GUÍA

SEGURIDAD DIGITAL Y PREVENCIÓN DE VIOLENCIAS: UNA GUÍA PARA EDUCADORES

Asociación Aguayo
INTERNET BOLIVIA .ORG
educo educar cura

Seguridad digital y prevención de violencias: una guía para educadores, ha sido desarrollada en el marco de un proceso colaborativo entre la Fundación InternetBolivia.org, Asociación Aguayo y la Fundación Educación y Cooperación - Educo.

Elaborado por:
Camilo Arratia y Wilfredo Jordán

Revisado por:
Equipo InternetBolivia.org:
Cristian León, Lisette Balbachan y Lu An Méndez

Equipo Educo:
Marcelo Claros, Mauricio Otasevic y Wendy Rivera

Proyecto asociado:
Alfabetización digital para la seguridad de la navegación en línea de niñas, niños y adolescentes *(Educo, InternetBolivia.org y Asociación Aguayo).*

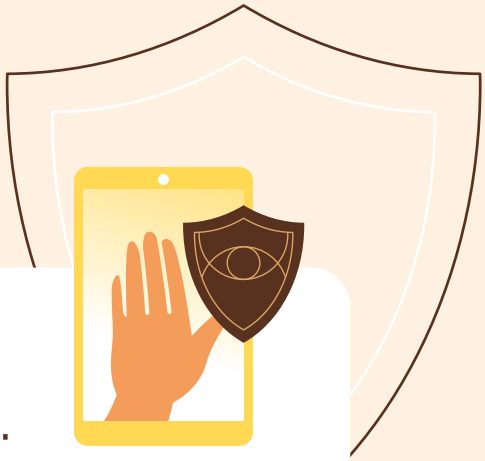
Diseño y diagramación:
Marcelo Lazarte

Impresión:
CODIGO M

Enero, 2025

La Paz – Bolivia

GUÍA



SEGURIDAD DIGITAL Y PREVENCIÓN DE VIOLENCIAS: **UNA GUÍA PARA EDUCADORES**

ÍNDICE

INTRODUCCIÓN

En la era digital actual, el acceso a Internet y a las Tecnologías de Información y Comunicación (TIC) ha transformado la manera en que las y los estudiantes aprenden, se comunican y se relacionan con el mundo que les rodea. Sin embargo, junto con estas oportunidades, también surgen nuevos desafíos que requieren una atención cuidadosa, especialmente en lo que respecta a la violencia digital, el uso crítico de las tecnologías y la protección de la privacidad.

La violencia digital se ha convertido en una preocupación creciente en las escuelas, ya que se manifiesta de diversas formas, como el ciberacoso, la suplantación de identidad, el grooming, entre otros. Es fundamental que educadores y estudiantes comprendan qué es la violencia digital, sus efectos y la importancia de prevenirla, así como habilidades básicas de seguridad digital.

Además, es crucial fomentar un pensamiento crítico en el uso de las tecnologías. Internet, aunque es una herramienta poderosa para el aprendizaje, a menudo reproduce cánones de belleza y éxito que pueden ser poco reales y perjudiciales. Es vital que las y los estudiantes desarrollen la capacidad de discernir entre la información veraz y la desinformación, aprendiendo a evaluar la calidad de las fuentes que consultan. La autorregulación y el establecimiento de límites en el uso de dispositivos de conexión (tabletas, computadoras, teléfonos celulares) también son estrategias clave para cuidar la salud mental y emocional de las niñas, niños y adolescentes, en lugar de simplemente prohibir el uso de estos aparatos.

Finalmente, el uso responsable de Internet también implica aprovechar sus características como herramienta colaborativa. Las plataformas digitales pueden facilitar la comunicación y el trabajo en equipo, permitiendo que las y los estudiantes se conecten y aprendan juntos, sin importar la distancia física. Con un enfoque en la protección de la privacidad, la búsqueda de información de calidad y el equilibrio entre el aprendizaje digital y otras formas de educación, podemos preparar a las y los estudiantes a navegar por el mundo digital de manera segura y eficaz.

Este documento busca ofrecer una guía práctica y educativa para maestras/os y directoras/es, abordando la prevención de la violencia digital, fomentando el pensamiento crítico en el uso de tecnologías y promoviendo Internet como una herramienta favorable y segura en el ámbito educativo.

1 ¿QUÉ ES LA **VIOLENCIA DIGITAL**?

LA BROMA QUE DUELE

El profesor Javier está dando una lección sobre el uso responsable de la tecnología cuando nota que algunos estudiantes se ríen al ver algo en sus teléfonos.

Objetivo: Enseñar a nuestros/as estudiantes que debemos ser empáticos y responsables en línea, como comunidad educativa debemos crear así un ambiente seguro en el aula.

La violencia digital es un tipo de agresión que se ejerce mediante tecnologías digitales como Internet, las redes sociales y los dispositivos electrónicos. Se caracteriza por el uso de estas herramientas para intimidar, acosar, humillar, difamar o controlar a una persona.

