente, solo entre otros usuarios de la Dark Web*", explica Kubovič.

Esto **puede ser atractivo** para muchas personas, incluso adolescentes, porque no tienen que revelar tantas cosas sobre ellos mismos. Por otro lado, **permite que se hagan estafas**, donde los usuarios más antiguos abusan de su muy buena reputación para hacer una operación importante, robar una gran cantidad de dinero, para finalmente eliminar su identidad y desaparecer. **Estos son temas que puedes conversar con tus hijos cuando te pregunten sobre la Dark Web**. "Recomendaría explicarles que los riesgos son mayores en la Dark Web y que es más probable que se encuentren con un estafador allí que en la Internet común", dice Kubovič.

¿Cuándo corre riesgo el niño de entrar en la Dark Web?

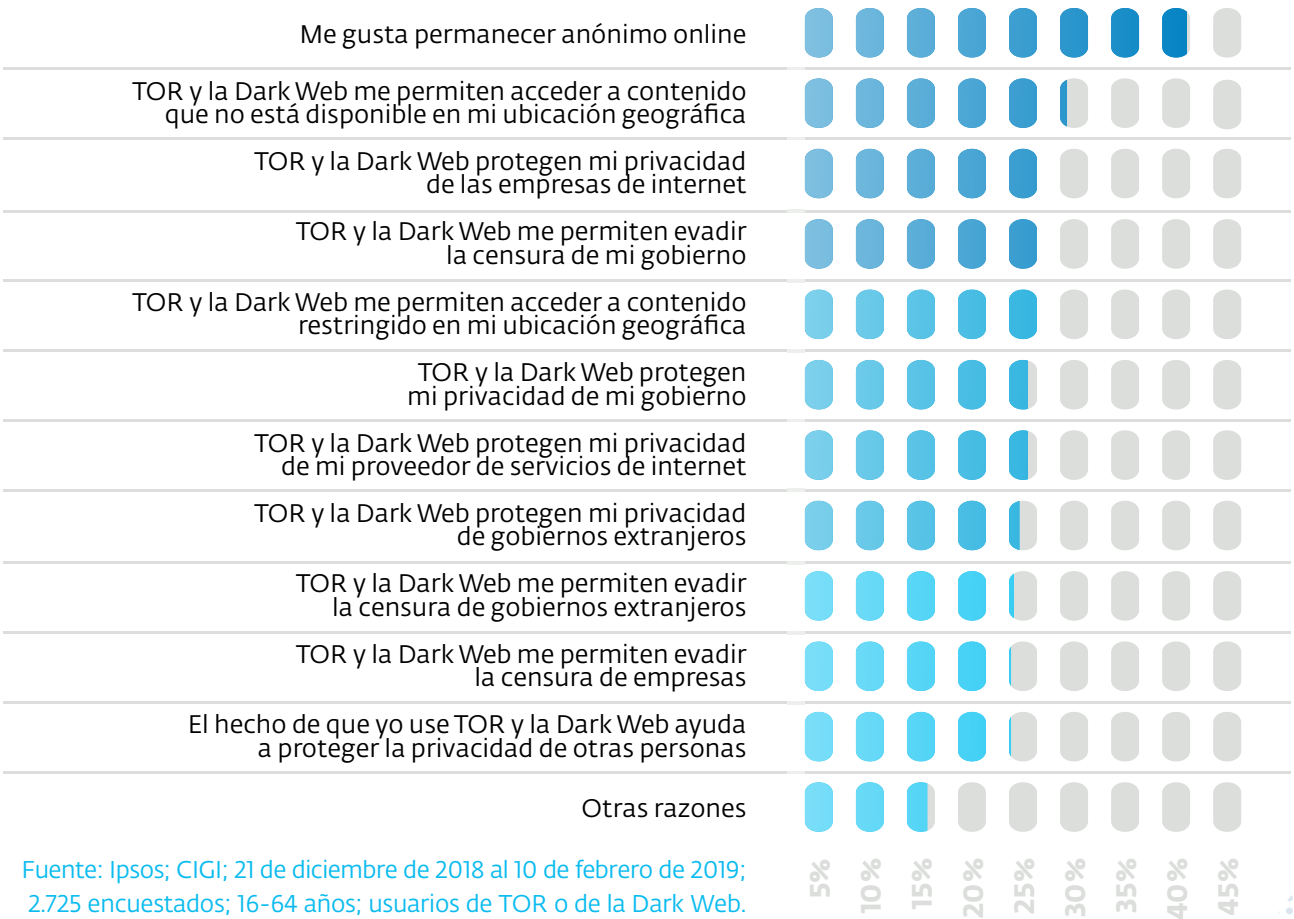
Acceder a la Dark Web **requiere conocimientos y experiencia**. Hay casos en los que un extraño entra en contacto con un niño y, una vez que ha ganado su confianza, lo guía a través de la Dark Web. Sin embargo, según Ondrej Kubovič, estas situaciones **no son muy comunes** y la mayoría de los niños no suelen sentir la necesidad de entrar a la Dark Web. Para aquellos pocos que lo hacen, esto probablemente no sucederá antes de la pubertad. Principalmente por los conocimientos técnicos que se necesitan para acceder a la Dark Web, **pero también por la lentitud de carga**.

