

Los derechos humanos en la era digital




 Prueba-previa


 Introducción

 ¿Qué son los derechos digitales?

 ¿Cómo puedo proteger mis derechos digitales?

 ¿Cómo puedo protegerme y responder ante el ciberacoso?

 Conclusiones

 Prueba-posterior

QUESTION BANKS

 Los derechos humanos en la era digital: prueba de evaluación inicial/final

Prueba-previa

Antes de tomar este nuevo módulo en la Universidad Digital, hagamos una pausa y reflexionemos sobre su conocimiento sobre este tema a través de una prueba previa. Todas las preguntas de esta prueba previa se abordarán en el módulo, ¡asi que está bien si aun no sabe todas las respuestas!

Pregunta

01/01

7 questions drawn randomly from Los derechos humanos en la era digital: prueba de evaluación inicial/final

Introducción

Nuestras vidas y nuestra labor de defensa dependen cada vez más del uso de la tecnología, incluyendo las redes sociales. La tecnología puede ser una herramienta muy valiosa para nuestro trabajo de defensa. Sin embargo, la tecnología puede hacer que estemos más expuestos a las violaciones de la privacidad, a la discriminación y al acoso. Además, la desigualdad en el acceso a la tecnología digital impide que muchas personas puedan disfrutar de la igualdad de derechos.

El término «digital» hace referencia al uso de dispositivos electrónicos que almacenan y procesan datos (como los teléfonos móviles y los ordenadores), así como a los programas de *software* y las aplicaciones que se usan en dichos dispositivos (como el correo electrónico y las redes sociales). En el mundo digital, una persona ostenta los mismos derechos que en el mundo físico, aunque no todo el mundo sabe identificar y proteger estos derechos.

Este módulo te dará las herramientas necesarias para que puedas protegerte a ti mismo y a los demás y te enseñará a hacer uso de tus derechos digitales para alcanzar así un mayor impacto.

Al final de este módulo, serás capaz de:

- 1 Describir qué son los derechos digitales.
- 2 Entender cómo puedes proteger tus derechos digitales y los de los demás.
- 3 Tomar medidas para protegerte contra el ciberacoso y saber cómo responder cuando otros lo sufren.

¡EMPECEMOS!

¿Qué son los derechos digitales?

Entender tus derechos digitales es el primer paso para tomar el control de tu presencia en Internet. Incluso si no usas mucho la tecnología, en la era de Internet los derechos digitales son un componente fundamental de los derechos humanos.

¿Qué son los derechos digitales?

El [Consejo de Derechos Humanos de las Naciones Unidas](#) afirma que todos los derechos humanos que ostentamos en el mundo físico (fuera de Internet) se aplican a tu «yo» digital cuando navegas por Internet, cuando interactúas en redes sociales y cuando usas dispositivos como tu teléfono o tu smartphone. Los derechos digitales incluyen el derecho a la privacidad, a la libertad de expresión y a vivir libres de violencia y acoso.



¿Cómo se traduce esto a nivel nacional e internacional?

Pulsa en cada elemento para saber más.



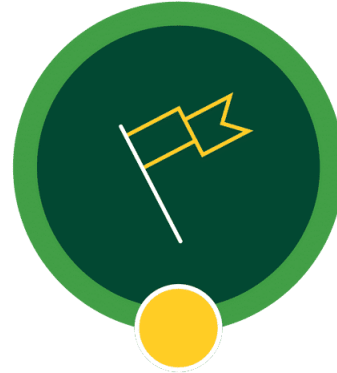
Internacional



Nacional



Internacional



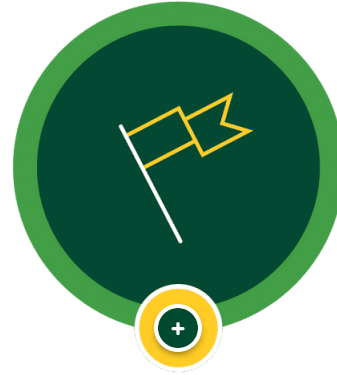
Nacional

Internacional

Muchos de los marcos internacionales de derechos humanos en los que nos basamos como activistas se crearon antes de que se inventara Internet y se difundieran las tecnologías digitales, tales como la [Convención sobre los Derechos del Niño \(CDN\)](#) o la [Convención para la eliminación de todas las formas de discriminación contra la mujer \(CEDAW\)](#). Aunque se han introducido ciertas modificaciones en estos convenios durante la era digital, sigue sin haber un marco internacional en materia de derechos digitales.



Internacional



Nacional

Nacional

A nivel nacional, es decir, de país, las leyes que regulan el uso de Internet se centran fundamentalmente en las actividades transaccionales, financieras y de comercio electrónico, en lugar de en proteger y garantizar los derechos digitales de los ciudadanos. Son pocos los países que cuentan con leyes en materia de acoso en Internet; además, estas leyes son muy limitadas y pueden no abordar todas las formas de acoso y ciberacoso a las que se enfrentan las personas (especialmente las poblaciones marginalizadas).

¿Por qué son importantes los derechos digitales?

Incluso antes de la pandemia de la COVID-19, una gran parte de nuestras vidas tenía lugar en Internet. Gracias a Internet, nos comunicamos con amigos y familiares, extraemos información y accedemos a importantes servicios y recursos. Como consecuencia de la pandemia de COVID-19, ahora somos aún más dependientes de las tecnologías digitales.



Veamos algunas estadísticas. Pulsa en cada elemento para saber más.

**4570
millones**

El número de usuarios
activos en Internet en
abril de 2020.

59%

Porcentaje de la población mundial que tiene acceso a Internet. Nueve de los diez países con la menor tasa de acceso a Internet están en África.

98%

Porcentaje de mujeres o niñas encuestadas en 22 países que utilizan las redes sociales. Las plataformas más utilizadas son Instagram, Facebook y WhatsApp.