Esta violencia incluye manifestaciones como el ciberbullying, la difusión de información personal o imágenes privadas, el grooming (engaño con fines de violencia sexual), la suplantación de identidad o la vigilancia. Es una extensión de las violencias que ocurren en el mundo físico, pero con el agravante de que puede tener un impacto masivo y continuo debido a su permanencia y difusión en Internet.

1.1 **FORMAS** DE LA VIOLENCIA DIGITAL

En nuestro país aún no existe un consenso sobre los tipos y formas de violencia digital en entornos educativos; sin embargo, sí es posible mencionar sus expresiones más recurrentes:

FORMAS DE VIOLENCIA DIGITAL	EJEMPLO
Ciberbullying (acoso escolar en línea) Es el conjunto de acciones que se realizan a través de medios digitales para generar malestar o molestar, atacar o alarmar a un/a compañero o compañera de una unidad educativa.	Un/a compañero/a de curso crea stickers de WhatsApp con imágenes editadas sobre otra/o compañera/o y lo comparte en un grupo para burlarse o hacerle quedar mal.
Doxing Es el uso y/o difusión de datos personales sin autorización para generar daño.	Cuando alguien introduce sus datos personales (Ej. teléfono o dirección) en algún registro electrónico y posteriormente estos datos se hacen públicos o son usados para enviar mensajes intimidantes.
Suplantación de identidad Cuando alguien usa los datos personales de otra persona para hacerse pasar por ella, con el propósito de engañar a otros/as o causarle daño.	Una o un compañero de clase crea un perfil falso en una red social usando fotos y el nombre de otro/a compañero/a para publicar comentarios ofensivos y difundir rumores.
Grooming Cuando una persona adulta intenta engañar a un niño, niña o adolescente a través de Internet para ganarse su confianza y luego hacerle daño.	Una persona adulta se hace pasar por una niña, niño o adolescente en Internet para hablar con otra niña, niño o adolescente a fin de promover encuentros personales, solicitar fotos o videos, chantajear o acosar con fines sexuales.
Amenazas Mensajes agresivos a través de Internet donde una persona dice que va a hacer daño a alguien o a su familia si no hacen lo que él o ella quiere.	Una o un adolescente recibe mensajes en sus redes sociales diciendo que si no hace lo que le dicen, su familia sufrirá daño.
Control El seguimiento constante de lo que una persona hace en Internet o fuera de él. Esta es una forma de violencia que puede generarse utilizando diferentes tecnologías y además puede darse en relaciones de enamoramiento o noviazgo.	Una pareja o ex pareja instala una aplicación en el teléfono de un o una adolescente sin que lo sepa, para luego rastrear su ubicación o ver sus mensajes privados. Luego utiliza esa información para hacer comentarios inapropiados sobre esas actividades o chats.
Difusión de imágenes íntimas Cuando alguien comparte o publica fotos privadas de otra persona.	Un o una adolescente, después de terminar con su pareja, decide compartir fotos íntimas de su ex pareja para dañar su reputación.

Fuente: Elaboración propia con la información de "La violencia de género en línea contra las mujeres y niñas: Guía de conceptos básicos, herramientas de seguridad digital y estrategias de respuesta" [Preparado por la Secretaría General de la Organización de los Estados Americanos]

1.2 CARACTERÍSTICAS Y EFECTOS DE LA VIOLENCIA DIGITAL

La violencia digital es una forma de agresión que afecta principalmente a mujeres y niñas. Aunque tiene la misma raíz que otras violencias, la violencia digital tiene características propias que la hacen diferente, por ejemplo:

- **No necesita cercanía física.** La persona que ejerce violencia digital puede estar en cualquier parte del mundo, ya que no es necesario estar en el mismo lugar para causar daño.
- **Anonimato.** El anonimato en Internet permite utilizar y expresarse libremente sin revelar información personal identificable. Esto hace que muchas personas utilicen este medio para ejercer violencia ocultando su identidad para no ser detectadas.
- **Se mezcla con otras violencias.** Muchas veces, la violencia digital no actúa sola. Quienes enfrentan violencia digital también suelen enfrentar otros tipos de violencia fuera de Internet, como violencia física, violencia psicológica, violencia sexual, por mencionar algunas.

La violencia digital, aunque sucede a través de una pantalla, tiene consecuencias reales en la vida de quienes la enfrentan. Los efectos más comunes que pueden enfrentar las niñas, niños y adolescentes son:

- **Afectaciones emocionales.** Estrés, miedo, depresión, baja autoestima y pensamientos de aislamiento. Las víctimas pueden sentirse solas y culpables por lo que les ocurre.
- **Afectaciones físicas.** La violencia digital también puede provocar problemas de salud física debido a la angustia emocional que genera.
- **Impacto en la vida diaria.** La violencia digital puede afectar el desempeño escolar y hacer que las víctimas dejen de hacer actividades que disfrutaban o que realizaban cotidianamente.
- **Desconfianza en la tecnología.** Las víctimas pueden desarrollar miedo al uso de tecnologías, sobre todo vinculadas al Internet, lo que implica restar oportunidades de aprendizaje, crecimiento, de entretenimiento e incluso de conectividad con otras personas.

