CARTILLA

GUÍA PARA UN viaje seguro en Internet

Asociación Aguayo · INTERNET BOLIVIA.ORG · REALIDADES · educo educar cura · ChildFund Bolivia · Save the Children

La *"Guía para un viaje seguro en Internet. Cartilla didáctica sobre habilidades digitales básicas y de mitigación de violencias digitales"*, dirigida a estudiantes de 12 a 17 años, ha sido desarrollada en el marco de un proceso colaborativo entre la Fundación InternetBolivia.org, Save the Children y la Fundación Educación y Cooperación - Educo.

Proyectos Asociados

- **PROSEM: Protegidos, Seguros y Empoderados. Cambiando el mundo en línea y fuera de ella.**
  Coordinador:
  Fernando Rivera Arzabe
  Save the Children

- **Alfabetización digital para la seguridad de la navegación en línea de niñas, niños y adolescentes.**
  Coordinador:
  Marcelo Claros Pinilla
  Educo

Elaborado por

Camilo Arratia Toledo
Sabrina Lanza Bugueño

Revisado por

- **Equipo Save the Children**
  Jimena Tito Rosquellas
  Fabiola Calderón
  Fernando Rivera Arzabe

- **Equipo Educo**
  Marcelo Claros Pinilla
  Mauricio Otasevic
  Wendy Rivera

- **Equipo Childfund**
  Patricia Monje
  Karla Calderón

- **Equipo Fundación InternetBolivia.org**
  Cristian León
  Lisette Balbachan
  Lu An Méndez
  Wilfredo Jordán

Diseño

Marcelo Lazarte

Edición

Primera edición

Impresión

Vértice

Agosto, 2024
La Paz – Bolivia

GUÍA PARA UN viaje seguro en Internet

Cartilla didáctica de habilidades digitales básicas y de mitigación de violencias digitales para estudiantes de 12 a 17 años.

Índice

Presentación

La presente cartilla es una invitación a mejorar tus conocimientos y habilidades en el uso de Internet y las redes sociales que hoy en día forman parte de nuestras vidas. Esto significa no sólo saber cómo funcionan, sino también usarlas de manera segura y respetuosa con las demás personas.

La presente cartilla tiene ocho temas de aprendizaje, cada uno con actividades divertidas y prácticas que podrás realizar ya sea individualmente o en grupo, donde desarrollarás: teoría, es decir, aprender cómo funcionan estas tecnologías; práctica, vale decir, utilizar los servicios y aplicaciones de nuestros teléfonos, computadoras o tablets; y valoración, que quiere decir, pensar y actuar según nuestros valores y evitar peligros.

Te invitamos a que tomes un poco de tu tiempo para explorar estos contenidos, que hacen parte del actual Sistema Educativo Plurinacional, y hagas un viaje seguro en Internet para que lo puedas aplicar en tu vida cotidiana.

Orientaciones

A continuación, te explicamos brevemente cómo abordaremos cada tema desarrollado en esta guía, para que comprendas el proceso de aprendizaje que alcanzarás al aplicarla.

Cada ícono implicará una parte de este proceso

Teoría

Profundizaremos en conceptos y categorías relacionados con el tema del módulo.

Práctica

Fomentaremos la aplicación de este nuevo conocimiento, permitiéndote utilizar lo aprendido y reflexionado en los pasos anteriores de teoría y valoración a través de pequeñas actividades.

Valoración

Nos adueñaremos de criterios que nos capacitarán para reflexionar y analizar nuestra realidad a partir de los contenidos presentados en cada tema.

Para ayudarte en este viaje te presentamos a:

Rasky

Es sabia e inteligente, conocida por su vasto conocimiento en tecnología, aplicaciones y seguridad digital. Siempre lleva una tablet y un pequeño celular en su bolsillo. Enseña a los y las más jóvenes sobre la importancia de proteger sus datos y mantenerse seguros/as en el ciberespacio. Rasky es una mentora generosa y paciente, dispuesta a ayudar a cualquiera que busque aprender más sobre el mundo digital.

Capy

Es fuerte y decidido, un verdadero defensor de los derechos digitales y un apasionado activista. Con su personalidad carismática y su valentía, lucha contra la injusticia en el mundo digital, abogando por la privacidad, la libertad de expresión y el acceso equitativo a la tecnología. Equipado con una pechera llena de herramientas tecnológicas y un escudo. Capy es siempre el primero en la línea de batalla para proteger los derechos de adolescentes.

Chip

Chip es tierna y de buen corazón, conocida por su ingenuidad y su naturaleza inocente. Aunque es extremadamente amable y siempre busca lo mejor en las y los demás, su falta de experiencia en el mundo digital la lleva a encontrarse en situaciones complicadas y de inseguridad en Internet. Chip aprende valiosas lecciones a través de estas experiencias, siempre con una sonrisa en su rostro y una actitud positiva. A menudo busca la ayuda de Rasky y Capy para superar sus desafíos digitales.

