La internet también es de las infancias

Manual para talleristas sobre herramientas básicas de seguridad digital

Hijas de Internet

CENTRO DECULTURA DIGITAL

CULTURA
SECRETARÍA DE CULTURA

CENTRO DE CULTURA DIGITAL

Título: La internet también es de las infancias. Manual para talleristas sobre herramientas básicas de seguridad digital
Autoría: Luisa Alfaro Luna y Montserrat López Pérez (Hijas de Internet)

Diseño y formación: María Fernanda Arnaut
Ilustraciones: María Alejandra Alfaro Luna
Edición y corrección de estilo: Miriam Millán y Xitlalitl Rodríguez Mendoza

Este material forma parte del proyecto La internet también es de las infancias.

Primera edición, abril de 2024
Centro de Cultura Digital

En Hijas de Internet buscamos promover una internet más segura, diversa e inclusiva para todas las personas. En México y, en general, en América Latina las infancias y adolescencias suelen ser las personas más vulneradas a experimentar violencia, ya sea en los espacios digitales o en otros. Por eso, nuestros esfuerzos se concentran en escuchar las experiencias y las propias voces de las infancias y adolescencias para crear herramientas de cuidados digitales, individuales y colectivos. En este contexto, en conjunto con el Centro de Cultura Digital, desarrollamos la metodología del taller **Herramientas básicas de seguridad digital**, el cual quiso proveer herramientas útiles de cuidados digitales para las infancias.

A partir de la experiencia de este taller, que fue facilitado por Luisa Fernanda Alfaro Luna, integrante del colectivo Hijas de Internet, a lo largo del mes de octubre de 2023 en la Ciudad de México como parte del *programa Semilleros Creativos del área de Inclusión Digital del Centro de Cultura Digital*, decidimos compartir este manual para la impartición de talleres de herramientas básicas de seguridad digital ***La internet también es de las infancias.***

Los objetivos de las cuatro sesiones realizadas fueron 1) entender los riesgos que existen en internet, 2) comprender conceptos como **adultocentrismo** y **derechos digitales**, y 3) adquirir herramientas de cuidados digitales.

Si bien el manual pretende ser antes que un instructivo, una guía que pueda adaptarse a cada contexto, vemos necesario compartir la metodología que nos funcionó con el fin de ejemplificar nuestro andar pedagógico. El taller se compuso de cuatro sesiones con una duración de 2 hrs., cada una.

Para la realización del taller, existen algunos requerimientos logísticos:

- Calcomanías para hacer identificadores
- Computadora
- Proyector
- Presentación
- 200 Impresiones del Anexo 1

La metodología del taller se enmarca en un enfoque participativo, diseñado especialmente para guiar a niños, niñas, niñes y adolescentes (NNNA) en un emocionante viaje de descubrimiento hacia el mundo de los derechos digitales.

En las siguientes páginas compartimos actividades, preguntas detonadoras y ejemplos para complementar el taller. La persona tallerista debe guiar el espacio y debe esforzarse por crear un ambiente seguro y abierto, fomentando la reflexión y el diálogo.

La metodología se centra en crear herramientas colectivas para que NNNA comprendan la importancia de la privacidad, derechos digitales, la seguridad en línea y otros conceptos fundamentales en el entorno digital.

El propósito es que les talleristas busquen inspirar a los participantes a tomar decisiones informadas y responsables mientras navegan por el mundo digital que está en constante evolución, fortaleciendo así su capacidad para ejercer sus derechos con confianza y responsabilidad.

10 minutos

Como tallerista, debes presentarte y establecer un ambiente cálido y de respeto para incentivar la participación de les asistentes.

La primera actividad consiste en:

- Hacer un gafete para que les asistentes puedan identificarse por su nombre durante el encuentro.
- Preséntate como tallerista y explica las razones por las que tanto tú como les asistentes se encuentran en este espacio.

Luego, puedes comenzar con las preguntas detonadoras, tales como: ¿Qué me gusta de internet? ¿Qué es lo que más me gusta hacer?

Es necesario que se recuperen palabras clave de las respuestas para después retomarlas durante el taller.

