



Laboratorio # 2 Protección

Tu huella digital: seguridad en línea



¿De qué trata?

Este laboratorio se concibe como una herramienta esencial para educadores comprometidos en impartir conocimientos cruciales sobre seguridad digital a sus estudiantes. La misión central es sensibilizar a los estudiantes sobre las amenazas en línea, empoderándolos con estrategias sólidas para resguardar la información personal y promover un bienestar digital integral. En este espacio, promoverás la idea de protección sin recurrir a la prohibición. Este laboratorio te ofrece una plataforma para que guíes a tus estudiantes en la exploración segura y responsable del ciberespacio, fomentando una cultura digital fundamentada en el conocimiento y la prudencia.

¿Cuál es el objetivo del laboratorio?

Sensibilizar a los estudiantes sobre las amenazas en línea y empoderarlos con conocimientos y estrategias para proteger su información personal y su bienestar digital. Fomentar la protección sin prohibición, estableciendo reglas en un marco de confianza, respeto y consentimiento.



¿A quién va dirigido?

Estudiantes que estén cursando entre el grado sexto a undécimo.





¿Qué se necesita?

1

Un computador o dispositivos móviles como celulares o tabletas, conectados a Internet.

Presentación de PowerPoint del Laboratorio#2 previamente descargada.

2**3**

Implementos para escribir, como notas adhesivas, hojas de cuaderno, libretas, lápices, lapiceros, marcadores, entre otros.

Manos a la obra

Este laboratorio cuenta con una presentación en archivo PowerPoint, allí encontrarás paso a paso y de manera muy clara cada uno de los momentos propuestos para guiar los temas.

La parte inicial cuenta con:

01.

La bienvenida.

Es un texto corto con un mensaje cordial que introduce a los participantes al laboratorio. El propósito de esta diapositiva es brindar información inicial sobre el taller y establecer una conexión significativa con el tema, generando expectativas positivas entre los estudiantes. Por lo tanto, te animamos a compartir este mensaje con ellos desde el principio, para que tengan una comprensión clara de lo que van a aprender.

2.

Seguido, se encuentra la agenda del laboratorio.

Socialízala con tus estudiantes para que conozcan la estructura de este. La agenda contiene: los acuerdos, los objetivos y los temas que se abordarán durante el encuentro. Esta, está diseñada para guiar la participación de los asistentes a través de una serie de actividades y discusiones que les permitirán adquirir conocimientos y habilidades relacionadas con la seguridad y el bienestar en línea.

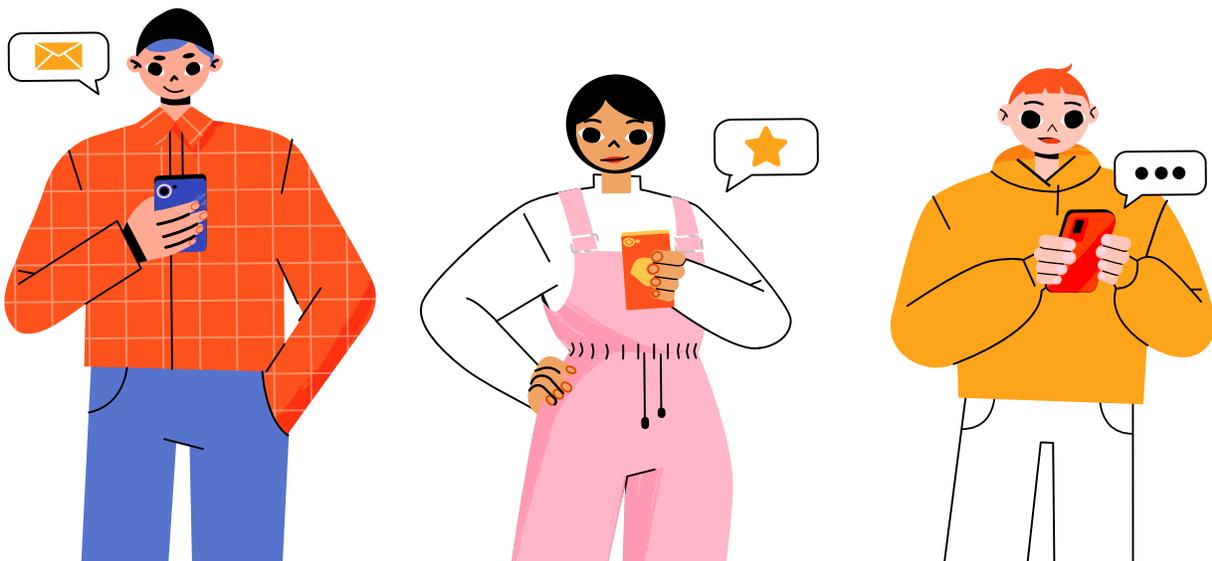
3.