Rasky, Capy y Chip te ayudarán en estos nuevos conocimientos

MÓDULO 1

Internet y plataformas digitales

TEMA 1

Introducción a Internet y plataformas digitales

TEMA 2

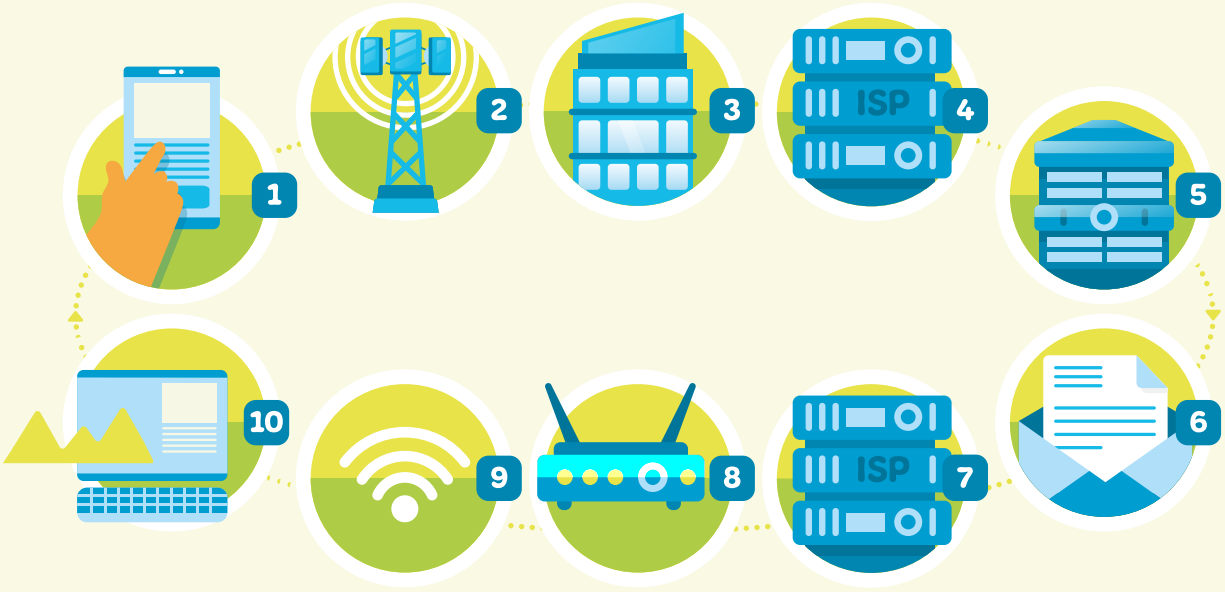
Identidad digital y empatía digital

TEMA 1

Introducción a Internet y plataformas digitales

¿Cómo viaja Internet?[1]

Primero debemos entender a los siguientes actores en Internet



1 10 Dispositivo (como teléfono móvil, tablet, PC o laptop):

Este es el aparato que utilizas para conectarte a Internet y realizar diversas actividades. Es como tu puerta de entrada al mundo digital.

2 Torre celular:

Imagina que esta torre es como una gigantesca antena que envía y recibe señales.

3 Empresa de telecomunicaciones:

Esta es una compañía especializada que te brinda servicios para comunicarte. Pueden ser servicios como hacer llamadas, enviar mensajes de texto o conectarte a Internet.

4 7 Proveedor de Internet:

¿Alguna vez te has preguntado quién te proporciona el acceso a Internet en tu casa o en tu dispositivo? Bueno, eso es precisamente lo que hace un proveedor de Internet. Son como los conductores que te llevan por la autopista de la información en línea.

5 Servidor:

Piensa en el servidor como una especie de supercomputadora que almacena y organiza toda la información que ves en Internet. Todo está guardado en estos servidores y se distribuye a través de la red cuando lo necesitas.

6 Proveedor Webmail:

Cuando creas una cuenta de correo electrónico en línea, estás utilizando los servicios de un proveedor webmail. Ellos se encargan de gestionar tu correo electrónico y asegurarse de que puedas enviar y recibir mensajes de forma rápida y segura.

8 Router:

Este es un dispositivo inteligente que se encarga de dirigir el tráfico de datos entre diferentes redes de computadoras.

9 Señal de Wifi / cable:

¿Cómo se conectan tus dispositivos a Internet? Pueden hacerlo de dos formas principales: a través de una conexión inalámbrica, utilizando una red Wifi, o mediante un cable físico que se conecta a un router o módem.

1 Esta manera de ver cómo funciona Internet pertenece a la currícula formativa - Instituto de Género y Tecnología de Tactical Tech: Disponible en: https://es.gendersec.train.tacticaltech.org/

Imagina que deseas enviar un correo electrónico desde tu dispositivo, ya sea una tablet o un celular 1, a tu amigo/a que está usando una laptop o PC 10. Primero, escribes y envías el correo electrónico desde tu dispositivo. La información viaja desde tu dispositivo hasta la torre celular 2, que la transmite a la empresa de telecomunicaciones 3.

Desde allí, la información se dirige al proveedor de Internet 4 de tu área, quien la envía al proveedor webmail 6, donde se almacena temporalmente en un servidor 5. Una vez que el correo electrónico está en el servidor, el proveedor webmail se encarga de distribuirlo hacia el proveedor de Internet 7 de tu amigo o amiga.

La señal de Wifi o cable 9 lleva la información desde el router 8 del proveedor de Internet de tu amigo o amiga hasta su laptop o PC 10, donde puede leer tu correo electrónico. Este proceso ocurre en cuestión de segundos y es lo que permite que la comunicación por correo electrónico sea tan rápida y efectiva, ¡viajando a través de diferentes dispositivos y redes hasta llegar a su destino final!

Reflexionemos:

¿Sabes qué son las brechas digitales?

Son las desigualdades en el acceso, uso o impacto de las Tecnologías de la Información y la Comunicación (TIC) entre grupos sociales.

Además, la brecha digital afecta en mayor medida a mujeres, adultos mayores y a quienes viven en áreas rurales o remotas.

