

Guía sobre Seguridad y Cuidados Digitales

para Comunicadores Indígenas y
Defensores del Territorio en Oaxaca



Guía sobre Seguridad y Ciudades Digitales para Comunicadores Indígenas y Defensores del Territorio en Oaxaca

Elizabeth Mosqueda Rivera
Kiado Cruz Miguel
Nallely Guadalupe Tello Méndez
Oliver Fröhling
Coordinación

Argelia Rodríguez
Sistematización

SURCO Oaxaca A.C. y Consorcio Oaxaca
Revisión y edición

**Oaxaca de Juárez, Oaxaca, México
2023**

Una Guía publicada por:



En colaboración y con el financiamiento de:



Unión Europea



«La presente publicación ha sido elaborada con el apoyo financiero de la Unión Europea. Su contenido es responsabilidad exclusiva de SURCO Oaxaca A.C. y Consorcio Oaxaca y no necesariamente refleja los puntos de vista de la Unión Europea».

CONTENIDO

PRÓLOGO

INTRODUCCIÓN

Cuidados y Derechos digitales colectivos

Facilitación: La Jes (Sursiendo-Comunicación y Cultura Digital)

BLOQUE 1. RELACIONES E INTERACCIONES DIGITALES

1.1 De la arquitectura de las redes a los cuidados digitales

Facilitación: Oliver Fröhling y Kiado Cruz (SURCO Oaxaca A.C.) y Elizabeth Mosqueda (Consortio Oaxaca)

1.2 Las redes en nosotr@s, cómo atraviesan nuestras corporalidades

Facilitación: Oliver Fröhling y Kiado Cruz (SURCO Oaxaca A.C.), Nallely Tello y Elizabeth Mosqueda (Consortio Oaxaca)

1.3 El traslado de las violencias a los espacios digitales

Facilitación: Elizabeth Mosqueda (Consortio Oaxaca)

BLOQUE 2. ACTIVISMO DIGITAL

2.1 Ciberactivismo y Ciberfeminismo

Facilitación: Soledad Venegas Nava (Estudio Mantis) y Elizabeth Mosqueda (Consortio Oaxaca); Oliver Fröhling y Kiado Cruz (SURCO Oaxaca A.C.)

2.2 Activismo digital en lenguas indígenas

Facilitación: Tajëw Díaz Robles (Colmix-Colectivo Mixe), Rodrigo Pérez (Zapoteco 3.0) y Eddie Avila (Rising Voices)

2.3 Humanidades Digitales

Facilitación: Alejandra Méndez (CEU-XHIDZA)

BLOQUE 3. DERECHOS DIGITALES

3.1 ¿Qué son los derechos digitales?

Facilitación: Martha Tudón (Article 19)

3.2. Libertad de Expresión

Facilitación: Pedro Matías (Página 3)

3.3 Protección de Datos

Facilitación: Instituto Nacional de Acceso a la Información (INAI)

BLOQUE 4. APROPIACIÓN DE LAS TECNOLOGÍAS DIGITALES

4.1. Seguridad digital/Privacidad

Facilitación: Paul Aguilar (SocialTIC)

4.2 Twitter y cuidados para el teléfono celular

Facilitación: Yásnaya Aguilar.

4.3. El derecho a las tecnologías y cuidados digitales

Oliver Fröhling (SURCO Oaxaca A.C.) y Elizabeth Mosqueda (Consortio Oaxaca)

Nota: El uso de @, x, -es. Representa nuestra intención de expresarnos colectivamente como participantes de este Laboratorio. Consideramos que de esta forma logramos incluir y visibilizar a todas las personas y géneros. Aun cuando las normas tradicionales de lenguaje y la gramática no los acepten, partimos de la idea de que el lenguaje es dinámico y se transforma para adaptarse a las necesidades de comunicación de la sociedad.

PRÓLOGO

La presente Guía de Seguridad y Cuidados Digitales para Comunicador@s Indígenas y Defensor@s del Territorio en Oaxaca es el resultado de un valioso esfuerzo colaborativo entre organizaciones comprometidas con la defensa de los derechos humanos, la igualdad de género y la preservación de las culturas indígenas. En este contexto, Consorcio para el Diálogo Parlamentario y la Equidad Oaxaca (Consorcio Oaxaca) y Servicios Universitarios y Redes de Conocimientos en Oaxaca (SURCO Oaxaca A.C.) han unido fuerzas para brindar herramientas prácticas y conocimientos que fortalezcan la protección integral de lxs comunicadores indígenas y defensores del territorio en el ámbito digital.

Esta guía surge a partir de las reflexiones y experiencias compartidas en el Laboratorio de Narrativas, un espacio de escritura, reflexión y discusión colectivas en el que participaron 27 personas comprometidas con diversos procesos comunitarios, educativos y académicos. La guía se estructura en bloques temáticos que abordan aspectos fundamentales para el cuidado digital, proporcionando un enfoque integral y centrado en las particularidades de lxs comunicadores indígenas y defensores del territorio en Oaxaca.

El primer bloque, "Relaciones e Interacciones Digitales", explora la importancia de comprender la arquitectura de las redes y cómo influye en los cuidados digitales, así como el impacto de las redes en nuestras corporalidades y las violencias digitales a las que nos enfrentamos.

En el bloque "Activismo Digital", se aborda el ciberactivismo y el ciberfeminismo, así como el activismo digital en lenguas indígenas y las posibilidades que ofrecen las humanidades digitales para fortalecer las prácticas de defensa de los derechos humanos.

El tercer bloque, "Derechos Digitales", examina los fundamentos y alcances de los derechos digitales, incluyendo la libertad de expresión y la protección de datos, destacando la importancia de garantizar estos derechos en el entorno digital.

Finalmente, el bloque "Apropiación de las Tecnologías Digitales" se centra en la seguridad digital y la privacidad, los cuidados para el uso de Twitter y el derecho a las tecnologías, proporcionando herramientas y conocimientos necesarios para una apropiación responsable y consciente de las tecnologías digitales.

Esta guía representa un esfuerzo conjunto por reconocer y respetar la cosmovisión, los contextos culturales y el derecho a la libre expresión de lxs comunicadores indígenas y defensores del territorio en Oaxaca. Ha sido construida con la convicción de que el acceso y el uso seguro de las tecnologías digitales son fundamentales para

fortalecer su labor en la defensa de los derechos humanos, la diversidad cultural y la preservación de los territorios indígenas.

Esperamos que esta guía sea una herramienta útil y práctica, proporcionando las orientaciones necesarias para navegar de manera segura en el mundo digital, y que contribuya a maximizar las oportunidades que ofrece la tecnología y a minimizar los riesgos a los que se enfrentan lxs comunicadores indígenas y defensores del territorio en Oaxaca. Su valioso trabajo es esencial para la construcción de sociedades más justas, equitativas y respetuosas de la diversidad.

¡Bienvenidxs a este viaje de aprendizaje y empoderamiento digital!

INTRODUCCIÓN

En un contexto en el cual lxs comunicadorxs indígenas y defensorxs del territorio en Oaxaca enfrentan múltiples desafíos y riesgos en el ejercicio de su labor, resulta fundamental abordar la importancia de la seguridad y los cuidados digitales en su trabajo cotidiano. Estas personas desempeñan un papel crucial en la defensa de los Derechos Humanos, la justicia social y la preservación de las culturas indígenas y se encuentran expuestas a amenazas, censura, vigilancia y ataques tanto en el ámbito físico como en el digital.

Consortio para el Diálogo Parlamentario y la Equidad Oaxaca (Consortio Oaxaca) y Servicios Universitarios y Redes de Conocimientos en Oaxaca (SURCO Oaxaca A.C.) reconocen la importancia de garantizar la seguridad y protección de lxs comunicadorxs indígenas y defensorxs del territorio en el entorno digital. Ambas organizaciones, comprometidas con la promoción de los Derechos Humanos, la igualdad de género y el fortalecimiento de las comunidades indígenas, han unido esfuerzos para desarrollar esta guía con el objetivo de proporcionar herramientas prácticas y conocimientos que contribuyan a su protección integral en el ámbito digital.

La realidad actual nos muestra que la Internet y las tecnologías digitales ofrecen tanto oportunidades como riesgos para lxs comunicadorxs indígenas y defensorxs del territorio. Por un lado, estas herramientas les permiten amplificar sus voces, visibilizar las problemáticas que viven y acceder a redes de apoyo a nivel local e internacional. También ayudan en la difusión de información relevante, compartir testimonios y promover la defensa de los Derechos Humanos de sus comunidades. Sin embargo, al mismo tiempo, al hacer uso de estas tecnologías también están expuestos a amenazas, campañas de difamación, hackeos y violaciones de su privacidad.

El objetivo de esta Guía es dotar de conocimientos y estrategias a lxs comunicadorxs indígenas y defensorxs del territorio en Oaxaca, minimizando los riesgos y maximizando las oportunidades que ofrece la tecnología para protegerse en el entorno digital. Se abordarán temas clave como la privacidad en línea, la seguridad de las comunicaciones, la gestión de contraseñas, la protección contra el acoso digital y la ciberseguridad en general.

Es importante destacar que la Guía ha sido construida de manera colaborativa y participativa, incorporando las reflexiones y experiencias compartidas en el Laboratorio de Narrativas realizado por Consortio Oaxaca y SURCO Oaxaca A.C. Además, se ha tenido en cuenta la particularidad de las situaciones que enfrentan lxs

comunicadorxs indígenas y defensorxs del territorio en Oaxaca, respetando su cosmovisión, contextos culturales y su derecho a la libre expresión.

En conclusión, buscamos que esta Guía sea una herramienta útil y práctica que contribuya a fortalecer la seguridad y protección digital de lxs comunicadorxs indígenas y defensorxs del territorio en Oaxaca. Esperamos que les brinde las orientaciones necesarias para navegar de manera segura en el mundo digital y fortalecer su valioso trabajo en la defensa de los Derechos Humanos, la diversidad cultural y la preservación de los territorios indígenas.

Cuidados y derechos digitales colectivos

Facilitación: La Jes (Sursiendo-Comunicación y Cultura Digital¹)

Los cuidados y derechos digitales han sido un tema de interés para diversas organizaciones y colectivos debido a los contextos de inseguridad en el que viven las personas defensoras de Derechos Humanos. Ante la necesidad de hacer un activismo bajo otras lógicas, más seguras y protegidas, consideramos la urgencia de habitar de otro modo los espacios digitales.

Los cuidados digitales se inscriben como prácticas de protección individual y colectiva que requieren un uso consciente e informado de diferentes tecnologías, así como de las relaciones que establecemos con lo-s otro-s, la materia, el territorio y la infraestructura tecnológica. Los derechos digitales garantizan el acceso a la información y el ejercicio de nuestra humanidad digital, protegiendo nuestros datos de toda forma de abuso y divulgación sin permiso.

En esta sección reflexionamos en torno al uso e impactos de la tecnología en las relaciones y procesos colectivos dentro de los espacios digitales, los cuales deberían ser habitables para todas, todos, todes.

¿Qué es la Comunalidad y la Autonomía digital?

Podemos reconocer el término *comunalidad digital* como “una propuesta que pone en evidencia las estructuras sociotécnicas de poder en el diseño, extracción, producción, uso y desecho de las tecnologías digitales y su relación con el ambiente” (<https://sursiendo.org/>). La *comunalidad digital* se caracteriza por colocar en el centro la diversidad social, cultural y natural. Implica una responsabilidad compartida en las relaciones y prácticas cotidianas que se dan en la Internet y busca que este sea un bien común considerando que existe una comunidad que lo habita y un modo de gestionar ese modo de habitarlo.

La *comunalidad digital* implica reflexionar y actuar sobre los impactos que tienen las tecnologías en los territorios, las relaciones que emergen entre quienes los habitan, las corporalidades que se despliegan en el proceso de lucha y defensa. La comunalidad digital también supone que existen otros modos de hacer y apropiarse de la tecnología para el beneficio común, más allá de funcionar como herramienta de acceso a la información y la comunicación.

Por otro lado, la autonomía *digital* es una idea que plantea que la tecnología debería responder a la necesidad de un grupo o comunidad y no sólo a intereses de las grandes corporaciones. Esto significa tener acceso a otras interfaces lingüísticas,

¹ *Sur-Siendo-Comunicación y Cultura Digital* es una organización de activistas dedicada a la comunicación y diseño, software y cultura libres, educación popular, arte y gestión cultural, también se relacionan con procesos de defensa de derechos humanos, de la tierra y el territorio.

desde la disposición de íconos en la pantalla, es decir desde el uso del dispositivo físico tecnológico, hasta el uso informado de su función sociotécnica, afectiva y relacional.

El uso de plataformas privadas nos permite acceder a ciertos campos de conocimiento e información, pero nos limita de muchos otros, sobre todo cuando se trata de sectores o comunidades que no cuentan con recursos o espacios indispensables para acceder al uso de la tecnología.

Las plataformas digitales imponen narrativas creando la sensación de que la Internet es para quien lo desee, como si las relaciones en los espacios digitales pudieran suplir las relaciones entre las personas. Sin embargo uno de los retos a los que nos enfrentamos es el de la creación de plataformas sociotecnológicas que hagan uso de códigos e íconos vinculados al modo de ver, sentir y pensar de las personas o comunidades que se mueven y organizan políticamente desde otras lógicas ajenas a las del mercado.

¿Cómo podemos habitar las tecnologías que queremos?

- Tengamos presente que las narrativas y tecnologías no son neutrales ni de acceso universal, obedecen a una nueva forma de capitalismo que mercantiliza el ejercicio de los derechos digitales.
- Busquemos una tecnología diferente a la que se nos impone por defecto. Las plataformas privadas, su arquitectura y diseño, en general son completamente ajenas a la diversidad de personas y comunidades que las habitan.
- Probemos otras posibilidades de uso tecnológico, de acuerdo a las necesidades de comunicación e información que requerimos. La Intranet², por ejemplo, es una forma de comunicación que puede resultar suficiente para no depender del uso de grandes plataformas digitales.
- Participemos del uso y construcción de otras tecnologías -como el software libre, por ejemplo-, sin dejar de erradicar prácticas y discursos patriarcales, capitalistas y coloniales que siguen afectando la vida y las relaciones de l@s usuari@s, dentro y fuera de los espacios digitales.
- Analicemos el contexto en el que nos movemos para identificar qué podemos hacer para cuidarnos en el espacio digital, en qué condiciones lo habitamos, qué estrategias utilizar, cuáles son las brechas digitales que nos atraviesan o si requerimos mayor capacitación, etc.

² Intranet es una red informática que utiliza la tecnología del protocolo de Internet para compartir información, sistemas operativos o servicios de computación dentro de una organización. Suele ser interna, en vez de pública como Internet, por lo que solo los miembros de esa organización tienen acceso a ella.

- Reflexionemos sobre los contextos digitales o virtuales que deseamos habitar, por ejemplo, para las comunidades indígenas y aquellas que se sostienen a partir de su relación con los ciclos de la tierra y el territorio, es necesaria otra forma de conexión que considere la cosmovisión comunitaria y local.
- Destaquemos el invaluable aporte de aquellos que han hecho posible el acceso a las tecnologías de la información y comunicación. La Internet que utilizamos en la actualidad es el resultado del trabajo y la contribución de mujeres como Radia Perlman, conocida como la madre de la Internet, y Hedy Lamarr, inventora del Wi-Fi.
- Acompañemos los procesos y movimientos de aquellxs que defienden el territorio frente a la explotación de las grandes corporaciones tecnológicas. Busquemos construir nuevas formas de relaciones y narrativas como usuari@s de la Internet, participando y cuestionando cómo podemos utilizar las tecnologías de manera diferente, basándonos en diversas experiencias de lucha y de resistencia.

Otras referencias:

Sursiendo-Comunicación y Cultura Digital (07 de junio de 2021). *Derechos digitales colectivos*. Disponible en: <https://sursiendo.org/ejes-tematicos/>.

BLOQUE I

Relaciones e interacciones digitales

Es fundamental tener claridad sobre el significado del espacio digital, la virtualidad y la Internet para habitar los entornos digitales de manera segura. En este primer bloque, exploraremos las diferencias y matices entre estos términos, ya que a menudo los utilizamos como sinónimos.

Aprenderemos sobre cómo funciona la Internet, cuáles son las dinámicas cotidianas en el uso de las tecnologías y cómo nos relacionamos con los entornos y dispositivos digitales. Esto nos permitirá protegernos de las vulnerabilidades que existen y aprovechar los beneficios que nos ofrecen.

1.1. De la arquitectura de las redes a los cuidados digitales

Facilitación: Oliver Fröhling y Kiado Cruz (SURCO Oaxaca A.C.³) y Elizabeth Mosqueda (Consortio Oaxaca⁴)

¿Qué es la Internet y cómo funciona?