No se interrumpe ninguna participación de las infancias y adolescencias.

10 minutos

Continúa el diálogo con otra pregunta detonadora. Por ejemplo, ¿qué es lo que menos me gusta de internet?

En este punto es importante validar todas las experiencias negativas y lo que éstas les hicieron sentir a les compañeres asistentes.

En caso de que identifiques alguna situación de violencia digital, como grooming o violencia sexual digital, es de suma importante que se canalice.

15 minutos

¿Qué es el adultocentrismo?

Es la idea de que sólo en la adultez te realizas como ser humano.

Para el adultocentrismo, las etapas previas de la infancia y la adolescencia no son relevantes, sino que son un peldaño para ser un "humano completo" sólo en la adultez.

Es una narrativa que da por sentado que las niñas, niños, niñes y adolescentes son carentes de "algo" y, por eso, les adultes deberíamos decidir por elles.

Para enmarcar esto, como tallerista puedes preguntar en qué momentos de su vida, o bien del día a día de les asistentes, identifican el adultocentrismo. Por ejemplo, cuando no les dejan decidir sobre algo que tiene que ver con sus propias vidas:

- En la escuela no se les pregunta sobre sus necesidades y expectativas en su día a día.

- En los hogares no siempre se tienen la consideración de lo que desean comer.

- Cuando se presupone que niñas, niños y niñes tienen menos conocimientos sobre un tema y no se les pregunta primero qué es lo que saben.

¿Qué son los derechos digitales?

Son una extensión de los derechos humanos en el entorno digital, por lo que se relacionan con la manera en que se ejercen, promueven y defienden los derechos mediante el uso de las tecnologías digitales de la información y las comunicaciones.

En este punto hay que sondear si hay alguna duda o algún comentario sobre estos dos temas.

Para cerrar la actividad, puedes hacerles preguntas a les asistentes sobre los dos temas para que no olviden el marco del taller.

15 minutos

En el siguiente punto se busca exponer los riesgos que existen en internet. Antes de dar la definición de los conceptos por revisar, se pregunta a qué les suena o si alguna vez ya habían escuchado hablar sobre estos temas.

EXPLICACIÓN DE RIESGOS:

Violencia digital

Es toda violencia que sucede en medios digitales como redes sociales, correo electrónico o aplicaciones de mensajería móvil, y que causa daños a la dignidad y la integridad, e impide el empoderamiento, desarrollo y el pleno disfrute de derechos humanos como la dignidad, la libertad de expresión y a la información, la protección de datos personales y el acceso a la justicia.

Ataques maliciosos

Son intentos de robar, exponer, alterar o destruir información mediante el acceso no autorizado a nuestras computadoras o cuentas de correo y redes sociales.