Fuente: Plan International

Dado que una gran parte de nuestras vidas está estrechamente relacionada con estas tecnologías, es importante comprender quién es el dueño de estas las plataformas y sistemas de los que tanto dependemos. En general, los espacios que frecuentamos en Internet son propiedad de empresas

del sector privado con ánimo de lucro, como Meta, Google, Alibaba, TenCent o Apple. Las normativas que garantizan que estas empresas protejan nuestros derechos varían en todo el mundo y no suelen ser lo suficientemente sólidas



La violación de derechos en Internet puede darse de muchas formas distintas, tales como el ciberacoso, la minería de datos y la vigilancia. Es probable que hayas experimentado algunas de estas violaciones de derechos en primera persona. Al igual que sucede con los derechos humanos, no todo el mundo puede disfrutar de sus derechos digitales de igual manera. Las personas que sufren discriminación en el mundo físico, como las personas negras, indígenas y de color (es decir, las personas racializadas), el colectivo LGBTQIA+ y otros grupos tradicionalmente marginalizados, también suelen sufrir discriminación y marginación en el espacio digital.

¿Quién tiene la responsabilidad de garantizar y proteger los derechos digitales?

Los Estados, las empresas, las personas y las organizaciones de la sociedad civil tienen la responsabilidad de proteger los derechos digitales.



Pulsa en cada uno de los elementos a continuación para saber más.

Los Estados —

Al igual que sucede con los derechos humanos, los Estados (o los Gobiernos), tienen la responsabilidad de garantizar y de proteger los derechos digitales. Esto está contemplado en el [Pacto Internacional de Derechos Civiles y Políticos](#), un tratado internacional ratificado por 173 Estados miembro de las Naciones Unidas. Los Estados están obligados a no violar los derechos digitales (medidas «negativas») y a emprender acciones para proteger y garantizar dichos derechos (medidas «positivas»). Por ejemplo, los Estados no pueden vigilar a alguien sin seguir el procedimiento jurídico pertinente en el país. Esta es una medida «negativa». Los Estados también tienen la obligación de regular las empresas tecnológicas para garantizar que no están llevando a cabo actividades de minería de datos para venderlos sin consentimiento. Esta es una medida «positiva».

Las empresas —

Aunque los Estados son los principales responsables de proteger tus derechos, las empresas están obligadas a respetar los derechos humanos, más allá del cumplimiento de la legislación nacional vigente. Así lo dictan los [Principios Rectores de las Naciones Unidas sobre las Empresas y los Derechos Humanos](#), en los que se establecen normas internacionales de conducta empresarial en materia de derechos humanos. Las empresas deben analizar de manera proactiva el impacto que sus modelos de negocio tienen sobre los derechos humanos y evitar ocasionar un impacto negativo mediante sus actividades, tanto de forma directa como indirecta. En caso de que se produzca un impacto negativo sobre los derechos humanos, las empresas deben tomar acciones para mitigarlo.

Las organizaciones de la sociedad civil —

Las organizaciones de la sociedad civil y los activistas desempeñamos una importante labor a la hora de exigir a los Estados y a las empresas el cumplimiento de estos compromisos. La defensa de los derechos digitales es un movimiento que está creciendo rápidamente a nivel local, nacional, regional y mundial. Para involucrarte, revisa las sugerencias de defensa de los derechos digitales que figuran en el informe [Libres para estar en Internet](#). También puedes consultar las organizaciones que llevan a cabo labores de defensa de los derechos digitales en todo el mundo:

- [Global Network Initiative](#)
- [Privacy International](#)
- [Ranking Digital Rights](#)
- [Digital Rights Nepal](#)
- [Fundación Karisma](#)
- [IPANDETEC](#)
- [Digital Grassroots](#)

Los organismos internacionales, como las Naciones Unidas, también están monitorizando los derechos digitales e introduciendo nuevas instituciones y mecanismos, como el recién nombrado [Relator Especial de las Naciones Unidas sobre el derecho a la privacidad](#).

Las personas —

Por último, nosotros tenemos, a título personal, la obligación de respetar los derechos digitales de las demás personas. Esto incluye no acosar a otras personas en Internet y proteger toda la información personal o los datos que se compartan con nosotros. ¡Continúa leyendo este módulo para saber cómo puedes respetar y proteger los derechos digitales de tus homólogos, de tus conciudadanos o de los usuarios de la tecnología!





Imagina el siguiente caso: Utiliza lo que has aprendido hasta ahora sobre los derechos digitales para responder correctamente.

Estás organizando una campaña en redes sociales para un proyecto de defensa en el que estás trabajando. ¿Qué medidas puedes tomar para garantizar que se tienen en cuenta los derechos digitales?

Selecciona las mejores respuestas entre las cuatro opciones siguientes.

Valorar quién tendrá acceso a las redes sociales para participar en la campaña y qué se podría hacer para garantizar la participación de las personas que no tienen acceso.

Pensar cómo se puede proteger a las personas que participan en la campaña frente al ciberacoso.

Asegurarse de que todos los datos recopilados se usan para la finalidad prevista y se almacenan de forma segura.

Revisar los ajustes de seguridad de las cuentas en redes sociales.

SUBMIT

A CONTINUACIÓN: ¿CÓMO PUEDO PROTEGER MIS DERECHOS DIGITALES?

¿Cómo puedo proteger mis derechos digitales?

Ahora que ya sabes qué son los derechos digitales, es importante que seas consciente de las posibles violaciones de los derechos digitales para tomar precauciones para evitarlas.

¿Qué es la brecha digital de género?

El acceso a la tecnología digital y a Internet es un derecho fundamental. Sin embargo, el acceso puede variar en las distintas comunidades y países en función del lugar de residencia, los ingresos, el sexo, el idioma, la raza o la etnia. Como defensores de la igualdad de género, es importante que conozcamos el concepto de «brecha digital de género», es decir, la desigualdad en el acceso digital de las personas en función de su género.



Echa un vistazo a estas estadísticas sobre la brecha digital de género.

Si solo hubiese 10 personas en el mundo...

...5 de ellas no tendrían acceso a Internet.

**Si solo 10 personas
tuviera acceso a
Internet...**

...solo 1,5 de ellas tendría
una conexión a Internet
accesible y asequible.