La Internet es una red que mueve al mundo y va más allá de las redes sociales, plataformas digitales y aplicaciones de comunicación instantánea. Requiere del uso de una infraestructura tecnológica global, de ahí que sea un recurso finito y no sea de fácil acceso para todas las personas. La Internet es la infraestructura física y lo virtual se forma en nuestras cabezas.

La Internet también forma parte de nuestras corporalidades y emotividades, permea las relaciones que vamos construyendo en un entorno virtual de intercambios socioafectivos y psicosociales, se trata de un sistema de vida moderna al que no tiene acceso más del 50% de la población mundial.

Para que funcione la Internet es indispensable el uso de energía eléctrica, sin ese recurso sería imposible hablar de una red que nos ofrezca servicios, facilite la conexión para comunicarnos, cree lenguajes pero también los expropia, excluya y cosifique.

A través de cables que se interconectan desde el subsuelo marino hasta satélites artificiales, la Internet funciona bajo una lógica del despojo en territorios donde se extraen los elementos que dan soporte a su infraestructura. A pesar de tener su origen en la tecnología desarrollada para uso militar, se ha ido transformando de manera acelerada en los últimos 50 años tal y como se muestra el siguiente cuadro:

Datos históricos de la Internet y plataformas digitales	
1960s-80s	Ligada al complejo científico-militar de EEUU: ARPANET, protocolos, conexión entre redes distribuidas Vocabulario de servidores, dominios, DNS, www (80s, navegadores desde 1993)
1988	Primera conexión a México: (UNAM, ITESM)
Hasta el 1995	Principalmente instituciones académicas usan la red
1994	Privatización de la internet, Acceso al público, crecimiento exponencial

³ SURCO Oaxaca A.C. es una organización civil que promueve el acceso y la apropiación tecnológica de comunidades indígenas, el uso de las tecnologías libres y lucha contra el cambio climático.

⁴ Consortio Oaxaca es una organización civil feminista que promueve el respeto y ejercicio de los derechos humanos de las mujeres y la igualdad de género.

1998	Fundación de Google
2000	Colapso de los “.com”, de conexión telefónica a banda ancha
2004	Lanzamiento de Facebook
2006	Creación la red social Twitter
2007	Lanzamiento de la 1ra generación de Iphone, línea de teléfonos inteligentes
2008	Telcel 3G (conexión de datos, se conectan la internet y celular)
2009	Lanzamiento de la aplicación de mensajería instantánea WhatsApp
2010	Lanzamiento de la aplicación y red social Instagram
2013	Lanzamiento de la aplicación de mensajería instantánea y VOIP Telegram
2016	Lanzamiento de la red social Tik Tok
El uso de la Internet requiere 9.2 % del consumo global de electricidad	

¿Qué son las plataformas digitales?

Las plataformas digitales son una infraestructura que permiten que dos o más grupos interactúen por medio de la Internet, en un portal o ciber sitio, donde se almacena información y que depende de intermediarios para fluir a través de la red.

Las plataformas dependen del impacto que puedan tener en las redes sociales, ya que son fáciles de difundir y pueden desencadenar el crecimiento viral. Estos sitios son espacios donde se produce la interacción entre los usuarios y se extraen datos. Además, las plataformas tienen la capacidad de desarrollar sistemas de gobernanza.

Existen diversos tipos de plataformas:

- De anuncios comerciales (Facebook)
- De nubes (Amazon, Microsoft)
- Industriales (Siemens, GE)
- De productos vueltos servicios (Spotify, Adobe)
- Plataformas “delgadas” (Uber, Airbnb, Zoom)

¿Cuáles son las dinámicas de cada red? ¿Por qué estamos ahí?

La Internet nos da la sensación de movilidad, de estar dentro o fuera de 'algo' que influye en nuestras corporalidades y emotividades, es por eso que el uso de las redes sociales en la actualidad resultan importantes. A pesar de que demandan inmediatez y acumulación, continuamos activos en ellas.

En la lógica del sistema económico global cualquier espacio se puede intervenir en la red, sin embargo existen movimientos sociales que inciden en el uso y apropiación de los medios digitales. Ejemplo de ello han sido el levantamiento zapatista en Chiapas en 1994 o la creación de la plataforma Oaxaca Libre en 2006, mismas que lograron intervenir las narrativas de los movimientos sociales para ir construyendo espacios digitales alternativos a las lógicas de la capitalización dentro de las plataformas digitales.

¿Cómo nos cuidamos en la red?

Es indispensable asumir una postura política frente al uso y modo de habitar la Internet, saber qué son los cuidados digitales y qué relaciones afectivas estamos trasladando al espacio digital. De ahí que retomemos las siguientes aportaciones del texto *"Internet, romanticismo, amor y filosofía"* del autor surcoreano Byung-Chul Han:

Las redes sociales no son el principio ni el final de Internet (...)

Las redes nos obligan a interactuar alrededor de un amor puramente narcisista. Por eso borra al Otro, que no es más que un obstáculo molesto para la proyección completa y armoniosa de nuestro propio yo.

Nadie va a salvarnos si primero no queremos ser salvados.

Mapeo de interacciones virtuales

Representa de forma gráfica -con dibujos, pintura, fotografía, collage de texturas o fotos- las reflexiones que te surjan a partir de las siguientes preguntas:

- ¿Cuánto tiempo pasas en la Internet?
- ¿En qué aplicaciones y/o plataformas digitales pasas más tiempo?
- ¿Cómo te sientes con esa forma de interactuar?
- ¿Qué llama tu atención de tus entramados e interacciones en la red?

Reflexiona con otras personas sobre cada una de las preguntas detonantes y explora los mapas compartiendo sus hallazgos en relación al tema.

Otras referencias:

Mavrakis, N. (16 de Marzo de 2021). *Internet, romanticismo, amor y filosofía según Byung-Chul Han*. En: Revista Paco. <https://revistapaco.com/internet-romanticismo-amor-y-filosofia-segun-byung-chul-han/>

Peirano, M. (25 de septiembre de 2020). *Capitalismo de plataformas: tres libros y un documental*.

El País. https://elpais.com/cultura/2020/09/25/babelia/1601048485_287643.html

Un mundo inmenso (14 de febrero de 2019). *Cómo funciona internet: los cables submarinos que conectan al mundo*. [Video]. Youtube. <https://www.youtube.com/watch?v=u1xxZ8r2rRc>

Wachowski, L. (Directora). (1999). *Matrix* [película]. Warner Bros.

1.2: Las redes en nosotr@s: cómo atraviesan nuestras corporalidades

Facilitación: Oliver Fröhling y Kiado Cruz (SURCO Oaxaca A.C.), Nallely Tello y Elizabeth Mosqueda (Consortio Oaxaca)

Muchas palabras que están asociadas con el uso de la Internet tales como *virtual*, *digital*, *realidad* y *tecnología*, son términos que utilizamos indistintamente en la vida cotidiana. Es por ello que consideramos necesario revisar sus significados y reconocer sus diferencias, de esta forma podremos comprender mejor la manera en que estos conceptos impactan en nuestras relaciones dentro y fuera de los espacios digitales.

En esta sección, reflexionaremos sobre el tiempo que pasamos en las redes y cuestionaremos por qué elegimos estos espacios y no otros, cómo es que hacemos un uso diferenciado de las aplicaciones que utilizamos y la capacidad que tenemos de elegir por dónde se cruzan nuestras interacciones en el mundo digital.

¿Cómo nos interpelan las redes sociales?

En el Laboratorio de Narrativas 6.0 reflexionamos sobre la necesidad de preguntarnos cómo la tecnología interpela nuestras realidades afectando la relación con nuestro propio cuerpo y en las relaciones con las demás personas.

Asociamos nuestro habitar en la red con la oportunidad de incidir en la transformación social desde los espacios digitales, sin embargo también coincidimos que esto nos puede provocar afectaciones corporales y emocionales como ansiedad, depresión o generar una sensación de placer cuando recibimos más *likes* y con ello incrementar nuestra popularidad en redes sociales.

¿Qué entendemos por lo virtual y lo digital? ¿Qué es la tecnología y la realidad virtual?

El término 'virtual' se ha vuelto más común en las últimas décadas. Entendemos lo virtual como aquellos espacios de interacción en la Internet. Existen relaciones personales que son virtuales gracias a las herramientas digitales que hacen posible la interconexión con otr@s interpellando nuestras corporalidades y espacios de socialización, lo que nos hace preguntarnos qué tanto lo virtual se ha convertido en una extensión de nuestros cuerpos.

El término '*digital*' se usa comúnmente para referirse a todos los sistemas que representan, almacenan o usan la información en el sistema binario. Ejemplo de ello son casi todos los aparatos electrónicos e informáticos que nos rodean. Si lo pensamos en términos musicales, antes había discos LP que funcionaban con tecnología analógica y las ondas de sonido grabadas en un disco de vinilo. Con el paso del tiempo se creó el disco compacto o CD, que almacena datos en formato

digital y el sonido se reproduce en un aparato que transmite la información por medio de números, es decir, dígitos.

Lo digital significa la representación del mundo por medio de algoritmos matemáticos, ya que al final los sistemas que hacen funcionar a las computadoras están contruidos a partir de números. Lo que vemos en las pantallas de nuestros dispositivos representa el llamado sistema binario. Se puede asociar lo digital con lo táctil y lo virtual con un espacio que se simula. Por ejemplo, la biblioteca virtual es un espacio que simula serlo y la biblioteca digital es una colección de recursos digitalizados que requieren del uso de un equipo tecnológico.

En los últimos años hemos pasado de un mundo analógico al digital, y en ese transitar vertiginoso hemos aprovechado la tecnología para poder vernos, expresarnos, relacionarnos y conectarnos bajo la sensación de estar mucho más cerca un@s de otr@s.

El término '*tecnología*' se relaciona con el hecho de realizar una actividad y finalizarla para satisfacer necesidades. Pueden ser conceptos, habilidades, formas organizativas, instrumentos, recursos y procedimientos que permitan resolver problemas de la vida cotidiana. La escritura o una lengua son una forma de tecnología.

Por otra parte, el concepto de '*realidad*' puede ser plural, complejo e incluso filosófico. Lo que se vive todos los días es nuestra realidad. Actualmente con el uso de las tecnologías es posible vivir esta realidad de manera presencial o virtual, individual o colectiva y al mismo tiempo, podemos o no estar en ella.

¿Cómo queremos que la(s) red(es) sean parte de nuestra realidad?

- Queremos una tecnología asequible para todas las personas, pues sabemos que la idea de que la Internet es universalmente para todas, todos y todes no es real. En nuestro país hay quienes no pueden pagarlo o no tienen acceso.
- Queremos habitar las redes con libertad y respeto a la diversidad y que estas características permeen las interacciones y contenidos que se nos ofrecen bajo los ideales de pluralidad, justicia y equidad.
- Queremos otro modo de relacionarnos en las redes. Esto requiere construir en colectivo un habitar más diverso, incluyente, plural, no violento y justo.
- Queremos incidir en las estructuras y hegemonías tecnológicas que imponen un sólo modo de alojarse y usar la Internet.
- Queremos ser libres de explorar, escuchar, informarnos y comunicarnos a través de la red sin que nuestros datos sean extraídos y utilizados con fines de lucro o de

mercado. Necesitamos revertirlo y contar con mejores estructuras sociales y no de explotación.

La realidad actual está dominada por la tecnología y se extiende cada vez más a muchos espacios en nuestras vidas. Es una ilusión pensar que no participamos en este mundo tecnológico y aunque estemos o no conectados resulta importante mirar qué tenemos a nuestro alcance para lograr que el uso de la Internet sea en beneficio de la humanidad y no una amenaza para ella.

¿Cómo nos cuidamos en redes sociales?

Existe una serie de prácticas para cuidarnos en el uso y habitar de los espacios digitales, por ejemplo, conservar el anonimato al usar redes sociales o reducir el uso desmedido de aplicaciones en nuestros dispositivos. La apuesta es pensar cómo apropiarse de estas tecnologías, cuestionando cómo se usan, adaptan y transforman socialmente para ocupar los espacios de una forma más segura e igualitaria.

Mis tránsitos por la Internet

En una serie de seis u ocho imágenes -fotos, dibujos- cuenta o representa dónde estás ahora y a dónde te gustaría llegar en tu relación con la Internet; te invitamos a pensar la forma en que lo habitas y cómo te gustaría habitarlo para sentirte mejor contigo mismo y con tus personas cercanas.

Otras referencias:

Generación Anáhuac. (20 de febrero de 2019). *La influencia de la tecnología en nuestra vida cotidiana*. <https://www.anahuac.mx/generacion-anahuac/la-influencia-de-la-tecnologia-en-nuestra-vida-cotidiana>

Monterrosa, A. (Mayo de 2013). *Siempre fuimos Ciborgs*. FACEA-ITM. Disponible en: <https://monterroza.blogspot.com/2013/06/siempre-fuimos-ciborgs.html>

Escobar, S. (27 de septiembre de 2020). *Viví sin redes sociales por 2 años. ¿Qué aprendí?*. [Video] https://www.youtube.com/watch?v=_62UB_yh5_k

Sesión 1.3 : El traslado de las violencias a los espacios digitales

Facilitación: Elizabeth Mosqueda (Consortio Oaxaca)

Las tecnologías han desarrollado conductas que afectan a las y los usuarios de las plataformas digitales y representan amenazas derivadas de la violencia con la que se difunde la información, especialmente perjudicando a las mujeres. Por lo tanto, es necesario reconocer las violencias que enfrentamos en el espacio virtual. Existen una serie de agresiones que trascienden nuestra condición de género, y las estructuras de desigualdad también se trasladan al ámbito digital.

En esta sección, abordamos qué es la violencia digital, sus formas más comunes y las medidas para prevenirla y erradicarla.

¿Qué es la violencia digital?

El Infoem (Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios) define la violencia digital como toda acción dolosa realizada mediante el uso de tecnologías de la información y la comunicación, por la que se exponga, distribuya, difunda, exhiba, transmita; comercialice, oferte, intercambie o comparta imágenes, audios o videos reales o simulados de contenido íntimo sexual de una persona sin su consentimiento y que le cause daño psicológico o emocional en cualquier ámbito de su vida.

Este concepto confluye con otras prácticas como el ciberacoso o cyberbullying, mismas que no están alejadas de la violencia de género que muchas mujeres sufren en la vida offline. En cualquiera de estos casos supone un ataque a la seguridad, integridad y dignidad de la víctima.

¿Qué tipos de violencias existen en el espacio digital?

Puede resultar difícil identificar cuáles son los distintos tipos de violencias que enfrentamos y cuáles son sus impactos; ya que no sabemos cómo nombrarla, o no queda claro a qué se refiere cada tipo de violencia, porque tampoco existen estadísticas claras de su ocurrencia.

Tedic es una organización que desarrolla tecnología cívica abierta y defiende los derechos digitales por una Cultura Libre en la Internet, en su sitio web describe diversas formas de violencias de género que ocurren en el uso de la tecnología digital⁵. De ellas recopilamos las siguientes:

→ **Acceso y control no autorizado de cuentas.** Ataques no autorizados para ganar acceso a las cuentas o dispositivos de otras personas. Esto puede implicar la

⁵ Tedic. Tipos de violencia de género digital. Disponible en línea en: <https://violenciadigital.tedic.org/es/b/guia/tipos-de-violencia-de-genero-digital/>

recopilación no autorizada de información como el bloqueo o desactivación de la cuenta de la víctima, así como la utilización de la cuenta hackeada para ejercer comportamientos que generen desprestigio o desacreditación de la persona titular de la cuenta.

- **Acoso.** Actos repetidos y no solicitados contra una persona u organización que son percibidos como intrusivos o amenazadores.
- **Control y manipulación de la información.** La recopilación o robo de información puede implicar una pérdida de información, así como su modificación sin autorización.
- **Vigilancia.** Es el monitoreo constante de las actividades en línea de la persona, su vida diaria, o información, sea pública o privada.
- **Difusión de fotos íntimas o información privada.** Compartir de manera no autorizada cualquier tipo de información, datos o detalles privados relacionados a una persona.
- **Sextorsión o extorsión sexual.** Forma de explotación sexual, en la cual una persona es inducida o chantajeada, generalmente por aplicaciones de mensajería por la Internet, con una imagen o video de sí misma con contenido íntimo o realizando actos sexuales, mediante sexting.
- **Distorsión de imágenes o videos, u otro contenido falso.** Elaboración de contenido falso, manipulado o fuera de contexto y su divulgación con el fin de desprestigiar y dañar a una persona o grupo.
- **Robo de identidad/creación de perfiles falsos.** El uso de la identidad de alguien sin su consentimiento, o la creación y divulgación de datos personales falsos, con la intención de dañar la reputación de una persona u organización.
- **Ciberacoso.** El ciberacoso o cyberbullying se da cuando una persona es víctima de algún tipo de violencia por parte de un individuo o grupo. Estas agresiones pueden tomar distinta forma, pero todas tienen en común que, además de condicionar la forma de actuar de una víctima, pueden provocar daños que afectan la salud mental o física.
- **Discurso de odio.** Discurso que refleja modelos culturales que incitan violencia, ya sea a través de comentarios, insultos, o agresiones verbales.
- **Amenazas.** Discurso y contenido (verbal o escrito, en imágenes, etc.) con un tono agresivo y/o amenazador. Amenazas directas de violencia de cualquier índole.