"*Si tuviera 14 años y mis amigos se me acercaran y me preguntaran si quisiera ver lo que hay en la Dark Web, me sentaría con ellos y lo probaría. Cuando ya tienes cierta edad no es tan difícil, porque se pueden encontrar instrucciones en Internet que te guían a través de todo el proceso.* ***No es necesario iniciar sesión ni crear una cuenta***", explica el experto en TI.

"*Pero I2P y, a veces, incluso TOR pueden ser terriblemente lentos y creo que eso* ***frustraría totalmente a casi cualquier adolescente****. Los niños de hoy ya no están acostumbrados a esperar y no lo disfrutarían. Incluso TOR es más lento que un navegador normal*", aclara Kubovič. Según él, la cantidad de contenido peligroso que los adolescentes pueden ver en la Dark Web no es tan grande, pero siempre es una cuestión de motivación, curiosidad e interés individual.

Razones más comunes por las que los usuarios acceden a la Dark Web en todo el mundo

FEB 2019



Fuente: Ipsos; CIGI; 21 de diciembre de 2018 al 10 de febrero de 2019; 2.725 encuestados; 16-64 años; usuarios de TOR o de la Dark Web.

¿Qué medidas preventivas puedes tomar como padre?

Si tienes una fuerte sospecha de que tu hijo está activo en la Dark Web, verifica los sistemas operativos y el software instalados en sus dispositivos. Busca **TOR** (TheOnionRouter), **I2P**, **Freenet**; aplicaciones que configuran una red privada virtual (**VPN**); o el uso de sistemas operativos como **Whonix**, **Subgraph**, **Tails** o **Qubes**. Para proteger aún más a tus hijos, **instala software parental** con filtrado de contenido capaz de bloquear sitios.

Otro paso es pensar en las consecuencias y el impacto de dichas actividades. **No les prohíbas a tus hijos acceder a la Dark Web**, ya que **solo fomentarás su curiosidad**. Si eres un padre conocedor de la tecnología, puedes **mirar algunos sitios junto a ellos** para demostrarles que no son tan interesantes. Trata de explicarles lo que puede suceder si visitan la Dark Web, o qué información sobre ellos puede aparecer allí si comparten demasiados datos personales en las redes sociales de la Surface Web. Además, podrían encontrar contenido perturbador, como foros de suicidio, casos extremos de contenido para adultos que no están disponibles en la Surface Web, o podrían descubrir foros con temas comerciales ilegales.

Queremos que más **Digipadres** potencien a los niños
y les enseñen a navegar seguros.

¿Estás listo para acompañarnos en este desafío?

www.digipadres.com