**Preguntas para Profesores**

**1. Conocimientos actuales sobre privacidad y seguridad digital**

Hoy en día, casi todo lo que hacemos en internet deja un rastro: cuando usamos redes sociales, descargamos aplicaciones, compramos algo en línea o incluso cuando los alumnos entregan tareas en plataformas digitales. En todas esas situaciones, se piden datos personales como nombre, correo, dirección, fotos o hasta la ubicación. Sin embargo, no todas las personas saben realmente cómo se debe proteger esa información, qué derechos tienen sobre ella o qué pueden hacer si alguien la usa sin su permiso.

**¿Qué tan familiarizado está con el tema de protección de datos personales?**

1. Nada familiarizado (no conozco casi nada del tema)
2. Poco (he escuchado, pero no lo entiendo bien)
3. Algo (tengo una idea general, aunque no lo aplico mucho)
4. Muy familiarizado (conozco el tema y sé cómo aplicarlo en la práctica)

En México, todas las personas tienen derechos sobre su propia información personal. Por ejemplo, si una empresa, una escuela o una aplicación guarda tus datos, tú puedes pedir ver qué información tienen (Acceso), corregirla si está equivocada (Rectificación), pedir que la eliminen cuando ya no quieras que la usen (Cancelación) o solicitar que no la utilicen para ciertos fines, como publicidad (Oposición). Estos se conocen como **Derechos ARCO** y son la base legal para que nadie use tus datos sin tu permiso.

**¿Conoce los Derechos ARCO (Acceso, Rectificación, Cancelación y Oposición)?**

* Sí (los conozco y sé de qué tratan)
* No (nunca los he escuchado)
* He escuchado, pero no los manejo bien (sé que existen, pero no estoy seguro de cómo se aplican)

Cada vez que un alumno usa internet, deja un rastro de su actividad: lo que publica en redes sociales, los videos que ve, las fotos que sube, las páginas que visita o hasta los "likes" que da. A toda esta información se le llama **huella digital**. Esta huella puede ser positiva si muestra logros y aprendizajes, pero también puede ser riesgosa si incluye datos personales, imágenes privadas o comentarios que los acompañarán incluso cuando quieran borrarlos. Comprender este concepto ayuda a enseñar a los alumnos a pensar antes de publicar o compartir algo en línea.

**¿Qué tanto sabe sobre la huella digital que dejan los alumnos en internet?**

* Nada (no conozco el concepto)
* Poco (lo he escuchado, pero no lo entiendo bien)
* Suficiente (sé qué significa y cómo afecta a los alumnos)
* Mucho (lo conozco y puedo explicarlo claramente a mis estudiantes)

En internet, los alumnos pueden encontrarse con varios tipos de riesgos:

* **Phishing:** mensajes o correos que parecen legítimos, pero buscan engañarlos para robar contraseñas, datos o dinero.
* **Grooming:** cuando un adulto intenta ganarse la confianza de un menor para manipularlo o explotarlo sexualmente.
* **Ciberacoso:** burlas, amenazas o humillaciones que ocurren en redes sociales, chats o grupos de la escuela.

Identificar estos riesgos es fundamental para poder prevenirlos y enseñar a los estudiantes a actuar de manera segura cuando los enfrenten.

**¿Sabe identificar riesgos como phishing, grooming o ciberacoso?**

* Sí, todos
* Algunos
* Muy pocos
* Ninguno

Muchos estudiantes usan internet a diario para redes sociales, juegos, tareas o chats, pero no siempre son conscientes de que lo que comparten puede ser visto por personas que no conocen, puede afectar su reputación o incluso poner en riesgo su seguridad. Entender la **importancia de la privacidad en internet** significa reconocer que no todo debe compartirse y que hay que proteger datos personales como fotos, ubicación, contraseñas y mensajes privados.