- **Extorsión.** Forzar a una persona a actuar de acuerdo a la voluntad de otra, a través de amenazas e intimidación.
- **Mobbing.** Consiste en el acoso laboral ejercido tanto a una persona como a un grupo. Esta conducta se da tanto fuera como dentro de los espacios digitales.
- **Filtración de información o Doxing.** Investigar y difundir información que permita identificar a una persona sin su consentimiento, muchas veces con la intención de tener acceso o contacto con fines de acoso u otros fines nocivos.
- **Ataques coordinados.** Son aquellos que se realizan de manera coordinada y por más de una persona hacia otra, una publicación específica o una página en las redes. La finalidad puede ser variada: difusión de datos personales para causar hostigamiento y acoso, o incluso lograr la eliminación de los perfiles de las víctimas, crear identidades falsas para así poder difundir publicaciones y noticias falsas.
- **Grooming.** Es la práctica en la que un adulto contacta a un/una menor de edad por la Internet, para ganar su confianza y amistad con la verdadera intención de abusar sexualmente de la víctima. El abuso puede ser al establecer una conversación de índole sexual, pedirle que envíe fotos, videos o realizar prácticas sexuales. Estas comunicaciones comienzan a través de redes sociales o de cualquier medio digital que permita la interacción entre dos o más personas.

Otras forma de violencia digital es el **bombing**, que se da cuando el ciberagresor ocupa un programa sistematizado para colapsar un correo electrónico mediante el *phishing* (delito de engañar a personas para que compartan información confidencial); y el **ciberdating**, que es un cortejo violento para ejercer control sobre la pareja.

Para identificar la violencia digital es necesario nombrarla y conocer las distintas formas de agresiones y ataques que podemos sufrir o reproducir, ya que nuestras prácticas en los espacios digitales no siempre surgen ahí sino en otros espacios o medios, con o sin uso de las tecnologías.

Es importante tener en cuenta que lo que sucede en el espacio virtual no se queda ahí, ya que muchas veces se combina con otro tipo de violencias sociales, físicas, económicas y de género.

¿Cómo actuar ante las distintas formas de Violencia digital?

- No difundir material, imágenes o publicidad de terceras personas sin su consentimiento.

- Cortando la cadena. Si alguien envía material que daña, vulnera o viola la intimidad de otra persona, no reenviarlo ni compartir el contenido.
- No hacer ni publicar en la Internet lo que no se haría ni diría en el mundo físico. Si algo incomoda, decir NO.
- Denunciar las publicaciones agresivas o que violen la intimidad de las personas usuarias de redes sociales para que los administradores de estas plataformas puedan revisarlas y en el mejor caso, estas sean eliminadas de la Internet.
- La violencia digital se puede denunciar ante la justicia. Si tu o alguien cercano a ti es víctima de grooming, acoso, robo de identidad, difusión no consentida de imágenes y otras formas de violencia, denuncia ante las autoridades competentes.
- Cuidar que las aplicaciones que instalamos en la computadora no tengan acceso a toda nuestra información personal.
- Verificar la información que se comparte antes de dar “clic” cuando se accede al espacio digital.
- Denunciar ante la autoridad competente el acoso de empresas que marcan a nuestras líneas telefónicas, puede ser *arrobandoles* (@) en Twitter o en casos severos actuar legalmente.
- Evaluar lo que se desea compartir en los espacios digitales.
- Tomar capturas de pantalla ante situaciones específicas de acoso, ya que en algún momento servirán de evidencia para respaldar la denuncia.
- Dimensionar cuánto tiempo pasamos inmovilizad@s frente a la computadora.
- Para prevenir impactos físicos es importante tomar descansos cada hora, mover el cuerpo y realizar técnicas de respiración, además otorga beneficios de concentración.
- Antes de realizar o compartir una publicación en redes sociales, es necesario reflexionar lo siguiente: ¿Está confirmada la información?, ¿Puede agredir a alguien?, ¿Es información útil?, ¿Involucra a otras personas? y sí involucra a otros, ¿Tienes permiso para compartirla?

Es importante crear redes de apoyo y saber qué organizaciones trabajan el tema. Así como quienes pueden cobijar a l@s que sufren este tipo de violencias, brindando asesoramiento y orientación.

Por último, reflexionar en colectivo por qué ayudaría a salirse de ciertos grupos o chats que comparten información que viola la privacidad de otras personas. Y de este modo poder encontrar formas de prevención y erradicación de la violencia en los espacios digitales.

¿Qué ciberviolencias has enfrentado y cómo las superaste?

Sabemos que muchas personas han vivido alguna situación de violencia digital. Por ello, te invitamos a que compartas con otrxs qué tipo de violencias has enfrentado, cómo te afectaron y qué hiciste para frenarlas.

- A partir de un caso compartido en colectivo, enlista los tipos de violencia digital que lograste detectar.
- Discute en colectivo qué herramientas u organizaciones pueden ser útiles para apoyar y denunciar en caso necesario. Comparte esta información a quienes puedan requerir ayuda.

Otras referencias:

Tedic.org. (2021). *¿Qué es la violencia de género digital?* <https://violenciadigital.tedic.org/>

BLOQUE 2

Activismo digital

El ciberespacio puede convertirse en un campo de batalla para desafiar un sistema capitalista que impone agendas de control y extracción de datos. En este segundo bloque, presentamos una serie de herramientas disponibles en el espacio digital que podemos utilizar para habitar una Internet más inclusiva y accesible para todas las personas. Además, destacaremos dos movimientos sociales que ejemplifican el ciberactivismo: el ciberfeminismo y el activismo digital en lenguas indígenas.

2.1 Ciberactivismo y Ciberfeminismo

Facilitación: Soledad Venegas Nava (Estudio Mantis⁶), Elizabeth Mosqueda (Consortio Oaxaca), Oliver Fröhling y Kiado Cruz (SURCO Oaxaca A. C.)

Hoy en día el activismo ha cobrado más fuerza dentro de los espacios digitales, como en las redes y plataformas. Por medio de redes, blogs, páginas web, mensajes de texto, y otros recursos, las y los activistas digitales difunden informaciones que potencian la movilización que sucede alternativamente en las calles y otros espacios.

En este contexto, las TICs (Tecnologías de la Información y las Comunicaciones) son medios que sirven para construir subjetividades políticas que constituyen otros modos de apropiación y uso alternativo de la tecnología, influyendo en los procesos de cambio y resignificación de la cultural digital, redefiniendo valores, creencias e identidades de quienes protagonizan las experiencias. Las revoluciones de las multitudes conectadas se extienden por el mundo en una nueva forma de activismo social.

¿Qué es el Ciberactivismo y por qué es importante?

Simona Levi, activista y fundadora de la plataforma por los Derechos Digitales Xnet, menciona que *el ciberactivismo es antes que nada Activismo. No es el diseño de campañas digitales. No es la suma de expresiones individuales en las redes. Es acción colectiva para generar hechos políticos, utilizando estratégicamente la tecnología⁷.*

El ciberactivismo es otro modo de informar, concientizar, denunciar y movilizar con el uso de las TICs. Permite a personas, colectivos y organizaciones utilizar las redes sociales y otras tecnologías para lanzar mensajes, reunir seguidores, emitir campañas y avanzar en una causa o movimiento social.

Hace quince años era mucho más caro y complicado hacer un video y difundirlo para denunciar un hecho. Hoy usamos la cámara del teléfono móvil para compartirlo en la red de forma inmediata. El activismo en la calle y en el espacio digital coexisten, pues no se necesitan grandes recursos para llevarse a cabo.

El ciberactivismo facilita la relación entre personas y comunidades no sólo a nivel local, sino global. A través de las diversas plataformas y herramientas digitales las personas dejan de ser sujetos receptores y se convierten en protagonistas que intercambian opiniones y experiencias para hacer efectiva una denuncia social.

⁶ Estudio Mantis es un espacio que brinda apoyo, asesoría, talleres, cursos y soluciones basadas en las Tecnologías de la Información y las Comunicaciones a diferentes sectores de la sociedad, al lado de un equipo de mujeres profesionales y programadoras.

⁷ Fossatti, Mariana (2017). *Ciberactivismo feminista*. Disponible en la biblioteca digital del 1º Encuentro de Feministas Desorganizadas. Encuentro de Feministas Desorganizadas. <https://biblioteca.efd.uy/document/121>

El uso de las TICs en suma con el activismo constituyen una herramienta para incidir en políticas públicas. Sin embargo es necesario contar con un objetivo estratégico para lograr los resultados deseados, considerando que el activismo digital funciona en conjunto con todo el repertorio de activismos y refleja sus efectos en otros espacios de la realidad. Así, se sintetiza que el ciberactivismo no reemplaza una protesta, más bien antecede un conjunto de procesos que culminan en una eventual manifestación (Casanueva, 2011)⁸.

Los movimientos *Democracia Real Ya* (España), *Occupy Wall Street* (EUA), *Yo Soy 132* (México) y la *Primavera Árabe*, que en 2011 comenzó en Túnez y se extendió a diversos países del Oriente Medio y norte de África, son algunos ejemplos de ciberactivismo que en años recientes han desafiado las políticas y decisiones autoritarias de los gobiernos involucrados.

¿Qué es el Ciberfeminismo? ¿Cuáles son las ventajas de la tecnología para la lucha feminista?

El ciberfeminismo es un movimiento dentro del espacio digital que hace visibles las asimetrías de la participación de las mujeres en los espacios digitales. Simona Levi, explica que la Internet es una herramienta y al mismo tiempo un campo de batalla que constituye una herramienta para la lucha, entretenimiento, fuente de información y comunicación. Es además un bien común y por lo tanto está sujeto a la disputa de poder y la apropiación pública, colectiva y común de la red⁹. Ambas dimensiones están presentes de manera permanente. De ahí que es indispensable generar medios y redes de comunicación que no sean controlados solamente por el Estado o empresas privadas.

Disponer de redes descentralizadas y más libres ofrece la posibilidad de configurar contenidos propios, sin que se imponga una agenda mediada. Permite una forma rápida para la organización y el trabajo colectivo, articular datos, intereses, lenguajes comunes, formar nodos de comunicación más horizontales que logran alcanzar más personas.

La performance “Un violador en tu camino”, que empezó como un acto callejero en Chile, en tan solo unos días se multiplicó alrededor del mundo. Estas formas de organización son ejemplo del ciberfeminismo y tiene una potencia masiva y rápida, sin embargo es importante no olvidarse de los procesos colectivos que hay detrás de ello.

⁸ Casanueva, Juan Manuel. (2011) “¿Cuáles son los alcances del activismo digital? #CPMX3”. Periódico Independiente Digital Animal Político, 19 de Julio.

⁹ SURCO Oaxaca A.C. (01 de julio de 2021). Ciberactivismo con Mariana Fossatti. [Video]. YouTube. <https://www.youtube.com/watch?v=rgGKYpCyNYo>

El movimiento feminista ha creado múltiples estrategias colectivas para resistir dentro de la Internet, las cuáles según Fossatti tienen principalmente dos dimensiones:

- La dimensión ética: Surge al compartir archivos y conocimiento de manera más libre, se reivindica el compartir la cultura que se produce y con ello se hace cultura colaborativa.
- La dimensión política: Es la acción ciudadana en red, la disminución de las mediaciones en las posibilidades democráticas que aún están en disputa.

Una de las preocupaciones del ciberfeminismo es la sociedad de control, de ahí que se busque autonomía de conocimiento e información entre pares, para deliberar, decidir y construir niveles de formación autónoma para ocupar los espacios digitales y deconstruirlos (Fossatti, 2021).

¿Cuándo surge el Ciberfeminismo y cuáles son sus potencialidades?

El término ciberfeminismo se recupera dentro de la tercera ola del feminismo, en la que las mujeres hacen un análisis crítico de lo que estaban viviendo dentro de los entornos tecnológicos y se cuestionan el significado de ser mujer en estos espacios y cómo es la participación dentro de ellos.

Hoy usamos las tecnologías para comunicar, analizar, categorizar y hacer una inmersión profunda de lo que estamos viviendo y los movimientos feministas no son la excepción. Dentro y fuera de los espacios digitales es posible analizar cómo está construida la red, cómo impacta en las identidades de las mujeres que habitan el ciberespacio y es posible tejer red con otras luchas a partir de estas interconexiones, para construir y deconstruir - desde el hardware hasta el software -, protocolos de comunicación, cuestionar las asimetrías que estamos reproduciendo y analizar cómo se usan las TICs en favor de los movimientos que hoy trascienden la lucha en las calles y otros espacios físicos.

En este encuentro de realidades, las ciberfeministas han llevado el debate más allá del uso de los dispositivos y la red y han dejado de ser consumidoras para convertirse en prosumidoras¹⁰. Llegando a posicionar temas como el acceso a la Internet igualitaria entre hombres y mujeres, la brecha de género digital, las violencias que se reproducen en estos espacios y los riesgos e impactos que esto tiene en sus vidas y relaciones cotidianas.

¹⁰ Prosumidora es aquella persona que desarrolla una doble acción de cara a las nuevas tecnologías de la información y la comunicación. Estas acciones son la del productor y la del consumidor de contenidos. Esto quiere decir que desarrolla prácticas asociadas a la web 2.0, en la cual puede producir contenidos digitales (imágenes, vídeos, música, etc.). *El prosumidor. Pildoras educativas*. Revista Comunicar. Disponible en: <https://www.revistacomunicar.com/wp/revista-comunicar/tag/cultura-prosumidora/>

El ciberfeminismo ha propiciado que cada día más mujeres se sumen a este otro modo de activismo global, ampliando sus capacidades y habilidades para erradicar la violencia de género en todos los ámbitos de su vida. Ejemplo de ello son las campañas de denuncia y exigencia de justicia en Twitter como #Justicia para Sol, #niunamas, #LeyOlimpia, @MareaVerdeMex, #LeyIngrid, #MeToo y #altoalfemicidio, entre muchos otros.

¿Lo virtual es realidad? Ley Olimpia

“Lo virtual es real” es una frase que describe la potencialidad de la Ley Olimpia, aprobada en 2021 en todo México. Olimpia Coral Melo es una mujer de Huauchinango, Puebla que, tras haber sido víctima de la difusión viral sin su consentimiento, de un video suyo con contenido íntimo sexual, conoció el rechazo colectivo, el juicio, el estigma social y la inimaginable violencia comunitaria, social, estructural e institucional que pesa sobre las mujeres por el simple hecho de tener cuerpo de mujer, de ejercer su sexualidad y no encajar en los apretados moldes de “buena mujer” que impone un sistema patriarcal. Para fortuna de todas las mujeres en el país, tras un duro proceso de gran resiliencia, ella decidió no callar lo que le había pasado y buscar justicia. Lo intentó mediante las instituciones al acudir a un Ministerio Público en donde vivió una terrible revictimización, además de que se le dijo que lo que a ella le había sucedido no era un delito¹¹.

Es el primer proyecto de reformas en México en materia de violencia digital desde la realidad de las víctimas y con perspectiva de género. La Ley Olimpia implica dos cambios legislativos: el primero es el reconocimiento de esta modalidad de violencia dentro la Ley de Acceso de las Mujeres a una vida libre de violencia y el segundo, la tipificación del delito contra la intimidación sexual en los Códigos Penales de todo el país.

La Ley Olimpia sanciona la violencia digital contra las mujeres en sus diferentes formas, tales como el acoso, hostigamiento, amenazas, insultos y vulneración de información privada, además de la difusión de contenido sexual sin consentimiento, textos, fotos, videos o datos personales a través de la Internet, redes sociales, correo, apps, o cualquier entorno digital.

A partir de esta experiencia se integró el *Frente Nacional de la Sororidad* que constituye un movimiento de denuncia y visibilización de la violencia que viven las mujeres en entornos virtuales y digitales.

Esta iniciativa, construida a partir de la historia de Olimpia Coral y con el apoyo de muchas otras mujeres que han vivido esta experiencia, demuestra la importancia de reconocer la violencia sexual y el ciberacoso en el uso de las tecnologías digitales,

¹¹ Secretaría de las Mujeres - Ciudad de México. Manual de contenidos Laboratorio de Análisis Multidisciplinario sobre la Ley Olimpia. Disponible en: <https://semujeres.cdmx.gob.mx/violencia-digital>

particularmente desde las mujeres y poniendo en alto la demanda de justicia para exigir a las autoridades que se proceda en contra de quien la ejerce.