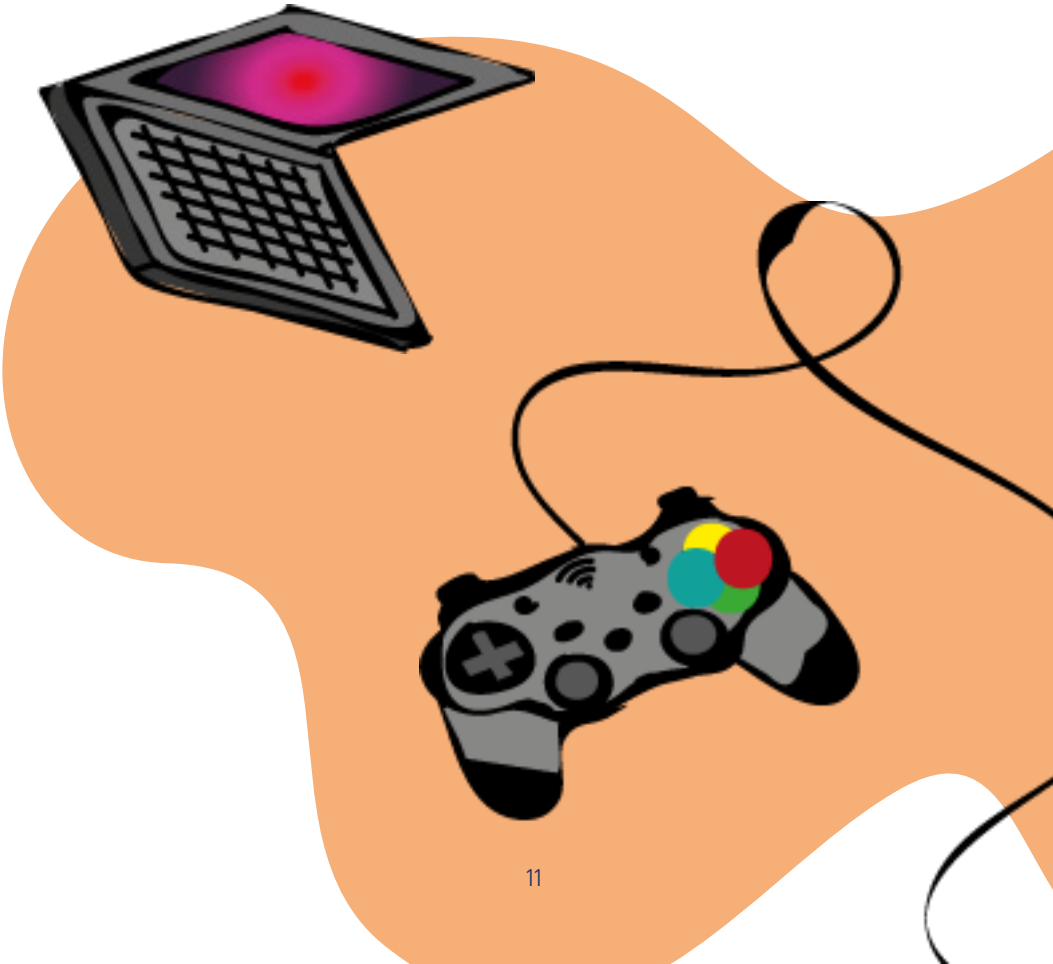
Grooming

Es la práctica que realiza un adulto en internet con el fin de acercarse a un menor de edad para ganarse

su confianza. Quienes lo practican, suelen crear una conexión emocional con la intención de causarle daño.

Daños físicos (postura, pérdida de visión, etc.)

Si se utilizan excesivamente los dispositivos electrónicos, pueden existir consecuencias físicas como daño visual, dolores musculares en el cuello o el pulgar, mala calidad del sueño o pérdida auditiva.



Consejos de seguridad digital

15 minutos

Seguridad digital

En este apartado es necesario mencionar que frente a los riesgos anteriores hay herramientas de autocuidado y cuidado digital que se pueden hacer para sentirnos segures en línea.

- ¿Cuáles son las prácticas a realizar para sentirse segures en línea?

- ¿A qué les suena ciberseguridad?

¿Qué es ciberseguridad?

Es la práctica de defender la información que contienen nuestros celulares, computadoras, servidores, sistemas electrónicos y redes de ataques maliciosos.

Un malware —o un software malicioso— son tipos de programas que son instalados intencionalmente en tus dispositivos y pueden robar tu información, dirigir publicidad, espiar tus conversaciones e, incluso, extorsionar por tu información robada.

Tips para protegernos

- Ponle atención a tus contraseñas. Para almacenarlas y que no las olvides puedes utilizar un administrador de contraseñas como bitwarden o 1Password.
    - Los administradores de contraseñas te permiten guardarlas en un único lugar, y sólo necesitas recordar una contraseña maestra para acceder a ellas. No olvides lo siguiente:
    - Una contraseña segura debe tener: más de 15 carácteres (entre más larga mejor). Combina letras, números, carácteres especiales, mayúsculas y minúsculas.
    - No utilices información personal, como fechas de cumpleaños o el nombre de tu mascota.
- Cambia tus contraseñas al menos una vez al año y trata de no repetirlas.
- Tus contraseñas son sólo tuyas, no las compartas.
- Utiliza frases largas y combina letras, números y carácteres especiales.