**¿Qué tanto cree que los estudiantes entienden la importancia de su privacidad en** internet?

* Nada (no tienen conciencia de los riesgos)
* Poco (saben algo, pero no lo aplican)
* Regular (tienen cierta idea y tratan de cuidarse)
* Mucho (son conscientes y aplican medidas de protección)

**2. Prácticas en el aula**

En algunas clases, los docentes aprovechan el momento para hablar con los estudiantes sobre cómo navegar de manera segura, cómo proteger sus contraseñas, cómo identificar mensajes sospechosos o cómo comportarse responsablemente en redes sociales. Estas prácticas ayudan a que los alumnos comprendan mejor los riesgos y aprendan a cuidar su información personal mientras usan internet.

**¿Ha trabajado temas de seguridad digital o uso responsable de internet en su clase?**

* Sí, frecuentemente (lo abordo de manera regular en mis clases)
* Algunas veces (lo he tratado en algunas ocasiones)
* Rara vez (muy pocas veces lo he mencionado)
* Nunca (no he abordado este tema en mis clases)

Los temas de seguridad digital y privacidad pueden enseñarse en diferentes materias según cómo se integren al plan de estudios. Por ejemplo:

* En **Tecnología o Computación**, los alumnos pueden aprender sobre contraseñas, seguridad de dispositivos y configuración de privacidad en apps.
* En **Formación Cívica y Ética**, se pueden abordar valores, respeto a la privacidad de otros y responsabilidad en redes.
* En **Tutoría u orientación**, se puede hablar de casos concretos de ciberacoso o riesgos digitales y cómo pedir ayuda.
* También podrían integrarse en otras materias de forma transversal.

**¿En qué materias cree que encajan mejor estos temas?**

* Tecnología / Computación
* Formación Cívica y Ética
* Tutoría u orientación
* Otra (especificar)

Cuando los docentes explican riesgos digitales usando **situaciones reales**, los alumnos suelen comprender mejor y recordar la información. Por ejemplo, mostrar casos de ciberacoso que sucedieron en otras escuelas, mensajes de phishing que recibieron estudiantes o noticias sobre robo de información ayuda a que vean que los riesgos son reales y que la privacidad en internet es importante.

**¿Utiliza ejemplos de la vida real para explicar riesgos en línea?**

* Sí, siempre (los incorporo en todas mis clases)
* Algunas veces (los uso ocasionalmente)
* Casi nunca (raramente uso ejemplos concretos)
* Nunca (no los utilizo)

A veces los alumnos se acercan al maestro para contar que han sido molestados en redes sociales, que alguien les pidió información personal, o que vivieron algún tipo de ciberacoso. La forma en que el docente reacciona puede marcar la diferencia: ayudar al alumno, derivarlo a especialistas de la escuela o involucrar a los padres puede protegerlo y enseñarle cómo manejar estas situaciones.

**Cuando un alumno comenta una experiencia de ciberacoso o problema digital, ¿qué hace?**

* Lo atiendo directamente (ofrezco apoyo inmediato y consejos)
* Lo canalizo a la dirección/psicología (derivo a especialistas para que intervengan)
* Lo comento con padres o tutores (busco que los padres también actúen)
* No sé cómo actuar (no estoy seguro de la mejor manera de ayudar)

Existen cursos, talleres o programas de formación que enseñan a los docentes sobre **seguridad digital, privacidad y ciberacoso**, con estrategias para prevenir riesgos y apoyar a los estudiantes. Recibir capacitación formal permite estar mejor preparado para enseñar y reaccionar adecuadamente ante problemas digitales.

¿Ha recibido capacitación formal sobre estos temas?