Actividades

Repasemos a los actores en Internet, relaciona con una flecha cada actor con su respectivo significado

- **Dispositivo (como teléfono móvil, tablet, PC o laptop):**
- **Torre celular:**
- **Empresa de telecomunicaciones:**
- **Proveedor de Internet:**
- **Servidor:**
- **Proveedor Webmail:**
- **Router:**
- **Señal de Wifi/cable:**

- Imagina que esta torre es como una gigantesca antena que envía y recibe señales.
- Ellos se encargan de gestionar tu correo electrónico y asegurarse de que puedas enviar y recibir mensajes de forma rápida y segura.
- Una especie de supercomputadora que almacena y organiza toda la información que ves en Internet.
- ¿Cómo se conectan tus dispositivos a Internet? Pueden hacerlo de dos formas principales: a través de una conexión inalámbrica o mediante un cable físico.
- Este es el aparato que utilizas para conectarte a Internet y realizar diversas actividades. Es como tu puerta de entrada al mundo digital.
- Este es un dispositivo inteligente que se encarga de dirigir el tráfico de datos entre diferentes redes de computadoras.
- Son como los conductores que te llevan por la autopista de la información en línea.
- Compañía especializada que te brinda servicios para comunicarte. Pueden ser servicios como hacer llamadas, enviar mensajes de texto o conectarte a Internet.

¿Cómo es la conexión a Internet en tu casa?

¿Qué grupos vulnerables que no tienen conexión a Internet conoces?

TEMA 2

Identidad y empatía digital

¿Quién soy yo en Internet?

La **identidad digital** es cómo nos mostramos y nos relacionamos en Internet.

La **huella digital** es el rastro que se deja en Internet cada vez que se hace algo "en línea", por ejemplo, cuando publicamos en redes sociales, comentamos en videos o escribimos en blogs.

Ambas son importantes porque pueden influir en cómo nos ven las y los demás y en las oportunidades que tenemos en Internet y en la vida real.

Recuerda:

Que si se publica algo muy personal tuyo, esto podría tener consecuencias en la vida fuera de Internet como problemas en la escuela o con amigos/as. Además de que las personas que quieren ejercer agresiones en Internet usan la información de tu huella digital para estafas, acoso, robo de cuentas, etc.

Seudónimos:

En Internet se usan a veces seudónimos, estos son una máscara que nos protege de que la gente utilice nuestra información para hacernos daño. Aunque recuerda que también algunos usan estos seudónimos para hacer daño.

Chip y Rasky están en el bosque reflexionando sobre lo aprendido.

Reflexionemos:

Es importante ser conscientes de lo que compartimos y cómo nos comportamos en línea, para construir una identidad digital que refleje quiénes somos realmente y nos ayude a tener una experiencia positiva en el mundo digital.

Así como respetar las identidades digitales de las personas de nuestro entorno.

Actividades

A continuación responderemos las siguientes preguntas para entender y reflexionar sobre nuestra realidad:

- ¿Qué información nos puede poner en riesgo?
- ¿Qué información nuestra preferimos que no sea pública?
- ¿Qué tipo de información mía no me gustaría que esté en Internet?

Hagamos un plan para cuidar nuestra identidad digital y la de nuestro entorno.

Lo haremos respondiendo las siguientes preguntas (puedes usar una hoja aparte)

- ¿Qué información o situaciones voy a compartir en mis redes sociales? ¿Por qué?
- ¿Qué información o situaciones no voy a compartir en mis redes sociales? ¿Por qué?
- ¿Con quiénes voy a compartir la información en mis redes sociales? (¿El contenido será público sólo para contactos o seguidores?)
- ¿Cómo voy a cuidar la información de mis amigas, amigos, hermanos, hermanas y familiares? (Por ejemplo: pedir permiso para etiquetar, mostrar o nombrar personas en las fotos y videos publicados)
- ¿Qué haré para cuidar la huella digital de otras personas cuando reciba un video de alguien sin su autorización?

¿Qué es la empatía digital?

La **empatía digital** es la capacidad de ser consciente, sensible y apoyar los sentimientos, necesidades y preocupaciones de uno/a mismo/a y de los/as demás en el entorno en línea.

En el contexto digital, esto implica reconocer cómo nuestras palabras y acciones pueden afectar emocionalmente a otros/as y actuar de manera compasiva y respetuosa.

Importancia de la empatía digital

En el mundo digital, las interacciones carecen de las señales no verbales que tenemos en la comunicación cara a cara, como el tono de voz y el lenguaje corporal. Esto puede llevar a malentendidos y comportamientos hirientes.

Acciones para practicar la empatía digital

- **Piensa antes de publicar:** Reflexiona sobre el impacto de tus palabras. Evita comentarios impulsivos y revisa lo que escribes antes de enviarlo.
- **Usa un lenguaje positivo:** Elige palabras que sean amables y constructivas. Incluso si tienes una crítica, exprésala de manera respetuosa.
- **Escucha activamente:** En las conversaciones en línea, muestra interés genuino por las opiniones y sentimientos de los/as demás. Haz preguntas y muestra comprensión.
- **Ofrece apoyo:** Si ves que alguien está siendo atacado/a o está pasando por un mal momento, bríndale tu apoyo. Un mensaje de aliento puede marcar una gran diferencia.
- **Aprende a disculparte:** Si cometes un error y lastimas a alguien, pide disculpas sinceramente. Reconocer tus errores es una muestra de madurez y empatía.

Actividades

Vamos a practicar y reflexionar sobre empatía digital

- Describe una interacción en línea reciente (mensaje, comentario, publicación, etc.) en la que te sentiste bien.
  - ¿Qué hizo que esta interacción fuera positiva?
  - ¿Cómo te sentiste después de la interacción?

- Describe una interacción en línea reciente que no fue positiva.
  - ¿Qué hizo que esta interacción fuera negativa?
  - ¿Cómo te sentiste después de la interacción?

