#Generación Digital

Adolescentes seguros en la web

Google™

Introducción general

EL PROGRAMA

En Google creemos en el poder de la educación y la tecnología para mejorar la vida de estudiantes y educadores y construir nueva generación de aprendizaje en el aula. Si bien los estudiantes conviven a diario con el mundo digital, como educador es importante que cuentes con los recursos necesarios para ayudarlos a convertirse en ciudadanos digitales responsables.

Google ha desarrollado un programa de entrenamiento para docentes con el objetivo de generar y compartir conocimiento acerca del uso seguro de la web. El programa incluye actividades que están diseñadas para que los estudiantes aprendan a evaluar fuentes de información de manera crítica, incorporen el concepto de ciudadanía digital responsable, desarrollen habilidades para reconocer situaciones de riesgo en forma autónoma y tomen acciones que refuercen el uso seguro de los medios digitales.

OBJETIVOS GENERALES

- Promover el uso responsable de internet.
- Desarrollar habilidades que contribuyan a utilizar internet de forma segura.

OBJETIVOS ESPECIFICOS

- Desarrollar el sentido crítico para evaluar fuentes de información confiables en internet.
- Aprender a crear contraseñas fuertes y únicas.
- Comprender las pautas de conducta ética y responsable en internet.
- Aprender a reconocer engaños en línea y estrategias para prevenir el robo de identidad.
- Comprender qué información es apropiada publicar para salvaguardar la información personal y las cuentas en línea.

MÓDULOS TEMÁTICOS

1. Búsqueda de información en internet
2. Contraseñas seguras
3. Engaños virtuales
4. Ciudadanía digital responsable

ACTIVIDADES

En este cuadernillo se presentan un conjunto de actividades para alumnos de 10 a 14 años diseñadas para ser implementadas en el aula e integradas con el contenido de la currícula escolar. Como maestro, podés elegir aquellas que son más apropiadas para tus estudiantes, entorno de aprendizaje y que mejor se adaptan a las inquietudes actuales de la escuela. Si bien los módulos temáticos pueden ser implementados en cualquier orden, se recomienda seguir el hilo del cuadernillo.

APÉNDICE

El cuadernillo incluye un apéndice de consejos y herramientas gratuitas que te permitirán crear un entorno de navegación seguro en el aula. Estos recursos también pueden resultar de valor para trabajar conjuntamente con padres y madres.

Índice

MÓDULO 1

Búsqueda de información en internet

INTRODUCCIÓN

Internet es una extensa fuente de información. Es importante enseñar a los estudiantes a desarrollar una actitud crítica para que aprendan a evaluar y seleccionar información confiable.

OBJETIVOS DE APRENDIZAJE

- Reconocer la importancia de evaluar la confiabilidad de un sitio web.
- Evaluar la confiabilidad y la veracidad de las fuentes de información en internet.

TIEMPO ESTIMADO

40 minutos.

GUÍA DE TRABAJO

ACTIVIDAD 1 *(10 mins)*

Copiá las siguientes afirmaciones en el pizarrón y solicitá a los estudiantes que indiquen Verdadero o Falso en sus carpetas.

Sugerencia: si los estudiantes tienen acceso a dispositivos con conexión a internet, se recomienda realizar la actividad mediante la herramienta Google forms. **Enlace:** https://docs.google.com/forms/

¿Verdadero o Falso?

- Si puedo encontrarlo online, entonces debe ser cierto. (F)
- Siempre debo revisar las fuentes de información y los autores de un sitio web. (T)
- Hay un correo electrónico de contacto en el sitio web, por lo tanto, debe ser un sitio legítimo. (F)
- Hay un logo del gobierno en la parte superior de la página. Puedo confiar en este sitio. (F)
- Siempre debo comparar la información que encuentro en internet con al menos dos fuentes alternativas. (T)
- Hay muchos gráficos y cuadros en el sitio. Con toda esta información debe ser confiable. (F)
- Es evidente quién escribió el contenido porque hay información del contacto en el sitio, parece confiable y sin errores. Por lo tanto, puedo usar esta información para mis tareas escolares. (F)
- El sitio web se ve oficial. La información que ofrece debe ser confiable. (F)

ACTIVIDAD 2 *(10 mins)*

1.1 ¿Qué hace a un sitio web confiable? Solicitá a tus alumnos que creen un listado de factores que piensen hacen a un sitio confiable y lo compartan con el resto de la clase.

1.2 Discutí con el grupo los factores mencionados, haciendo énfasis en estos elementos:

- Cualquier persona puede escribir en internet.
- Aunque muchas cosas en internet son interesantes y ciertas, no podemos estar siempre seguros de que todo lo que encontramos es veraz.
- No todas las personas son expertas en el tema que escriben.
- Dado que no siempre sabemos quién escribió la información o si tiene las calificaciones necesarias para escribir sobre el tema, debemos estar atentos y verificar la información antes de confiar en ella.