* Sí (he participado en cursos o talleres oficiales)
* No (nunca he recibido capacitación formal sobre seguridad digital y privacidad)

**3. Capacitación e intereses**

Los docentes pueden interesarse en diferentes áreas dentro de la seguridad digital y la privacidad según sus necesidades o el contexto de sus clases:

* **Huella digital y redes sociales:** aprender cómo los alumnos dejan rastros en internet y cómo enseñarlos a protegerlos.
* **Creación de contraseñas seguras:** conocer métodos prácticos para proteger cuentas y enseñar a los alumnos a hacer lo mismo.
* **Legislación mexicana en privacidad:** comprender las leyes que protegen los datos personales y cómo aplicarlas en la escuela.
* **Estrategias para prevenir ciberacoso:** aprender técnicas para detectar, prevenir y actuar ante situaciones de acoso en línea.

**¿Qué tema le interesaría más aprender?**

* Huella digital y redes sociales
* Creación de contraseñas seguras
* Legislación mexicana en privacidad
* Estrategias para prevenir ciberacoso

Los docentes pueden aprender sobre seguridad digital y privacidad de distintas maneras según lo que les resulte más cómodo y útil:

* **Curso presencial:** asistir a clases en persona con un instructor que explique los temas y resuelva dudas.
* **Curso en línea:** estudiar desde cualquier lugar, a su ritmo, usando plataformas digitales.
* **Taller práctico:** aprender mediante ejercicios y actividades donde se simulan situaciones reales.
* **Manual o guía descargable:** tener un documento que puedan consultar cuando lo necesiten, con ejemplos y consejos prácticos.

**¿Qué tipo de capacitación preferiría?**

* Curso presencial
* Curso en línea
* Taller práctico
* Manual o guía descargable

Una **plataforma gamificada** usa juegos, retos o dinámicas interactivas para enseñar a los alumnos sobre privacidad digital, seguridad en internet y cuidado de sus datos personales. Este tipo de herramientas puede hacer que los estudiantes se involucren más, aprendan jugando y retengan mejor la información que con métodos tradicionales de enseñanza.

**¿Qué tanta importancia le daría a una plataforma gamificada para enseñar a adolescentes sobre privacidad?**

* Ninguna (no la considero útil)
* Poca (creo que no aporta mucho)
* Regular (podría ser útil en algunos casos)
* Mucha (es muy útil y motivadora para los alumnos)

Si existiera una plataforma que enseñara a los alumnos sobre **privacidad digital, riesgos en internet y seguridad de datos** de manera interactiva y divertida, la disposición del docente a integrarla en sus clases es clave. Esta pregunta busca conocer qué tan abierto estaría a **incorporar nuevas herramientas digitales** para mejorar el aprendizaje de los estudiantes sobre estos temas.

**¿Qué tan dispuesto estaría a usar esa plataforma en sus clases?**

* Nada (no la usaría)
* Poco (probablemente no la usaría)
* Regular (podría usarla de vez en cuando)
* Mucho (la integraría de manera constante en mis clases)

La seguridad y privacidad en internet no solo dependen de los estudiantes, sino también del acompañamiento de los padres o tutores. Los adultos pueden enseñar hábitos seguros, supervisar el uso de dispositivos, hablar sobre riesgos digitales y apoyar a los hijos si enfrentan problemas en línea. Por eso es importante conocer la opinión del docente sobre **cuánto deberían participar los padres** en estos temas.

**¿Qué tanto cree que los padres deben estar involucrados en este tema?**

* Nada (no deberían intervenir)
* Poco (solo de manera mínima)
* Regular (deberían tener cierta participación)
* Mucho (su participación es clave para la seguridad de los alumnos)

**Dificultades y retos**

Aunque los docentes saben que la seguridad digital y la privacidad son importantes, a veces es difícil enseñar estos temas. Pueden existir distintos obstáculos: no tener suficiente tiempo dentro del horario de clases, carecer de materiales didácticos adecuados, enfrentar poco interés de los alumnos o incluso no contar con conocimientos suficientes sobre el tema para explicarlo correctamente.