- Piensa en una situación en la que alguien te haya apoyado en línea.
  - ¿Qué hizo esta persona para mostrarte apoyo?
  - ¿Cómo te hizo sentir su apoyo?

MÓDULO 2

Filtrado, consumo responsable y trabajo colaborativo

TEMA 1

Navegadores, motores de búsqueda e inteligencia artificial

TEMA 2

Consumo responsable

TEMA 1

Navegadores, motores de búsqueda e inteligencia artifical

¿Qué es un navegador web?

El navegador web es la herramienta que utilizamos para acceder y explorar el mundo de Internet. Es decir, una puerta de entrada que nos permite navegar por diferentes páginas web, acceder a contenido multimedia, realizar compras en línea y mucho más.

¿Ejemplos de navegadores web?

Google Chrome, Mozilla Firefox, Safari y Microsoft Edge.

Y ¿qué es un motor de búsqueda?

El motor de búsqueda es el mecanismo que nos ayuda a encontrar información específica dentro de Internet. Funciona recopilando datos de millones de páginas web y proporcionándonos resultados relevantes a nuestras consultas y palabras claves.

¿Ejemplos de motor de búsqueda?

Google, Bing, Yahoo y DuckDuckGo.

Lo que debes saber antes de navegar:

- Para lograr una mejor búsqueda de información, consulta al menos tres páginas diferentes (o más) para contrastar los datos y asegúrate de que sean recientes.
- Identifica si la página es seria: Es decir, que debe tener las fechas en las que fue publicado el contenido, la fuente de los datos, la dirección y contacto de la institución.
- Usa la búsqueda avanzada (por imágenes, videos, documentos, mapas) para tener resultados más precisos, o aplica comandos como por ejemplo agregar comillas a las palabras para que las búsquedas coincidan exactamente con éstas.

Inteligencia artificial (IA) generativa

Hemos escuchado muchísimo en los últimos años la palabra inteligencia artificial (IA). Por eso, es importante saber qué es la IA, sus alcances y los cuidados que debemos tener.

¿Qué es la inteligencia artificial generativa?

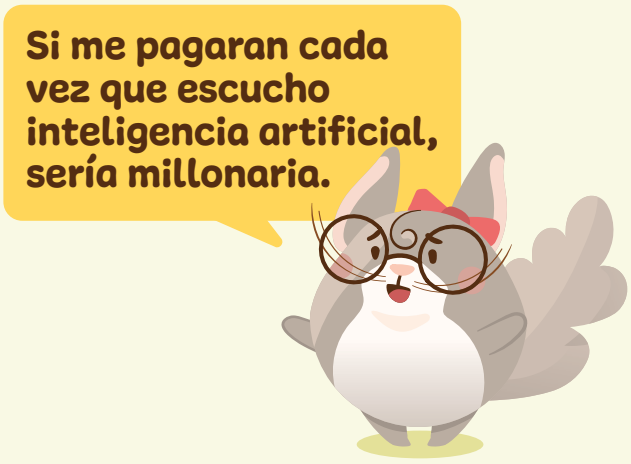
La inteligencia artificial generativa se refiere a un tipo de IA capaz de generar contenido nuevo, como texto, imágenes o música, imitando el estilo y patrones aprendidos de datos de entrada.

¿Cómo funciona la IA?

- **Transformers:** La IA usa algo llamado “transformers”. Son como herramientas que le ayudan a entender lo que le decimos.
- **Capas:** Imagina que estas IA están formadas por muchas capas, como si fueran escalones en una escalera. Cada capa le ayuda a entender un poco más lo que le estamos preguntando.
- **Aprendizaje:** Las IA aprenden leyendo muchos textos. Cuanto más lee, más inteligente se vuelve. Es decir, mientras tenga más información, logrará mejores respuestas.

Para entender mejor, aquí mencionamos algunos ejemplos:

- **Asistencia al cliente:** Ejemplo de cómo la IA generativa se utiliza para brindar soporte y responder preguntas de los clientes en sitios web.
- **Redacción automática:** Ayudan a la redacción de correos electrónicos, informes y otros documentos (debes tener en cuenta que no razona como los humanos).
- **Creación de contenido:** Generación de contenido para redes sociales, blogs o medios de comunicación.



Chip prueba un nuevo asistente de inteligencia artificial en su computadora.

A paso lento pero seguro con la IA

- Es importante saber que la IA es sólo una herramienta, así que no la conviertas en tu única fuente de consulta, ni con la que haces todas tus tareas. ¿Cómo la piensas usar?
- No todo lo que responde la IA es cierto, así que ten el cuidado de verificar los datos que te brinda.
- La IA puede ser una buena fuente de consulta, por ejemplo, le puedes preguntar dónde encontrar bases de datos de un tema en específico.
- ¿Qué datos piensas darle a la IA? Te recomendamos que sean generales y no específicos ni personales.
- Recuerda ademas que la información de la IA tiene sesgos en grupos menos representados como pueblos indígenas.

Actividades

Enlaza las respuestas a las situaciones

- Chip quiere ingresar a una página web de recetas bolivianas, entonces tiene que ingresar la página en un...
- Chip escribió un informe de las poblaciones de chinchillas en Bolivia y quiere asegurarse de que la ortografía está bien. Para corregirlo, podría pedirle una revisión a una...
- Chip quiere encontrar imágenes de las reservas de chinchillas en Chile. Tendría que ingresar a un...

- Navegador
- Motor de búsqueda
- Inteligencia artificial

Practica IA en tu casa

- En tu casa usa ChatGPT para pedirle recetas de comidas bolivianas.
- Compáralas con las recetas de tu abuela o de tu mamá.