1.3 Solicitá a los estudiantes que tomen nota de los criterios que deben utilizar para evaluar la confiabilidad de un sitio web

1. Quién: idoneidad del autor

- ¿Se puede identificar al autor en la página?
- ¿Hay información sobre los estudios y ocupación laboral del autor?
- ¿Hay citas bibliográficas que dirijan a fuentes confiables?
- ¿Hay sitios de referencia o enlaces?
- ¿Se trata de una opinión o es información derivada de un trabajo de investigación?

2. Qué: dominio y objetivos del sitio

- ¿El sitio pertenece a alguna entidad gubernamental, institución educativa u organización comercial?
- ¿A qué país pertenece el sitio web? (verificar el dominio: .ar para Argentina, .co para Colombia, .cl para Chile, .mx para México)

- ¿Cuál es el propósito del sitio (vender, informar, etc.)?
- ¿A qué audiencia se dirige el sitio web?

3. Cuándo: actualizaciones

- Si se requiere información actualizada vale la pena preguntarse: ¿Cuándo se publicaron los contenidos? ¿Son actuales? ¿Están vigentes?
- ¿El sitio web se actualiza regularmente? ¿Pueden encontrarse enlaces desactualizados?

4. Otros criterios:

- ¿Hay errores de ortografía?
- ¿Hay claridad en la redacción?

ACTIVIDAD 3 *(10 mins)*

Requerimientos técnicos: una computadora o tablet por grupo de alumnos.

Explicá a los estudiantes que practicarán cómo evaluar fuentes de información online respondiendo a la pregunta: ¿puede haber vida en otros planetas? Organizá a los alumnos en grupos y pediles que completen la información de la tabla para cada sitio web:

Sitio web 1: http://www.astromia.com/astronomia/vidasolar.htm
Sitio web 2: http://spaceplace.nasa.gov/review/dr-marc-solar-system/life-on-mars.sp.html
Sitio web 3: http://exploracionovni.com/

EVALUACIÓN DE SITIOS WEB	SITIO 1		SITIO 2		SITIO 3	
	Si	No	Si	No	Si	No
Idoneidad del autor						
Es claro quién escribió el contenido						
¿El autor es experto en el tema? ¿Tiene una buena reputación?						
¿Se puede verificar la información de contacto?						
Exactitud						
¿Pensás que el contenido es veraz?						
¿Hay errores de ortografía o redacción?						
Si hay fotos en el sitio, ¿creés que son reales?						
Objetividad						
¿Pensás que la información está completa y es objetiva?						
¿Hay anuncios en el sitio? ¿Se relacionan con el contenido?						
Actualizaciones						
¿Podés ver cuándo fue creado el contenido?						
¿Podés ver cuándo fue actualizado el contenido?						
¿Hay enlaces que no funcionan?						
Cobertura						
¿El tema es explicado en profundidad?						
¿Podés encontrar la información que estás buscando?						
¿Los enlaces de la página llevan a buenas fuentes de información?						

MENSAJE INTEGRADOR

"Siempre estamos evaluando lo que vemos y lo que oímos. Sin embargo, a veces nos olvidamos de hacerlo con la información que encontramos en línea. Internet nos permite encontrar casi cualquier información que deseamos pero sólo porque esté online no significa que sea cierta. Debés estar atento y preguntarte: ¿Cuál es el punto de vista del sitio?, ¿Qué están intentando que crea?, ¿Quién está publicando la información? Recordá que una fuente confiable, como una universidad, tiende a ser más creíble. Por último, seguí la fórmula del *qué, quién y cuándo* para evaluar un sitio web. Las respuestas a estas preguntas te ayudarán a saber si un sitio es lo suficientemente bueno para ser utilizado en la escuela: ¿quién creó el sitio?, ¿qué información podemos encontrar?, ¿cuándo fue actualizada?"

PARA REFORZAR LO APRENDIDO

1.1 Indicá a los estudiantes que revisen en casa los siguientes sitios y completen la información de la tabla:

SITIO WEB	AUTOR	TIPO DE CONTENIDO	TIPO DE SITIO	¿ES CONFIABLE?
www.rincondelvago.com				
es.wikipedia.org				
www.portales.educacion.gov.ar				
nuestrorincondelasciencias.blogspot.com.ar				
www.museo.fcnym.unlp.edu.ar				
www.meteored.com.ar				
franciscomietovidal.blogspot.com.ar				

1.2 Asimismo, solicitales que respondan las siguientes consignas:

- Mencioná tres tipos de sitios web que pueden ser confiables.
- Eligí uno de los sitios que consideraste como no confiable y explica porqué no lo es.

MÓDULO 2

Contraseñas seguras

INTRODUCCIÓN

En esta sección los estudiantes aprenderán cómo crear contraseñas únicas, fuertes y difíciles de adivinar.