¿Por qué es importante legislar en materia de violencia digital en México?

Antes de que se aprobara la Ley Olimpia, en México no existía otro mecanismo de investigación y castigo para las violencias sexuales a través de los espacios digitales, donde las mujeres son exhibidas en la Internet sin que las autoridades tuvieran competencia para investigar y castigar el delito.

La importancia de la Ley Olimpia radica en que a través de ella se colocó un tema antes invisible en la agenda pública y lo ha llevado hasta algunas agendas de gobierno: la violencia digital contra la intimidación sexual de las mujeres no es nueva en los hechos, las vidas de muchas mujeres la han conocido desde que se masificaron los espacios digitales, sin embargo, no había sido una problemática visible. Actualmente el delito contra la intimidación sexual establecido en el Código Penal se castiga hasta con 6 años de cárcel a quien comparta 'packs' sin consentimiento.

En Oaxaca esta ley se aprobó con la reforma al artículo 249 y 250 del Código Penal vigente donde se tipifican delitos contra la intimidación sexual. Esta conducta se sancionará de cuatro a ocho años de prisión y multa de mil a dos mil veces el valor diario de la unidad de medida y actualización vigente al momento de que se cometa el delito.

De acuerdo con las reformas estipuladas en el Código Penal, el Artículo 249 establece que comete el delito de violación a la intimidación sexual quien por cualquier medio divulgue, comparta, distribuya, publique o solicite imágenes, audios o videos de una persona, de contenido íntimo erótico o sexual, ya sea impreso, grabado o digital sin el consentimiento de la víctima.

La Ley Olimpia da ejemplo de cómo el ciberactivismo que sucede en redes se trasladó a las calles, articulándose con la lucha organizada de otras colectivas feministas que desde hace mucho tiempo vienen haciendo una labor de denuncia en contra de la violencia de género en contextos digitales.

Además de velar por la búsqueda de justicia para las mujeres en un espacio digital seguro, la Ley Olimpia ha generado que esta información se difunda a través de conferencias, charlas y conservatorios en universidades e instituciones públicas; lo que implica que cada vez más espacios la reconocen como una modalidad de violencia con base en género y en consecuencia asumen el compromiso de emplear recursos y trabajo en favor de su prevención y combate.

¿Cómo nos cuidamos de la ciberviolencia?

- Usando y apropiando las tecnologías de la forma en que queremos y no desde el sentido que se impone de forma hegemónica patriarcal.
- Promoviendo y practicando el uso de software que permita la formación y acceso a la cultura libre y abierta para todas las mujeres.
- Construyendo espacios de militancia seguros y autónomos en los que podamos ser libres de censura y de violencia digital.
- Creando una Internet feminista y hackeando al patriarcado. Organizándonos ante la vigilancia, privacidad, acoso y violencia en línea. Estos también son temas en disputa y de batalla feminista.

¿Qué tipos de activismo digital hacemos y qué herramientas usamos?

- Te invitamos a reconocer qué herramientas, espacios, recursos y/o estrategias utilizas para realizar activismo en tu transitar cotidiano de los espacios digitales.
- Comparte tu reflexión en colectivo, definan cuáles podrían ser otras formas para potenciar el uso de las tecnologías para generar una forma de comunicación y acceso a la información más libre y autónoma, que permita el uso y apropiación de la Internet de acuerdo a lo que necesitan o desean para el bien común.

Otras referencias:

Grupo Reforma (25 de diciembre de 2020). *La Ley O limpia. ¿Qué es y cómo funciona?*. [Video]. YouTube. <https://www.youtube.com/watch?v=1ee5eEiL0qw>

SURCO Oaxaca AC (01 de julio de 2021). Ciberactivismo con Mariana Fossati. [Audio]. YouTube. <https://www.youtube.com/watch?v=rgGKYpCyNYo>

Plataforma Xnet. Internet, Derechos y Democracia en la era Digital <https://xnet-x.net/es/quienes-somos/>

2.2 Activismo digital en Lenguas Indígenas

Facilitación: Tajëëw Díaz Robles (Colmix-Colectivo Mixe), Rodrigo Pérez (Zapoteco 3.0) y Eddie Avila (Rising Voices¹²)

El activismo digital en lenguas indígenas constituye un modo de promover redes de activistas y defensores digitales impulsores de la enseñanza y el aprendizaje de lenguas indígenas, así como para el intercambio de mejores prácticas relacionadas con el uso de la tecnología.

En este apartado conoceremos cómo el activismo digital puede ser instrumento de cambio para combatir la violencia simbólica contra las lenguas indígenas, mostrando las grandes ventajas y posibilidades que ofrecen las TICs para que las personas ejerzan su derecho a hablarlas y difundirlas en cualquier medio, red social y espacios digitales.

¿Qué es el activismo digital en lenguas indígenas?

El concepto del activismo digital ha sido reconocido como parte de una campaña estratégica para preservar y difundir las lenguas indígenas. La Internet y los medios digitales son herramientas para hacer más visible una lengua, generar interés en las personas jóvenes o promover que las nuevas generaciones compartan de manera creativa y didáctica contenidos en sus propias lenguas.

Cada vez son más las comunidades indígenas que promueven el uso de su lengua en campañas, foros y espacios diversos. Buscan que sus voces sean escuchadas y amplificadas y mediante la creación de diversos recursos digitales, comparten las necesidades y desafíos que implican el ejercicio de ese derecho. Estos grupos y comunidades se identifican como parte de un activismo que enfoca sus esfuerzos en el diseño y utilización de herramientas digitales para crear contenidos propios. Reconocerse en el camino del uso de las lenguas indígenas en la Internet y en plataformas digitales constituye para este movimiento, una apuesta política amplia.

Los sistemas económicos capitalistas dificultan el acceso a comunidades hablantes hacia el uso de herramientas digitales. De ahí la apuesta política de l@s activistas en lenguas indígenas para que todas las lenguas tengan su propio espacio en las plataformas digitales, ya que si se considera que todas las lenguas son iguales y útiles, todas las lenguas podrían ocupar y utilizarse en los espacios digitales.

Como resultado de este movimiento de activismo digital en lenguas indígenas, actualmente podemos acceder a versiones de Firefox (navegador de internet) en los

¹² Rising Voices es una iniciativa de divulgación de Global Voices, tiene como objetivo ayudar a que nuevas voces de nuevas comunidades y que hablen lenguas indígenas o en peligro de extinción participen en el debate mundial, proporcionando formación, recursos, microdonaciones y tutoría a las comunidades locales infrarrepresentadas que quieran contar su propia historia digital utilizando herramientas de medios participativos.

idiomas zapoteco, kaqchikel¹³ o ayuuk. Los esfuerzos por realizar estas versiones de Firefox se enfocan en generar una amplia oferta de programas, redes sociales y plataformas multilingües para todas las personas que hacen uso de ellas, es decir de las y los consumidores. La creación de estas versiones de Firefox ha sido resultado de un proceso colaborativo en el que equipos conformados por personas hablantes de las lenguas han trabajado por crear y mejorar la interfaz; esto a diferencia de las plataformas y redes sociales que usan software privativo, en el que los términos y condiciones de uso de estos servicios atentan contra la privacidad y, al tener dueño, no se pueden manipular.

Por ello el software libre ha sido un gran aliado para el activismo digital y para la difusión del uso de las lenguas indígenas en Internet ya que su dimensión colaborativa permite mayor libertad en la creación de contenidos en formato blog, fotografía, memes, audio o videos.

¿Cuál es la importancia del uso de lenguas indígenas en la Internet?

Uno de los mayores retos del activismo digital en lenguas indígenas es el de involucrar a más personas tomando en cuenta que la brecha digital para quienes pueden acceder al uso de internet, no favorece a la población indígena. Esta lucha trae consigo un compromiso no sólo en los espacios digitales, sino en la defensa de la dignidad, la vida y los territorios.

Otro reto es el de desmontar el uso folclórico que se le ha dado a las lenguas originarias en la literatura y otras expresiones artísticas y culturales. Son las personas hablantes de estas lenguas las que tienen el derecho a decidir cómo y en qué espacios utilizar su lengua. Es por eso que formar nuevas generaciones de activistas en lenguas indígenas, para la promoción y fortalecimiento de estos cambios, resulta necesario.

¿Qué herramientas digitales existen para la enseñanza de la lengua indígena?

En Oaxaca se organiza la Semana de Vida y Lengua Mixes (SEVILEM), la cual ya es una tradición entre las diferentes comunidades ayuuk ja'ay en donde se discute, promueve y fortalece la lecto-escritura de la lengua y la cultura ayuuk. Si bien en este encuentro han participado principalmente personas habitantes de la región y hablantes de la lengua ayuuk, en los últimos años, se han integrado personas que provienen de otras culturas y lenguas, que quieren conocer, compartir y aportar con trabajo y pensamiento a la misión de la SEVILEM.

¹³ El idioma kaqchikel o kakchikel es una lengua mayense de la rama quicheana hablada por la población kaqchikel en el sur del estado de Chiapas, México y en la región centro occidental de Guatemala.

El COLMIX, Colectivo de personas mixes, Ticha-Explorador digital de zapoteco del Valle y Tlahuitoltepec.com son algunos colectivos que promueven espacios digitales para fortalecer el uso y conocimiento de las lenguas indígenas en la Internet.

La realización de seminarios en plataformas digitales, talleres de didáctica para enseñar y compartir métodos para la lectoescritura, cursos para aprender vocabulario básico y cotidiano, así como herramientas de investigación para conocer los nombres de los pueblos y consultar textos antiguos, constituyen espacios virtuales de uso y fortalecimiento de las lenguas indígenas de Oaxaca.

¿Es posible alcanzar la justicia lingüística en México?

La invisibilización de las lenguas indígenas es un problema sistémico. La justicia lingüística se está construyendo con todos los activismos, desde diversas organizaciones y colectivos, incluso desde instituciones como el sector salud. La justicia para pueblos indígenas no existe aún en un país como México, un claro ejemplo es el despojo del territorio que atenta contra el derecho a la tierra y la vida. Para que las lenguas no mueran existe una lucha de supervivencia, pues el Estado y el sistema capitalista las invisibiliza todo el tiempo, porque no implican producción, ganancias o grandes ventajas.

A la par de exigir y luchar por la justicia lingüística es importante que padres, madres, familiares y personas hablantes, hablen su lengua sin miedo a la discriminación. Que de forma amorosa y natural les hablen a sus hijos e hijas en su lengua, y con ello la validen tanto como a otras. Habrá que enseñar a leer y escribir en forma monolingüe, desde los primeros años de vida, como una decisión personal que de alguna forma representa un activismo que debemos comenzar desde edades tempranas, esto permitirá que niñas y niños vayan configurando estas interacciones.

Además, se requiere de contenidos que permitan el uso cotidiano de las lenguas en todo momento. Los espacios de reflexión en donde esto se cuestione abonará al logro de la justicia lingüística y social. Al final se trata de un trabajo intergeneracional que deberá tomar en cuenta que ninguna tecnología es neutral: los sesgos de género, raza y lengua la habitan.

Es importante articular con otras personas y discutir lo que se necesita para aprovechar mejor los esfuerzos y recursos digitales en la creación de materiales. Empezar a alfabetizar desde edades tempranas en lengua materna, además de tener acceso a materiales y recursos como sucede con otros idiomas en la red. Sin embargo, este proceso es más amplio, no puede solo responder al uso y apropiación de herramientas digitales.

El primer obstáculo es la discriminación, que impide que las hijas o hijos que desean aprender su lengua no la hereden por la violencia que han vivido generaciones

anteriores. En México parece existir una política que discrimina el uso de las lenguas indígenas. Recibir educación bilingüe real e intercultural y generar espacios institucionales, es un camino para lograr un cambio. Lo anterior son aspectos fundamentales para alcanzar la justicia lingüística en donde las políticas públicas tienen un papel fundamental.

¿Cómo cuidamos que las lenguas indígenas pervivan?

- Hablemos a los bebés en su lengua cuando nos sea posible. Enseñar la práctica de la diversidad desde la niñez es un hecho fundamental.
- Busquemos materiales digitales o herramientas didácticas para posicionar el uso de las lenguas indígenas como un Derecho Humano, como una práctica de comunicación intercultural.
- Dentro de las comunidades indígenas, es importante que los padres hablen con sus hijos e hijas en sus lenguas nativas. Esto contribuirá a que la lengua se mantenga y a su vez, que sea heredada de generación en generación.

¿Qué tipos de activismo digital hacemos y qué herramientas usamos?

- Te sugerimos leer el texto “Origen, evolución y estado actual del activismo digital y su compromiso social. Ciberactivismo, hacktivismo y slacktivismo” para reconocer qué tipo de activista digital eres y con qué herramientas cuentas para ello.

Otras referencias:

Globalvoices.org. (2021). *Apropiarse de las Redes para Fortalecer la Palabra. (Una introducción al Activismo Digital de Lenguas Indígenas en América Latina)*. Activismo Lenguas. <https://rising.globalvoices.org/lenguas/>

CEAS (16 de febrero de 2017). *Indígenas virtuales. El activismo digital como nuevo campo de estudio*. Universidad Autónoma de San Luis Potosí. Disponible en: https://aulavirtual.ceuxhidza.org/pluginfile.php/773/mod_resource/content/1/Indigenasvirtuales.ElactivismodigitalcomonuevocampodeestudioAnthroDayColegiodeEtnologosyAntropologosSocialesA.C.CEAS.pdf

García, N. (Octubre 2017). *Origen, evolución y estado actual del activismo digital y su compromiso social. Ciberactivismo, hacktivismo y slacktivismo*. Actas del II Congreso Internacional Move.net sobre Movimientos Sociales y TIC, 25-27 de octubre 2017 – Universidad de Sevilla, COMPOLITICAS. https://aulavirtual.ceuxhidza.org/pluginfile.php/774/mod_resource/content/2/157763846.pdf

COLMIX. (15 de octubre de 2021). *Más de 20 libros en lengua mixe*. <https://colmix.org/?p=193>

2.3 Humanidades digitales

Facilitación: Alejandra Méndez (CEU-XHIDZA¹⁴)

Los conceptos de tecnología y humanidades son clave para configurar un nuevo campo de conocimiento que denominamos humanidades digitales, un espacio que engloba un conjunto de prácticas en el ámbito de la investigación, docencia y transferencia del conocimiento que surgen de la incorporación de las tecnologías digitales en esta área.

¿Cómo entender las humanidades digitales?

Las humanidades digitales son un conjunto de prácticas que, dependiendo de la región donde se lleven a cabo, constituyen una forma de aproximación y/o apropiación humanista del entorno digital. Es la aplicación de las tecnologías con información ya existente, para dar a conocer, analizar y difundir información que sea de interés y acceso más libre para todas las personas interesadas en ello.

Desde el Norte Global, las humanidades digitales (archivos, imágenes, videos, textos literarios, etc.) se definen como un conjunto de tecnologías para procesar computacionalmente las fuentes de información.

Desde el Sur Global, principalmente desde los espacios universitarios públicos, son una o varias formas de problematizar el espacio digital como nuevo territorio en disputa, desde una postura política, donde no sólo es importante el procesamiento de la información en las tecnologías digitales, sino la búsqueda de otras narrativas poniendo a disposición recursos y archivos, ante la necesidad de compartir y disponer de toda aquella información y/o experiencia que aún no está accesible en la red.

Es importante señalar que los espacios digitales también excluyen información que debería estar en la Internet, por ejemplo, las formas de vivir, costumbres e ideas que no encajan en estos espacios digitales.

Por ello, las humanidades digitales implican el uso de la red como herramienta, es decir la relación e interacción del ser humano con los diferentes ámbitos de su vida dentro del contexto digital.

¹⁴ CEU-XHIDZA trabaja de manera conjunta con la comunidad, a través de prácticas, intercambio de conocimientos y vivencias; para ello se formulan proyectos que son asesorados por facilitadorxs expertxs en su campo de estudio. Con ello esperamos que surjan sujetos conscientes de la realidad de su entorno y comprometidos con el beneficio y el bienestar de las comunidades.

¿Qué distingue a las humanidades digitales?

Esta idea viene del software libre, que se fundamenta de la postura filosófica de que los conocimientos son abiertos y libres. Todos los datos en la red se usan para interpretación y análisis, pero desde las humanidades digitales, el uso de este corpus es de otro modo.

Las humanidades digitales promueven la creación de otras narrativas y prácticas que permitan dar acceso a otro tipo de información, buscan digitalizar la información que se ha ido generando.

En los proyectos de humanidades digitales, a diferencia de lo que sucede con la lectura de un libro o un artículo, ya no recibimos pasivamente el conocimiento de un especialista sino que lo asumimos, a la vez, en un rol activo; estos tienen el objetivo de realizar y, en algunos casos, guiar la transformación digital de los saberes humanístico-sociales. Son un fenómeno que está cambiando la economía, la política, la educación de manera particular, las formas de acceso y producción de los saberes y las memorias culturales.