**Si solo hubiese 10
personas en el
mundo, 4,9 de ellas
serían mujeres...**

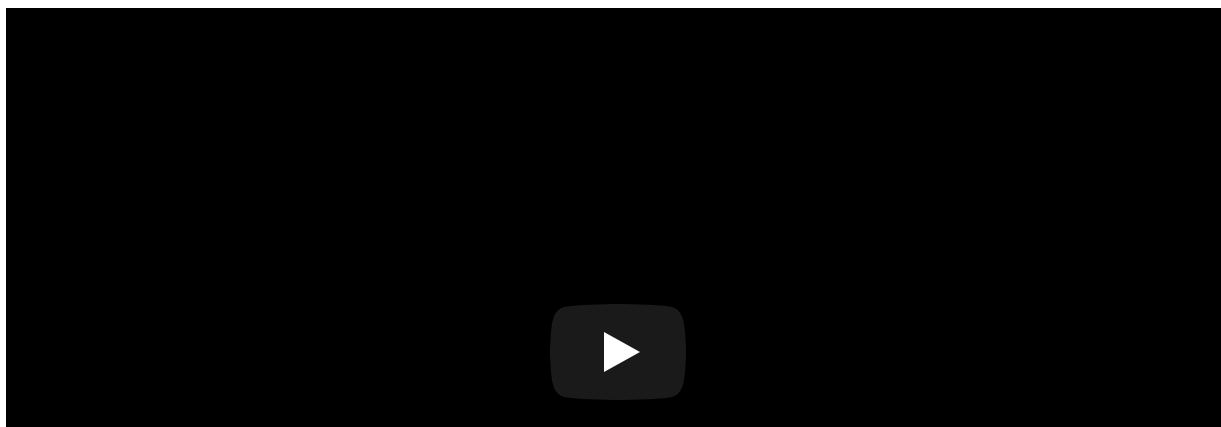
...y solo 2 de ellas tendrían
acceso a Internet desde un
dispositivo móvil.

Fuente: Asociación Mundial de Guías Scouts

¿Cómo se puede hacer un mal uso de los datos?

El término «datos» hace referencia a aquella información bruta sobre nuestra identidad (nombre, fecha de nacimiento o dirección) y nuestros comportamientos en Internet (qué sitios web visitamos o qué términos de búsqueda utilizamos). De hecho, estos datos revelan mucha información sobre quién eres como persona y cuáles son las cosas que te importan. Estos datos, en su conjunto, se denominan tu «huella digital». La huella digital lo engloba todo, desde las fotos que te han gustado en Facebook hasta el tiempo que pasas viendo un anuncio en Instagram.

En este vídeo podrás aprender más sobre cuándo debes compartir información privada y personal (¡y cuándo no!).



Repasemos las diversas maneras en las que puede hacerse un mal uso de tus datos, el uso de algoritmos y la explotación de tu información personal. Pulsa en cada elemento para saber más.



Discriminación



Control de la información



Explotación de datos



Discriminación



Control de la información

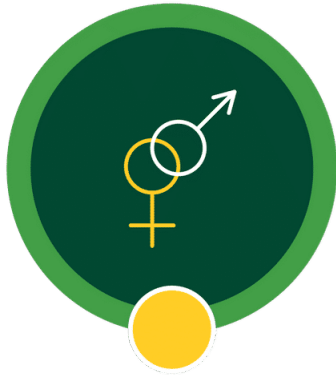


Explotación de datos

Discriminación

En ocasiones, nuestra huella digital incluye datos que pueden no reflejar de forma precisa nuestras complejas identidades. Por ejemplo, cuando un sitio web pide a sus usuarios que se identifiquen con una etiqueta binaria como «hombre» o «mujer».

En estos casos, se pueden utilizar estos datos para discriminar a una persona, ya que, como veremos más adelante, se suelen utilizar estos datos y rasgos personales extraídos de la información de un usuario para controlar el tipo de información que puede visualizar. Por ejemplo, es posible que solo se muestre información sobre métodos anticonceptivos a usuarios codificados como «mujeres» y «mayores de 18 años», aunque sabemos que es importante que todas las personas tengan un acceso igualitario a esta información.



Discriminación



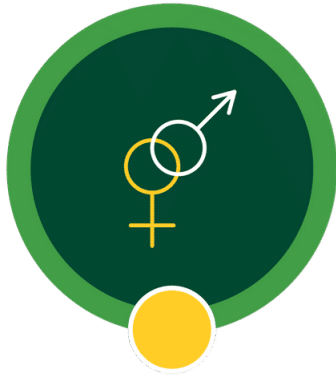
Control de la información



Explotación de datos

Control de la información

Tienes derecho a la información y a expresarte libremente en Internet. Sin embargo, los algoritmos y la inteligencia artificial que muchas empresas tecnológicas utilizan para mejorar su capacidad de búsqueda impiden el intercambio libre y justo de información e ideas en Internet. Por ejemplo, muchos algoritmos priorizan contenidos falsos o incorrectos en función del número de visitas. Por este motivo, la desinformación y los rumores sensacionalistas, como los mitos sobre la COVID-19, pueden difundirse muy rápidamente en Internet. Los algoritmos pueden ser muy complejos. En función de los factores que un algoritmo utilice, el programador de dicho algoritmo puede controlar qué tipo de contenido visualiza cada usuario cuando usa una red social o una plataforma de búsqueda. Por ejemplo, en función del contenido que sueles ver en Internet (por ejemplo, una fuente específica de noticias o un partido político concreto), los algoritmos pueden estar programados para continuar mostrándote contenidos similares. Esto puede impedir que te expongas a diferentes perspectivas sobre un mismo tema y puede conducir a la difusión de información falsa. Este control de la información pone mucho poder en manos de las empresas tecnológicas, pues pueden decidir qué información difundir. La información que consumimos influye en gran medida en nuestras opiniones e ideas sobre nuestro comportamiento, nuestras creencias y nuestra visión del mundo. Esto puede limitar nuestra capacidad para pensar con claridad y perseguir nuestros propios objetivos (la libertad de pensamiento). Sin embargo, permanecer alerta ante esta potencial influencia puede ayudarnos a romper su control. Por ello, hay activistas que están presionando para aumentar la supervisión y la regulación de estas empresas.