OBJETIVOS DE APRENDIZAJE

- Aprender a crear contraseñas fuertes y únicas.
- Comprender porqué es importante salvaguardar las contraseñas.
- Incorporar buenas prácticas para proteger nuestras cuentas.

TIEMPO ESTIMADO

45 minutos.

GUÍA DE TRABAJO

ACTIVIDAD 1 *(15 mins)*

1.1 Copiá este listado de contraseñas en el pizarrón y permití a los estudiantes adivinar qué son.

Respuesta: contraseñas muy comunes y poco seguras.

- 123456
- Password
- 1234
- 12345678
- Qwerty
- Football
- Dragon
- 111111
- Abc123

Fuente: "Peores contraseñas de 2015". Disponible en: https://www.teamsid.com/worst-passwords-2015/

1.2 Preguntá a la clase:

- ¿Qué notan de estas contraseñas?
- ¿Cuántas sólo contienen números? ¿Cuántas sólo letras?
- ¿Cuán extensas son estas contraseñas?
- ¿Pueden sugerir otras malas contraseñas?
- ¿Cuáles son las ventajas y desventajas de crear contraseñas fáciles de recordar o contraseñas difíciles de adivinar?
- ¿Creés que es seguro usar la misma contraseña para todas las cuentas? ¿Por qué no?

1.3 A continuación, explicá los elementos a tener en cuenta para crear buenas contraseñas a partir de la información que se presenta en la tabla:

SI	NO
Usá al menos 6 caracteres, idealmente 8.	No uses información de tu identidad en la contraseña (nombre, dirección, correo electrónico, número de teléfono o de documento.
Combiná letras, números, símbolos, mayúsculas y minúsculas.	No uses una contraseña fácil de adivinar como el nombre de tu mascota o tu fecha de nacimiento.
Usá contraseñas distintas para cada cuenta importante que tengas.	No compartas tus contraseñas con nadie, excepto tus padres o adultos de confianza.
Intentá cambiar tu contraseña con regularidad, en lo posible, cada 6 meses.	No escribas tu contraseña para recordarla y, si vas a hacerlo, guardá el papel en un lugar seguro.

1.4 Explicá los métodos para crear contraseñas fuertes y fáciles de recordar:

Método 1 (nivel básico)

1. Pensá en una frase que te resulte divertida y fácil de recordar. Podés utilizar el título de tu canción, libro o película favorita, tu equipo de fútbol, etc.
2. Tomá la primera letra de cada palabra en la frase.
3. Cambiá algunas letras por símbolos.

4. Usá algunas letras mayúsculas y otras minúsculas.

A continuación un ejemplo:
Frase: Mi prima Laura tiene dos perros y un gato
Contraseña: MpLt2P&1g

Método 2 (nivel avanzado)
1. Pensá en una contraseña maestra súper fuerte basada en una frase
2. Modificala para cada sitio o aplicación que uses...de una forma que sólo vos sepas.

A continuación un ejemplo:
Frase: Mis papás juegan cartas dos veces por semana
Contraseña maestra: mPjC#2vS
Sitio web: Gmail
Contraseña para Gmail: mPjC#2vGMsAIL

ACTIVIDAD 2 *(15 mins)*

Copiá en el pizarrón la tabla de contraseñas que se muestra a continuación y solicitá a los alumnos que tomen nota de la siguiente situación:

Marina Gutiérrez vive en Mendoza con su familia (su papá Francisco, su mamá María, su hermano Juan, su hermana Jésica y su perro Rover) en la calle Roca 1557. Su cumpleaños es el 4 de marzo de 2003. Es fanática de Selena Gómez, le gusta escuchar música y leer libros. Ayer terminó Harry Potter y la Cámara de los Secretos. Acaba de abrir una cuenta de correo electrónico y no sabe qué contraseña utilizar. ¿Podés ayudarla a elegir entre las siguientes opciones? Indicá en la tabla cuáles te parecen fuertes, moderadas o débiles y porqué.

CONTRASEÑA	CLASIFICACIÓN *(respuestas)*	PORQUÉ *(respuestas)*
Gutierrez	Débil	Apellido.
Roca1557	Débil	Dirección de su casa.
Selena1557	Moderada	Cantante favorita y dirección del hogar.
MGLhp&e1c	Fuerte	Aleatorio y difícil de adivinar: "Mónica Gutiérrez lee Harry Potter y escucha una canción".
MaRo1557	Moderada	Primeras dos letras de su nombre, el de su perro y el número de su casa.
04032003	Débil	Fecha de nacimiento.
FrMa0403	Moderada	Primeras dos letras del nombre de su papá, de su mamá, día y mes de su nacimiento.