Puedes guiar un juego para fortalecer los conocimientos de cómo crear contraseñas seguras, siguiendo los siguientes pasos y leyendo en voz alta las instrucciones (diapositiva 16):

1. Abre este enlace

2. Crea un nombre de usuario y da click en comenzar. Ejemplo: Carabana23

3. Da click en "Jugar el juego"

4. Lee las instrucciones y da click en "Siguiente"

5. Escribe "Contraseña" y da click en "Siguiente"

6. Escribe una palabra. Le tallerista puede decir que piensen en su sabor de pastel favorito, por ejemplo, "Chocolate", y da click en "Siguiente"

7. Agrega dos números y da click en "Siguiente". Por ejemplo, "Ch0c0late"

8. Agrega un símbolo y da click en "Siguiente". Por ejemplo "Ch0col@te!!"

Tips extra de seguridad digital:

- Activa la verificación de dos pasos en tus redes sociales y correo electrónico.
- Evita acceder a enlaces o descargar archivos adjuntos de correos electrónicos sospechosos.
- Si diste click al enlace e identificas que es falso, cambia tus contraseñas de forma inmediata y avisa a la aplicación.
- Desactiva permisos. Revisa tus permisos de ubicación en las aplicaciones que utilizas. Procura no compartir tu ubicación en tiempo real.
- Si te encuentras en una situación que no sabes cómo manejar, acércate a une adulte de confianza y cuéntale lo que estás viviendo.
- Bloquea y reporta en redes sociales o en videojuegos a las cuentas que te hagan sentir incómode.

10 minutos

Bienestar digital

En este apartado hay que recalcar que frente a los riesgos hay herramientas de autocuidado y cuidado digital que se pueden hacer para experimentar bienestar digital.

Explica la idea de que, así como tenemos hábitos de cuidados en la vida diaria como bañarnos, lavarnos los dientes o no comer tantos dulces, existen hábitos digitales que nos ayudan a experimentar el bienestar digital.

Puedes plantear preguntas como: ¿Cuáles son estas prácticas utilizadas para sentirse bien en línea? ¿A qué les suena bienestar digital?

¿Qué es bienestar digital?

Consiste en desarrollar y mantener una relación saludable con la tecnología, y ser conscientes de cómo los medios digitales afectan a nuestro bienestar mental, físico, social y emocional.

Tips para protegernos

- Desactiva las notificaciones del celular en momentos específicos del día. Quita sonidos o vibraciones de las notificaciones de las aplicaciones del celular.

- Utiliza aplicaciones que reduzcan las distracciones y que faciliten la concentración (Adblock, Self Control).

- Aprovecha las opciones de bienestar digital de las aplicaciones. Google desarrolló una tecnología, disponible en los dispositivos Android, llamada bienestar digital, la encuentras en la opción de ajustes de tu celular. En TikTok también puedes activar una opción de bienestar digital, en la que puedes recordar el tiempo que llevas en la aplicación.

- Desintoxicación digital. Desconectarnos un momento o buscar minimizar utilizar el celular cuando estamos en ciertos contextos como en reuniones familiares o sociales.

- No olvides la conexión con la naturaleza.

10 minutos

Privacidad digital

Así como se hizo en el apartado de bienestar digital, en este punto también hay que recalcar que existen herramientas de autocuidado y cuidado digital que se pueden hacer para procurar la privacidad digital.

Explica que así como tenemos hábitos de cuidados en la vida diaria para procurar la privacidad digital —tener llaves en nuestra casa y no compartirlas, tener cortinas en las ventanas, no dar nuestros datos personales como nuestra dirección a todas las personas que vemos en la calle—, así también existen acciones que procuran la privacidad digital.

¿A qué les suena la privacidad digital?

¿Qué es privacidad digital?

Es la práctica de proteger la información que compartimos en medios digitales; es el derecho de les usuaries para decidir cuáles datos personales compartir y cuáles no.