**¿Qué obstáculos enfrenta al enseñar sobre seguridad digital?**

* Falta de tiempo (no hay espacio en el horario para abordarlo)
* Falta de materiales (no hay recursos adecuados para enseñar)
* Falta de interés de los alumnos (no participan o prestan atención)
* Desconocimiento del tema (no me siento preparado para explicarlo)

Algunos estudiantes muestran entusiasmo por aprender sobre seguridad digital y privacidad, mientras que otros no prestan atención o consideran que no es relevante. Conocer el **nivel de interés de los alumnos** ayuda a los docentes a planear estrategias más efectivas y atractivas para enseñar estos temas en clase.

**¿Cómo describiría el interés de los alumnos en estos temas?**

* Muy bajo (la mayoría de los alumnos no muestra interés)
* Bajo (solo algunos se interesan)
* Medio (un grupo participa, otro no)
* Alto (la mayoría se interesa y participa activamente)

Los alumnos pueden enfrentar distintos **riesgos digitales**, como ciberacoso, robo de información personal, mensajes falsos o exposición involuntaria de fotos. Observar si los docentes han visto estos casos ayuda a entender la frecuencia de estos problemas en la escuela y la necesidad de medidas preventivas.

**¿Ha visto casos de alumnos afectados por riesgos digitales?**

* Sí, varios (he observado que muchos alumnos han pasado por estas situaciones)
* Sí, pocos (solo algunos alumnos han tenido problemas)
* No, nunca (no he presenciado ningún caso)

Algunas escuelas tienen **protocolos o procedimientos** para actuar cuando un alumno enfrenta problemas de privacidad o ciberacoso. Estos pueden incluir guías para reportar incidentes, pasos para notificar a los padres, apoyo psicológico o medidas disciplinarias. Conocer si la escuela cuenta con estas normas ayuda a identificar si los docentes y alumnos están respaldados ante estas situaciones.

**¿Cuenta su escuela con protocolos para atender problemas de privacidad o ciberacoso?**

* Sí (la escuela tiene reglas y procedimientos claros)
* No (no existen protocolos establecidos)
* No lo sé (no estoy seguro si hay protocolos)

Existen distintas maneras de enseñar a los alumnos sobre **seguridad digital, privacidad y ciberacoso**. Algunas herramientas pueden ser más efectivas según la edad y el interés de los estudiantes:

* **Juegos o simulaciones:** permiten practicar situaciones reales de manera segura y divertida.
* **Videos:** muestran ejemplos claros y concretos que ayudan a entender los riesgos.
* **Guías impresas:** ofrecen material de consulta que los alumnos pueden revisar cuando lo necesiten.
* **Charlas con expertos:** permiten aprender directamente de personas con experiencia y resolver dudas específicas.

**¿Qué herramienta considera más útil para enseñar estos temas?**

* Juegos o simulaciones
* Videos
* Guías impresas
* Charlas con expertos

**Preguntas para Adolescentes (13-17 años)**

**Uso de internet y redes**

Hoy en día, muchos adolescentes usan internet para **redes sociales, juegos, videos, tareas o chats**. El tiempo que pasan conectados puede influir en su exposición a riesgos como ciberacoso, phishing o pérdida de privacidad. Esta pregunta busca conocer **cuánto tiempo diario dedican a internet** y cómo eso puede afectar su seguridad y hábitos en línea.

**¿Cuánto tiempo pasas conectado(a) a internet al día?**

* Menos de 1 hora
* 1-3 horas
* 3-5 horas
* Más de 5 horas

Los adolescentes utilizan internet para distintas actividades diarias:

* **Redes sociales:** chatear, publicar fotos, ver historias o interactuar con amigos.
* **Juegos en línea:** jugar con otros en tiempo real o competir en plataformas digitales.
* **Videos / streaming:** ver contenido en YouTube, TikTok, Netflix u otras plataformas.
* **Tareas / estudio:** buscar información, entregar trabajos o usar plataformas educativas.

Conocer qué usan más ayuda a identificar **dónde podrían estar más expuestos a riesgos digitales** y cómo guiarlos mejor.