ACTIVIDAD 3 *(15 mins)*

Indicá a los estudiantes que creen dos nuevas contraseñas fuertes y fáciles de recordar para Marina a partir de estos elementos:
- Pensá una frase
- Elegí la primera letra o dos letras de cada palabra en tu frase

- Cambiá algunas letras por símbolos
- Cambiá algunas letras por mayúsculas y minúsculas
- Usá por lo menos 6 caracteres

MENSAJE INTEGRADOR

"Elegir la misma contraseña para todas tus cuentas es como usar la misma llave para la puerta de tu casa y el candado de tu bicicleta. Si alguien logra el acceso a una de ellas, todas las demás están en riesgo. Por lo tanto, no utilices la misma contraseña para tu correo electrónico y tus redes sociales. Puede que te parezca menos conveniente, pero elegir contraseñas distintas ayuda a proteger tu información personal y evitar que cualquier persona acceda a ella".

ACTIVIDAD 4 *(15 mins)*

1.1 Explicá a los estudiantes que tendrán la posibilidad de practicar sus habilidades para crear contraseñas en el "Juego de las Contraseñas". Enfatizá en la idea de crear contraseñas fuertes y fáciles de recordar. Dividí a los estudiantes en grupos pequeños e indicales que tienen 40 segundos para crear una contraseña. Invitá a dos grupos al frente para que escriban las contraseñas que pensaron en el pizarrón. Realizá una votación de la contraseña más fuerte con el resto de la clase y pedí que justifiquen su voto en voz alta.

Sugerencia: si tenés acceso a un proyector y computadora, podés introducir cada contraseña en este sitio web para que mida su fortaleza y seguridad: http://password.social-kaspersky.com/es

1.2 Mientras tanto, anotá la contraseña ganadora en un papel y luego borrala del pizarrón. Pedile al equipo ganador que diga la contraseña de memoria y confirmá con tus notas si es correcta.

PARA REFORZAR LO APRENDIDO

Pedile a los estudiantes que hagan su propia investigación sobre contraseñas.

1.1 Creá una encuesta sobre contraseñas y pedile a familiares y amigos que respondan las preguntas. Recordá que no debés pedirles sus contraseñas sino qué tipo de información utilizan para crearlas. Documentá las respuestas para compartir con tus compañeros en la próxima clase. Podés usar estas preguntas a modo de referencia:

- ¿Cuál es la extensión de tu contraseña?
- ¿Tiene símbolos?
- ¿Tiene números?
- ¿Escribís tus contraseñas en algún lugar para recordarlas?
- ¿Utilizás la misma contraseña en distintas cuentas?
- ¿Utilizás nombres o fechas en tus contraseñas?

1.2 Una vez que completes la encuesta respondé: ¿qué aprendiste sobre los hábitos de las personas para crear contraseñas?

MÓDULO 3

Engaños virtuales

INTRODUCCIÓN

En este módulo, los estudiantes aprenderán a reconocer engaños virtuales, desarrollar habilidades para el autocuidado e incorporar buenas prácticas para navegar seguros en internet.

OBJETIVOS DE APRENDIZAJE

- Aprender a reconocer engaños virtuales.
- Desarrollar estrategias para evitar el robo de identidad y los datos personales.
- Tomar acciones frente a un engaño virtual.

TIEMPO ESTIMADO

60 minutos.

GUÍA DE TRABAJO

ACTIVIDAD 1 *(15 mins)*

1.1 Comenzá la lección con algunas preguntas disparadoras para determinar el nivel de conocimiento de los estudiantes. Podés pedirles que debatan en grupo o realicen entrevistas a sus compañeros.

PREGUNTAS	OBJETIVO
¿Conocés a alguien que haya sido víctima de una estafa? ¿Qué le pasó?	Permití a los estudiantes compartir historias que les hayan sucedido o que hayan escuchado sobre otras personas.
¿Cuál es el propósito de una estafa o engaño? ¿Qué trucos se utilizan para llevar adelante una estafa?	Es importante que los estudiantes comprendan que la finalidad de estos engaños es hacerse con dinero o información que permita acceder al dinero como números de tarjeta, contraseñas, etc. Para lograrlo, los estafadores se hacen pasar por otras personas o dan información falsa.
¿Las personas pueden ser engañadas por internet? ¿De qué manera?	Permití a los estudiantes compartir historias que les hayan sucedido a ellos o a sus amigos a través de internet.

A modo de síntesis, explicá a los estudiantes que en esta lección aprenderán acerca de las estafas virtuales, qué tipo de información buscan los estafadores y cómo puede ser utilizada. También aprenderán cómo protegerse ante este tipo de engaños.