¿Qué ejemplos de humanidades digitales encontramos en la Internet?

El proyecto oaxaqueño *Ticha* es un explorador digital de texto en zapoteco colonial que permite acceder y explorar múltiples niveles relacionados de textos de un corpus de Zapoteco colonial del Valle, manuscritos y libros impresos, incluyendo imágenes de los documentos originales, transcripciones, traducciones y análisis lingüísticos, como el análisis interlinear morfológico (<https://ticha.haverford.edu/es/>).

La *Red de Humanidades Digitales* es otro proyecto que ha encontrado formas de difusión en este sentido, es una iniciativa de académicos y académicas que impulsan la formalización de las humanidades digitales realizando foros, encuentros, espacios de discusión, análisis y reflexión con el objetivo de promover y fortalecer la comunicación entre los humanistas digitales, la formación de recursos humanos, la elaboración de documentación y buenas prácticas, la promoción de los proyectos de humanidades digitales, la difusión de eventos, así como el impulso, la discusión y el reconocimiento del campo. Adicionalmente promueve iniciativas regionales a nivel internacional (<http://humanidadesdigitales.net/>).

The Programming Historian en español publica tutoriales revisados por pares dirigidos a humanistas que quieran aprender una amplia gama de herramientas digitales, técnicas computacionales y flujos de trabajo útiles para investigar y enseñar. Están comprometidos en la promoción de una comunidad diversa de editores, autores y lectores (<https://programminghistorian.org/es/>).

Storymap

Puedes usar StoryMap Js, una aplicación que te permite crear historias haciendo énfasis en localizaciones en un mapa. Accede a través de la siguiente liga <https://storymap.knightlab.com/> para crear una historia en torno a un tema de tu interés.

Otras referencias:

Fiormonte D. y Sordi, P. (Mayo de 2019). *Humanidades Digitales del Sur y GAFAM. Para una geopolítica del conocimiento digital*. Liinc em Revista, Rio de Janeiro, Vol.15, No.1, págs. 108-130, mayo 2019.

[Http://revista.ibict.br/liinc/article/view/4730/4137](http://revista.ibict.br/liinc/article/view/4730/4137)

Cátedra UNESCO-AMIDI. (29 de abril de 2021). *¿Qué son las humanidades digitales?*. [Video]. YouTube.

[Https://www.youtube.com/watch?v=DMxD-VLLovg](https://www.youtube.com/watch?v=DMxD-VLLovg)

BLOQUE 3

Derechos digitales

En la era de la tecnología, los derechos digitales son fundamentales. Al avanzar la tecnología, también evolucionan los derechos humanos que corresponden en el ámbito digital. Es crucial proteger estos derechos en todos los espacios, incluyendo los espacios cívicos en línea.

En este tercer bloque se abordarán los derechos digitales, como el acceso a la información digital desde nuestra diversidad cultural. Además, se busca garantizar la protección de nuestros datos personales contra el abuso y la divulgación sin consentimiento. La protección de nuestros derechos digitales nos permite ejercer nuestra humanidad digital de manera segura y consciente.

3.1 ¿Qué son los derechos digitales?

Facilitación: Martha Tudón (Article 19¹⁵)

Los derechos digitales son de cuarta generación, y han surgido como demanda de protección y seguridad de grandes sectores de la población que exigen condiciones más seguras en el uso y apropiación de las Tecnologías de la Información y las Comunicaciones. A continuación enunciamos algunos de estos derechos, de acuerdo a lo que nos comparte Martha Tudón:

- **Acceso universal a Internet.** Ejercer este derecho aún es un privilegio. Una persona que tiene acceso a internet tiene una ventaja comparativa frente a otras que no tienen las mismas oportunidades, esto cruza con otros factores como la edad, el género, clases sociales, entre otros. Hacer uso de este derecho significa tener acceso a contenidos, capacitación digital, información contextualizada, etc. Este derecho posibilita el ejercicio de otros derechos. Si no tienes Internet no tienes acceso a los derechos digitales.
- **Derechos económicos, sociales, culturales, ambientales y de salud.** Los diversos contextos sociales demuestran que quiénes ejercen el derecho al acceso, uso y conexión de la Internet son los mismos que disfrutan del derecho al entretenimiento, educación y a la información de calidad, veraz y oportuna.
- **Libertad de expresión.** Es el derecho que tenemos todas, todos y todes de poder expresar, difundir, buscar, recibir y compartir toda clase de contenidos e ideas de manera libre y sin miedo a injerencias de cualquier tipo.
- **Derecho a la información.** Este derecho permite a todas las personas acceder, buscar, recibir y solicitar información de interés; de esta forma contrastar con la realidad.
- **Privacidad y protección de datos personales.** Se refiere al derecho que tiene toda persona a no ser invadido en su privacidad. Así mismo, las instituciones gubernamentales y privadas están obligadas a no recabar nuestros datos personales para venderlos y utilizarlos con fines contrarios a este derecho.
- **Cifrado y anonimato.** Son derechos que nos permiten ejercer con mayor libertad otros derechos como la libertad de expresión y el derecho al acceso a la información.

¹⁵ Article 19 México y Centroamérica es una organización independiente y apartidista que promueve y defiende el avance progresivo de los derechos de libertad de expresión y acceso a la información de todas las personas, de acuerdo a los más altos estándares internacionales de derechos humanos, contribuyendo así al fortalecimiento de la democracia.

→ **Derecho de reunión y asociación.** Está relacionado con el derecho a la protesta, que consiste en que toda persona puede reunirse de manera pacífica, crear o integrarse a organizaciones para abordar temas de interés.

¿Cuáles son las amenazas a estos Derechos?

→ **Moderación de contenidos.** Son los términos y condiciones que tienen las plataformas digitales, los cuales no siempre están apegados a los derechos humanos. Esto impacta directamente a defensores, activistas y comunicadores indígenas porque los algoritmos y las reglas de las plataformas son creados en contextos ajenos a la diversidad de cosmovisiones de los usuarios de estos espacios.

→ **Leyes restrictivas.** Son aquellas que obstruyen el ejercicio de los derechos humanos en la Internet, debido a que limitan la publicación de contenidos en las plataformas digitales. Los sujetos o entidades principalmente beneficiados por estas leyes son quienes ejercen actos de corrupción y violación de derechos humanos.

→ **Brecha digital.** Tiene que ver con tres factores, el primero de ellos refiere a la existencia de infraestructura, el segundo, consiste en el uso óptimo del internet y las plataformas digitales, el cual está vinculado con la alfabetización digital; por último, el tercero está relacionado con la posibilidad de sufragar el costo del servicio de internet y de un dispositivo con el cual acceder.

En México solo el 70% de las personas tienen acceso a la Internet, que al observar desde una perspectiva interseccional (como su origen, clase social, identidad de pertenencia, género, etc) podemos visualizar cómo la brecha digital es una constante en los distintos grupos históricamente vulnerabilizados, quienes se ven en desventaja respecto al uso y acceso a una información de calidad.

→ **Malware.** Es otro tipo de amenaza a los derechos digitales, el cual consiste en la intromisión a los dispositivos celulares. Estos programas maliciosos pretenden tener acceso y control a toda la información existente en el equipo infiltrado. Esta amenaza limita el uso pleno de la tecnología a la que tenemos acceso, por el temor de ser víctima de espionaje y constituye otros modos de violación a los derechos digitales, esto provoca autocensura en el ejercicio de estos derechos.

Un ejemplo de esta amenaza es el malware Pegasus, uno de los software de espionaje o spyware más potentes para dispositivos iOS y Android. Fue generado y vendido por una empresa privada al gobierno mexicano para ejercer vigilancia y espionaje a distintas personas, periodistas, activistas, políticos y defensores de derechos humanos, entre otros. Esto representa una violación a los derechos humanos digitales.

- **Capitalismo de vigilancia.** Se entiende como mercantilización de los datos personales, en esta modalidad del capitalismo su generación de valor está relacionado al rastreo de las búsquedas realizadas en las Plataformas digitales, con cada clic, movimiento del cursor y el tiempo que pasas en un sitio de Internet. Estos algoritmos crean burbujas a partir de nuestros intereses, lo que limita nuestra capacidad de ver y entender el mundo desde otros aspectos en la red.

- **Robo de datos.** Se entiende como la transferencia o extracción ilegal de datos e información personal, pública o privada. Es una amenaza muy frecuente que no se le ha dado la suficiente seriedad considerando que se vincula con otro tipo de amenazas criminales. Este tipo de delito genera un efecto de autocensura y restricción respecto a los derechos políticos y sociales, que afecta el ejercicio de los derechos humanos en el espacio físico.

¿Quién defiende nuestros derechos en la Internet?

Existen tres ámbitos o herramientas que protegen los derechos humanos desde el uso de las tecnologías y el habitar de los espacios digitales.

- 1. Estándares nacionales e internacionales.** Desde hace diez años se ha estado creando el derecho internacional y regional en América Latina que protege los derechos humanos en la Internet y los reconoce. Gozan de la misma importancia tanto en el entorno digital como en el físico.

El Sistema Interamericano de Derechos Humanos ha legislado en el tema, para que los gobiernos no espíen ni vigilen a las personas usuarias. Esta legislación en América Latina es de avanzada respecto a otras regiones del mundo, debido a la tradición de gobiernos autoritarios.

La Legislación sobre el uso de datos personales es de las más desarrolladas. El marco legal que se está creando destaca el trabajo sobre las herramientas de vigilancia y monitoreo. México no ha mostrado voluntad política para acatar recomendaciones emitidas por los relatores en el tema. Esto es una clara violación de derechos humanos, porque implica afectaciones en la labor cotidiana de las personas como es el caso de periodistas o activistas.

- 2. Gobernanza de Internet.** Es la manera en que se toman decisiones sobre los contenidos que pueden existir en la Internet. En la práctica, los grandes monopolios intervienen en el flujo de información y deciden quién puede crear o utilizar la infraestructura física de Internet. Cada año hay foros en distintos países para discutir este tema, y se cuestionan sobre las prácticas monopólicas en el sector: espectro radioeléctrico, cómo se usa la conectividad, el uso de recursos para la estructura que hace funcionar la Internet.

3. Las personas usuarias de las tecnologías. Es la capacidad que tenemos como personas usuarias de la red para capacitarnos, adquirir, crear y compartir conocimiento acerca de las formas y estrategias de cuidado dentro de los entornos digitales.

La seguridad y cuidados digitales se pueden entender como un proceso, el cual implica observar ciertas medidas al navegar por la internet; ser disciplinado en ello porque involucra cambio de hábitos. Cada persona es responsable de su seguridad digital; especialmente por su labor, lxs periodistas y defensores están más expuestos, deben cuidar de ellos mismos y de su colectivo. En este proceso es útil establecer protocolos de seguridad.

¿Cómo cuidamos nuestra seguridad y privacidad en la Internet?

Aprender a cuidar de nuestra seguridad es un proceso, debemos tener cierta higiene en el uso de la Internet y Plataformas digitales. Por ejemplo, es importante que al ingresar a Gmail o plataformas (Amazon, Mercado Libre, Linio, etc.) considerar utilizar un navegador que ofrezca mayor privacidad para reducir el riesgo de ser escuchados o rastreados.

Debemos aprender a usar y entender las herramientas digitales. A medida que se identifican nuestros derechos y vulnerabilidades en la Internet buscaremos alternativas que protejan nuestros datos personales y colectivos, esto nos permitirá generar acuerdos colectivos en el uso de las tecnologías. Es importante reconocer que no estamos completamente indefensos frente a estas amenazas, por ello, vale la pena generar acuerdos y conversaciones sobre cómo interactuar con las personas en los espacios digitales.

Otras referencias:

Riofrío J. (2014). *La cuarta ola de derechos humanos: los derechos digitales*. Revista Latinoamericana de Derechos Humanos. Vol. 25 (I), 2014.

Bordachar, M. (Mayo de 2021). *¿Quién defiende tus datos?*. Derechos Digitales América Latina: Electronic Frontier Foundation.

<https://www.eff.org/es/deeplinks/2019/10/quien-defiende-tus-datos-four-years-setting-bar-privacy-protections-latin-america>

3.2. Libertad de Expresión

Facilitación: Pedro Matías (Página 3¹⁶)

La tecnología ha tenido impacto en el modo de hacer periodismo. Actualmente se pueden difundir casi minuto a minuto temas o noticias de manera ágil e inmediata, debido a la implementación de la tecnología digital. De este modo se reducen tiempos y formas operativas en comparación con el periodismo de papel.

Tanto el periodismo tradicional como el digital deberían partir del derecho que tienen las personas a la libertad de expresión y de información, cubriendo las necesidades de comunicación y acceso a contenidos de interés. Sin embargo, el uso de la tecnología convierte a la información digital en volátil, con un sentido de inmediatez y masificación que, sobre todo en redes sociales e Internet, limita la profundización de temas, impacta en la veracidad y por tanto afecta el ejercicio pleno del derecho a la información y la comunicación.

¿Qué es la libertad de expresión?

La libertad de expresión significa que podemos comunicarnos y expresarnos de manera libre, es una garantía que se incluye en la Declaración Universal de los Derechos Humanos. De acuerdo con esta declaración, toda persona tiene derecho a expresar, difundir, buscar, recibir y compartir información e ideas sin miedo ni injerencias ilegítimas. Este derecho es primordial para formarnos como personas y nos da la posibilidad de ayudar a las comunidades a acceder a la justicia¹⁷.

Ejercer el periodismo -sea de modo tradicional o digital- en un contexto hostil como es el caso de México, implica contar con experiencia, capacitación e investigación constante, basándose de fuentes serias que permitan comprobar, comunicar, explicar e interpretar la información.

La comunicación global ha visibilizado la importancia de la libertad de expresión y los límites de la sociedad digital, para que este derecho no transgreda otras libertades, pues ya sabemos que la infraestructura de la Internet está controlada por las grandes corporaciones, esto implica un sesgo de intereses ideológicos, políticos y económicos. Además, debido a la brecha digital en México, no todas las personas tienen acceso a espacios digitales y por lo tanto a contenidos y herramientas que permitan su óptimo uso y manejo.

En palabras del periodista Pedro Matías, hacer periodismo en la era digital implica recuperar la memoria histórica, generando notas que informen lo que las audiencias necesitan en el ejercicio de su derecho a la información veraz y oportuna: “las radios

¹⁶ Página 3 es un portal de periodismo independiente que ofrece noticias de Oaxaca, sobre la defensa de los derechos humanos de las mujeres y pueblos indígenas de México.

¹⁷ Amnistía Internacional. Disponible en: <https://www.es.amnesty.org/en-que-estamos/temas/libertad-de-expresion/>

comunitarias son un claro ejemplo de esto y su labor nos demuestra la necesidad de reinventar-nos para expresar libremente el sentir y pensar de la sociedad mexicana. Sembrar conciencia a través de la crítica, la duda y la veracidad es una tarea primordial del periodista y de las y los comunicadores en el contexto actual” (Matías, 2021).

¿Cómo prevenir la censura?

Nadie debe tener miedo de expresar su sentir. Es preferible manifestarse sin temor a la descalificación. El periodismo debe acercarse más a las audiencias para que su voz sea escuchada a través de la nota periodística; además deben acudir a los distintos contextos en donde se mira la necesidad de las audiencias y lectorxs de comunicar lo que sienten, piensan y desean denunciar desde la perspectiva de su sabiduría vivencial.

¿Cómo trabajar en contextos violentos?

La labor de lxs periodistas -en espacios físicos como digitales- implica colocar su vida bajo riesgo al hacer su trabajo en un contexto como el de México; donde el periodismo suele ser mal pagado, sin las mínimas prestaciones sociales por lo que viven bajo estrés constante. Por ello es necesario tener presente las siguientes recomendaciones:

- Es fundamental documentar bien la nota periodística en temas o actores que estén directamente involucrados con organizaciones criminales, para no ponerse en riesgo. Evitar enfocarse en aspectos personales si no se tienen pruebas.
- Usar un lenguaje incluyente para erradicar la violencia de género. No revictimizar a las personas a través de los medios de información y comunicación.
- Generar vínculos de confianza. Crear redes de apoyo entre colegas, con organizaciones y colectivos que acompañan a este sector.
- Elaborar un protocolo de seguridad digital para el registro y seguimiento de incidentes. Hacer el análisis de riesgo y tomar las medidas preventivas indispensables.

¿Cómo liberar el desgaste personal y emocional en la tarea de hacer periodismo?