1.3 **ATENCIÓN Y RESPUESTA** A LA VIOLENCIA DIGITAL EN UNIDADES EDUCATIVAS

Es muy importante que las unidades educativas cuenten con protocolos o mecanismos adecuados de prevención, atención y respuesta ante posibles casos de violencia digital en el entorno educativo. Algunas acciones que pueden incluirse en éstos son:

- **Detección temprana.** Capacitar a maestros y maestras para identificar signos de violencia digital, como cambios en el comportamiento o rendimiento de las y los estudiantes.
- **Espacios seguros de denuncia.** Crear un mecanismo confidencial donde las y los estudiantes puedan reportar casos de violencia sin temor a represalias.
- **Intervención inmediata.** Cuando se detecte un caso de violencia digital, se debe actuar rápidamente para proteger a la víctima, deteniendo la agresión y ofreciendo apoyo psicológico integral, según las necesidades de la persona.
- **Sensibilizacón y colaboración con las familias.** Mantener una comunicación abierta con las madres, padres o cuidadores, informándoles sobre los riesgos y las medidas que se están tomando, manteniendo espacios de reflexión para prevenir situaciones de violencia digital y socializar los protocolos o mecanismos de actuación en caso de que se presenten casos de violencia digital.
- **Sanciones claras.** Establecer consecuencias disciplinarias para quienes cometan actos de violencia digital, siempre dentro de un enfoque restaurativo, socializando adecuadamente con todas las personas que son parte de la comunidad educativa.
- **Capacitación a las y los estudiantes.** Es importante crear espacios de capacitación sobre las formas de violencia digital, su prevención y denuncia, dirigidos a las y los estudiantes de las unidades educativas.

1.4 FORMAS DE **SENSIBILIZACIÓN PARA LA PREVENCIÓN** DE LA VIOLENCIA DIGITAL

Las formas de sensibilización pueden ser varias de acuerdo al contexto de cada unidad educativa, pero se sugieren al menos realizar algunas de las siguientes actividades para comenzar a sensibilizar sobre el tema:

- **Talleres y campañas.** Organizar talleres para educar tanto a estudiantes como a profesores sobre las formas de violencia digital, sus consecuencias y cómo prevenirlas.
- **Capacitaciones sobre el uso seguro y responsable de Internet.** Incorporar espacios de análisis y recomendaciones sobre el uso seguro y responsable del Internet, con contenidos didácticos acordes a la edad de las y los estudiantes.
- **Charlas con expertos.** Invitar a profesionales en ciberseguridad o psicología para hablar sobre la importancia de la seguridad digital y el impacto emocional de la violencia digital.
- **Foros y espacios de discusión.** Crear espacios donde las y los estudiantes puedan intercambiar sus experiencias, dudas y soluciones sobre el uso seguro de las tecnologías.

ACTIVIDADES **DE APOYO**

ACTIVIDAD 1

ANÁLISIS DE CASOS DE VIOLENCIA DIGITAL

Objetivo: Identificar y comprender las características y efectos de diferentes tipos de violencia digital mediante el análisis de casos hipotéticos.

Instrucciones:

Lectura de ejemplo: Lea atentamente el siguiente ejemplo de violencia digital:

Un compañero de clase instala una aplicación en el teléfono de su compañera para rastrear su ubicación o ver sus mensajes privados, luego utiliza esa información para hacer comentarios inapropiados o para intimidarla con amenazas de hacer pública su información.

1. **Reflexión personal:** Responda las siguientes preguntas:

» ¿Qué emociones podría experimentar la víctima en esta situación?

» ¿Qué acciones podrían tomarse en la unidad educativa para prevenir o detener este tipo de violencia?

» ¿Qué rol podrías desempeñar como maestro/a para apoyar a la víctima?

Aplicación en el aula: Luego de este ejercicio, piensa en una breve acción educativa que podrías implementar en el aula para abordar este tema con las y los estudiantes. Por ejemplo, una charla sobre el uso responsable de la tecnología o la creación de un espacio seguro para hablar de sus experiencias en línea, entre otros.

ACTIVIDAD 2

REFLEXIÓN SOBRE LOS EFECTOS DE LA VIOLENCIA DIGITAL

Objetivo: Comprender los efectos emocionales, físicos y sociales de la violencia digital en las y los estudiantes y explorar estrategias de prevención y apoyo.

Instrucciones:

Lee los efectos de la violencia digital mencionados en la página 6 de esta guía (1.2 Características y efectos de la violencia digital) y responde a las siguientes preguntas:

» ¿Cómo crees que la violencia digital afecta a las y los estudiantes en su unidad educativa?