Discriminación



Control de la información



Explotación de datos

Explotación de datos

Otra manera por la que se puede dar un mal uso a los datos es cuando las empresas tecnológicas que pueden recopilar datos comparten esa información con otras empresas que los utilizan para orientar la publicidad o bien con gobiernos que la utilizan para censurar y controlar a sus ciudadanos. Muchas empresas tecnológicas operan conforme a un modelo de negocio (es decir, la forma en la que una empresa obtiene beneficios) que se basa en la extracción de datos o en la vigilancia. En ocasiones, los gobiernos pueden incluso exigirle a una empresa que entregue los datos o que tenga su propia tecnología de vigilancia. Los ciberdelincuentes también pueden robar estos datos mediante actividades de piratería informática y ciberataques, cada vez más frecuentes en los últimos años.

Reglamentos de protección de datos

Por suerte, hay algunos reglamentos que protegen los datos, como el [Reglamento General de Protección de Datos \(RGPD\)](#). El RGPD entró en vigor en la Unión Europea (UE) en 2018 y regula a las empresas tecnológicas que operan en la UE, incluyendo Meta y Google. El RGPD exige a las empresas que recopilan datos personales que sean claras respecto a los fines de dichos datos y que obtengan el consentimiento del usuario antes de recopilarlos. Esta información normalmente se comunica a través de la sección de «Términos y condiciones» que los usuarios deben leer y aceptar antes de utilizar una plataforma. Sin embargo, los activistas argumentan que, a la luz de la preponderancia de determinados «gigantes» de la tecnología en nuestra vida cotidiana (como

Meta, Apple y Google), los usuarios no tienen mucha más opción que aceptar estas condiciones. Por tanto, podría decirse que el consentimiento que damos para que se puedan recopilar y utilizar nuestros datos no se da de forma libre, sino bajo coacción.

¿Cómo puedo protegerme en Internet?

Ahora vamos a abordar algunas acciones que puedes tomar desde ya para protegerte y proteger a las organizaciones con las que trabajas. Puedes pausar el curso después de cada sección para realizar algunas de estas acciones.

Selecciona cada estrategia para leer más.

Utiliza contraseñas seguras —

- Utiliza contraseñas de, como mínimo, 8 caracteres que incluyan números, símbolos, mayúsculas y minúsculas.
- Evita las contraseñas que puedan averiguarse fácilmente y no utilices información personal.
- Utiliza contraseñas distintas para cada cuenta.
- Cierra siempre la sesión cuando hayas terminado de utilizar un sitio web, independientemente del ordenador o del dispositivo que estés utilizando.
- Utiliza inicios de sesión con doble autenticación. Esto es cuando, además de tu contraseña, debes introducir un código recibido por mensaje de texto o al que se accede a través de una aplicación móvil.
- Si tienes que guardar tu contraseña, escríbela en un papel o utiliza un sistema de gestión de contraseñas seguro y encriptado. Esto es especialmente importante si trabajas en una organización en la que varias personas deben compartir contraseñas y pueden acceder a las cuentas desde distintos dispositivos. Comparte las contraseñas solo con aquellas personas que necesiten acceder a un sitio web.

¿Aún no sabes si tu contraseña es segura? Utiliza herramientas como [The Password Meter](#) para comprobarlo.



Protege tu huella digital —

Mantén a salvo tu información personal y la de los demás mediante estas acciones:

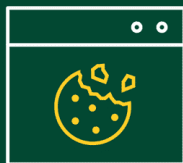
- No compartas tu nombre completo ni otra información que te identifique (como tu edad, tu ubicación específica, tu número de teléfono o el nombre de tu centro educativo) en redes sociales ni en foros públicos.
- Comprueba los ajustes de privacidad en redes sociales para asegurarte de que sabes con quién estás compartiendo la información, como una foto, una actualización de estado o tu ubicación.
- Recuerda que, una vez que hemos publicado algo en Internet, nunca podremos eliminarlo por completo, ¡así que publica de forma sensata! Esto incluye tus reacciones y comentarios en otros perfiles, así que recuerda interactuar con los demás del mismo modo que te gustaría que los demás interactuaran contigo.
- Piensa si es seguro etiquetar tu ubicación, ya que esto le indica a los demás dónde te encuentras.
- Pregunta siempre antes de publicar fotos, vídeos o contenido sobre otras personas. Si diriges una organización, esto también se aplica a las actividades de tu organización en Internet. ¡Pide siempre permiso antes de compartir cualquier cosa! Si alguien publica algo sobre ti que te incomoda, pídele a esa persona que lo elimine.
- Si eres menor de edad o si trabajas con menores (personas de menos de 18 años), habla con un adulto de confianza sobre la presencia de los menores en redes sociales.
- Si almacenas en tu lugar de trabajo datos personales o información sensible sobre tus trabajadores, socios, miembros o participantes, asegúrate de que esta información se almacena en una plataforma protegida por contraseña, encriptada o segura.
- Si trabajas en una organización, plantéate pedir u ofrecer formación en ciberseguridad al resto de trabajadores, si es posible.



Presta atención a las cookies

¡Las cookies son más que simples galletas! También sirven para que tu ordenador pueda rastrear tu actividad, lo que puede ser útil para guardar las credenciales de acceso o autocompletar tu nombre y tu dirección cuando compras en Internet. Sin embargo, en ocasiones las cookies también esconden problemas de seguridad, así que comprueba con frecuencia qué cookies se han almacenado en tu navegador.

Para más información, visualiza el vídeo "[Las cookies y tu privacidad en Internet](#)." También puedes visitar [¿Cómo se borran las cookies?](#)



Ten cuidado con la desinformación

Hay muchísima información en Internet, pero ¿cómo podemos saber cuál es cierta? Aquí encontrarás algunos consejos para distinguir los mitos de la realidad:

- Analiza la fuente original de la información. ¿Qué podemos averiguar sobre esa persona, organismo o medio de comunicación para determinar si es creíble o no? Los medios de comunicación fiables cuentan con periodistas con experiencia que son independientes de cualquier afiliación gubernamental, empresarial o institucional.

- Compara la información con otras fuentes que también estén informando sobre el mismo asunto para determinar si están abordando el tema de manera diferente. Esto te ayudará a evitar cualquier sesgo que un determinado medio de comunicación pueda tener.
- Comprueba tus propios sesgos. ¿Es posible que tu opinión esté nublando tu juicio sobre la veracidad de esta información?
- Cuando tengas dudas, acude a una persona experta en ese ámbito. ¿Qué dicen las personas expertas sobre dicho tema?