**¿Qué usas más en internet?**

* Redes sociales
* Juegos en línea
* Videos / streaming
* Tareas / estudio

Tener redes sociales propias significa que los adolescentes pueden **publicar, comentar y comunicarse** con otras personas de manera directa. Esto implica responsabilidades y riesgos: exposición de información personal, interacciones con desconocidos, ciberacoso o presión social. Saber si los estudiantes tienen redes propias ayuda a los docentes a **adaptar la educación sobre privacidad y seguridad digital** según el nivel de exposición.

**¿Tienes redes sociales propias?**

* Sí (tengo cuentas que uso personalmente)
* No (no tengo cuentas propias, uso solo las de mis padres o no tengo)

Compartir el **nombre real en redes sociales** puede facilitar que otras personas los identifiquen, lo que a veces aumenta riesgos como acoso, robo de información o contacto con desconocidos. Algunos adolescentes usan apodos o nombres falsos para proteger su privacidad y seguridad. Esta pregunta busca entender **qué tan conscientes son de la importancia de mantener cierta privacidad en línea**.

**¿Compartes tu nombre real en tus redes?**

* Sí (uso mi nombre real en mis perfiles)
* No (uso un apodo o nombre falso)
* A veces (depende de la red o la situación)

Compartir fotos en redes sociales puede ser divertido y permitir mostrar momentos de la vida diaria, pero también **aumenta los riesgos de exposición**, como que extraños vean información personal o se compartan sin consentimiento. Algunos adolescentes lo hacen con frecuencia, otros solo ocasionalmente o nunca, dependiendo de cuánto valoren su privacidad.

**¿Compartes fotos tuyas en redes sociales?**

* Sí, muchas (publico fotos regularmente)
* Algunas veces (solo ocasionalmente)
* Muy pocas (casi nunca)
* Nunca (no comparto fotos propias)

Los **datos personales** son toda la información que permite identificar a una persona, como su nombre, dirección, número de teléfono, fotos, cuentas de redes sociales, entre otros. Conocer qué son ayuda a los adolescentes a **entender qué información deben proteger** y cómo evitar que otros la usen de manera indebida.

**¿Sabes qué son los datos personales?**

* Sí (entiendo qué información se considera personal y cómo protegerla)
* No (no sé qué son o no estoy seguro)
* Más o menos (he escuchado del tema, pero no lo entiendo completamente)

La **huella digital** es el rastro que dejamos en internet cada vez que navegamos, publicamos, comentamos o descargamos algo. Incluye fotos, mensajes, historiales de búsqueda y actividad en redes sociales. Conocerla ayuda a los adolescentes a **entender que sus acciones en línea dejan evidencia y que deben cuidar su privacidad**.

**¿Conoces qué es la huella digital?**

* Sí (sé que mis acciones en línea dejan un rastro y entiendo sus riesgos)
* No (no tengo idea de lo que es)
* He escuchado, pero no entiendo bien (sé que existe pero no cómo funciona ni cómo afecta mi privacidad)

Un **aviso de privacidad** es un documento que las aplicaciones, páginas web o servicios en línea muestran para explicar **cómo recopilan, usan y protegen tus datos personales**. Saber qué es permite a los adolescentes **tomar decisiones informadas sobre qué información compartir y con quién**.

**¿Sabes qué es un aviso de privacidad?**

* Sí (entiendo para qué sirve y por qué es importante leerlo)
* No (no sé qué es ni para qué sirve)

Cuando instalas apps o juegos, muchas veces aparecen **condiciones o avisos de privacidad** que explican qué información recopilan y cómo la usarán. Leerlos ayuda a los adolescentes a **proteger sus datos y entender qué permisos están otorgando**, aunque muchas veces se omiten por ser largos o complicados.