A continuación, encontrarás algunos términos que pueden ser de utilidad para realizar las actividades:

- **Engaño virtual:** intento de estafa para que se proporcione información personal o dinero de forma fraudulenta.
- **Información personal:** cualquier información que revele algo sobre la identidad de una persona (nombre, edad, escuela, número de identificación personal, teléfono, etc.)
- **Ingeniería social o phishing:** tipo de engaño que busca robar información personal y financiera haciéndose pasar por alguien de confianza como un amigo, el banco o el proveedor de correo electrónico.
- **Mensaje en cadena:** carta, correo electrónico o mensaje que solicita reenviar un mensaje a nuestros contactos o amigos.
- **Pop-up o mensaje emergente:** mensaje que aparece mientras navegás en internet para informarte que ganaste un premio y pedirte que descargues un archivo o ingreses datos personales.
- **Robo de identidad:** apropiación o robo de información personal para ser utilizada en actividades criminales.
- **Virus o software malicioso:** programa aparentemente legítimo o inofensivo que al ejecutarlo ocasiona daños en el funcionamiento del dispositivo.

1.2 Solicitá a los estudiantes que compartan con la clase qué tipo de información creen que los estafadores virtuales buscan y anotala en el pizarrón. Hacé hincapié en que los estafadores usualmente buscan cualquier tipo de información que pueda ayudarlos a hacerse pasar por sus víctimas.

1. Nombre completo
2. Fecha y lugar de nacimiento
3. Direcciones actuales y pasadas
4. Números de teléfono y celular
5. Números de cuentas bancarias o de compras (por ejemplo: Amazon, eBay, PayPal, etc.)
6. Número de pasaporte o documento
7. Nombres de usuario y contraseñas

ACTIVIDAD 2 *(15 mins)*

Indicá a los estudiantes que verán algunos ejemplos reales de estafas virtuales. Pediles que trabajen en parejas para identificar al menos tres indicios de engaño en los correos electrónicos que pueden alertarlos que se trata de una estafa. Para cada ejemplo, discutí con los estudiantes los riesgos, las medidas preventivas y qué acciones tomar en caso que se encuentren ante un engaño.

Indicios de Ingeniería Social en los correos electrónicos:
- Solicita verificar datos de la cuenta
- Solicita hacer click en un enlace o descargar un archivo adjunto
- Genera un sentido de urgencia y proporciona poco tiempo para responder
- Ofrece algo demasiado bueno para ser cierto
- Se observan errores de redacción o de ortografía
- El encabezado muestra un saludo genérico, no dirigido al receptor
- Se alerta sobre problemas en la cuenta

1) Correo electrónico del banco:
De: noreply@banco_nacion.com
Asunto: Actualización del Estado de su Cuenta

Estimado Cliente:
Debido a una reciente verificación de seguridad en su cuenta, debemos confirmar sus datos. De no registrarse la confirmación en las próximas 24 horas, su cuenta será suspendida. Por favor, haga click en el siguiente enlace para confirmar su cuenta bancaria: https://login.personal.bank.com/verification.asp?d=1
Si decide no responder este mensaje, nos veremos obligados a suspender temporalmente su cuenta.

Atentamente
Servicio al Cliente Banco Nación
Departamento de Seguridad Electrónica

2) Actualización de tu cuenta de GMAIL:
De: servicioalcliente@gmaiil.com
Asunto: Cambio de contraseña

Estimado/a:
Por motivos de seguridad, necesitamos actualizar la información de su cuenta de correo electrónico ya que nuestrso sistemas han detectado un acceso no autorizado. Por favor, responda este correo con su usuario y contraseña antes del 1/12 o su cuenta será suspendida de forma indeterminada. Muchas gracias por su comprensión.

El Equipo de Gmail

3) Estafa de premios
De: encuestasmx@encuestas.com
Asunto: ¡Felicitaciones! Participas por 150USD

Estimado Sr/Sra,
¡Felicitaciones! Usted ha sido seleccionado para participar de una encuesta de opinión para ciudadanos de habla hispana. Le tomará sólo 5 minutos. Todas sus respuesta son confidenciales y serán utilizadas con fines de investigación. Para completar la encuesta haga click en el enlace a continuación:
https://encuestaonline.com/Survey/250Dollar.html
Cada persona que complete la encuesta recibirá un cheque por $150 USD.

Gracias por su participación.
Atentamente,
John Muller
Survey Manager

ACTIVIDAD 3 *(15 mins)*

1.1 Explicá a los estudiantes que se les mostrará un video desarrollado por Google sobre cómo evitar los ataques de ingeniería social en la web. Solicitá que tomen nota de los consejos para prevenirlos y los compartan con la clase.
Enlace al video: https://goo.gl/JZFwDx

1.2 Podés sintetizar el debate a partir de la información que se presenta a continuación:

CÓMO RECONOCER UN ENGAÑO VIRTUAL	
¿Ofrece algo de manera gratuita?	Las ofertas gratuitas o demasiado buenas para ser ciertas suelen ser un engaño para acceder a tu información personal. Por ejemplo, los "tests de personalidad" son una forma de conocer información sobre vos para que resulte más fácil adivinar tu usuario y contraseña.
¿Solicita el envío de datos personales?	La mayoría de los negocios legítimos nunca solicitan el envío de información personal (números de cuenta, contraseñas, identificación, etc.) por correo electrónico.
¿Se trata de un mensaje en cadena?	Los mensajes en cadena pueden ponerte en riesgo. No los reenvíes a tus contactos.