Tips para protegernos

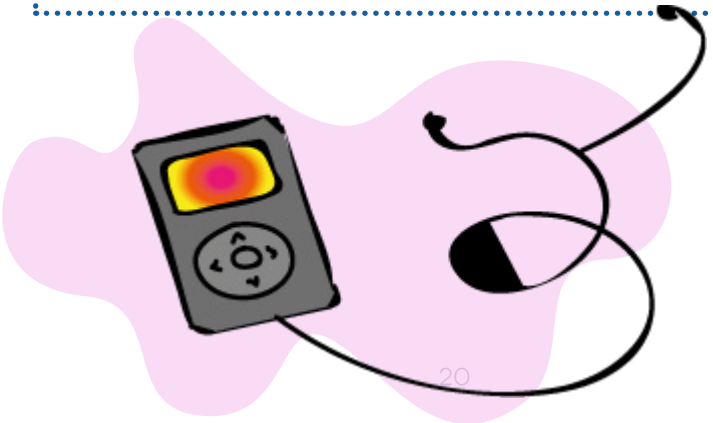
- Ten cuidado con lo que compartes en redes sociales. Es importante tener control sobre la información personal que publicas. Puedes hacer tu perfil privado o si es público sé precavide con la información que expones.

- No compartas datos personales, como tu nombre completo o edad. Te recomendamos el uso de seudónimos o sólo utilizar uno de tus dos apellidos.

- Evita subir fotografías o indicios de la dirección de tu casa o escuela, y no compartas información personal sobre familiares y amigues.

- Trata de buscar tu nombre en Google periódicamente para que sepas qué información tuya está pública en la red.

- Elimina de forma periódica tu historial de navegación y las cookies. También puedes utilizar un buscador privado (Brave, por ejemplo) que no monetiza tu información. Si quieres utilizar un buscador como Google procura no ligarlo con tu cuenta personal.



10 minutos

Desinformación

Aquí hay que enfatizar la existencia de un fenómeno mundial: la desinformación. Puedes comenzar hablando de la responsabilidad que tenemos frente a este hecho, pues la desinformación tiene consecuencias negativas sobre cómo construimos y concebimos el mundo.

Comienza preguntándole a les asistentes a qué les suena la desinformación.

¿Qué es?

La Unión Europea define la **desinformación** como: "información falsa o engañosa que se crea, presenta y divulga para engañar deliberadamente a la población, y que puede causar un perjuicio público".

Mucha de la desinformación que se propaga en internet tiene intereses financieros. Es resultado del modelo de negocios dependiente de la economía de la atención con el que funcionan algunas redes sociales como META, X (antes Twitter), TikTok o YouTube.

Se ha descubierto que las historias e imágenes más susceptibles a ser virales son las que nos generan miedo, disgusto, asombro, irritación, enfado o ansiedad.

Tips para protegernos

- Identifica la desinformación. Cada vez hay hay técnicas más sofisticadas para propagar información falsa, como las *deepfakes*. Por eso es inminente que aprendamos a identificar contenido sospechoso.

- Por lo general son discursos imprecisos, con pocos detalles, susceptibles a la malinterpretación, descontextualizados o sesgados.

- Hacer preguntas críticas. Pregúntate ¿quién creó la información?, ¿cuándo se creó?, ¿a quién favorece o perjudica?, ¿presenta referencias fiables?, ¿se ajusta el titular al contenido?

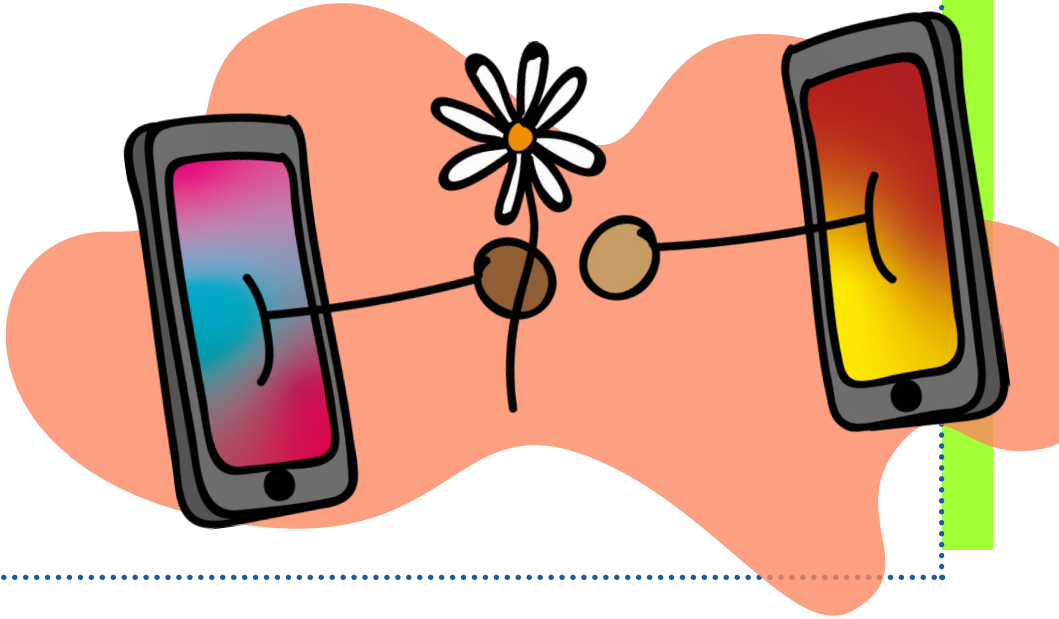
- Desconfiar. No todo lo que aparece en internet es cierto.