**¿Lees las condiciones o avisos cuando instalas apps o juegos?**

* Siempre (leo todo antes de aceptar)
* A veces (solo reviso algunas partes o cuando me interesa)
* Nunca (acepto sin leer)

Compartir contraseñas con amigos o familiares puede parecer inofensivo, pero **pone en riesgo tu privacidad y seguridad digital**, ya que otros podrían acceder a tu información personal, cuentas o conversaciones. Saber si los adolescentes comparten sus contraseñas ayuda a identificar **hábitos de seguridad digital** y posibles vulnerabilidades.

**¿Compartes contraseñas con amigos o familiares?**

* Sí (les doy acceso a mis cuentas)
* No (mantengo mis contraseñas privadas y seguras)

**Prácticas y hábitos**

Tener una contraseña diferente para cada cuenta es importante para **proteger tu información personal**. Si alguien descubre la contraseña de una cuenta y usas la misma en otras, podría acceder a todas tus cuentas y datos. Esta pregunta busca conocer **si los adolescentes aplican buenas prácticas de seguridad digital**.

**¿Tienes una contraseña diferente para cada cuenta?**

* Sí (cada cuenta tiene su propia contraseña segura)
* No (uso la misma contraseña en varias cuentas)

Algunas contraseñas son **muy fáciles de adivinar**, como “1234”, nombres, fechas de cumpleaños o combinaciones simples. Usar contraseñas débiles **aumenta el riesgo de que alguien entre en tus cuentas** y acceda a información personal. Esta pregunta busca identificar **qué tan seguros son los hábitos de los adolescentes al crear contraseñas**.

**¿Tus contraseñas son fáciles de adivinar (ej. “1234”, tu nombre, tu cumpleaños)?**

* Sí (mis contraseñas son simples y fáciles de adivinar)
* No (mis contraseñas son seguras y difíciles de adivinar)
* Algunas sí, otras no (depende de la cuenta o situación)

Las redes sociales permiten ajustar **quién puede ver tus publicaciones, fotos o información personal** mediante la configuración de privacidad. Revisar estas opciones ayuda a proteger tus datos y controlar tu exposición en línea. Esta pregunta busca entender **qué tanto los adolescentes cuidan su privacidad en redes sociales**.

**¿Revisas la configuración de privacidad en tus redes sociales?**

* Sí (siempre reviso y ajusto mi privacidad)
* No (nunca reviso estas opciones)
* A veces (lo hago ocasionalmente o cuando me acuerdo)

Aceptar solicitudes de amistad de personas desconocidas en redes sociales puede **exponer tu información personal, fotos y actividades** a extraños. Algunos adolescentes aceptan a cualquiera, mientras que otros solo agregan a amigos y conocidos. Esta pregunta busca entender **cómo manejan los adolescentes su seguridad en línea frente a desconocidos**.

**¿Aceptas solicitudes de amistad de desconocidos?**

* Sí (acepto a cualquier persona que me agregue)
* No (solo acepto a personas que conozco)
* A veces (depende de la situación o red social)

Usar **redes WiFi públicas** en lugares como cafeterías, plazas o bibliotecas es común, pero estas conexiones pueden ser **menos seguras**, lo que facilita que alguien acceda a tu información personal o cuentas en línea. Esta pregunta busca conocer **si los adolescentes se exponen a riesgos por conectarse a redes abiertas**.

**¿Has usado alguna vez una red WiFi pública (cafeterías, plazas)?**

* Sí (he usado redes abiertas fuera de casa o escuela)
* No (solo uso redes seguras, como la de casa o escuela)
* No sé (no estoy seguro si la red que usé era pública o segura)

**Riesgos digitales**

El **ciberacoso** ocurre cuando alguien utiliza internet, redes sociales o aplicaciones para **molestar, insultar, amenazar o intimidar** a otra persona de manera constante. Conocer qué es ayuda a los adolescentes a **identificar conductas peligrosas y saber cómo actuar o pedir ayuda**.