La situación de riesgo y estrés en la que viven lxs periodistas dificulta el contacto consigo mismxs, esto se ve reflejado en la salud física, psicosocial y socioemocional. Estar centrados en información trágica puede provocar dolor en el cuerpo, estrés postraumático, insomnio, ansiedad, entre otros, pues las historias de violencia afectan

y tiene un impacto en la persona que las recibe. Los cuidados colectivos son muy importantes en este caso, por ejemplo:

- Leer algo que no tenga relación con el tema laboral o periodístico.
- Hacer ejercicio mejora la salud en general y reduce el riesgo de sufrir calambres o entumecimientos.
- Escuchar música, acudir a terapia, darse un buen masaje o tomar un baño de hierbas¹⁸ ayuda a liberar emociones.
- Contarle a personas cercanas sus emociones y recibir su ayuda.

Directorio de instituciones y organizaciones defensoras de datos y privacidad

- Te invitamos a armar un directorio colectivo de organizaciones o instituciones que son un apoyo en temas de seguridad y activismo digital.

Otras referencias:

Ohlheiser, A. (Junio 2021). *Cinco preguntas sobre la prohibición de Facebook a Donald Trump*. MIT Technology Review.

<https://www.technologyreview.es/s/13432/cinco-preguntas-sobre-la-prohibicion-de-facebook-donald-trump>

Goldsman, F. (14 de julio de 2021). *Okupar las redes sociales del amo*. Picasa. Online Magazine.

<https://www.pikaramagazine.com/2021/07/okupar-las-redes-sociales-del-amo/>

Miranta, F. (19 de octubre de 2020). *Activistas recuperan cuenta de Twitter de Yásnaya Aguilar Gil, lingüista oaxaqueña*. El Universal Oaxaca: México.

<https://oaxaca.eluniversal.com.mx/sociedad/19-11-2020/activistas-recuperan-cuenta-de-twitter-de-yasnaya-a-aquilar-gil-linguista>

Consortio Oaxaca (Abril de 2020). *Compendio de herramientas de autocuidado y sanación*. Consortio para el Diálogo Parlamentario y la Equidad Oaxaca A.C., Casa La Serena y la Iniciativa Mesoamericana de Defensoras de Derechos Humanos –IM-Defensoras.

https://consorciooaxaca.org/wp-content/uploads/2020/05/compendio_Autocuidado.pdf

¹⁸ Consortio Oaxaca (Abril de 2020). *Compendio de herramientas de autocuidado y sanación*. Consortio para el Diálogo Parlamentario y la Equidad Oaxaca, Casa La Serena y la Iniciativa Mesoamericana de Defensoras de Derechos Humanos –IM-Defensoras. https://consorciooaxaca.org/wp-content/uploads/2020/05/compendio_Autocuidado.pdf

3.3 Protección de Datos

Facilitación: INAI¹⁹

Garantiza el uso adecuado de los datos personales, así como el ejercicio y tutela de los derechos de acceso, rectificación, cancelación y oposición que toda persona goza con respecto a su información.

¿Qué es el derecho de acceso a la información pública?

Es el derecho que tiene toda persona a acceder, buscar, recibir y solicitar información pública, el cual se sustenta en el Artículo 6º de la Constitución Política de los Estados Unidos Mexicanos. Este artículo señala la obligación del Estado mexicano de promover y garantizar el libre acceso a la información de forma gratuita, plural y oportuna.

La información en posesión de cualquier autoridad federal, estatal y municipal es pública. De ahí que toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información.

El derecho al acceso a la información pública garantiza que cualquier autoridad federal, estatal o municipal; órganos autónomos, partidos políticos, fideicomisos, fondos públicos y sindicatos; o cualquier persona física o moral que reciba y ejerza recursos públicos o realice actos de autoridad deba entregar la información pública solicitada.

¿Qué es la información pública?

Es toda la información relacionada con las acciones, decisiones y el ejercicio de funciones de las autoridades, partidos políticos, sindicatos, fondos públicos o de las personas que reciben y ejercen recursos públicos o realizan actos de autoridad.

¿Qué es la rendición de cuentas?

Es una obligación de todos los servidores públicos y representantes políticos de informar sobre sus acciones y justificarlas. Se entiende que esto exige transparencia de la información en poder de los gobernantes. La sociedad civil organizada ha tenido un trabajo fundamental en favor del derecho al Acceso a la Información Pública y se ha vuelto un enlace entre las instancias gubernamentales y la ciudadanía.

¹⁹ El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, es el organismo constitucional autónomo garante del cumplimiento de dos derechos fundamentales: el de acceso a la información pública y el de protección de datos personales.

¿Qué es la transparencia?

Es la obligación de las instituciones de poner a disposición de cualquier persona información pública que no vulnere los datos personales ni el interés público. Esto implica que la información sea accesible y disponible aún cuando no se solicite; y con ello se pueda saber qué recursos se están empleando, cómo se están usando y qué resultados se han obtenido en beneficios de la ciudadanía.

Los organismos garantes promueven y protegen el derecho de Acceso a la Información Pública. El INAI está integrado por 1 garante nacional y 32 órganos garantes locales que se encuentran en cada una de las entidades federativas. Estos organismos de transparencia especializados se rigen bajo los principios de imparcialidad, autonomía y licitud.

¿Cuál es la utilidad del derecho al Acceso a la Información Pública?

Su ejercicio permite hacer exigibles otros derechos como el de la salud, la educación, el acceso a la vivienda, entre otros y con ello se atienden otras problemáticas sociales al visibilizarlas. Además de conocer y evaluar el desempeño de las autoridades en el ejercicio de la función pública, es decir, saber cómo ejercen el presupuesto público.

¿Cómo hacer una solicitud de información en la plataforma del INAI?

La Plataforma Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales es un sistema electrónico para solicitar información de interés de la ciudadanía.

La plataforma del INAI tiene tres secciones que son indispensables para acceder a la Información Pública:

1. **Información Pública**, en esta sección se puede consultar información que por ley las instituciones públicas del país deben publicar en la Plataforma Nacional de Transparencia.
2. **Solicitudes**, en esta sección la ciudadanía puede requerir información pública o datos personales a las instituciones públicas del país.
3. **Quejas de respuestas**, en esta sección se tiene la posibilidad de presentar una queja si alguna solicitud no fue atendida o si existe inconformidad con la respuesta obtenida.

¿Cómo puedes generar una solicitud en la Plataforma Nacional de Transparencia?

1. Debes acceder a la página <https://www.plataformadetransparencia.org.mx/>. A través de la sección Solicitudes, la plataforma te pedirá crear una cuenta para poder acceder, pues se requieren tus datos personales para darle seguimiento a tu solicitud y recibir notificaciones, quejas o alegatos de los recursos de revisión.
2. Una vez registrada tu cuenta, deberás ingresar nuevamente a la sección de Solicitudes y encontrarás tres secciones más: Acceso a la Información, Datos personales y Mi historial. Da clic en Solicitud de Acceso a la Información.
3. En seguida se despliega un formulario de los datos indispensables para realizar tu solicitud. Puedes agregar tu nombre completo, dejarlo en blanco, o poner cualquier otro alias para mantener tu anonimato.
4. Elige a qué institución deseas solicitar información. Al dar clic te aparecerán todos los sujetos obligados del ámbito que has seleccionado. Dentro de éstas, deberás escoger a la institución a la cual deseas solicitar información. Da clic en agregar. La plataforma permite que una misma solicitud pueda hacerse hasta con 33 instituciones de manera simultánea.
5. A continuación debes agregar el detalle de tu solicitud; la plataforma te permite adjuntar gráficos o tablas informativas. También podrás agregar de manera opcional datos que faciliten la búsqueda y localización de la información solicitada.
6. Ahora, deberás señalar el medio en el cual deseas recibir la información o notificación y el tipo de formato.
7. La ley establece que las personas que no puedan pagar por reproducción o envío de documentos, podrán indicar sus razones para que sea valorada por la unidad de transparencia. Esta sección también recaba datos estadísticos que retroalimentan al sistema.
8. La ley contempla realizar solicitudes en lenguas indígenas, para ello necesitas rellenar el formulario donde podrás señalar la lengua en que deseas recibir la información solicitada. Además te permitirá indicar si tienes alguna discapacidad para que se te asigne asistencia.

Por último, deberás leer el aviso de privacidad y confirmar si estás de acuerdo. Da clic en enviar. La plataforma generará los acuses de recibido, el cual podrás descargar en formato PDF como comprobante de tu trámite.

Otras referencias:

Infoem.org. mx (2021). *El ABC de los datos personales*. INFOEM: Conferencia Mexicana para el Acceso a la Información Pública. Disponible en: https://www.infoem.org.mx/doc/publicaciones/ABC_Datos.pdf

INAI. (Octubre de 2021). Plataforma Nacional de Transparencia.
<https://www.plataformadetransparencia.org.mx/>

BLOQUE 4

Apropiación de las tecnologías digitales

En este cuarto bloque, se enfoca en la importancia de la apropiación de las tecnologías digitales, considerando las amenazas que pueden surgir al navegar en la Internet y brindando algunas recomendaciones básicas para proteger la seguridad y privacidad en los distintos espacios digitales.

4.1. Seguridad digital/Privacidad

Facilitación: Paul Aguilar²⁰ (SocialTIC)

Para saber cómo funciona la Internet es importante reconocer qué son los dispositivos, los servidores y la nube, pues cuando hablamos de seguridad digital estamos hablando de la seguridad de la información.

Computadora vs. Celular ¿Son iguales? ¿Son diferentes?

Hace algunos años los dispositivos móviles eran muy distintos en su estructura y funcionalidad, sin embargo, el avance tecnológico ha hecho que converjan, por lo que actualmente son muy similares. A continuación se muestran algunas de sus características:

Computadora vs. Celular	
<p style="text-align: center;"><u>Computadora</u></p> <ul style="list-style-type: none">● Procesa información● Almacena información<ul style="list-style-type: none">○ Documentos○ Fotos○ Videos○ Audios● Se pueden instalar programas● Se puede navegar por Internet● Se pueden realizar tareas cotidianas o de trabajo	<p style="text-align: center;"><u>Teléfono celular</u></p> <ul style="list-style-type: none">● Procesa información● Almacena información<ul style="list-style-type: none">○ Documentos○ Fotos○ Videos○ Audios● Se pueden instalar aplicaciones● Se puede navegar por Internet● Se pueden realizar tareas cotidianas de trabajo

Podemos observar que ambos dispositivos son similares pero sus capacidades son diferentes:

- La computadora generalmente tiene mayor capacidad.
- Las características faltantes (por ej. llamadas en computadora) se pueden incorporar.
- Los dos tipos de dispositivos son susceptibles de amenazas.

Computadora personal, servidores y la nube ¿Son iguales o diferentes?

En realidad, son diferentes. Una computadora personal y un servidor comparten muchos componentes físicos, como disco duro, lector de discos, conexiones USB, tarjeta madre, fuente de alimentación, entre otros. Sin embargo, la principal

²⁰ SocialTIC es una organización sin fines de lucro dedicada a la investigación, formación, acompañamiento y promoción de la tecnología digital e información para fines sociales.

diferencia radica en el uso y capacidad. Un servidor está diseñado para un uso industrial o empresarial y generalmente tiene una capacidad mucho mayor que una computadora personal.

Por otro lado, la nube es un concepto que se refiere a la conexión a un espacio virtual en línea. Aunque la nube se conecta de forma virtual, todavía depende de servidores físicos que se encuentran en ubicaciones reales. Estos servidores en la nube son los encargados de almacenar y procesar la información de manera remota.

Es decir, la computadora personal y el servidor comparten componentes físicos, pero difieren en su capacidad y uso. Por otro lado, la nube se basa en la conexión virtual a servidores físicos ubicados en un espacio físico real.

Servidores vs. Nube	
<u>Servidor</u>	<u>Nube</u>
<ul style="list-style-type: none"> ● Procesa información ● Almacena información <ul style="list-style-type: none"> ○ Documentos. ○ Fotos ○ Videos ○ Audios ○ Bases de datos (es un conjunto de información estructurada pero en grandes dimensiones) ● Se pueden instalar programas para ofrecer servicios 	<p>Es el conjunto de servidores que pertenecen a una empresa proveedora de servicios (por ej. Google Drive funciona con un conjunto enorme de servidores que están almacenando información que utilizan sus usuarios)</p>
<p>La nube y los servidores son similares a las computadoras pero sus capacidades son mayores, son de acceso más público y ambos son susceptibles a las mismas amenazas que los dispositivos móviles.</p>	

¿Cómo viaja la información por la Internet? ¿Dónde se almacena? ¿Dónde están las amenazas?

Es indispensable que las personas usuarias de la tecnología digital reconozcan dónde se almacena la información que fluye a través de la Internet, para saber cómo protegerse.

Para enviar un mensaje a través de Internet, es necesario que el dispositivo esté conectado a una red, ya sea mediante una conexión cableada a un módem o a través de la red de datos en un celular (3G o 4G). Al conectarse a un módem, éste a su vez se encuentra conectado a un proveedor de servicios (como Telcel, Movistar, Izzi, etc.), quien se encarga de enviar la información a los servidores. Una vez en los servidores,

la información se gestiona para ser enviada a las personas con las que deseamos comunicarnos.

Podemos comparar el envío de un mensaje por la red con el envío de una carta a través de la oficina de correos: en el papel (la pantalla de tu dispositivo) escribes un mensaje, luego lo guardas dentro un sobre para depositarlo en un buzón (que es el módem); este es enviado (a través de los cables de cobre o fibra óptica) a la oficina postal (que es la empresa proveedora de Internet); la oficina postal lo identifica para enviarlo al destinatario correspondiente (que sería el servidor a través de Whatsapp, e-mail, Facebook, etc.). El servidor guarda el mensaje hasta que el destinatario abre la aplicación para recibir y/o leer el mensaje. Para responder utilizará la misma ruta de regreso.

A continuación podemos encontrar un diagrama²¹ que ilustra las distintas etapas por las cuales transita la información en Internet:

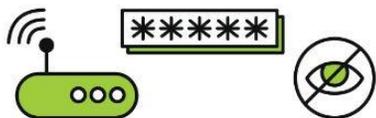
²¹ Social TIC (2018). ¿Cómo funciona internet?. Disponible en: <https://socialtic.org/blog/como-viaja-tu-informacion-en-internet-consejos-y-herramientas-para-protegerla/>

Cómo VIAJA tu información cuando navegas en Internet

Quando quieres conectarte a Internet, tus dispositivos buscan una red inalámbrica (WiFi) o un plan de datos para conectarse, el punto de acceso de esta red es el router o módem. Este aparato se encarga de distribuir los datos, es decir, enviar y recibir información por la red.



OJO: para proteger tu conexión a internet, cambia la contraseña que viene por defecto del módem y comprueba la configuración de seguridad.



El proveedor envía tus datos a la red social o sitio web que estás visitando (por ejemplo, Facebook, Google).



Después del módem, tus datos llegan a tu proveedor de servicios de Internet, es decir, empresas que proveen la conexión.



Los sitios web que visitas viven en los servidores de distintas páginas y servicios. Al conjunto de servidores se le conoce como "la nube" por su capacidad de almacenar archivos. Cuando subes archivos "a la nube" en realidad estás guardándolos en las computadoras de alguien más.



Facebook entrega tus datos a otro proveedor de Internet para que lleguen a su destino final.



El proveedor envía tus datos al módem de la destinataria.



Es importante tener en cuenta que hay empresas y gobiernos que observan tus datos en el trayecto y en el caso de las empresas, recolectan estos datos para venderlos. Esto va en contra del derecho a la privacidad y de una red libre y neutral.



Después de recorrer este camino, tu mensaje llega al dispositivo de la destinataria.



Amenazas vs. Riesgos ¿qué y cómo son?

<u>Amenazas</u>	<u>Riesgo</u>	<u>Incidente</u>
<ul style="list-style-type: none">• Son un peligro latente• Pueden estar asociadas a un fenómeno natural, tecnológico o social• Pueden manifestarse en un sitio y un tiempo específico• Producen efectos adversos (daños)	<p>Es un cálculo de la probabilidad y el impacto de una amenaza. El análisis de riesgo se puede calcular con la siguiente fórmula:</p> <p>Riesgo= impacto x probabilidad</p> <p>Riesgo de asalto= impacto (5) * probabilidad (5) 5*5=25</p> <p>Riesgo de asalto= 25</p>	<ul style="list-style-type: none">• Es un suceso inusual• No hay daño

Ataques digitales ¿Cuáles son y cómo identificarlos?

El término hackeo ha sido usado para referirse a las amenazas que enfrentamos cuando alguien accede a nuestra cuenta de correo o en redes sociales. Sin embargo, los distintos medios de comunicación han difundido una idea errónea y estigmatizadora de los llamados 'hackers', presentándolos como criminales que hacen un mal uso de la información a través de la red.