Responder ante la desinformación —

Si te percatas de que alguien está difundiendo información falsa, ¿cómo deberías reaccionar?

Empieza por hablar con respeto con dicha persona en un lugar privado y no la acuses de nada: eso solo servirá para que la persona se ponga a la defensiva. Usa los trucos que acabas de aprender y explícale por qué no crees que esa información sea cierta (por ejemplo: no proviene de una fuente fiable, otras agencias de noticias dan una cobertura muy diferente a ese suceso, un experto dice algo que lo contradice).

Puedes compartir información alternativa con esa persona si proviene de fuentes fiables y puedes hacerle preguntas sobre la información que está compartiendo para ayudarla a valorar por sí misma si dicha información es cierta o no. En ocasiones, las personas pueden estar cegadas por sus propias opiniones y negarse a escuchar lo que tienes que decir. Si la conversación sube de tono o si no están dispuestos a escucharte, pon fin a la conversación.

Aprende más mediante los siguientes dos videos:

- [Piensa antes de compartir | UNICEF](#)
- [Cómo ayudar al estudiantado a identificar las noticias falsas con las cinco C del consumo crítico](#) para aprender más formas de identificar las noticias falsas.



**Usa lo que has aprendido hasta ahora para
analizar el siguiente caso.**

Estás realizando una encuesta en línea con el fin de elaborar un informe sobre una política que está dirigido a los responsables de la toma de decisiones en tu comunidad. La encuesta contiene información personal de las personas encuestadas. ¿Cuál es la mejor manera de proteger esta información?

Selecciona las mejores respuestas entre las cinco opciones siguientes.

- Asegurarte de que los dispositivos y las cuentas en línea en las que se almacena la información privada tienen contraseñas seguras.

- Mantener la hoja de cálculo con los datos abierta en tu ordenador. Mientras nadie utilice tu teléfono u ordenador, nadie más podrá ver esa información.

- Comprobar los ajustes de privacidad y seguridad.

- Utilizar nombres completos y datos identificativos en el informe.

- Utilizar los datos únicamente según lo previsto y para los fines de esta investigación sobre políticas.

SUBMIT

A CONTINUACIÓN: ¿CÓMO PUEDO PROTEGERME Y RESPONDER ANTE EL CIBERACOSO?

¿Cómo puedo protegerme y responder ante el ciberacoso?

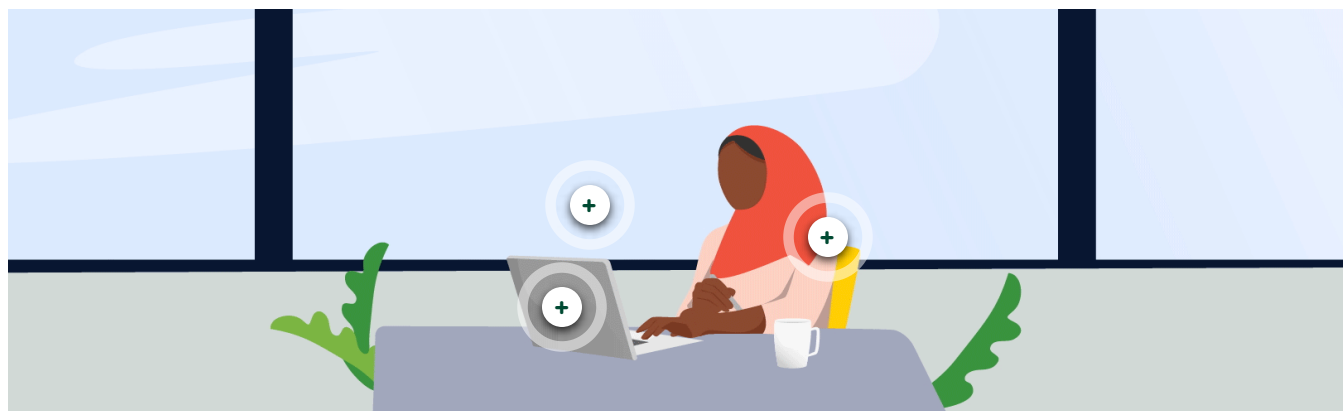
Según una encuesta realizada por Plan International en 2020, el 52% de las niñas han sufrido acoso o abuso en Internet. Es posible que tú u otras personas que conozcas también hayan sufrido ciberacoso. Es un problema grave que afecta a la salud y al bienestar de las personas en todo el mundo. Afortunadamente, hay maneras de impedir el ciberacoso y de apoyar a las personas que lo puedan estar padeciendo.

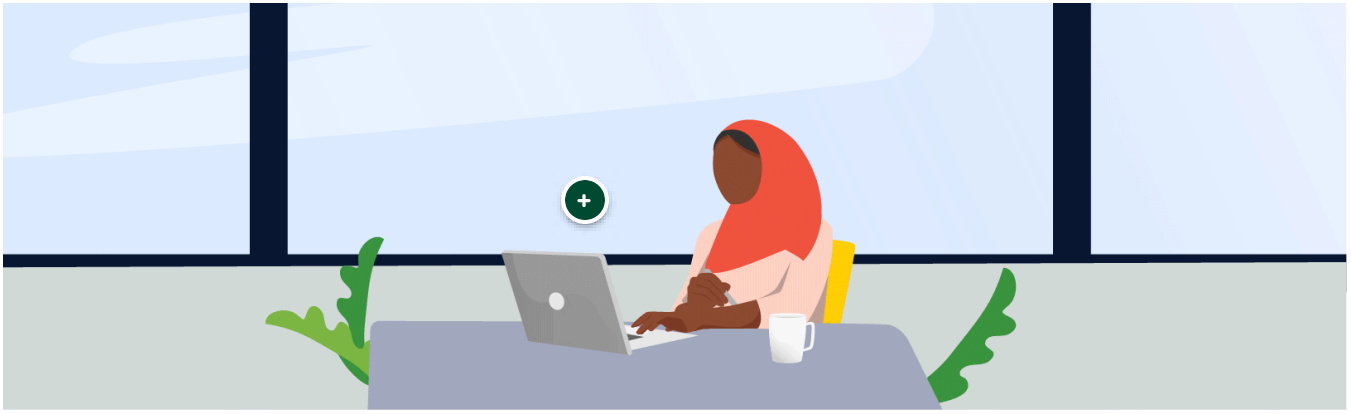
¿Qué es el ciberacoso?