» ¿Qué cambios podrías observar en un/a estudiante que está enfrentando violencia digital? Elabora una lista de posibles señales.

Plan de acción personal: Anota dos acciones que podrías emprender como maestro/a para crear un ambiente en el aula que sea seguro y de apoyo para estudiantes que puedan estar en riesgo de violencia digital.

Acción 1:

Acción 2:

2. **PENSAMIENTO CRÍTICO** EN EL USO DE LAS TECNOLOGÍAS

LA INFLUENCIA DE LAS REDES

La profesora Ana se da cuenta de que muchos/as estudiantes se comparan con las imágenes que ven en las redes sociales.

Objetivo: Reflexionar sobre cómo las redes sociales pueden distorsionar la realidad y desarrollar un criterio propio sobre el consumo de información para compartirlo con nuestras/os estudiantes.

2.1 INTERNET REPRODUCE CÁNONES QUE PUEDEN SER **POCO REALES**

El acceso a Internet ha permitido que una gran variedad de voces y experiencias se expresen. Sin embargo, también ha llevado a la difusión de estándares de belleza, éxito y comportamiento que son frecuentemente irreales y perjudiciales.

Plataformas como Instagram y TikTok, por ejemplo, suelen presentar imágenes altamente editadas y estilizadas que pueden provocar una presión social, llevando a las y los jóvenes a compararse con lo que ven y a desarrollar inseguridades sobre su apariencia o su vida.

Es importante que las y los estudiantes reconozcan que estas representaciones no siempre son un reflejo de la realidad y que muchas veces son el resultado de un proceso de edición.

La exposición constante a estos estereotipos puede generar problemas de autoestima, ansiedad y depresión. Fomentar un análisis crítico de estos contenidos es esencial para ayudar a las y los estudiantes a desarrollar una visión más equilibrada y realista de sí mismas/os y del mundo.

2.2 **AUTORREGULACIÓN** PARA EL CUIDADO DE LA SALUD MENTAL

La autorregulación es la habilidad de controlar nuestros propios pensamientos, emociones y comportamientos. En el contexto del uso de la tecnología, implica desarrollar la capacidad de gestionar el tiempo de pantalla, seleccionar los contenidos que consumimos y establecer límites en el uso de dispositivos.

Las y los estudiantes deben ser conscientes de su bienestar emocional y físico, y aprender a identificar cuándo el uso de la tecnología se vuelve perjudicial. Esto puede incluir la reducción del tiempo en redes sociales, el establecimiento de períodos sin tecnología y la búsqueda de actividades al aire libre o interacciones sociales que no dependan de dispositivos electrónicos.

2.3 PROHIBIR EL USO DE CELULARES **NO SIEMPRE ES LA RESPUESTA**

Aunque algunos/as educadores/as o madres y padres pueden sentir que la mejor forma de proteger a las y los jóvenes de los riesgos asociados con el uso de la tecnología es prohibir su uso, esta estrategia puede no ser efectiva a largo plazo. La prohibición puede generar curiosidad y llevar a las niñas, niños y adolescentes a buscar formas de evadir estas restricciones.

En lugar de prohibir el uso de celulares, es más constructivo fomentar un uso responsable y consciente. Educar a las y los estudiantes sobre los riesgos del uso irresponsable de la tecnología y proporcionarles las herramientas necesarias para navegar de forma segura puede ser más beneficioso.

Esto incluye enseñarles sobre la importancia de la privacidad, la seguridad en línea y la gestión de la información que comparten.

2.4 ALGUNOS **CASOS REALES**:

2.4.1 CASO DE ESSENA O'NEILL

Essena O'Neill era una influencer australiana con cientos de miles de seguidores en Instagram, donde compartía imágenes aparentemente perfectas de su vida. Sin embargo, en 2015, O'Neill decidió dejar las redes sociales, revelando que muchas de sus fotos eran cuidadosamente editadas y tomadas solo para cumplir con expectativas comerciales y estéticas.

Publicó mensajes en los que advertía a sus seguidores que sus publicaciones no eran una representación auténtica de su vida y que el proceso le había causado ansiedad y estrés. Su decisión llevó a una conversación global sobre la presión de las redes sociales y la importancia de la autenticidad en línea.

2.4.2 EL **EFECTO DE TIKTOK** Y LA "DISMORFIA DE SNAPCHAT"


"Dismorfia de Snapchat": el fenómeno por el que cada vez más pacientes de cirugía estética aspiran a parecerse a sus propios selfies con filtros