Los acuerdos hacen referencia al protocolo de participación en este laboratorio.

Te sugerimos compartirlos abiertamente con tus estudiantes para garantizar que tengan una comprensión clara sobre el comportamiento esperado durante el desarrollo de las actividades.

4.

Después de los acuerdos, encontrarás los objetivos, los cuales se presentan a manera de memes para que tengan un impacto significativo en los estudiantes. Mediante la asociación de cada objetivo con la imagen, estos pueden recordarlos. Compártelos con tus estudiantes para que entiendan que se refieren a metas específicas y medibles que van a alcanzar a través de la participación durante la sesión del laboratorio. Recuerda que estos objetivos proporcionan una guía clara sobre lo que se espera lograr.



5.

Seguido a los objetivos vas a encontrar la propuesta “saberes previos”.

Este espacio es relevante porque les permitirá a los estudiantes conectar los nuevos conceptos con las experiencias, habilidades o creencias que estos tengan antes de iniciar los temas del laboratorio. Anímalos a participar y responder para que conecten sus ideas con los temas que vas a desarrollar a lo largo del laboratorio.

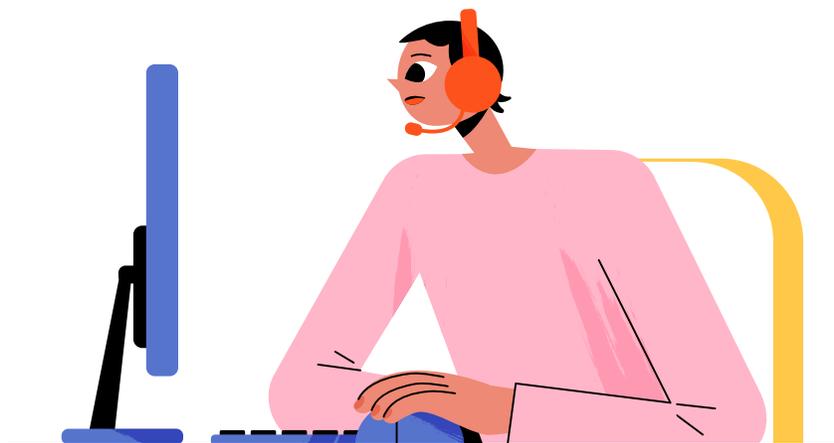
6.

Tras abordar los saberes previos, la siguiente diapositiva presenta el primer segmento denominado **Momento #1: Tu huella digital**. En esta sección, se incluye un párrafo introductorio diseñado para orientar el inicio de este tema y proporcionar a los estudiantes una visión general de su contenido.

6.1.

A través de un video, este **primer tema** se enfoca en concientizar sobre la importancia de la **huella digital** y cómo las interacciones en línea de cada persona pueden dejar rastros duraderos. Busca proporcionar a los estudiantes, información clave sobre cómo gestionar y proteger su huella digital, promoviendo un uso responsable de la tecnología y brindando estrategias para mantener una presencia en línea positiva.

Seguido vas a encontrar una pieza gráfica que menciona la importancia de ajustar la configuración de privacidad en las redes sociales, utilizar contraseñas seguras y limitar la información personal que comparten en línea. Socializa esta información con tus estudiantes para que estén enterados de estos parámetros de protección.



Recomendación:

Son ocho recomendaciones, a medida que vayas terminando cada una, permite que tus estudiantes participen de este momento realizando preguntas sobre lo que no les haya quedado claro o si tienen algo que aportar a lo expuesto sobre la temática. La interacción constante contribuirá a una comprensión más profunda y a un aprendizaje más significativo.

6.2.