El ciberacoso se produce cuando una persona es intencional y deliberadamente mala o cruel con otra persona mediante el uso de la tecnología, por ejemplo, a través de las redes sociales, mensajes de texto, correo electrónico o aplicaciones móviles.



Para descubrir el «qué», el «dónde» y el «cómo» del ciberacoso, pulsa en cada uno de los elementos.

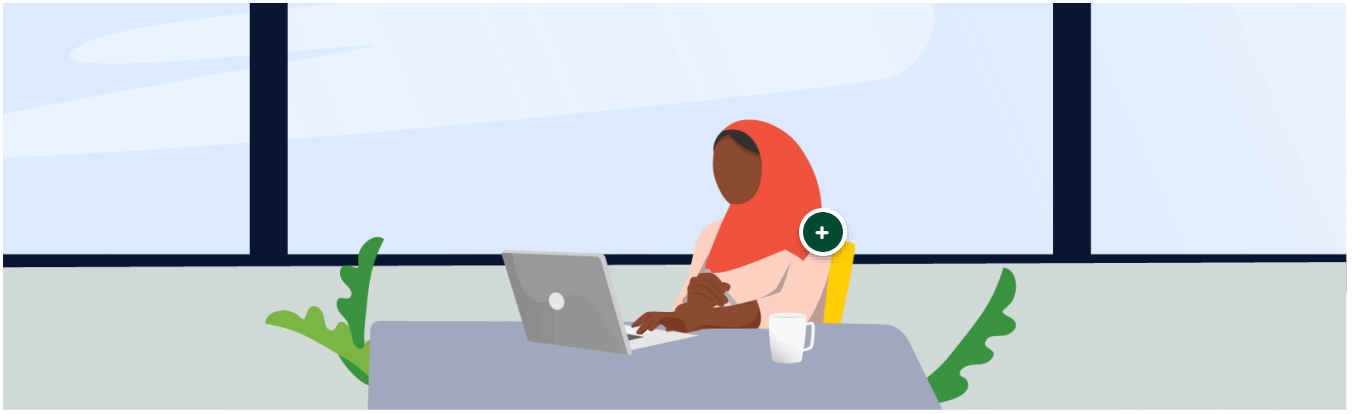




¿Dónde?

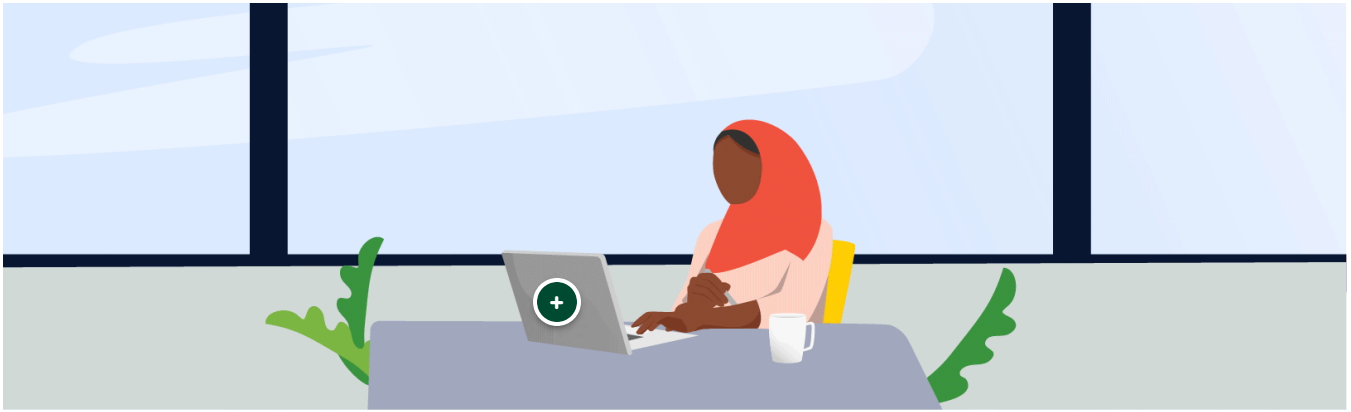
Ya que el ciberacoso tiene lugar en Internet, puede producirse en cualquier momento y desde cualquier lugar, pero suele suceder en espacios digitales públicos. A diferencia del acoso en persona, el ciberacoso puede parecer más anónimo o seguro porque tiene lugar a través de Internet, lo que lo hace más difícil de controlar y detener.

En ocasiones, el ciberacoso puede derivar en acoso o intimidación en persona, especialmente si los datos personales de una persona (como su nombre o su ubicación) se han compartido en Internet. Según un informe de Plan International, una de cada cuatro niñas que han sufrido ciberacoso se sienten físicamente inseguras en consecuencia.



¿Qué?

El ciberacoso puede incluir publicaciones, contenido o etiquetado de imágenes de forma inapropiada; la exclusión de personas de grupos o conversaciones en Internet; dejar comentarios irrespetuosos en el perfil de una persona, en sus fotos o en sus publicaciones; imitar o faltar al respeto a una persona a través de sus estados o contenidos en línea, o compartir información personal de otra persona sin su consentimiento.

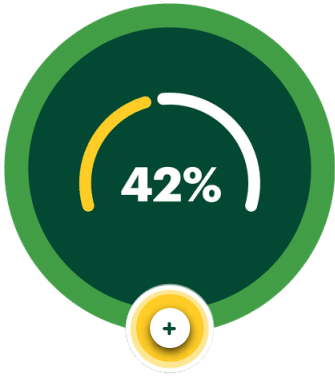


¿Quién?

Cualquier persona puede ser víctima de ciberacoso. Sin embargo, las personas que sufren una discriminación o una marginación adicional en el mundo físico por cuestiones de identidad suelen ser más susceptibles de sufrir ciberacoso (como las mujeres y las niñas; las personas negras, indígenas y de color; las personas del colectivo LGBTQIA+; las personas en las intersecciones de estas identidades y otras poblaciones tradicionalmente marginalizadas).