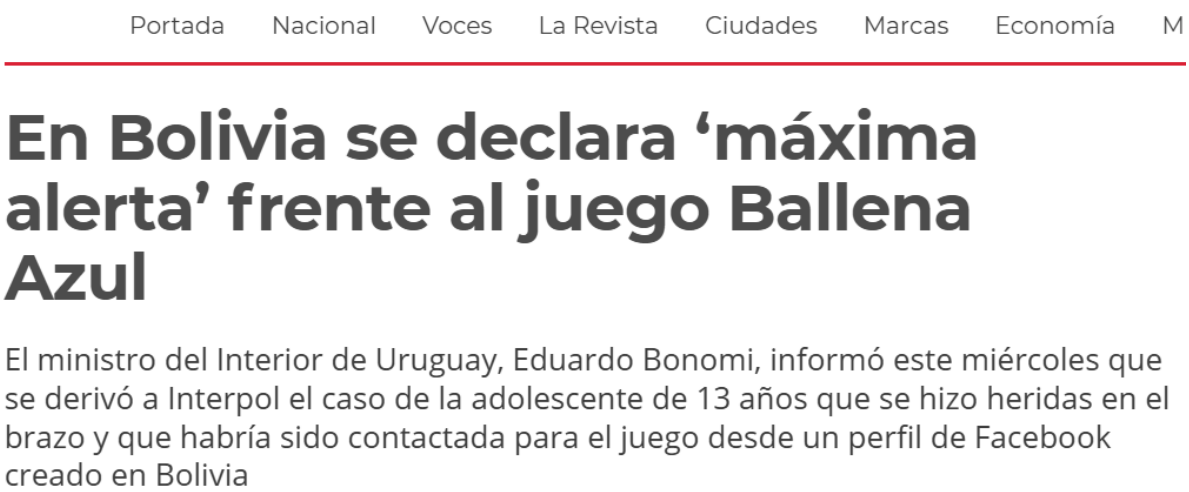
En los últimos años, estudios y casos médicos han destacado un aumento en las y los jóvenes que buscan intervenciones estéticas para parecerse más a las versiones filtradas de sí mismos que ven en aplicaciones como TikTok y Snapchat. Este fenómeno, conocido como "dismorfia de Snapchat", ha llevado a que muchas personas sientan una presión de conformarse con estándares de belleza irreales, impulsados por filtros que modifican radicalmente sus rostros.

Varios médicos han alertado sobre cómo este fenómeno afecta la salud mental, ya que estos estándares inalcanzables de perfección pueden llevar a una autoestima negativa y, en algunos casos, a depresión y ansiedad.

2.4.3 El reto de la **"ballena azul"**

Éste fue un desafío que comenzó a circular en redes sociales y aplicaciones de mensajería en 2016, principalmente en Rusia y luego se expandió a otros países. Se trataba de un "juego" que consistía en realizar una serie de desafíos durante varias semanas, que incluían autolesiones y, en su última etapa, terminaba en el suicidio.

Aunque el caso exacto y la existencia del "reto" se encuentran en discusión, existen registros de jóvenes que, motivados por contenidos oscuros en redes, llevaron a cabo actos de autolesión. Esto generó una serie de iniciativas para mejorar la educación digital y el control sobre este tipo de contenidos peligrosos.


Portada Nacional Voces La Revista Ciudades Marcas Economía M

En Bolivia se declara 'máxima alerta' frente al juego Ballena Azul

El ministro del Interior de Uruguay, Eduardo Bonomi, informó este miércoles que se derivó a Interpol el caso de la adolescente de 13 años que se hizo heridas en el brazo y que habría sido contactada para el juego desde un perfil de Facebook creado en Bolivia

ACTIVIDADES DE APOYO

ACTIVIDAD 1

ANÁLISIS CRÍTICO DE IMÁGENES

Objetivo: Reflexionar sobre los estándares de belleza y éxito que se presentan en las redes sociales.

Instrucciones:

Selecciona una imagen: Utilizando tu celular, elige una imagen de redes sociales que represente un estándar de belleza o éxito: puede ser una de tus propias publicaciones, una imagen viral o cualquier otra que encuentres en línea.

Análisis de contenido: Responde a las siguientes preguntas:

» ¿Qué mensaje crees que transmite esta imagen?

» ¿Qué elementos (como filtros, iluminación, poses u otros) se han utilizado para crear esta imagen?

» ¿Qué emociones o pensamientos te provoca al verla?

» ¿Crees que esta imagen representa una realidad auténtica? ¿Por qué sí o por qué no?

Reflexión: Escribe un breve párrafo reflexionando sobre cómo esta imagen se relaciona con la presión social que puede sentir un o una estudiante sobre su apariencia.

Aplicación en el aula: Luego de este ejercicio, piensa en una breve acción educativa que podrías implementar en el aula para abordar este tema con las y los estudiantes. Por ejemplo: Proyectos de grupo donde las y los estudiantes analicen y discutan el impacto de los estándares de belleza en las redes sociales, establecimiento de "días sin tecnología" donde las y los estudiantes participen en actividades al aire libre o interacciones en persona, etc.

3. **CÓMO UTILIZAR INTERNET** DE MANERA SEGURA EN LA EDUCACIÓN

TRABAJO COLABORATIVO

El profesor reflexiona con sus alumnos/as para usar fuentes confiables y hacer trabajo colaborativo en línea.