CÓMO EVITAR UN ENGAÑO VIRTUAL	
Pensá antes de hacer click.	No hagas click en ningún enlace o archivo adjunto en un correo que parezca sospechoso.
Evitá los concursos en los mensajes emergentes (pop-ups).	Es improbable que ganes el concurso. Por lo general, estos mensajes buscan recolectar información personal o infectar tu computadora con software malicioso.
No respondas correos que solicitan el envío de información personal.	Hacé una búsqueda del nombre de la empresa en la web antes de dar cualquier información personal.
Leé la letra chica.	La página puede decir que ganaste una tablet pero si leés la letra chica verás que hay que pagar $200 al mes para obtenerla.

¡OH, NO! CAÍ EN LA TRAMPA. ¿QUÉ DEBO HACER?	
Avisá a un adulto de confianza.	Mientras más demores, más graves pueden ser las consecuencias.
Si estás preocupado por tu cuenta bancaria o tarjeta de crédito.	Contactá al banco o la tarjeta de crédito inmediatamente por teléfono.
Si recibiste una estafa por correo electrónico o en tu red social.	Marcala como "correo basura" o "spam" en tu correo o reportala en tu red social.

ACTIVIDAD 4 *(15 mins)*

En esta actividad se enseñará a los estudiantes cómo identificar sitios web legítimos y seguros. Esto es especialmente importante para iniciar sesión en el correo personal, red social o para realizar compras en línea.

1.1 Comenzá la lección preguntando a los estudiantes si conocen el significado del término "encriptación". A continuación, explicá el origen de la encriptación y cómo se utiliza actualmente.

Encriptación: consiste en cifrar la información de manera tal que sólo quien tiene acceso al código secreto puede leerla. La encriptación es un método muy antiguo y se ha utilizado con diversos fines. Por ejemplo, la leyenda cuenta que en la Antigua Grecia cada vez que un general deseaba enviar un mensaje secreto a la ciudad, solicitaba rasurar la cabeza de un soldado para escribir el mensaje en su cuero cabelludo. Tan pronto el cabello crecía, el mensaje quedaba oculto en la cabeza del soldado. De esta forma, cuando llegaba a la ciudad, el oficial sabía cuál era el "código secreto": rasurar la cabeza del soldado para revelar el contenido del mensaje.

Hoy en día, la encriptación es fundamental para el comercio electrónico y el inicio de sesión porque permite enviar información confidencial de manera segura entre servidores. Los sitios web encriptan la información mediante un método llamado 'SSL' (en inglés: Secure Socket Layer). Podés identificarlo cuando aparece un candado verde en el margen izquierdo de la barra del navegador y la URL comienza con la leyenda HTTPS:// ('S' significa seguro).

1.2 Luego explicá que la mayoría de los sitios web tienen distintos niveles de seguridad en su conexión y solicitá a los alumnos que adivinen qué significa cada color.

Sugerencia: si tenés una computadora, podés realizar esta actividad con ejemplos reales.

NIVELES DE CONEXIÓN	
Candado verde	La conexión está encriptada y la identidad del sitio fue verificada.
Candado gris o ausencia de candado	La conexión al sitio puede estar encriptada, pero Google Chrome encontró algo en la página, como imágenes inapropiadas o anuncios. Se recomienda no ingresar información personal.
Candado rojo	Hay problemas con el certificado del sitio. Procedé con cautela porque alguien en la red (por ejemplo: alguien que usa tu mismo WiFi) podría poner tu información en peligro. Si ingresás información personal en el sitio, como tu tarjeta de crédito o contraseña, otras personas podrían verla.

MENSAJE INTEGRADOR

"Para evitar ser víctima de una estafa en la web es importante prestar mucha atención a los correos que recibimos, las ventanas emergentes, las cadenas de mensajes y los signos de páginas seguras (candados). Y, si tenés dudas, siempre pensá dos veces antes de hacer click".

PARA REFORZAR LO APRENDIDO

Solicitá a los estudiantes que creen un correo que incluya los elementos estudiados en clase y lo intercambien con un compañero para que identifique los indicios de engaño.

MÓDULO 4

Ciudadanía digital responsable

INTRODUCCIÓN

En este módulo, los estudiantes aprenderán a manejar su huella digital, comprenderán que las normas de convivencia son necesarias en la interacción del mundo digital y desarrollarán habilidades para actuar como ciudadanos digitales responsables.

OBJETIVOS DE APRENDIZAJE

- Aprender a manejar la huella digital.
- Reflexionar sobre las normas que rigen la convivencia en internet.
- Asumir un rol activo como Ciudadanos Digitales responsables.

TIEMPO ESTIMADO

45 minutos.