Continuando con este primer momento, vas a encontrar el **subtema: Tu kit de explorador en línea**. Allí podrás conversar con tus estudiantes sobre todo lo que pasa con la huella digital. La propuesta para este subtema es explicar una a una estas herramientas. Sugiere a tus estudiantes tomar nota o crear conceptos clave para que recuerden estas recomendaciones para explorar Internet.

Para terminar este primer momento, continúa con la **Actividad: Los arriesgados en línea**. Con esta actividad tus estudiantes aprenderán a identificar algunos riesgos en línea. Es muy sencilla de realizar. Proyecta las preguntas para que los participantes puedan leer con atención las situaciones. Deben elegir solo una opción. La actividad se presta para resolver todos en grupo. Al finalizar, pregunta a tus estudiantes qué situaciones llamaron más su atención y por qué.

7.

Ya has terminado el momento#1; ahora, continúas con el **momento #2** denominado **Proteger mi información personal**. Para introducir este tema inicia compartiendo el dato curioso. Motiva a tus estudiantes a cambiar sus contraseñas si es que tienen actualmente algunas de las mencionadas en el dato.

7.1.

Proyecta la información del **subtema** de este segundo momento **Contraseñas seguras**. Allí se explican estrategias y consejos clave sobre contraseñas seguras y autenticación de dos factores.

Invita a tus estudiantes a tomar nota de lo más importante y abre un espacio dentro de la explicación para que manifiesten dudas o realicen comentarios sobre el tema.

8.

Es momento de la **segunda actividad: falso o verdadero**. Desarrolla esta actividad con tu grupo de estudiantes. Esta consiste en poner a prueba lo que acabas de explicar. Son 10 afirmaciones a las cuales responden Falso o Verdadero según lo consideren.

Cuando hayan finalizado, socializa las respuestas y refuerza los conceptos de los temas explicados.

La actividad tiene calificación a manera de *ranking*, que corresponde con la asignación de un meme de acuerdo con el conteo de respuestas correctas e incorrectas. Invita a tus estudiantes a contar la cantidad de aciertos en sus respuestas y que así se identifiquen con uno de los tres mensajes de los memes.

9.

El **momento #3** es el último de los temas que vas a abordar en este segundo laboratorio, en este abordarás el **Top 10 principios de seguridad en línea**. Inicialmente vas a encontrar el texto de referencia que introduce al tema.

Luego, proyecta a los estudiantes la infografía que encontrarás en la siguiente diapositiva, explicando cada una de las normas o reglas que deben tener en cuenta como parámetros de seguridad.

9.1.

Continúa en la siguiente diapositiva con el **subtema: Vulnerabilidad en línea**. Allí encontrarás un texto corto para introducir la temática. La información, como verás a continuación, se expondrá a través de narraciones cortas.

Son seis microrrelatos que cuentan situaciones cotidianas donde sus protagonistas enfrentaron alguna situación de riesgo. Lee en voz alta cada relato o invita a los estudiantes a leerlas. Seguido anímalos a participar señalando cuál es el riesgo que pueden asociar con lo sucedido al personaje. Procura darles pistas para que lleguen por si mismos a las respuestas. Invítalos a argumentar las respuestas que ellos elijan.

9.2.

Terminados los relatos, continúa con la **actividad: El riesgo que falta**. Explícales que leyeron seis relatos y tenían siete opciones de respuestas. Incentívalos a recordar cuál fue el riesgo que no correspondió a ninguno de los relatos expuestos. Abre el debate sobre el riesgo en línea faltante y permite que tus estudiantes den sus opiniones si saben de qué trata o especulen sobre lo que puede ser este riesgo.

9.3.

En la siguiente diapositiva encontrarás la propuesta **Aprendamos más sobre seguridad en línea**. Esta consiste en recomendar a tus estudiantes un juego en línea y 3 videos para que exploren más sobre los temas tratados durante el laboratorio.

10.

Ya vas terminando el laboratorio. En este punto, presenta el **resumen** de los puntos clave de todo lo que has expuesto. La finalidad es proporcionar un cierre estructurado y claro, permitiendo a los participantes visualizar el panorama general y cómo los diferentes temas se relacionan entre sí.