Objetivo: Que como educadores usemos la tecnología para fomentar el trabajo en equipo y la responsabilidad, guiando a las y los estudiantes hacia un uso consciente y efectivo de Internet.

3.1 **PROTECCIÓN** DE LA PRIVACIDAD Y SEGURIDAD EN LÍNEA

La protección de la privacidad es esencial para garantizar la seguridad de las personas en el entorno digital. Con la cantidad de información personal que compartimos en línea, desde datos de contacto hasta detalles de ubicación, es crucial saber cómo protegernos.

Las y los estudiantes, así como maestras y maestros, deben entender la importancia de mantener su información personal privada y aprender a usar configuraciones de privacidad en las redes sociales o servicios digitales.

3.2 USO DE **CONTRASEÑAS SEGURAS**

Las contraseñas son las llaves de acceso a nuestra información personal, por tanto, deben estar bien protegidas y se recomienda que combinen letras, números y símbolos. Es recomendable cambiarlas regularmente y no compartirlas con otros.

Ejemplos de contraseñas seguras:

- G3l@t0!2024 (mezcla de letras mayúsculas, minúsculas, números y símbolos)
- 2B@3stD@y!456 (frase modificada que incluye números y caracteres especiales)
- S@f3Pa$$w0rd#2024 (combinación de palabras con alteraciones)

Consejos prácticos:

» Longitud: Asegúrate de que la contraseña tenga al menos 12 caracteres. Cuanto más larga, mejor.

» Combinaciones: Usa una combinación de palabras, números y símbolos. Evita usar información personal fácil de adivinar, como fechas de nacimiento o nombres.

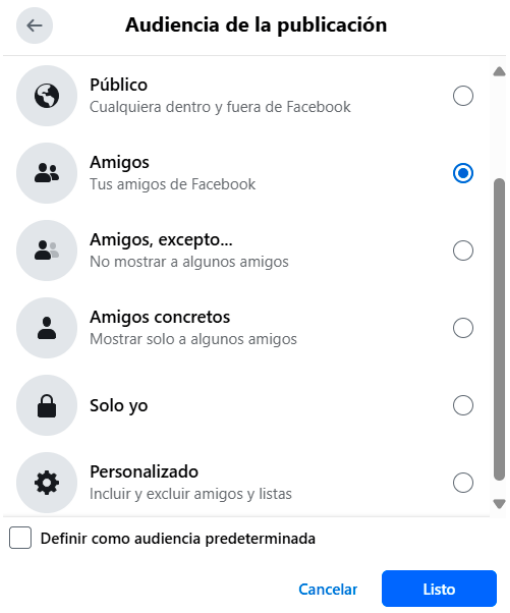
» Generadores de contraseñas: Utiliza herramientas en línea como para crear contraseñas fuertes y únicas, por ejemplo: https://www.dashlane.com/es/features/password-generator también puede ingresar a esta herramienta escaneando el siguiente QR:

» Cambio regular: Establece recordatorios para cambiar las contraseñas cada 3 a 6 meses.

3.3 **CONFIGURACIONES DE PRIVACIDAD** DE NUESTROS DISPOSITIVOS

Como usuarios de Internet debemos familiarizarnos con las configuraciones de privacidad de las redes sociales y otros servicios en línea, ajustándolas para limitar quién puede ver su información y publicaciones.

Las redes sociales que utilizamos tienen la opción de configurar el nivel de privacidad de lo que publicamos, en el caso de Facebook, al publicar un contenido, podemos decidir si lo hacemos público (que todos/as lo vean), visibles para nuestros/as amigos/as o visibles solo para nosotros/as, como se muestra a continuación:



En este sentido, es recomendable familiarizarnos y utilizar los diferentes íconos de seguridad de nuestras redes sociales.

3.4 VERIFICACIÓN EN **DOS PASOS** (2FA)

La verificación en dos pasos es como tener una cerradura adicional en la puerta de nuestra casa para hacerla más segura. Imagina que necesitas dos llaves para abrirla: una es tu contraseña y la otra es un código especial que solo tú puedes recibir en tu teléfono. Primero, usas la contraseña (la primera llave) y luego introduces el código que recibes (la segunda llave).

Esto ayuda a proteger nuestra información porque, aunque alguien descubra nuestra contraseña, no podrá acceder sin el código especial. Así, evitamos que nuestra información personal, como fotos y mensajes privados, se usen de manera indebida.

Hagamos el ejercicio con WhatsApp

- En WhatsApp, abre Ajustes.
- Toca Cuenta > Verificación en dos pasos > Activar o Configurar PIN.
- Ingresa un PIN de seis dígitos y confírmalo.
- Proporciona una dirección de correo electrónico a la que tengas acceso o, si no quieres hacerlo, toca Omitir.
- Toca Siguiente.

Confirma la dirección de correo electrónico y toca Guardar u OK

- Cómo desactivar la verificación en dos pasos
- En WhatsApp, abre Ajustes.
- Toca Cuenta > Verificación en dos pasos > Desactivar.