Reflexiona:

* ¿Qué impacto tienen las IA generativas en la creatividad humana?

* ¿Hasta qué punto las IA generativas pueden ser consideradas como creadoras genuinas?

* ¿Qué implicaciones tienen las IA generativas en la industria del entretenimiento y la cultura popular?

TEMA 2

Consumo responsable

¿Cómo consumir contenido en Internet?

Debemos ser capaces de filtrar y distinguir los contenidos confiables de aquellos falsos o en los que nos falta información. La desinformación son esos contenidos con poca evidencia y que normalmente causan una emoción, como el enfado o indignación.

Consejos para un consumo responsable:

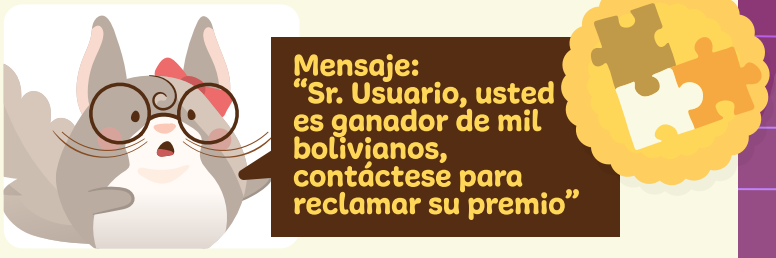
- **Evalúa la fuente:** Verifica quién publica el contenido, y si es anónimo, no es una fuente confiable[2].
- **Distingue si hay pruebas de lo que se dice:** ¿Hay datos estadísticos, estudios, testimonios, hechos o pruebas de lo que se dice?
- **Analiza cuánto sabes del tema:** ¿Sé mucho o poco del tema? Si no sabes mucho es bueno reconocerlo para buscar más información y no creer lo que se dice a la primera.
- **Chequea siempre:** Aunque conozcas a la persona que comparte una foto, un video o un texto, puede que el contenido sea falso. Todos/as podemos equivocarnos, así que verifica si es verdadero.
- **Identifica sesgos:** ¿Estoy compartiendo este contenido sólo porque pienso que está bien? No basta sólo con apoyar lo que compartes, debes asegurarte de que se trate de un contenido real.
- **Presta atención a los contextos y emociones.** ¿Estamos en un tiempo electoral o de conflicto social? ¿Este contenido me causa enojo? Si las respuestas son afirmativas, es posible que se trate de desinformación.
- **Busca el contenido en motores de búsqueda:** Si se trata de algo falso, es posible que alguna verificadora de noticias ya lo haya identificado.
- **Aplica la escucha activa:** Haz notar que alguien comparte un contenido falso de manera constructiva y si tú has cometido un error, reconócelo y aplica lo aprendido.

2 Estos consejos fueron extraídos de una guía de cómo identificar desinformación de la verificadora Chequeado. Disponible en: https://chequeado.com

Antes de la invención de Internet, recibíamos información de los medios de comunicación tradicionales como la radio, televisión y periódicos. Mientras que ahora, como usuarios/as de Internet, podemos consumir y producir contenidos. Es decir, somos "prosumidores". Esto generó la producción enorme de contenidos disponibles en páginas web y redes sociales. La sobreproducción de contenidos facilita que seamos víctimas de engaños y desinformación.

Actividades

Chip acaba de recibir un mensaje, vamos a ver de qué se trata:



¿Qué acciones debería tomar Chip?
(subraya las respuestas correctas)

- No proporcionar información personal ni responder al mensaje hasta confirmar la legitimidad del concurso.
- Creer de manera inmediata que ha ganado un premio sin verificar la autenticidad del mensaje.
- Consultar con amigos/as o familiares para obtener opiniones sobre la situación.
- Compartir el mensaje con más personas sin verificar su autenticidad.
- Contactar a la empresa organizadora del concurso para verificar la autenticidad del premio.
- Ignorar por completo el mensaje y no tomar ninguna acción al respecto.
- Buscar en línea reseñas y comentarios sobre la empresa o el concurso para detectar posibles estafas.
- Proporcionar de inmediato la información solicitada para reclamar el premio.

MÓDULO 3

Privacidad y ciberseguridad en entornos educativos

TEMA 1

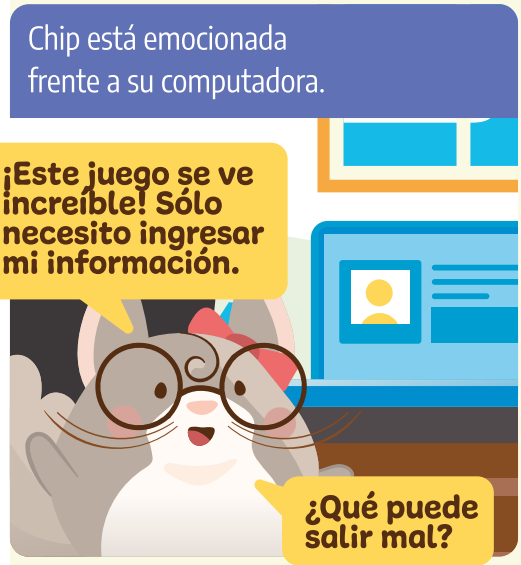
Datos personales

TEMA 2

Privacidad y seguridad en línea

TEMA 1

Datos personales



¿Qué son los datos personales?

Datos personales:

Un dato personal es la información sobre una persona que permite identificar, localizar o contactar a una persona física. Estos datos pueden ser numéricos, alfabéticos, fotográficos, biométricos, entre otros.