GUÍA DE TRABAJO

ACTIVIDAD 1 *10 mins)*

Comenzá la lección con un debate acerca de la importancia de manejar la información que compartimos en internet. Explicá las características de la información que compartimos en la web:

1. **Es fácil de encontrar:** la información que publicamos en internet tiene el potencial de ser vista por cualquiera, incluso por personas que no conocés y no son tus amigos.
2. **Se puede viralizar:** nuestras publicaciones pueden ser compartidas, copiadas, reenviadas y viralizadas rápidamente.
3. **Afecta tu reputación:** lo que otras personas piensan sobre vos se puede ver afectado por lo que compartís en internet y traerte consecuencias negativas en el futuro (pensá, por ejemplo, en tu futuro empleo o ingreso a la universidad).
4. **Permanece:** lo que compartimos en internet es muy difícil de borrar porque otras personas pueden haberlo fotografiado o reenviado antes que vos decidas eliminarlo.

1.1 Pedí a los estudiantes que reflexionen acerca de lo que habitualmente comparten en internet. Podés utilizar estas preguntas como guía: ¿Qué tipo de información publicás en internet?, ¿alguna vez te arrepentiste de lo que publicaste?, ¿te sentirías cómodo si tus papás, maestros o abuelos vieran todo lo que compartís en la web? Podés complementar la actividad con ejemplos de casos reales.

1.2 Para sintetizar, explicá el concepto de "huella digital" (es el rastro que dejan nuestras acciones en internet, como fotos, comentarios, videos y publicaciones).

1.3 Copiá las siguientes publicaciones en el pizarrón y pedile a los estudiantes que evalúen el nivel de privacidad de cada una (pública, privada, sólo algunas personas).

- Próximo martes a las 4pm fiesta en casa (Avenida Córdoba 1567). ¡Todos invitados!
- La nueva película de Disney está increíble. Hoy voy a verla por segunda vez.
- Odio la escuela...ojalá no tuviera que estudiar más!!!
- Protejamos a los animales en Argentina. Firmá la petición ahora.
- Fin de semana en la playa. ¡Aquí voy! #sol #playa #mdq
- Me robaron el celu :(nuevo número: 1554657654

ACTIVIDAD 2: *(15 mins)*

1.1 Solicitá a los estudiantes que revisen los perfiles que se presentan a continuación y usen tres palabras para describir a la persona o perfil.

Perfil 1

- Nombre: Sofía Fernández
- Número de teléfono: 15 4176 5463
- Dirección: Aráoz 671
- Estado: soltera
- Fecha de nacimiento: 25 de enero
- Intereses: comedias, One Direction, Justin Bieber, bailar, perros
- Publicación: "Hoy 19 hs juntada en el Abasto"

- Publicación: “November Rain”. La única canción en todo el mundo que podría escuchar 38199 veces y nunca me cansaría...
- Publicación: “Sofía just checked in: Palermo, Buenos Aires”
- Publicación: “Por favor compartan y comenten! Nuevo video de One Direction”
- Publicación: “Playa, arena y sol. Aquí vamos :)”

Perfil 2
- Nombre: Marco Santillán
- Teléfono: privada
- Dirección: privada
- Estado: privado
- Fecha de nacimiento: privado
- Intereses: Ciencia Ficción, tecnología, juegos en línea, Hunger Games
- Publicación: “Star wars la mejor película de todos los tiempos #goingcrazy”
- Publicación: “Vendo teléfonos celulares nuevos y liberados. Interesados por inbox”

Perfil 3
- Nombre: Ximena Figueroa
- Teléfono: Si sos mi amigo, sabés mi número
- Dirección: Mi casa
- Estado: privado
- Fecha de nacimiento: 17 de mayo
- Intereses: Violetta, Demi Lovatto, Endless Love, Monsters Inc, Iggy Azalea
- Publicación: privado

1.2 Discutí las siguientes preguntas con los estudiantes:

- ¿Qué tipo de información comparten estos perfiles? ¿Hay algo que no debiera ser publicado? ¿Por qué?
- ¿Creés que lo que publican en su perfil puede incidir en su futuro? Justificá
- ¿Por qué creés que es importante manejar la huella digital?

ACTIVIDAD 3 *(15 mins)*

1.1 Organizá a los estudiantes en grupos de 4 a 5 personas. Cada grupo representará una comunidad en línea. Puede tratarse de una comunidad real o imaginaria, grande o pequeña. Solicitá a cada grupo que invente un nombre (por ejemplo: La sociedad de los fanáticos de la pizza, La Asociación de Amantes de Perros, etc.), una misión y seis reglas para su comunidad – 3 reglas sobre lo permitido y 3 reglas sobre lo prohibido necesarias para que la comunidad funcione bien. Deberán justificar la finalidad de cada regla. Luego, pedí que cada grupo elija un embajador que explique al resto de la clase la comunidad que crearon, sus reglas y propósitos.