3.5 **CUIDADOS** AL COMPARTIR INFORMACIÓN

Antes de publicar información personal (como fotos, ubicaciones, etc.), debemos preguntarnos cómo podría afectar a nuestra su seguridad y la de nuestro entorno.

Ejemplo 1: Publicar ubicaciones.

- **Riesgo:** Si un/a maestro/a o estudiante publica su ubicación actual o que está de vacaciones, puede facilitar que personas malintencionadas sepan que su casa está vacía.

- **Recomendación:** Es mejor compartir ubicaciones solo después de haber estado en un lugar o usar opciones de privacidad que oculten la ubicación exacta.

Ejemplo 2: Fotos con información personal.

- **Riesgo:** Publicar fotos que muestren la dirección de casa, el número de placa del auto o documentos personales puede resultar en robos de identidad o estafas.

- **Recomendación:** Antes de publicar cualquier foto, revisa el fondo y asegúrate de que no haya información personal visible.

Ejemplo 3: Información sobre actividades.

- **Riesgo:** Compartir que se estará en un evento específico, como una fiesta, puede atraer a desconocidos o incluso a acosadores.

- **Recomendación:** Mantén la privacidad sobre tus actividades y evita publicaciones que indiquen dónde estarás en un momento dado.

3.6 **EQUILIBRIO** EN EL USO DE TECNOLOGÍAS Y OTRAS FORMAS DE APRENDIZAJE

El uso de tecnologías en la educación debe complementarse con métodos de aprendizaje tradicionales. Mientras que el acceso a Internet ofrece un sinfín de recursos educativos, es esencial fomentar un equilibrio entre el aprendizaje en línea y las experiencias de aprendizaje en el mundo real o físico.

Estrategias para lograr un equilibrio:

- **Actividades al aire libre.** Fomentar la participación en actividades físicas y al aire libre para desarrollar habilidades sociales y de comunicación.
- **Proyectos grupales.** Promover el trabajo en equipo mediante proyectos que involucren tanto la investigación en línea como la colaboración presencial.
- **Lectura de libros.** Integrar la lectura de libros y materiales impresos en el currículo para ayudar a las y los estudiantes a desarrollar habilidades de concentración y comprensión lectora.

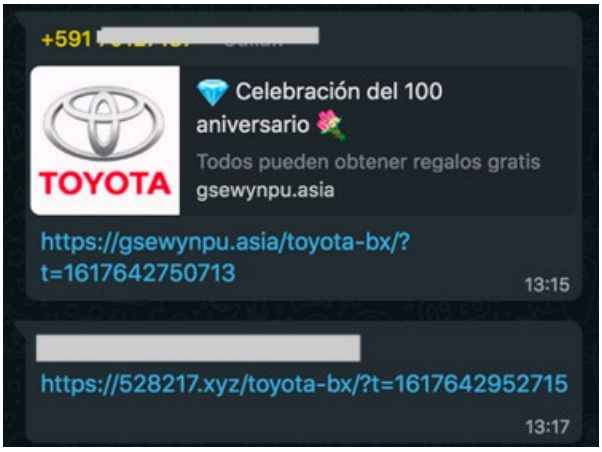
3.7 **CÓMO EVITAR** CONTENIDOS FALSOS

En la era digital, la capacidad de discernir entre fuentes confiables y no confiables es vital. Tanto educadores como estudiantes deben aprender a evaluar la veracidad de la información que encuentran en línea para evitar la desinformación.

3.7.1 **CÓMO IDENTIFICAR** INFORMACIÓN DE CALIDAD

- **Verificar la fuente.** Es fundamental comprobar quién publica la información. Sitios web de agencias de información o medios de comunicación oficiales y organizaciones educativas suelen ser más confiables.
- **Comprobar la fecha.** La información desactualizada puede ser engañosa, así que es importante asegurarse de que el contenido sea reciente y relevante.
- **Contrastar con otras fuentes.** Resulta una muy buena práctica comparar la información con al menos tres fuentes para asegurarnos de que sea información precisa y veraz.
- **Reconocer enlaces maliciosos.** Son esos enlaces que podemos recibir en nuestras cuentas de WhatsApp o perfiles de Facebook o incluso como mensajes de texto (sms), pero que tienen intenciones oscuras (estafas, fraudes). Se llama enlace malicioso porque su objetivo es engañar a la persona que recibe el enlace y robarle su información personal o ingresar a su cuenta.

Examinemos el siguiente mensaje:



Aparentemente, es un anuncio que invita a participar en una celebración donde se pueden ganar premios, incluido un vehículo Toyota. Si entramos al enlace, nos lleva a una página que pide información personal (nombre, número de teléfono, correo, contraseña, etc.).

No obstante, si examinamos la dirección de este sitio web, se trata de un sitio falso que se hace pasar por el oficial.