**¿Sabes qué es el ciberacoso?**

* Sí (entiendo qué conductas se consideran ciberacoso y cómo afectan a las personas)
* No (no sé qué significa ni cómo identificarlo)

El **ciberacoso** puede afectar a cualquier adolescente y se manifiesta mediante **mensajes ofensivos, difusión de rumores, insultos o amenazas en línea**. Conocer si los jóvenes han presenciado o experimentado estas situaciones ayuda a entender **la frecuencia de este riesgo y la necesidad de educación y prevención**.

**¿Has visto o vivido casos de ciberacoso?**

* Sí, lo viví (he sido víctima directa de ciberacoso)
* Sí, le pasó a alguien cercano (un amigo o familiar ha pasado por esto)
* No (nunca he presenciado ni vivido un caso)

El **phishing** ocurre cuando alguien envía mensajes falsos por correo, redes sociales o aplicaciones para **engañarte y robar información personal**, como contraseñas, datos bancarios o fotos privadas. Conocer qué es ayuda a los adolescentes a **identificar mensajes sospechosos y proteger su información**.

**¿Sabes qué es el phishing (mensajes falsos para robar datos)?**

* Sí (entiendo cómo funciona y cómo evitar caer en ellos)
* No (no sé qué es ni cómo identificarlo)

Al navegar en internet o usar redes sociales, es posible recibir **mensajes que parecen normales pero que buscan engañarte** para obtener tus datos personales o que hagas clic en enlaces peligrosos. Reconocer estos mensajes es clave para **proteger tu información y seguridad en línea**.

**¿Alguna vez has recibido un mensaje sospechoso pidiéndote datos o enlaces raros?**

* Sí (he recibido mensajes que me parecieron extraños o peligrosos)
* No (nunca he recibido mensajes sospechosos)
* No estoy seguro (no puedo identificar si eran peligrosos)

A veces, en internet o redes sociales, otros pueden **molestarte, amenazarte o acosarte**. Saber cómo reaccionar—como **bloquear, denunciar o pedir ayuda a un adulto de confianza**—es clave para proteger tu seguridad y bienestar.

**¿Sabes qué hacer si te molestan o amenazan por internet?**

* Sí (sé cómo actuar, bloquear, denunciar o pedir ayuda)
* No (no estoy seguro de cómo reaccionar en esas situaciones)

**Opiniones y actitudes**

Proteger tus datos en internet significa **evitar que otros accedan a información personal, fotos, contraseñas o conversaciones privadas** sin tu permiso. Reconocer la importancia de esto ayuda a los adolescentes a **tomar decisiones más seguras en línea y cuidar su privacidad**.

* Sí, mucho (entiendo que es fundamental para mi seguridad y privacidad)
* Un poco (pienso que es importante, pero no siempre lo aplico)
* No (no considero que sea necesario proteger mis datos)

Sentirse seguro al usar internet implica **poder navegar, chatear, jugar o estudiar sin preocuparse de ser acosado, engañado o que roben tu información personal**. Esta pregunta busca conocer **qué tan protegidos y confiados se sienten los adolescentes al estar en línea**.

**¿Te sientes seguro(a) usando internet?**

* Sí (me siento protegido y sé cómo manejar riesgos)
* A veces (depende de la situación o la plataforma que uso)
* No (me siento vulnerable o preocupado por posibles riesgos)

Tener adultos que comprendan los riesgos en internet—como **ciberacoso, phishing o exposición de datos personales**—puede ayudar a los adolescentes a **recibir orientación y protección adecuada**. Esta pregunta busca saber **qué tan apoyados se sienten por sus padres o maestros en temas de seguridad digital**.

**¿Crees que tus padres o maestros entienden bien los riesgos en internet?**

* Sí (ellos saben identificar los riesgos y dar consejos adecuados)
* A veces (conocen algunos riesgos, pero no todos)
* No (no entienden los peligros ni cómo protegernos)

Algunos padres revisan la actividad de sus hijos en internet para **protegerlos de riesgos como ciberacoso, phishing o contenido inapropiado**, mientras que otros confían en que sus hijos naveguen de forma segura. Esta pregunta busca entender **qué tan supervisados se sienten los adolescentes en línea**.