Por ejemplo, el ciberacoso por razón de género se produce cuando una persona sufre acoso en Internet debido a su orientación sexual o a su identidad de género real o percibida.

**Echa un vistazo a las conclusiones de un estudio
realizado por Plan International.**





42%

Porcentaje de mujeres que participaron en el estudio y dicen haber sido acosadas por pertenecer al colectivo LGBTQ+ (sobre el total de chicas que se identifican como LGBTQ+ y que han sufrido acoso).



14%

Porcentaje de mujeres que participaron en el estudio y dicen haber sido acosadas por tener una discapacidad (sobre el total de chicas que se identifican como personas con discapacidad y que han sufrido acoso).



37%

Porcentaje de mujeres que participaron en el estudio y dicen haber sido acosadas por pertenecer a una minoría étnica (sobre el total de chicas que se identifican como pertenecientes a una minoría étnica y que han sufrido acoso).

Fuente: Plan International

Dado que gran parte de las interacciones sociales quedaron limitadas a Internet durante la pandemia de COVID-19, muchos jóvenes informan de que el ciberacoso ha aumentado durante la pandemia.

Como activistas, solemos expresar abiertamente nuestras opiniones y creencias, las cuales pueden ser controvertidas o incluso radicales para nuestras comunidades. También podemos sufrir acoso en Internet por nuestras creencias, afiliaciones políticas u opiniones personales. En un estudio realizado por Plan International sobre jóvenes defensores de la igualdad de género, el 47% declaró haber sufrido ataques en Internet por sus opiniones. El ciberacoso de los activistas puede ser un intento de silenciar a quienes promueven la justicia social o la igualdad de género.

Veamos cómo podemos responder al ciberacoso. Pulsa en cada elemento para saber más.

¿Cómo puedo protegerme del ciberacoso? —

Las personas que cometen ciberacoso no suelen responder al pensamiento racional. Por tanto, es mejor no contestarles ni interactuar con ellas. Hacerlo podría empeorar las cosas. En su lugar, guarda copias o capturas de pantalla de las conductas de acoso, cambia tu configuración de privacidad y bloquea a la persona que te está acosando, si es posible. Algunas plataformas digitales cuentan con una opción para denunciar una agresión. Recuerda que, en muchos casos, las personas que acosan tienen que recibir varias denuncias antes de que una plataforma los bloquee, por lo que el acosador puede intentar volver a acosarte a ti o a otras personas a través de un perfil alternativo (no bloqueado). Si conoces personalmente a quien te acosa por tu centro educativo o tu lugar de trabajo, habla sobre lo sucedido con un miembro del profesorado o de la dirección. Es posible que sepan cómo ayudarte. En algunos casos, pueden existir leyes a nivel local o nacional para proteger del ciberacoso.

Además, al igual que sucede con el acoso en el mundo físico, el ciberacoso puede afectar negativamente a nuestra salud mental. Habla sobre tu experiencia con una amistad, mentor, familiar o profesional de la salud mental de tu confianza; busca ayuda en tu comunidad a través de [Child Helpline International](#), o busca recursos en línea.

¿Cómo debo responder ante el ciberacoso cuando son otras personas las que lo sufren? —

Ante todo, debes ser consciente de cómo tratas a los demás en Internet para asegurarte de que no contribuyes al ciberacoso. Si ves que alguien está sufriendo acoso en Internet, habla con esa persona y ofrécele tu apoyo, por ejemplo, escuchándola o ayudándola a acceder a recursos. No interactúes directamente con el acosador a través de Internet, ya que esto podría ponerte en peligro.

Concienciar sobre el impacto del ciberacoso puede ayudar a los y las jóvenes a darse cuenta del grave daño que puede ocasionar, lo que puede ayudar a evitar el ciberacoso antes de que se produzca. Además, los planes de estudios socioemocionales que educan a los jóvenes sobre cómo tener relaciones sanas y respetuosas no solo pueden enseñarles a interactuar con

amabilidad y compasión, sino que también sirven para generar resiliencia, de forma que puedan afrontar mejor cualquier experiencia de ciberacoso. A gran escala, las campañas de concienciación públicas pueden servir para difundir este mensaje y las leyes pueden hacer que los acosadores rindan cuentas. Algunos activistas también responsabilizan a las redes sociales por el impacto que sus plataformas tienen en los usuarios.

Estudio de caso: Un joven líder toma medidas para acabar con el ciberacoso

Además de apoyarnos mutuamente cuando se produce el ciberacoso, hay jóvenes que están tomando medidas para impedir que esto suceda y para prestar apoyo a quienes lo sufren. Agita Pasaribu, una joven líder de la promoción de 2020 de Women Deliver, es una de estas activistas. Agita, frustrada por que nadie se tomara en serio sus denuncias de acoso sexual en el lugar de trabajo, fundó Bullyid Indonesia. Bullyid ofrece apoyo psicológico y jurídico gratuito a las víctimas de ciberacoso. Como organización de defensa, el objetivo de Bullyid es concienciar en materia de derechos digitales, en particular en lo que se refiere al ciberacoso, y aumentar la capacidad de autocuidado y la resiliencia de la juventud que pueda ser víctima de acoso. Este enfoque multifacético aborda tanto las causas como las consecuencias del ciberacoso.



La pornografía de venganza es una forma de ciberacoso, conocida mediante el término jurídico «abuso sexual basado en las imágenes». La pornografía de venganza es el acto de compartir imágenes o vídeos íntimos de una persona sin su consentimiento, ya sea en línea o en otro medio, con la intención de causar

su malestar. Desde que la pandemia de COVID-19 azotara Indonesia, Bullyid ha ampliado el alcance de sus servicios y de sus actividades de defensa mediante su Centro de Ayuda contra la Pornografía de Venganza.

Entre marzo y mayo de 2020, los casos de abuso en línea aumentaron en más de un 300% en Indonesia en comparación con las estadísticas de 2019, según el Ministerio de Empoderamiento de la Mujer y Protección a la Infancia de Indonesia. Muchos de los casos que llegaron a Bullyid entran en la categoría de difamación en línea y pornografía de venganza. En vista de la situación, Bullyid envió una carta formal a varias empresas de redes sociales para pedirles que apoyaran a las víctimas de la pornografía de venganza y que retirasen dichos contenido rápidamente. En la actualidad, el Centro de Ayuda contra la Pornografía de Venganza colabora estrechamente con el Departamento de Políticas Públicas de Facebook, Instagram y Twitter Indonesia para eliminar con mayor agilidad cualquier contenido pornográfico vengativo que se comparta en dichas plataformas.