Tipos de datos personales

- **Generales:** Información que permite identificar, localizar o contactar de forma directa o indirecta a personas naturales.

Ej. Nombre, carnet identidad, dirección, fotos con uniforme de la unidad educativa, etc.

- **Sensibles:** Datos personales que se refieren a la intimidad de una persona y que se pueden usar para hacer daño o generar discriminación.

Ej. Historia médica, tus datos bancarios, etc.

- **Biométricos:** Referidos al cuerpo de una persona que posibiliten o aseguren su identificación única.

Ej. Huella digital, cara, voz, etc.

¿Es importante proteger nuestros datos personales?

Es crucial comprender la importancia de proteger nuestros datos personales en línea. La divulgación de información sensible puede exponernos a una serie de riesgos, desde el robo de identidad hasta la intrusión en nuestra privacidad. Al proteger nuestros datos personales, podemos reducir la probabilidad de convertirnos en víctimas de estos riesgos.

Actividades

Responde verdadero (V) o falso (F) a las siguientes situaciones:

- Si un perfil extraño me envía una solicitud de amistad, debo aceptarla para tener más amigos/as en las redes sociales: V F
- Al compartir imágenes en las redes sociales, es mejor si señalo mi ubicación actual, ocupación o datos familiares: V F
- Si recibo un mensaje inapropiado de un extraño en una red social, en lugar de responder, debo informar de inmediato a un adulto/a de confianza sobre la situación para obtener ayuda y orientación: V F
- Si recibo un mensaje que indica que gané un concurso al que nunca postulé, seguramente es verdad y debo seguir todos los pasos que me indique para recoger mi premio: V F
- Es necesario aprender a configurar la privacidad en nuestro perfil de redes sociales: V F
- Se deben considerar cuidadosamente los aspectos de privacidad, seguridad y uso de datos antes de proporcionar nuestro nombre completo para la suscripción a un juego en línea: V F

Reflexionemos

Debemos ser selectivos/as sobre la información que compartimos en Internet, utilizar contraseñas seguras, revisar y ajustar la configuración de privacidad en nuestras cuentas en redes sociales y estar alerta ante posibles intentos de fraude o robo de información.

TEMA 2

Privacidad y seguridad en línea

¿Cómo tener una contraseña segura?

Una contraseña segura es una clave que protege tu cuenta en línea de accesos no autorizados. Para ser segura, una contraseña debe cumplir con varios criterios.

Criterios

- **Longitud:** Debe tener al menos 12 caracteres.
- **Variedad de caracteres:** Debe incluir una combinación de letras mayúsculas, letras minúsculas, números y caracteres especiales (como: !, @, #, $, etc.).
- **No ser obvia:** No debe incluir información personal fácilmente adivinable, como tu nombre, fecha de nacimiento o palabras comunes.
- **Única:** Debe ser diferente para cada cuenta que tengas.

Te muestro unos ejemplos de contraseñas seguras:

- Ch!pR0cks2024!
- Pa$$w0rd@Ex@mple
- 7r!ckyP@ssw0rd
- Un1qu3&Str0ng!

Estas contraseñas son seguras porque combinan diferentes tipos de caracteres y no son fácilmente adivinables. Además, es recomendable usar un gestor de contraseñas para mantener un registro seguro de tus contraseñas y facilitar la creación de contraseñas únicas y complejas para cada cuenta.

La verificación de 2 pasos es una capa extra de seguridad para tus cuentas en Internet.

Además de tu contraseña, te pide un código adicional que se envía a tu teléfono o se genera en una app (aplicación móvil). Esto asegura que sólo tú puedas acceder a tu cuenta, incluso si alguien más tiene tu contraseña.

Es como tener una cerradura extra en tu puerta. Mantiene tus cuentas más seguras y te protege contra los hackers. ¡Es una manera fácil y efectiva de cuidar tu información en línea!

Pero no es suficiente, también debes saber qué es la verificación de 2 pasos.

Actividades

Completa las frases:

Lee las frases incompletas sobre seguridad en Internet y complétala con la palabra o palabras que mejor se ajusten a la oración.

2 pasos **gestor** **segura** **contraseña**

- Es importante utilizar una contraseña _____ para proteger tu cuenta en Internet.
- La verificación de 2 pasos agrega una capa adicional de seguridad al requerir _____ para acceder a una cuenta.
- Un _____ de contraseñas puede ayudarte a gestionar y recordar contraseñas seguras para tus cuentas en Internet.
- No es seguro compartir tu _____ con personas desconocidas o en sitios web no confiables.

Practiquemos cómo crear una contraseña segura

- Construye una frase:

- Ahora reemplaza algunas letras por números como en la siguiente tabla:

La I por 1	La A por 4
La E por 3	La S por 5
La T por 7	La B por 8
La O por 0	

- Ahora escribe la frase resultante:

Reflexionemos

Es importante tener una contraseña segura, pero también existen otras formas de mantener tu seguridad en línea, como la verificación de 2 pasos, el uso de gestores de contraseñas y más.

MÓDULO 4

Prevención de violencias digitales

TEMA 1

Mitos de la violencia digital

TEMA 2

Violencia digital en el noviazgo

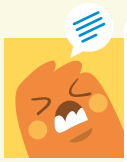
TEMA 1

Mitos de la violencia digital

¿Existe la violencia digital?

La violencia digital o en línea, se refiere a actos de violencia cometidos, instigados o agravados, en parte o totalmente, por el uso de las Tecnologías de la Información y la Comunicación (TIC), plataformas de redes sociales y correo electrónico. Estas violencias causan daño psicológico y emocional, refuerzan los prejuicios, dañan la reputación, causan pérdidas económicas y plantean barreras a la participación en la vida pública y pueden conducir a formas de violencia sexual y otras formas de violencia física.