- Rompe la cadena. Hay que verificar la información que nos llega a través de las redes sociales o los mensajes de nuestras amistades y familiares y compartirla únicamente cuando tengamos la certeza de que la información es verídica.

- No piques el anzuelo. El **"ciberanzuelo"** ***(clickbait)*** es un término utilizado para describir titulares sensacionalistas, deshonestos o inventados con el fin de que los pinches con tu ratón. Identifícalos y no caigas en ellos.

- Ve la fuente, no te quedes sólo con el titular.

- Encuentra y utiliza fuentes de información fiables. Identifica las fuentes confiables de información en términos científicos, por ejemplo: la Organización Mundial de la Salud (OMS), Instituciones públicas de cada país, universidades o centros de investigación, organizaciones de la sociedad civil o prensa nacional o internacional confiable.



10 minutos

Para cerrar el taller es necesario preguntar si no hay dudas de los temas tratados y si les asistentes quisieran regresar a algún punto.

Haz un repaso general de los temas vistos:

- ¿Qué es el **adultocentrismo**?

- ¿Qué son los **derechos digitales**?

- ¿Cuáles son algunos de los **riesgos** de navegar en internet?

- ¿Qué podemos hacer para **cuidarnos** en internet?

- ¿Qué es una **contraseña segura**?

Después del repaso general y colectivo se entregan las hojas de apoyo Anexo 1.

Tienen 5 minutos para dibujar o escribir en su hoja.

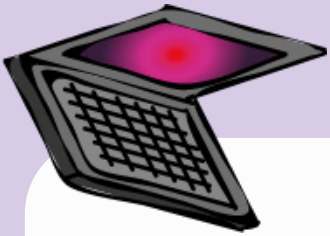
Para cerrar el taller pide que expresen en una palabra cómo se van después de haber compartido esa experiencia.

Ejemplos:

-Contenta, reflexivo, triste, aburrida, cansade.

ANEXO 1

¿Qué es lo qu
el día d



Puedes dibuj

ue aprendiste
le hoy?

jar o escribir

Referencias

Riesgos

ONU Mujeres (2020). Violencia contra mujeres y niñas en el espacio digital: lo que es virtual también es real. https://mexico.unwomen.org/sites/default/files/Field%20Office%20Mexico/Documentos/Publicaciones/2020/Diciembre%202020/FactSheet%20Violencia%20digital.pdf

Ciudad defensora. (2023), "Derechos digitales", Ciudad defensora, Revista de derechos humanos, 24. https://cdhcm.org.mx/wp-content/uploads/2023/05/Ciudad-Defensora-24.pdf

Seguridad Digital

Hijas de Internet. (2021). La Internet tambien es de las infancias. https://descargas.lacnic.net/lideres/2021/luisa-alfaro/VERSION%20FINAL%20AMIGABLE_La%20Internet%20tambie%CC%81n%20es%20de%20las%20Infancias.pdf

Hijas de internet. (02 de mayo de 2022). "S1. EP3. La seguridad digital de NNA", [Podcast], Spotify. https://anchor.fm/hijas-de-internet/episodes/S1–EP3–La-seguridad-digital-de-NNA-e1hunde