- **Dirección falsa** (No suele comenzar con el nombre de la empresa, tienda o servicio, sino con combinaciones de números o letras): https://528217.xyz/toyota-bx/
- **Dirección oficial** (Comienza con el nombre oficial de la empresa, tienda o servicio): https://www.toyota.com/

¿Cómo reconocemos los enlaces maliciosos?

- Pregúntate quién te envió el enlace: Si no conoces a esa persona, es mejor ignorar el enlace y no abrirlo.
- Suelen estar acompañados con mensajes relacionados a premios o intentan asustarte diciendo que ingresando al enlace encontrarás un vídeo o una foto tuya.
- Cuando ingresas, usualmente te piden datos personales como nombre completo, número de teléfono, correo electrónico o contraseñas.
- Juegan con la urgencia, el mensaje puede decir que tenemos que actuar de inmediato, haciéndose pasar por un familiar lejano que se encuentra en problemas.

Si el enlace cumple con alguno de los puntos anteriores, no ingreses a él.

3.8 UTILIZAR INTERNET COMO UNA **HERRAMIENTA COLABORATIVA**

Internet no solo es una herramienta de búsqueda de información, sino también un medio para colaborar y aprender juntos/as. Tantos educadores como estudiantes pueden beneficiarse enormemente de las plataformas en línea que les permiten interactuar y trabajar en equipo, independientemente de la distancia física.

Herramientas colaborativas en línea:

- **Documentos compartidos:** Plataformas como Google Docs permiten a las y los estudiantes trabajar juntos en tiempo real, facilitando la colaboración en Proyectos grupales. https://drive.google.com/
- **Plataformas de aprendizaje en línea:** Herramientas como Moodle ofrecen un entorno seguro para que las y los estudiantes se conecten, compartan recursos y colaboren en tareas. Una de ellas también puede ser Google Classroom https://classroom.google.com
- **Foros y grupos de discusión:** Participar en foros en línea o grupos de discusión sobre temas académicos puede enriquecer la experiencia de aprendizaje al permitir que los estudiantes compartan ideas y resuelvan dudas.

ACTIVIDADES DE APOYO

ACTIVIDAD 1

CREACIÓN DE **CONTRASEÑAS SEGURAS**

Objetivo: Aprender a crear y gestionar contraseñas seguras.

Instrucciones:

Reflexiona sobre una de tus contraseñas actuales. Piensa, recuerda o escribe en una hoja aparte una contraseña que utilizas en una de tus redes sociales (puedes modificar las contraseñas para mantener la privacidad) y evalúa si cumplen con los siguientes criterios:

» ¿Tienen al menos 12 caracteres?

SI. NO

» ¿Incluyen letras mayúsculas, minúsculas, números y símbolos?

SI NO

» ¿Evitaste usar información personal fácil de adivinar?

SI NO

Crea una contraseña segura

Paso 1. Piensa en una frase larga y escríbela en el siguiente espacio (una letra por cuadro y sin espacios, por ejemplo: leermemotiva):

Paso 2: Ahora reemplaza algunas letras por números como en la siguiente tabla:

La I por 1, la E por 3, la T por 7. ña O por 0, la A por 4, la S por 5 y la B por 8

Paso 3. Ahora escribe la frase resultante (Siguiendo el ejemplo de leermemotiva, la frase resultante sería: l33rm3m0t1v4):

Reflexiona sobre el proceso. Escribe un breve párrafo sobre lo que aprendiste al crear contraseñas seguras y cómo planeas aplicar este conocimiento con tus estudiantes.

ACTIVIDAD 2

EVALUACIÓN DE **CONFIGURACIONES DE PRIVACIDAD**

Objetivo: Familiarizarse con las configuraciones de privacidad de las redes sociales y comprender su importancia.

Instrucciones:

Elige una red social. Selecciona una red social que utilices regularmente (por ejemplo: Facebook, WhatsApp, Tik Tok).

Revisa la configuración de privacidad. Accede a las configuraciones de privacidad de la plataforma elegida. Busca las siguientes opciones y anota tus hallazgos:

» ¿Tienes activada la verificación en dos pasos? Sí / No, ¿por qué es importante activarla?

» ¿Quién puede ver tus publicaciones y fotos? Es decir, ¿cómo está configurada la visibilidad de tus publicaciones? (Ajusta esta configuración si es necesario).

Aplicación en el aula. Con base en tu experiencia como maestro/a, esboza una lección, actividad o contenido que podrías impartir a tus estudiantes sobre la importancia de la privacidad en línea y cómo usar las configuraciones de sus redes sociales para protegerse.

Recuerda que ante una situación de violencia en línea puedes escribir al **centro SOS Digital** de forma gratuita.

CENTRO SOS DIGITAL

EQUIPO DE ACOMPAÑAMIENTO Y RESPUESTA A VIOLENCIAS DIGITALES

LÍNEA DE APOYO:

+591 62342430

Signal Telegram WhatsApp

www.**sosdigital**.internetbolivia.org

Asociación Aguayo

INTERNET BOLIVIA .ORG

educo
educar cura