Tipos de violencia digital en entornos educativos



Ciberacoso

Conductas frecuentes que resultan hostiles, molestas, intimidantes y perturbadoras.

Por ejemplo: Sofía es una niña de 11 años que no es muy buena en deportes y suele ser la última en ser elegida para los equipos en sus clases de deporte. En el chat del grupo, cuando alguien hace referencia a juegos o competencias deportivas, algunos niños envían stickers con la imagen de Sofía tropezando y frases como: "La campeona de las caídas" o "Sofía siempre al último.".

Difamación

Descalificación de la trayectoria credibilidad o imagen pública de una persona en medios digitales.

Por ejemplo: Marcela es la mejor alumna del curso, pero en un grupo de WhatsApp del colegio retocan una foto con ella haciendo trampa en el examen y se vuelve viral.

Difusión de imágenes tuyas o de tu familia sin consentimiento

Compartir o publicar sin consentimiento imágenes íntimas.

Por ejemplo: Carla es una niña que sube una imagen de su familia a sus redes sociales, pero se entera de que alguien desconocido la pudo descargar y la está difundiendo.

Amenazas

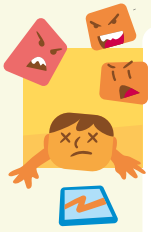
Mensajes con contenido agresivo que manifiestan una intención de hacer daño a la persona, a sus familiares o bienes.

Por ejemplo: Gabriela recibe mensajes en los cuales les piden hacer ciertas cosas, diciéndole que le provocarán daño a ella o a su familia si no lo hace.

Grooming

Acoso ejercido por un adulto hacia una niña, niño o adolescente y se refiere a acciones realizadas deliberadamente para establecer una relación y control emocional con fines sexuales.

Por ejemplo: Cuando una persona adulta se hace pasar por un niño o niña de tu edad en Internet para contactarse contigo, ganar tu confianza y solicitarte fotos o videos íntimos.



Cyberbullying

El cyberbullying, también denominado acoso escolar entre pares en línea, ocurre cuando una persona, de forma intencionada y repetida, ejerce su poder o presión sobre otra mediante el uso de dispositivos en línea y de forma maliciosa, con comportamientos agresivos, tales como insultar, molestar, abusar verbalmente, amenazar, humillar, etc.

Por ejemplo: Cuando una niña o niño por medio de perfiles falsos escribe a su compañero/a de curso mensajes insultantes y amenazantes.

Actividades

Identificando violencias digitales

Instrucciones:

Lee cada situación y decide a qué tipo de violencia digital corresponde.

Situaciones:

- Juan es constantemente ridiculizado con memes y comentarios hirientes sobre su apariencia y rendimiento académico en un chat grupal.
- Marcela es acusada falsamente de hacer trampa en un examen a través de una imagen manipulada que se comparte en un grupo de Instagram.
- Carla descubre que su expareja ha compartido imágenes íntimas de ella sin su consentimiento después de su ruptura.
- Un adolescente recibe mensajes amenazantes en sus redes sociales, donde se le advierte de hacer daño a su familia si no cumple ciertas demandas.
- Un adulto se hace pasar por un adolescente en línea para ganarse la confianza de una niña y solicitarle fotos íntimas.
- Un adolescente crea perfiles falsos para enviar insultos y amenazas a su compañero/a de clase en las redes sociales.

TEMA 2

Violencia digital en el noviazgo

Situaciones de violencia digital en pareja

- Tu expareja te ha pedido la contraseña de tu celular y/o redes sociales.
- Tu expareja te ha pedido insistentemente o te ha obligado a compartir tu ubicación.
- Tu expareja te ha pedido insistentemente o te ha obligado a compartir fotos íntimas.
- Tu expareja ha compartido fotos tuyas en redes sociales sin tu permiso.
- Tu expareja ha controlado tus relaciones de amistad en redes sociales (con quién chateas, a quién agregas, etc.).

Si has experimentado lo siguiente, debes saber que sufriste violencia digital en pareja.

Además, no olvides que el experimentar esta violencia tiene diversos efectos.

Efectos de la violencia digital

Impacto psicológico: Las repercusiones en la salud mental son significativas, por ejemplo, síntomas depresivos, angustia, tristeza y soledad.

Perjuicios económicos: Pueden producirse cuando la imagen de una víctima de abusos cibernéticos aparece en varias páginas de resultados de los buscadores, lo que dificulta a la víctima la obtención de empleo o su conservación. Además, puede frenarla a buscar oportunidades laborales.

Autocensura: Quienes enfrentan violencias digitales recurren a retirarse de la vida pública, familiar y social y aislarse.

Daños físicos: La violencia digital puede ocasionar daños físicos haciendo que las niñas y niños que la sufren se lastimen a sí mismos.

Actividad

A continuación, harás una actividad en tu casa, lee las siguientes instrucciones y sé creativo/a:

Carteles creativos "Digitalmente seguros"

Objetivo: Diseñar carteles creativos que transmitan mensajes positivos sobre la importancia de la seguridad en línea y la prevención de la violencia digital en tu curso:

Materiales necesarios:

- Papel grande o cartulina.
- Lápices de colores, marcadores, crayones, etc.
- Hojas de ideas o notas sobre temas relacionados con la seguridad en línea y prevención de violencia digital.

Pasos a seguir:

1. Lluvia de ideas:

- Dedica unos minutos a pensar en ideas sobre mensajes positivos y creativos relacionados con la seguridad en línea y prevención de violencia digital.
- Anota estas ideas en una hoja de papel o en tu celular para utilizarlas durante la creación de tu cartel.