Hijas de internet. (04 de octubre de 2020). "T1 EP2. Ciberseguridad", [Podcast], Spotify. https://anchor.fm/hijas-de-internet/episodes/T1-EP2–Ciberseguridad-ekjlbd

Hijas de internet. (14 de febrero de 2022). Seguridad digital con perspectiva de género. Vita-Activa. https://vita-activa.org/seguridad-digital-con-perspectiva-de-genero/

Meta. Protege tu cuenta. https://about.meta.com/es_LA/actions/safety/topics/safety-basics/tools/security/

Social TIC. “Rutas de aprendizaje de seguridad digital”. Protege.la. http://Protege.la

Tactical Tech. “Data detox kit”. Data detox, https://datadetoxkit.org/ee/security/essentials

Teachers’ Essential Guide to Cybersecurity. Common Sense: https://www.commonsense.org/education/articles/teachers-essential-guide-to-cybersecurity

Privacidad Digital

Hijas de internet (abril de 2021). “T2 EP8. Privacidad digital”, [Podcast], Spotify. https://open.spotify.com/episode/6L7j6aAmyndGZENtGnRtdY

INAI, Privacidad en el entorno digital. https://micrositios.inai.org.mx/marcocompetencias/?page_id=657

Internet Society. (12 de enero de 2016). Cuatro Razones Para Cuidar Nuestras Huellas Digitales, [Archivo de Vídeo]. Youtube. https://youtu.be/cpH-zSRV6Ug?si=YFY1XyJsqF4wD8mP

Libres en línea, La privacidad digital es un derecho. https://www.libresenlinea.mx/autodefensa/internet-feminista/la-privacidad-digital-es-un-derecho/

Mejora tu privacidad en línea. Data Detox Kit. https://datadetoxkit.org/ee/privacy/essentials/#step-1

Bienestar Digital

Android. Bienestar Digital. https://www.android.com/intl/es-419_mx/digital-wellbeing/

Comisión Europea. Estudio detallado sobre la Educación del Bienestar Digital: un compendio de prácticas innovadoras y recursos educativos abiertos, Comisión Europea: https://ec.europa.eu/programmes/erasmus-plus/project-result-content/eab5911c-50ac-479e-8070-2e7fa9b942db/DWE-Compendium_Spanish.pdf

Hijas de internet (noviembre de 2020). "T1 EP8. Bienestar digital", [Podcast], Spotify. https://open.spotify.com/episode/3OMyacti2jRNG8j92LUaLW?si=db780349501c42bf

INFOBAE. (2023). #ModoSeguro: la encuesta de bienestar digital que mide la relación que tenemos con la tecnología. [Archivo de Vídeo]. Youtube. https://www.youtube.com/watch?v=NGarodHzsNA

Paz García Pastormerlo (mayo de 2021). Consigue equilibrar el uso de la tecnología a través del bienestar digital. Think With Google. https://www.thinkwithgoogle.com/intl/es-419/futuro-del-marketing/transformacion-digital/consigue-equilibrar-el-uso-de-la-tecnologia-a-traves-del-bienestar-digital/

Desinformacion

Data Detox Kit. 6 consejos para evitar la desinformación en línea. https://datadetoxkit.org/ee/misinformation/steerclear/

Hijas de internet (octubre de 2020). “T1EP4 Infodemia”, [Podcast], Spotify. https://open.spotify.com/episode/2RE-4Py4ggH84nZAJE6zXkQ?si=OVNFhO_GQIOR-SzYVo4I9A

LISA Institute. Deepfakes: Qué es, tipos, riesgos y amenazas. https://www.lisainstitute.com/blogs/blog/deepfakes-tipos-consejos-riesgos-amenazas

Impulso 06. Cómo combatir la desinformación desde el aula. https://impulso06.com/como-combatir-la-desinformacion-desde-el-aula/

Internet Matters. ¿Qué es la desinformación? https://www.internetmatters.org/es/issues/fake-news-and-misinformation-advice-hub/learn-about-fake-news-to-support-children/