**¿Tus padres revisan lo que haces en internet?**

* Sí (mis padres supervisan regularmente mi actividad en línea)
* A veces (solo revisan de vez en cuando)
* No (no supervisan ni controlan lo que hago en internet)

Algunas escuelas ofrecen **clases o pláticas sobre privacidad digital** para enseñar a los estudiantes cómo **proteger su información, crear contraseñas seguras y prevenir riesgos en línea**. Esta pregunta busca conocer **si los adolescentes han recibido educación formal sobre seguridad y privacidad en internet**.

**¿Has recibido clases o pláticas sobre privacidad digital en tu escuela?**

* Sí (he participado en actividades o clases que enseñan cómo proteger mis datos y navegar seguro)
* No (nunca he tenido educación sobre privacidad digital en la escuela)

Crear **contraseñas seguras** ayuda a proteger tus cuentas de redes sociales, correos y juegos de accesos no autorizados. Aprender a hacerlas correctamente permite **evitar que otras personas roben tu información o se hagan pasar por ti en línea**.

¿Te gustaría aprender a crear contraseñas más seguras?

* Sí (quiero aprender técnicas para proteger mejor mis cuentas)
* No (no me interesa o creo que no lo necesito)

En internet a veces llegan **mensajes falsos o engañosos** que buscan robar información personal, como contraseñas o fotos, o que intentan engañarte con noticias falsas. Aprender a reconocerlos ayuda a **evitar fraudes y mantener tu seguridad en línea**.

**¿Te gustaría aprender a reconocer mensajes falsos o peligrosos en internet?**

* Sí (quiero aprender a identificar y evitar mensajes peligrosos)
* No (no creo que sea necesario o interesante para mí)

Existen diferentes maneras de **aprender sobre seguridad y privacidad en internet**. Algunos adolescentes prefieren métodos interactivos como **juegos o aplicaciones**, otros aprenden mejor con **videos explicativos, pláticas en clase**, o leyendo **guías impresas**. Esta pregunta busca conocer **qué método les resulta más efectivo y atractivo**.

**¿Cómo prefieres aprender sobre estos temas de seguridad y privacidad en internet?**

* Juegos o apps (aprendo mejor interactuando y practicando)
* Videos (me gusta ver ejemplos y explicaciones visuales)
* Pláticas en clase (prefiero que alguien me explique y pueda hacer preguntas)
* Guías impresas (me gusta leer y tener material escrito para consultar)

Algunas plataformas en línea permiten **practicar seguridad digital de manera divertida**, enseñando a crear contraseñas seguras, identificar mensajes peligrosos y proteger la privacidad en internet. Esta pregunta busca conocer **el interés de los adolescentes en aprender mediante herramientas interactivas**.

**¿Te gustaría usar una plataforma en línea para practicar seguridad digital?**

* Sí (me interesa aprender usando herramientas digitales y prácticas)
* No (prefiero otros métodos de aprendizaje)
* Tal vez (no estoy seguro, depende de cómo sea la plataforma)

Hablar de privacidad digital en la escuela ayuda a los estudiantes a **entender los riesgos en internet, cómo proteger su información personal y cómo actuar ante situaciones de ciberacoso o mensajes peligrosos**. Esta pregunta busca saber **qué tan relevante consideran los adolescentes que sea este tema dentro de su educación**.

**¿Qué tan importante crees que es hablar de privacidad digital en tu escuela?**

* Nada (no creo que sea necesario tratar este tema en la escuela)
* Poco (es un tema interesante, pero no muy importante)
* Regular (es importante, pero no urgente)
* Mucho (es muy importante y debería enseñarse regularmente)