En los espacios de discusión sobre el tema, el 'hacker' es una persona que tiene una forma distinta y creativa para resolver problemas a través de las tecnologías digitales. De ahí que nos referiremos a ciberatacantes o ciberdelincuentes cuando se está cometiendo una acción delictiva que tiene un impacto negativo para cualquier persona.

A continuación vamos a mostrar los tipos de ataques digitales que SocialTIC ha clasificado para analizar el nivel de riesgo de tus hábitos digitales. Además, nos brindan recomendaciones adecuadas a implementar en cada caso:

1. Ataques digitales mediante vulneraciones técnicas. Implican abusar del diseño de la tecnología para modificar o romper aspectos técnicos con fines maliciosos:

→ **Robo de dispositivos.** En este caso, la vulnerabilidad personal o colectiva aumenta si el dispositivo contiene información sensible.

→ **Accesos no autorizados.** Se trata del acceso sin consentimiento a tus redes sociales y/o correos electrónicos.

→ **Phishing.** Es una forma de ingeniería social que representa una de las mayores amenazas para la seguridad digital, ya que su objetivo no es atacar directamente los dispositivos, sino a las personas. Esta táctica se basa en aprovechar aspectos humanos para explotarlos mental o emocionalmente, con el fin de obtener información confidencial o inducir a los usuarios a visitar sitios web maliciosos. Por ejemplo, puedes recibir correos electrónicos o mensajes de texto que contienen enlaces sospechosos o no reconocidos.

→ **Denegación de servicios.** La denegación de servicios (DDoS, por sus siglas en inglés) es un tipo de ataque que tiene como objetivo saturar un sitio web o servicio en línea, de manera que no pueda responder a las solicitudes de los usuarios. Esto se logra enviando una gran cantidad de tráfico malicioso o solicitudes falsas desde múltiples fuentes, sobrecargando los recursos del sistema y afectando su rendimiento.

Además, existe otra forma de denegación de servicio que consiste en bloquear las señales de telecomunicación, impidiendo su uso normal. Para llevar a cabo esta acción, se utilizan dispositivos conocidos como "jammers" o inhibidores de señal, los cuales emiten señales de interferencia que cancelan o bloquean las comunicaciones, impidiendo el funcionamiento adecuado de los dispositivos conectados a la red afectada.

→ **Intervención de sistemas o equipos.** Esto ocurre cuando un malware, como virus, troyanos, gusanos, entre otros, se instala en un dispositivo y lleva a cabo diversas acciones perjudiciales. Este tipo de software malicioso tiene la capacidad de extraer información confidencial, robar datos personales y realizar capturas de pantalla desde el interior del dispositivo comprometido.

→ **Intervención de líneas de comunicación.** Es también conocida como "línea pinchada", se refiere a la capacidad de alguien más para escuchar tus llamadas telefónicas. Sin embargo, es importante destacar que esta forma de intervención no permite acceder a la información almacenada en tu dispositivo. Solo se puede acceder a la información que se transmite a través de los cables, el módem o el proveedor de servicios, pero no al contenido específico que tienes guardado en tu dispositivo.

→ **La ingeniería social.** Es una técnica de manipulación que utilizan para obtener información confidencial, acceso no autorizado o permisos en sistemas de información. Mediante el engaño y la explotación de la confianza, los ingenieros sociales buscan vulnerar la seguridad y realizar acciones perjudiciales contra las

personas u organizaciones comprometidas. Esta práctica puede involucrar el uso de tácticas psicológicas y de persuasión para obtener información valiosa o inducir a las víctimas a realizar acciones que beneficien al atacante²².

2. Ataques digitales mediante conductas humanas. Los ataques digitales que se basan en conductas humanas, implican el abuso o aprovechamiento del factor humano y las relaciones sociales con el fin de causar daño. Este tipo de ataques se aprovechan de la vulnerabilidad humana y pueden involucrar también una o varias vulnerabilidades técnicas.

Los ataques de esta categoría están divididos en ataques de interacción directa e indirecta:

- **Ataques vía interacción directa.** Son aquellos en los que el atacante establece contacto directo con la persona agredida a través de medios digitales, como mensajes en redes sociales, correos electrónicos y chats. Estas conductas ofensivas pueden incluir discriminación, incitación al odio, acoso, amenazas, hostigamiento y extorsión. Estos son ejemplos de ataques que se llevan a cabo mediante la comunicación directa con la víctima.
- **Ataques vía interacción indirecta.** Este tipo de ataques suelen ser silenciosos o inadvertidos, lo que significa que la persona afectada puede o no darse cuenta de lo que está sucediendo.

Existen varios tipos de ataques de interacción indirecta en entornos digitales. Algunos ejemplos de ellos son: 1. Doxing: Revelación maliciosa de información personal, como su dirección, número de teléfono o información confidencial, con el propósito de dañarla o acosarla. 2. Fake news o campañas de desprestigio: Difusión intencionada de noticias falsas o información engañosa con el fin de perjudicar la reputación de una persona o entidad. 3. Robo o suplantación de identidad: Obtención y uso no autorizado de la identidad de otra persona para cometer fraudes o realizar actividades ilícitas en su nombre. 4. Cuentas falsas: Creación de perfiles falsos que toman información de una cuenta original para generar acciones que perjudiquen a la persona agredida, como difamación o propagación de contenidos negativos. 5. Vigilancia o monitoreo: Observación constante de las redes sociales o la actividad en Internet de una persona con el objetivo de recopilar información para diseñar ataques adicionales, como doxing, phishing o campañas de desprestigio. 6. Remoción o bloqueo de contenido: La remoción ocurre cuando un contenido previamente publicado es eliminado de la plataforma.

²² Wikipedia.com

Para obtener ayuda en estos casos puedes acudir a SocialTIC, Artículo 19 o Cimac²³.

Mapeo de información ¿Qué tipo de información quieres proteger? ¿Cómo elegir?

Es importante realizar un mapeo para identificar qué tipo de información deseas proteger y cómo resguardarla adecuadamente. A continuación, se describen tres categorizaciones de la información: a) La información es *pública* cuando está disponible para el público en general y no requiere medidas adicionales de protección. b) La información es *privada* cuando es accesible solo para un grupo selecto de personas y requiere mecanismos de acceso, como contraseñas para protegerla. Es recomendable proteger esta información, pero si no lo haces, el impacto podría ser limitado. c) La información *sensible* es de naturaleza privada y, al mismo tiempo, tiene el potencial de causar daño si cae en manos equivocadas. Es fundamental proteger esta información de manera rigurosa y tomar medidas para prevenir su filtración o uso no autorizado.

Es necesario evaluar el nivel de confidencialidad de la información y aplicar medidas de protección adecuadas en función de su clasificación, con especial atención a la información sensible, la cual debe ser resguardada de forma prioritaria.

¿Qué amenazas hay en el uso de Internet?

Vulneraciones técnicas y conductas humanas

Dispositivos	Wi-Fi	Proveedor de Internet	Servicios digitales
<ul style="list-style-type: none"> ● Daño, pérdida o robo ● Acceso no autorizado al dispositivo ● Phishing ● Intervención de dispositivos ● Extorsión ● Bloqueo de contenidos 	<ul style="list-style-type: none"> ● Intervención de líneas de comunicación ● Denegación de servicios ● Manipulación de los paquetes de datos en la red <ul style="list-style-type: none"> ■ Lectura ■ Alteración ■ Eliminación ● Bloqueo o control de la distribución de contenidos 	<ul style="list-style-type: none"> ● Acceso no autorizado ● Phishing ● Denegación de servicios <ul style="list-style-type: none"> ■ Dos/ODDoS ● Conductas intimidatorias <ul style="list-style-type: none"> ■ Discriminación ■ Amenazas ■ Acoso 	

²³ Cimac es una organización pionera en periodismo independiente y de investigación con perspectiva de género que trabaja en la agenda de medios de comunicación y género a fin de incorporar la perspectiva de género en los medios de comunicación, evidenciar la violación a los derechos humanos de las mujeres y generar narrativas por el derecho a una vida libre de violencia para todas.

¿De qué forma podemos comenzar a cuidar de nuestra seguridad digital? 6 hábitos de seguridad digital

1. Respaldo.

Has copias actualizadas de tu información y archivos cotidianos en la nube (se sugiere cada dos meses para hacerlo más fácil y práctico).

- La información y archivos históricos de preferencia haz los en discos externos o en USB.
- Respalda de manera cifrada²⁴ información sensible. Cryptomator es una herramienta sencilla que te permite cifrar la información de tu computadora o celular.

2. Los antivirus.

- Protégete de amenazas comunes usando los antivirus, este hábito puede evitarte problemas. Algunos antivirus gratuitos son Bitdefender o AVG.
- Instala antivirus en tus dispositivos. Recuerda que ninguna plataforma está libre de virus.

3. Contraseñas.

- Bloquea el acceso de tu computadora, tablet y celular.
- Utiliza contraseñas únicas y privadas para tus cuentas.
- Utiliza frases o combinaciones alfanuméricas, por ejemplo d3_12_C4R4T2R.
- Utiliza un gestor de contraseñas. Este es un programa diseñado para cifrar y proteger información confidencial, como las contraseñas. Hay varias opciones disponibles, como KeePassXC o StrongboxSafe, que te permiten almacenar tus contraseñas de forma segura. Estos gestores de contraseñas encriptan la información para brindar una capa adicional de protección.

4. Actualizaciones.

Permiten arreglar problemas de seguridad que existen en programas, apps y los sistemas operativos de computadoras y celulares. Actualiza constantemente todos tus dispositivos.

²⁴ El cifrado es una forma de tomar información y transformarla como si fuera una caja fuerte, de tal forma que cuando quieres acceder a esa información necesitas abrir esa caja fuerte que requiere algunos programas o claves, esto quiere decir que la información esta segura

5. Phishing.

En relación a esta amenaza, evita dar clic a correos o mensajes que te pidan:

- Información personal y contraseñas.
- Descargar archivos y enlaces sospechosos. La herramienta Should I click or not?²⁵ te permite comprobar previamente un enlace sospechoso y te avisará si es un virus potencial. Una herramienta similar es virus total disponible en <https://www.virustotal.com/gui/home/upload>

6. Comunicaciones cifradas.

Usar este método evita que toda información y comunicación sean intervenidas.

- En el caso de los chats, es recomendable utilizar aplicaciones como Signal o Wire, que priorizan la seguridad.
- Los correos y envío de archivos son más seguros desde Tutanota o Protonmail, que son servicios de correo electrónico seguro.
- Para realizar llamadas y videollamadas de forma segura, se recomienda Jitsi. Este programa cifra la información de manera eficiente y utiliza un código abierto que permite una revisión transparente de su seguridad. Además, no almacena copias de las comunicaciones ni registra tu actividad.
- Al utilizar HTTPS, los datos se transmiten de manera segura entre tu navegador y el servidor del sitio web, evitando que terceros puedan interceptar y leer la información confidencial, como contraseñas o datos personales. Verificar el HTTPS en los sitios web es una buena práctica para proteger tu privacidad y seguridad en línea.
- VPN es una red privada virtual que permite una extensión segura en áreas locales. Funciona como un túnel virtual a través del cual tus datos viajan de manera segura y protegida. Esta tecnología te permite navegar por la Internet ocultando tu ubicación y protegiendo tus datos.

¿Cómo cuidamos nuestra seguridad y privacidad en el entorno digital?

Es importante identificar cómo implementar estos hábitos de cuidado digital de acuerdo a nuestras necesidades, buscando el equilibrio entre seguridad y operatividad. A continuación te compartimos otras formas de cuidado en la red y espacios digitales:

²⁵ <https://www.shouldiclick.org/>

- Consulta herramientas y recursos con perspectiva de género en ámbitos digitales. Ingresa a ciberseguras.org/ y <https://luchadoras.mx/> donde puedes encontrar herramientas y recursos con esta perspectiva.
- Practica otras maneras de comunicarte con las demás personas. Infórmate acerca de los derechos digitales que puedes ejercer.
- Ejercita tu higiene digital: controla tu privacidad y seguridad para que tengas un mejor bienestar digital; esto se puede lograr con herramientas que se encuentran en la misma red.
- <https://datadetoxkit.org/> es un espacio donde puedes encontrar herramientas para el uso óptimo de las tecnologías, mecanismos para reducir el rastreo de tu información; los pasos a seguir para limpiar aplicaciones, redes sociales y dispositivos.²⁶

Otras referencias:

Aguilar, P. (30 de marzo de 2019). *¿Cómo viaja tu información en internet?*. Protege.la. Disponible en: <https://protege.la/como-viaja-tu-informacion-en-internet-2/>

Aguilar, P. (13 de diciembre de 2019). *6 hábitos básicos para tu seguridad digital*. Protege.la. Disponible en: <https://protege.la/basicos-seguridad-digital/>

ciberseguridad.com. *¿Qué es el modelado de amenazas?*. Disponible en: <https://ciberseguridad.com/herramientas/modelado-amenazas-ejemplos/>

Entrebits.org (13 de mayo de 2019). *Ingeniería social: Redes Sociales y cómo conseguir datos sin que se den cuenta*. Disponible en: <https://entrebits.org/ingeniera-de-la-buena-juegos-de-internet-y-como-conseguir-datos-sin-que-se-den-cuenta/>

²⁶ Datadetoxkit.org. Disponible en: <https://protege.la/data-detox/>

4.2 Twitter y cuidados para el teléfono celular

Facilitación: Yásnaya Aguilar²⁷

¿Qué potencialidades tienen las redes sociales en el mundo real?

Usar las redes sociales como espacio para expresarnos es algo muy cotidiano en el entorno digital actual. Sin embargo, aún existen grandes desigualdades en el acceso a la Internet y a las redes sociales. Esta realidad implica la construcción de otros modos de ser a través de los dispositivos digitales y detectar otros modos de riesgo que existen en ellos, que pueden tener consecuencias graves en la vida de las personas. Lo virtual interpela la realidad, por ello es importante reflexionar acerca de las afectaciones y potencialidades de los espacios digitales: en lo emocional, relacional, corporal, virtual, etc.

¿Los cuidados digitales son individuales o colectivos?

Yásnaya Aguilar sufrió acoso sexual y violencia digital en Twitter luego de denunciar el caso del chat “Sierra XXX”²⁸. Ella no tenía cuidados digitales por considerar innecesario aplicarlo en un contexto de vida comunitaria del que forma parte y en donde existen otras formas de relacionarse con las personas.

En el momento en que cancelaron su cuenta en Twitter, Yásnaya asumió que su paso por esta red había terminado, sin embargo, integrantes de la Red de Resistencia y Disidencia Sexual y de Género decidió apoyarla para recuperar su cuenta. La movilización resultó impresionante en redes, lograron ubicar a quienes la tenían en su poder y pudieron devolvérsela. Con esta experiencia se evidenció el riesgo latente de perder una cuenta y la existencia de un mercado clandestino internacional.

La experiencia de Yásnaya revela que la censura es un ejercicio de poder llevado a cabo por el Estado mexicano, el cual no presta atención a las demandas históricas de las comunidades indígenas, pero sí magnifica la importancia de escuchar un hashtag en las redes sociales. Al mismo tiempo, es importante reconocer el impacto de las plataformas digitales en la sociedad actual para la construcción de comunidades.

²⁷ Yásnaya Elena Aguilar Gil es lingüista, escritora, traductora, activista de derechos lingüísticos e investigadora ayuujk.

²⁸ En marzo del 2020 se dio a conocer públicamente la apertura de un grupo de WhatsApp titulado “Sierra XXX” en el que unos 100 hombres de la Sierra Mixe exponían sin su consentimiento imágenes de mujeres mixes de Oaxaca en México. Múltiples capturas de pantalla hechas públicas corroboran estos hechos. Dentro de los participantes hay políticos y figuras públicas de la región que alentaban a utilizar el grupo para compartir pornografía y fotos íntimas “de preferencia paisanas (Mixes)” En: Cultura Survival (05 de abril de 2021). Mujeres mixes en México denuncian violencia sexual de parte de políticos. Disponible en: <https://www.culturalsurvival.org/news/mujeres-mixes-en-mexico-denuncian-violencia-sexual-de-parte-de-politicos>

¿Cómo podemos incorporar hábitos de cuidado en nuestros dispositivos móviles?

Hay reglas que no podemos cambiar por más cuidados que existan para ello. Las empresas y los gobiernos tienen acuerdos que rebasan los derechos de seguridad y privacidad en el mundo digital.