Gracias a una subvención de Women Deliver, Bullyid consiguió añadir nuevas funciones a la plataforma. La plataforma de denuncias SHARE de Bullyid es la primera plataforma de denuncias de acoso segura y anónima para instituciones. SHARE permite al alumnado y a su personal denunciar cualquier comportamiento de acoso, ciberacoso o mala conducta. También contiene una plataforma de gestión de incidencias que permite a las universidades responder, gestionar y prestar apoyo psicológico a las víctimas. Desde su lanzamiento en mayo de 2021, la plataforma SHARE ha protegido del ciberacoso a 27 780 trabajadores y estudiantes de catorce empresas, cuatro universidades y dos organizaciones de Indonesia. Ya que se trata de la principal organización benéfica registrada en materia de prevención del acoso y del ciberacoso y de ayuda a las víctimas, Bullyid ha aparecido en 179 medios de comunicación y organizaciones, entre las que se incluyen la Organización Mundial de la Salud, UNICEF y One Young World, con las que se ha asociado. Hasta la fecha, Bullyid beneficia a más de 45 000 personas en línea en

Indonesia y continúa buscando nuevos socios y defendiendo la causa con el fin de aumentar el impacto y salvar un mayor número de vidas.



Es hora de que te plantees cómo responderías en estos casos, usando para ello los conocimientos que has adquirido hasta ahora.

Alguien a quien conociste hace poco en un evento escolar ha comenzado a enviarte mensajes personales por Facebook. Al principio, los mensajes son amables, pero pronto se convierten en propuestas insistentes para invitarte a cenar, pedirte tu número de teléfono y solicitarte fotografías personales.

¿Qué acciones puedes tomar para protegerte?

- Silenciar la conversación y bloquear al usuario que te está enviando estos mensajes.
- Guardar una copia de los mensajes..
- Responder directamente a los mensajes y decirle al usuario que te deje en paz.
- Denunciar la conversación tanto a Facebook como a tu centro educativo.
- Publicar el nombre de esa persona y lo que te ha dicho en tu estado para dejarla en evidencia.
- Pedirle a un familiar de confianza, a una amistad o a un profesional de la salud mental que te ayude a lidiar con esta experiencia.

SUBMIT

Una madre joven ha publicado en Instagram una foto en la que aparece volviendo a estudiar después de haber tenido un bebé. Ves numerosas respuestas negativas, principalmente de hombres que la acosan y le dicen que no debería estar estudiando ahora que es madre.

¿Cuál es la mejor forma de apoyar a esta joven?

-
- Ya que no conoces a esta mujer personalmente, no deberías involucrarte.
 - Comparte la publicación en diversas redes sociales para demostrar la injusticia que se está cometiendo.
 - Ponte en contacto con ella, escúchala y recomiéndale servicios que puedan brindarle apoyo adicional, si lo necesita.

SUBMIT

A CONTINUACIÓN: CONCLUSIONES

Conclusiones

Con todo lo que has aprendido sobre tus derechos digitales, cómo protegerlos y cómo protegerte del ciberacoso, ya cuentas con las herramientas para poner en práctica tus conocimientos en el mundo real.

Te recomendamos que apliques las mejores prácticas que has aprendido en este curso, especialmente en las secciones de casos prácticos.

Mantente alerta sobre los problemas y situaciones que puedan surgir en Internet con tus socios y aliados y presta asistencia siempre que puedas. Y no olvides contactar a un familiar o amigo de confianza cuando necesites apoyo.

[Próximos pasos](#)

Prueba-posterior

Ahora puedes realizar la prueba de evaluación final para comprobar de nuevo tus conocimientos.

Pregunta

01/01

7 questions drawn randomly from Los derechos humanos en la era digital: prueba de evaluación inicial/final

Los derechos humanos en la era digital: prueba de evaluación inicial/final

Pregunta

01/07

Verdadero o falso: Todos los derechos humanos que ostentas en el mundo físico se aplican a tu «yo» digital, en Internet.

Verdadero

Falso

Pregunta

02/07

Tus derechos digitales incluyen: (Selecciona todas las opciones correctas)

- El derecho a la privacidad
- El derecho a la libertad de expresión
- El derecho a una vida libre de violencia y acoso
- El derecho a hacer lo que quieras

Pregunta

03/07

¿Cuáles son las tres maneras por las que se pueden violar tus derechos digitales?

(Selecciona todas las opciones correctas)

Ciberacoso

Minería de datos

Publicación de *blogs*

Vigilancia

Pregunta

04/07

¿Quién tiene la responsabilidad de garantizar y proteger los derechos digitales?

(Selecciona todas las opciones correctas)

Los Estados

Las empresas

Los individuos

Las organizaciones de la sociedad civil

Pregunta

05/07

¿Qué debes hacer si detectas que están acosando a alguien por Internet?

- Enfrentarme públicamente al acosador y recriminarle su comportamiento para que otras personas aprendan de la situación.
- Enviarle un mensaje privado al acosador para decirle que su conducta es inapropiada y que he alertado a las autoridades competentes.
- No debo hacer nada, porque eso podría empeorar una situación que ya es negativa de por sí.
- Ofrecer apoyo y escuchar a la víctima.

Pregunta

06/07

Verdadero o falso: El 35 % de las niñas han denunciado haber sufrido acoso o abuso por Internet.

Verdadero

Falso

Pregunta

07/07

¿Cómo puedes protegerte a ti mismo y a tus datos en Internet? (Selecciona todas las opciones correctas)

- Uno no puede protegerse, salvo que no utilice Internet en absoluto.
- Utilizar contraseñas seguras.
- Comprobar los ajustes de privacidad de todos mis perfiles en redes sociales.
- Aceptar todas las cookies de los sitios web que visito.
- Estar alerta ante la información errónea, comprobando las fuentes e investigando en mayor profundidad.