Recuerda cada uno de los momentos con tus estudiantes:

- **Tu huella digital:** La huella digital se refiere a la información única y rastros digitales que dejamos en línea a través de nuestras actividades en la web. Esta huella puede incluir datos personales, publicaciones en redes sociales, historial de navegación y más. Es importante ser consciente de nuestra huella digital y cómo puede afectar nuestra privacidad y reputación en línea.
- **Riesgos en línea:** Identificamos varios riesgos en línea, como el ciberacoso, el phishing y la propagación de noticias falsas. Los riesgos en línea pueden tener consecuencias emocionales, sociales y de seguridad si no se manejan adecuadamente.
- **Seguridad de contraseñas:**

1. Se enfatizó la importancia de tener contraseñas seguras y únicas para cada cuenta en línea.

2. Se recomienda el uso de contraseñas largas que combinen letras, números y caracteres especiales.

3. Se destacó la importancia de no compartir contraseñas y de cambiarlas periódicamente.

- **Autenticación:**

1. La autenticación de dos pasos (2FA) se presentó como una forma efectiva de agregar una capa de seguridad adicional a las cuentas en línea.

2. Explicamos cómo 2FA utiliza un segundo paso, como un código de verificación en tu teléfono, para confirmar tu identidad.

11.

Para finalizar, presenta las **Conclusiones**. En este espacio, les darás la oportunidad a los estudiantes de aclarar conceptos y abordar preguntas finales, asegurando que comprendan adecuadamente lo tratado durante este segundo laboratorio.

Conversa con ellos sobre:

01

Los riesgos en línea

Hemos aprendido que debemos ser conscientes de los riesgos en línea y tomar medidas para proteger nuestra información y privacidad en línea.

La seguridad de las contraseñas en línea

Entendimos que las contraseñas son una parte fundamental de la seguridad en línea.

02

03

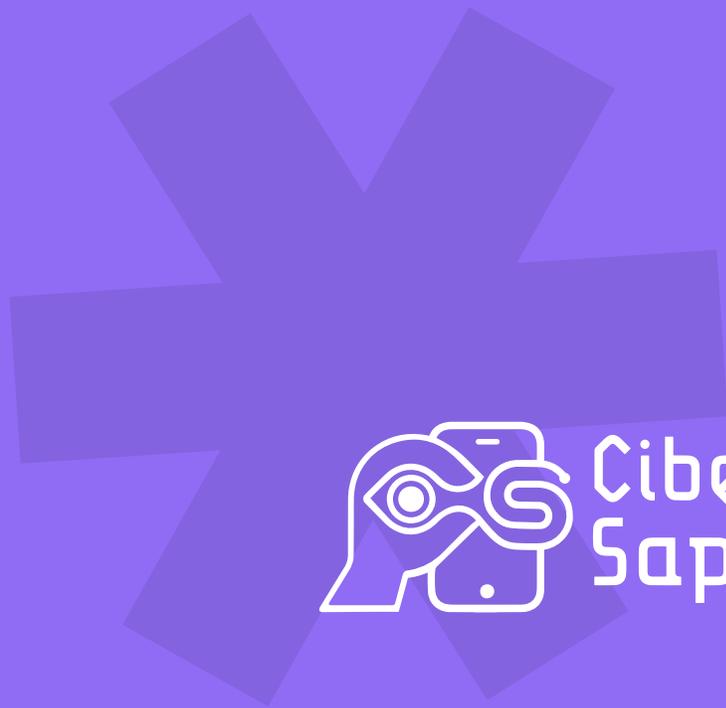
Huella digital

Ahora sabemos que cada uno de nosotros deja una huella digital en línea a través de nuestras actividades en Internet, y es importante ser consciente de ello.

Comparte por último esta reflexión: ***Recuerden que, la seguridad en línea es fundamental en el mundo digital actual. La educación y la concienciación sobre los riesgos en línea son esenciales para que protejamos nuestros datos y privacidad. Utilizar contraseñas seguras y adoptar medidas de autenticación adicionales, como 2FA, son prácticas recomendadas para mejorar la seguridad en línea.***

Cuéntales a tus estudiantes que hay un tercer laboratorio; explícales que trata sobre Construir relaciones positivas: respeto y aprendizaje colaborativo en línea. Anímalos a participar de este tercer encuentro y seguir aprendiendo más al respecto.





Ciber
Sapiens

UNIVERSIDAD
EAFIT[®]



SECRETARÍA
EDUCACIÓN