Cuando adquirimos un dispositivo móvil varias aplicaciones ya están preinstaladas, aunque muchas veces no las necesitamos. Además, es común que no dediquemos tiempo a leer detenidamente los términos y condiciones de estas aplicaciones, a pesar de que no siempre concuerdan con nuestros intereses. Por esta razón, es crucial adoptar los siguientes hábitos de cuidado y seguridad digital:

- Debes revisar qué aplicaciones tienes en tu teléfono celular y cuáles estás utilizando. Desinstala o inhabilita aquellas que no necesitas o no utilizas. Esto ayudará a reducir la cantidad de aplicaciones y potenciales riesgos de seguridad. Debido a que algunas de ellas podrían tener acceso a tus datos, fotos, archivos, micrófono, cámaras, etcétera, y esto pondría en riesgo tu información y te colocaría en un mayor nivel de vulnerabilidad.
- Es importante tener en cuenta que aquello que no deseamos que se difunda por la red y sus distintas plataformas, es preferible comunicarlo en persona. Esto debido a que cuando subimos información a Internet, ésta se vuelve pública. Tomar la decisión de comunicarlo directamente cara a cara nos otorga mayor autonomía y responsabilidad en los espacios digitales.
- Considera la importancia de tener contacto con otras personas, realizar actividades físicas y disfrutar de momentos placenteros, ya que esto nos conecta con una realidad diferente. Siempre existe la opción de cerrar la computadora o alejarse del teléfono celular para interactuar con el mundo que nos rodea. Como bien menciona Yásnaya, "Sentir me cura cuando pensar me enferma, pensar me cura cuando sentir me enferma", esta frase nos invita a reflexionar sobre cómo prevenir el impacto de la violencia digital en las redes sociales y encontrar un equilibrio entre nuestra vida digital y nuestra vida real.
- Es necesario leer "las letras chiquitas" de los términos y condiciones de las plataformas o redes sociales para saber qué servicios estamos usando y preguntarnos qué hay detrás de todo ello.

Cuidarnos en el entorno digital implica mucho más que el uso de contraseñas. Lo más importante es ser conscientes de nuestro modo de usar estas redes sociales. Es necesario reconocer la importancia de no dejar de construir y participar en los otros espacios de encuentro, diálogo, conspiraciones, convivencia y subversiones. Al hacerlo, cultivamos una

experiencia digital más enriquecedora y equilibrada, donde nuestras interacciones en línea se complementan con nuestras conexiones y actividades en el mundo real.

¿Es posible la construcción de comunidad en las redes sociales?

La construcción de comunidad desde lo virtual puede impactar en la vida real. Por ejemplo, cuando una denuncia se difunde en Twitter, la solidaridad manifestada por personas e instituciones puede respaldar una causa o demanda de justicia. No obstante, es importante tener precaución para asegurar que estas acciones no reemplacen ni oculten los procesos autogestivos y colaborativos de las comunidades, ya que esto podría dar lugar a una relación clientelar con ciertas instituciones y redes de apoyo externas a las dinámicas comunitarias.

Las redes sociales han generado un impacto significativo en la vida comunitaria, al introducir nuevos escenarios que antes no existían. Sin embargo, es crucial reconocer que estas plataformas no están exentas de actitudes racistas, clasistas o machistas. Por lo tanto, es una cuestión ética utilizarlas como herramientas para crear espacios de discusión pública que brinden voz a quienes históricamente han sido invisibilizados.

¿Qué otras aplicaciones son una alternativa para tu dispositivo móvil?

Te compartimos algunas aplicaciones y herramientas que te permiten explorar otros modos de interactuar en la red:

- **Canva.** Es un software y sitio web que brinda herramientas de diseño gráfico simplificado.
- **Firefox Focus.** Es un navegador dedicado a la privacidad con protección automática contra el rastreo. Con Focus las páginas se cargan más rápido y los datos se mantienen privados.
- **Signal.** Es una aplicación de mensajería instantánea, es una alternativa a WhatsApp o Telegram. Ofrece mayor privacidad y mayores estándares de seguridad.
- **Telegram.** Es una aplicación de mensajería enfocada en la velocidad y seguridad, es rápida, simple y gratuita.
- **DeepL.** Es un servicio de traducción automática en línea, es una alternativa a google translate y de Bing Microsoft Translator.

→ **Open Street Maps.** Es un proyecto colaborativo de código abierto para crear mapas editables y libres. La importancia de este proyecto radica en los datos generados, no en el mapa en sí.

→ **ProtonMail.** Es un servicio de correo electrónico que ofrece cifrado de extremo a extremo. Su enfoque se basa en el cifrado de acceso cero para garantizar la seguridad de los correos electrónicos. Es un proveedor de correo electrónico que prioriza la privacidad de las personas por encima de los intereses de los anunciantes.

¿Cómo nos cuidamos en las redes sociales?

Siempre tenemos la opción de cerrar la pantalla y de esta manera compartir el tiempo con las personas de nuestra comunidad, intercambiando ideas, actividades y emociones. No todo se encuentra en el ámbito digital, por lo que es fundamental mantener un contacto con las realidades en las que vivimos, disfrutando de momentos de alegría y recreación.

- Procura usar hábitos de seguridad y privacidad en la Internet y redes sociales. En el apartado 4.1. *Seguridad digital/Privacidad* de esta guía puedes encontrar 6 hábitos básicos para lograrlo.

Otras referencias:

Aguilar, P. (13 de diciembre de 2019). *¿Qué hacer ante agresiones y ataques en línea?*. Disponible en: <https://protege.la/ataques-en-linea/>

4.3. El derecho a las tecnologías y cuidados digitales

Facilitación: Oliver Fröhling (SURCO Oaxaca A.C.) y Elizabeth Mosqueda (Consortio Oaxaca)

El acceso y uso de las tecnologías digitales es un derecho humano, pero desafortunadamente no es universal, lo cual plantea la necesidad de resolver esta brecha para poder acceder a contenidos digitales de calidad. Las dinámicas virtuales y digitales han generado debates en el ámbito académico sobre los impactos de estas tecnologías, especialmente en el contexto de la pandemia por COVID-19.

En este apartado analizaremos el tema a partir del ensayo “El acceso a la tecnología como derecho humano” (Masdeagencia.com, 2021):

Impactos de la virtualización de la educación y cómo incidir en ello

La educación a distancia ha implicado más trabajo extra para madres y padres de familia. Este impacto no se contempla en las políticas educativas ni gubernamentales. La educación desde casa requiere otra forma de organización familiar, sin olvidar que muchas personas se han quedado sin la oportunidad de recibir educación debido a la falta de infraestructura en comunidades y sectores vulnerables. Al abordar a las tecnologías como derecho humano se debe hablar sobre el derecho al acceso a Internet.

Por otra parte, el uso de tecnologías digitales ofrece muchas posibilidades de hacer una enseñanza diferente, pero ha sido difícil crear y diseñar contenidos de calidad para quienes hoy educan en la virtualidad. Sin duda es necesaria la formación y capacitación en este nuevo escenario y se necesita el tiempo y capacitación adecuada para hacerlo.

El contexto de COVID-19 propició una educación con nuevos alcances. El modelo tradicional de transferencia vertical de conocimientos ha sido mediado por herramientas y dinámicas tecnológicas que exigen la creación de otros modos de enseñanza y aprendizaje más flexibles y creativos, que enriquezcan los procesos de formación, sin depender de las plataformas digitales.

El escenario de la escuela en casa resulta complejo, pues ya de por sí los modelos educativos tradicionales funcionan bajo un sistema reproductor de prácticas de control y verticalidad. El contexto de pandemia refleja la urgencia de adecuaciones curriculares virtuales que dejen de reproducir lógicas tradicionales de enseñanza y aprendizaje.

De la presencialidad a la virtualidad hay una exigencia de los gobiernos en la continuidad de los procesos pedagógicos, sin plantear políticas y modelos educativos que se adecuen a la realidad. Es necesario que los actores educativos analicen el cambio de roles en el proceso pedagógico que se ha dado a partir del contexto de COVID-19. El entorno digital

actual brinda la oportunidad de crear una educación diferente, con un alcance amplio, basada en la flexibilidad y la creatividad, especialmente en el contexto de la pandemia.

¿Qué desafíos implica el teletrabajo en contexto de pandemia?

La pandemia de COVID-19 ha introducido nuevos métodos de trabajo, ya sea desde casa o en un formato híbrido. Sin embargo, al analizar las relaciones y las condiciones laborales, surgen preguntas sobre quién asumirá los costos del servicio de Internet y los dispositivos utilizados para desempeñar nuestras tareas en estos nuevos escenarios. Además, nos preocupa cómo se puede gestionar el control de horarios laborales, ya que el trabajo desde casa implica una mayor flexibilidad, pero también puede resultar en jornadas laborales prolongadas, especialmente para aquellos que también son responsables del cuidado de sus hijas e hijos. Esta situación impacta negativamente en los derechos laborales que hemos conquistado a lo largo de la historia y contribuye al aumento de la violencia de género.

De ahí que nos preguntamos ¿Cómo podemos regularizar el trabajo en este contexto? ¿En qué dimensiones la brecha económica determinará quiénes tienen acceso a la Internet y quiénes no? ¿Cómo acceder al trabajo cuando no se tienen las condiciones mínimas para ejercer este derecho? Concluimos que los nuevos escenarios del empleo reflejan las dimensiones de la precarización de la vida.

La invasión a la privacidad de quienes trabajan desde casa es otra de las dinámicas que impone el teletrabajo. A pesar de la “comodidad” de no tener que trasladarse a la oficina, existen muchos aspectos que debemos replantearnos, pues resultan más complejos de lo que aparentan.

El capitalismo de plataformas se acentúa en la pandemia. Las empresas han adaptado su infraestructura para obtener ganancias. Sin embargo, el teletrabajo abre la puerta a la precarización laboral debido a que las empresas no asumen los costos en la salud mental y física de sus empleados.

En la actualidad, las empresas, las aplicaciones, la Internet y su infraestructura forman parte integral del sistema económico y político que reestructura nuestra vida. A veces parece que la única opción es estar constantemente conectados a esta realidad virtual para mantener nuestra economía. No obstante, nos planteamos cómo podemos aprovechar esta situación para enriquecer nuestras vidas y encontrar formas de mejora personal y colectiva.

¿Cómo reconocemos prácticas invasivas de monitoreo y vigilancia?

El contexto de pandemia ha acentuado la posibilidad de monitoreo y vigilancia, el uso de las tecnologías con este fin quizá no representa una preocupación en comunidades pequeñas, pero en las grandes ciudades tienen mayor presencia, sobre todo a través de las empresas privadas. Lo preocupante es que la vigilancia se lleva a cabo con todas las cargas sexistas, clasistas y racistas que existen en distintos ámbitos. Desde la presencia de cámaras de vigilancia en las calles hasta el uso de tecnologías en el reconocimiento facial, pueden tener implicaciones serias, por ejemplo, cuando una persona puede ser inculpada e ir a la cárcel por un error en los algoritmos. Además, el uso de datos personales en los espacios digitales puede tener consecuencias graves si son robados o modificados. Los vacíos en las leyes de protección y rectificación de datos representan un problema constante.

Existen países que restringen a las empresas privadas el uso de datos personales. En México hay intenciones de regular esto pero aún no es una realidad. En la actualidad, surge la interrogante sobre qué sucede con los datos y resultados de los casos de COVID-19 en México, cómo se protegen, quiénes tienen acceso a ellos y cómo se relacionan con otros datos. No disponemos de información precisa sobre si estos datos se encuentran seguros. Por lo tanto, resulta imperativo establecer mecanismos colectivos de protección de datos.

¿Cómo se han modificado las relaciones interpersonales dentro del mundo digital actual?

La pandemia de COVID-19 ha transformado la forma de relacionarnos al obligarnos a pasar más tiempo frente a las pantallas. Esta situación ha estimulado el uso y la adopción de diversas herramientas digitales, como es el caso de las redes sociales, las aplicaciones de mensajería y las plataformas virtuales. Aunque esta nueva dinámica nos brinda múltiples posibilidades para mantenernos en contacto con otras personas, resulta fundamental implementar una política de inclusión digital que acompañe estos avances, prestando especial atención en aquellos que carecen de conectividad o que no han logrado aprovechar estas oportunidades digitales “orientando respecto de las prescripciones que conlleva la tecnología, aportando recursos para trascender esas limitaciones, creando condiciones para que las personas exploren, aprendan y aprovechen críticamente” (masdeagencia.com).

¿Cuáles son las nuevas modalidades y horizontes del arte y entretenimiento?

Actualmente surge la pregunta sobre si existe la posibilidad de volver a modalidades de interacción cultural y recreativa que se realizaban antes de la pandemia. En este nuevo escenario, artistas, artesanas y artesanos han comenzado a utilizar la virtualidad para

ofrecer sus obras o productos. La digitalización ha posibilitado la democratización de la música y otros productos culturales. En la actualidad, resulta más fácil y económico adquirir arte y diversos productos a través de la Internet. Además de contar con una amplia variedad de aplicaciones que nos permiten interactuar, consumir, compartir, dialogar e informarnos sobre arte, cultura, entretenimiento y ciencia.

Es importante mirar los matices en esta ausencia de presencialidad en los espacios de arte y entretenimiento, sin dejar de tomar en cuenta las desigualdades económicas y la brecha digital. Las redes y plataformas representan espacios virtuales donde podemos encontrar una opción para generar contenidos artísticos y difundirlos a nivel global, ya que amplían el ejercicio de otros derechos como es el caso de la comunicación, el entretenimiento y la recreación.

¿Qué otros temas nos preocupan respecto al uso de las tecnologías digitales en el contexto de COVID-19?

Los modos de organización a través de grupos en plataformas como Facebook, WhatsApp, etc., plantean interrogantes sobre cómo esto afecta la participación política en la sociedad digital. Nos enfrenta al desafío de pensar si esta avalancha de información suma o resta a la participación política, y nos obliga a verificar la veracidad de la información y a seleccionar fuentes y recursos confiables para corroborarla. Si bien, estas plataformas pueden brindar un espacio para el intercambio de ideas y la organización ciudadana, también presentan el desafío de lidiar con la desinformación y las noticias falsas.

El impacto ambiental de las tecnologías digitales es otro tema en cuestión. Aproximadamente el 3% del uso energético mundial se usa para Internet. El uso de servidores y plataformas digitales consumen mucha energía, es indispensable preguntarnos de dónde vienen y cuáles son sus impactos en el medio ambiente. Además que, el uso y desecho de dispositivos electrónicos nos lleva a cuestionar cuál es su destino, cómo se manejan estos desechos y de qué forma podemos participar para prevenir estos impactos en el territorio.

Por último, es imprescindible cuestionarnos sobre cómo podemos desarrollar una tecnología que mejore nuestras vidas, al hacerlo, podremos aprovechar sus beneficios de manera positiva y constructiva. Es crucial pensar en cómo podemos diseñar herramientas y sistemas que fomenten un equilibrio saludable entre el trabajo y la vida personal, evitando la sensación de que el teletrabajo nunca termina.

Otras referencias:

Apropiacióndetecnologías.com. (Mayo de 2020). *El acceso a las tecnologías digitales como derecho humano*. GT-Clacso/RIAT. Disponible en: <https://apropiaciondetecnologias.com/documentos/el-acceso-a-las-tecnologias-digitales-como-derecho-humano/>

Grillo, O. (et. al). (2019). *Tecnologías digitales. Miradas críticas de la apropiación en América Latina*. Buenos Aires: CLACSO; Montevideo: RIAT, 2019.

Gnu.org. (2021). *¿Qué es el software libre?*. GNU. Disponible en: <https://www.gnu.org/philosophy/free-sw.es.html>

Kleyner, D. (20 de diciembre de 2011). *El Manifiesto Telecomunista*. Disponible en: https://endefensadelsl.org/manifiesto_telecomunista.html

Gnu.org. (Septiembre de 2021). *¿Qué es el Software Libre?* <https://www.gnu.org/philosophy/free>

Servicios Universitarios y Redes de Conocimientos en Oaxaca (SURCO Oaxaca A.C.) y Consorcio para el Diálogo Parlamentario y la Equidad Oaxaca (Consortio Oaxaca) se han unido para crear una guía que aborda la importancia de la seguridad digital y el cuidado de las personas comunicadoras indígenas y defensoras del territorio en Oaxaca.

El objetivo de esta Guía es proporcionar herramientas y conocimientos prácticos para garantizar la protección integral de estas personas, ya que si bien desempeñan un papel crucial en la defensa de los Derechos Humanos, la justicia social y la preservación de las culturas indígenas, también se enfrentan a amenazas y ataques tanto en el mundo físico como en el digital.

La Guía aborda temas como la privacidad en línea, la seguridad de las comunicaciones, la gestión de contraseñas, la protección contra el acoso digital y la ciberseguridad en general. Esta Guía es un recurso práctico y útil que busca proporcionar la orientación necesaria para navegar de manera segura en el mundo digital y fortalecer el valioso trabajo que realizan estas personas.

Es importante destacar que el proceso de creación fue realizado de forma colaborativa e integra los conocimientos y experiencias compartidas en el Laboratorio de Narrativa 6.0 sobre Seguridad y Cuidados Digitales, espacio de reflexión e intercambio convocado por SURCO Oaxaca A.C y Consortio Oaxaca.



Unión Europea