1.2 Discutí con los estudiantes las siguientes preguntas:

- ¿Las reglas son aplicables a otras comunidades?
- ¿Qué pasaría si no existieran?
- ¿Son aplicables a las comunidades offline?
- ¿Creen que es más sencillo romper las reglas online? ¿Por qué? (reforzá la idea de que las reglas de buena ciudadanía aplican tanto en el mundo offline como online)

1.3 Solicitá a los estudiantes que piensen posibles conflictos que pueden surgir en las interacción de sus comunidades y qué acciones tomarían para resolverlos. Posibles respuestas: miembros ofensivos, mensajes violentos, incumplimiento de las normas, etc.

Elementos a tener en cuenta para la resolución de conflictos online:
- No respondas
- No tomes venganza
- Utilizá las herramientas para reportar
- Guardá la evidencia
- Pedí ayuda
- Tomá la iniciativa para defender a quién es agredido, no seas un mero espectador

MENSAJE INTEGRADOR

"Al igual que en el mundo offline, existen reglas de buena ciudadanía que debemos cumplir en en el mundo online. Recordá: la comunidad en línea es una comunidad global de personas conectadas a internet. Cuando participas de ella, se espera que puedas cumplir con las normas que regulan ese espacio"

PARA REFORZAR LO APRENDIDO

1.1 Solicitá a los estudiantes que diseñen su propia huella digital (10 a 12 años)

¿Qué tipo de información te gustaría encontrar sobre vos en internet en 10 años? Diseñá tu propia huella digital y llenala con imágenes, hitos y toda aquella información que te gustaría ver asociada a tu nombre en el futuro. ¡Dejá volar tu imaginación!

1.2 Solicitá a los estudiantes que revisen la privacidad de sus redes sociales (13 años y más)

Ingresá a la configuración de privacidad de tu red social y verificá:
- ¿Qué tipo de información estás compartiendo?
- ¿Hay muchos detalles públicos sobre tu vida privada ?
- ¿Hay alguna información que podría ponerte en riesgo?
- ¿Cuál es el tono de tus publicaciones? ¿Positivas y amigables? ¿Negativas y ofensivas?

Editá tu perfil y cambiá la información que consideres puede ponerte en riesgo o causar una mala imagen ante otras personas.

APÉNDICE

Consejos y herramientas

SAFESEARCH

SafeSearch es un filtro de seguridad gratuito que puede ayudarte a bloquear imágenes inadecuadas o explícitas de los resultados de la Búsqueda de Google. Si SafeSearch está activado, las imágenes y los vídeos con contenido sexual explícito, así como los resultados que puedan dirigir a contenido explícito, se excluirán de las páginas de resultados de la Búsqueda de Google. Si utilizás una computadora o tablet, podés bloquear SafeSearch para evitar que otros usuarios lo desactiven. Esta opción es útil si hay niños cerca o si otros usuarios utilizan tu computadora.
Enlace: https://goo.gl/f8ZTNx

MODO RESTRINGIDO EN YOUTUBE

El Modo restringido es una configuración que te ayuda a descartar contenido potencialmente ofensivo que no querés ver en YouTube. El Modo restringido se habilita en el nivel del navegador o del dispositivo, así que debes habilitarlo en cada uno de los navegadores que uses. Si el navegador admite varios perfiles, debés habilitarlo para cada perfil.
Enlace: https://goo.gl/ZdikZo

REPORTAR CONTENIDO EN YOUTUBE

YouTube permite a los usuarios reportar vídeos, comentarios y canales inapropiados, así como bloquear otros usuarios de la plataforma. El equipo de YouTube revisa el contenido reportado las 24 horas y remueve aquel que viola las Reglas de la Comunidad.
Enlace: https://goo.gl/OAmAqj

USUARIOS SUPERVISADOS DE CHROME

Podés crear una cuenta de usuario supervisado para controlar los sitios web a los que acceden otros usuarios en Chrome. Por ejemplo, podés configurar una cuenta para tu hijo o hija y controlar diferentes acciones en Chrome, como permitir o bloquear determinados sitios web, consultar los sitios web que visitaron, ajustar la configuración del usuario, etc.
Enlace: https://goo.gl/mtHfMq

PERFILES RESTRINGIDOS PARA ANDROID

En la tablet, podés elegir las aplicaciones, las funciones y el contenido al que tiene acceso un usuario restringido. Por ejemplo, podés crear un perfil restringido para evitar que un miembro de la familia use la tablet para mirar contenido para adultos.
Enlace: https://goo.gl/KTYaCN

MI CUENTA

Mi cuenta te brinda acceso rápido a las opciones de configuración y las herramientas que te permiten proteger los datos y la privacidad en productos como Gmail, YouTube, Google+, Maps, etc.
Enlace: https://goo.gl/uzkpgE

CENTRO DE SEGURIDAD

Aprende más sobre lo que podés hacer para proteger a tus alumnos cuando navegan en internet.
Enlace: g.co/CentrodeSeguridad

Notas

Google™