2. Planificación:

- Planifica el diseño de tu cartel, incluyendo el esquema de colores, el texto y los dibujos que utilizarás.
- Utiliza las ideas que generaste durante la lluvia de ideas para inspirar tu diseño.

3. Creación:

- Una vez que tengas tu planificación lista, comienza a crear tu cartel en casa.
- Utiliza los materiales artísticos que tengas disponibles, como lápices de colores, marcadores, crayones, etc.
- Sé creativo y original en tu diseño.

4. Presentación:

- Una vez que hayas completado tu cartel, tómale una foto.
- Comparte la foto de tu cartel en un espacio compartido en línea o Internet, como un grupo de mensajería o en tu curso, para que pueda ser visto por tus compañeros/as y profesores/as.

5. Reflexión:

- Después de terminar tu cartel, tómate un momento para reflexionar sobre el proceso de creación y el mensaje que has transmitido.
- Comenta y discute los carteles creados por tus compañeros/as en el espacio compartido en línea.

La violencia digital es un hilo de continuidad de la violencia estructural. Con frecuencia se ejerce contra poblaciones históricamente discriminadas.

Además, pasa muy frecuentemente en nuestras unidades educativas y fuera de ellas, porque no tiene espacio geográfico definido.

Es momento de hacer algo, ¿nos acompañas?

Recursos útiles

Links

- www.cuidadosdigitales.com
- www.pantallasamigas.net
- www.datadetoxkit.org/ee/families/datadetox-x-youth
- www.causasdigitaleslac.editorx.io/mysite
- www.digimente.org

Material de consulta

Save the Children Digital Citizenship Competency Framework
Marco de inclusión digital e intercultural

¿Necesitas apoyo?

No estás solo/a

Líneas de apoyo

La Paz – El Alto

Centro S.O.S. Digital, línea de apoyo 62342430

Policía Boliviana

Fuerza Especial de
Lucha contra la Violencia 800 14 0348

Sucre

salvaguarda@realidadesbolivia.org
Centro Yachaywasi 67869650
Realidades 6435612

Defensorías de la niñez y adolescencia (DNA) y Servicios Legales Integrales Municipales (SLIM)

DNA y SLIM – La Paz ..... 156 (Línea de emergencia)
DNA y SLIM – El Alto ..... 800164343 – 2836200 (Línea de emergencia)
DNA y SLIM - Sucre ..... 71160187 (Línea corporativa)

Qué SÍ hacer y NO hacer en línea

Recomendaciones para adolescentes sobre habilidades digitales y prevención de violencias

Qué SÍ hacer

1 Cuida tu imagen virtual
Tu imagen en línea construye lo que otros piensan de ti.

2 Elige un buen entorno
Busca un lugar cómodo en tu hogar para participar en actividades en línea. Evita que otras personas aparezcan en cámara.

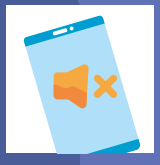
3 Haz comentarios respetuosos
Sé amable al comentar y aportar en línea.

4 Respeta la privacidad
Trata la privacidad de los y las demás como te gustaría que respeten la tuya.

5 Mantén un ambiente agradable
Contribuye a un ambiente confiable y positivo.

6 Reacciona con calma
Si algo te molesta, reacciona de manera calmada y no violenta.

7 Usa los dispositivos adecuadamente en clase
Mantén tu teléfono y otros dispositivos en modo silencioso durante las clases presenciales. Úsalos sólo cuando sea permitido y necesario.



8 Respeta a los y las demás en entornos presenciales
No interrumpas ni distraigas a tus compañeros/as con el uso de dispositivos. Sigue las reglas establecidas en tu familia, en la escuela o en los espacios en los que te encuentres.

Qué NO hacer

1 No publiques datos personales
Evita compartir tu número de teléfono, dirección o información de tu escuela.

2 No te reúnas con desconocidos/as en persona
Si alguien en línea quiere reunirse contigo, avisa a tu padre/madre.

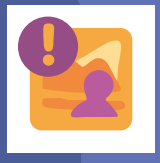
3 No respondas a mensajes negativos
Elimina correos o publicaciones malas, desagradables o groseras.

4 Sal de chats incómodos
Si alguien te hace sentir incómodo/a en un chat, sal de inmediato.

5 No descargues software sin permiso
Consulta con tu padre/madre antes de instalar algo en tus dispositivos.

6 No compartas tu contraseña
Mantén tus contraseñas seguras y no las compartas con nadie.

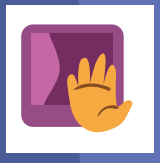
7 Informa sobre contenido inapropiado
Avisa a tu padre/madre si ves malas palabras, imágenes o videos inapropiados en línea.



8 Desconfía de ofertas demasiado buenas
Si algo parece demasiado bueno para ser verdad, probablemente es una trampa.

9 No publiques fotos sin permiso
Pide autorización antes de compartir fotos o videos.

10 No publiques fotos inapropiadas
Evita compartir fotos inapropiadas de ti mismo/a, tu familia o amigos/as.



Fuente:

- Consideraciones éticas de trabajo en proyectos con niñas, niños y adolescentes de la Fundación InternetBolivia.org https://internetbolivia.maadix.org/nextcloud/index.php/s/XzjHsSfLLAPwTYw
- Política de salvaguarda Save the Children.
- Política de salvaguarda Educo.


Asociación Aguayo
INTERNET BOLIVIA .ORG
REALIDADES
educo
educar cura
ChildFund
Bolivia
Save the Children