Mochila Digital
Guía para padres en el nuevo curso escolar

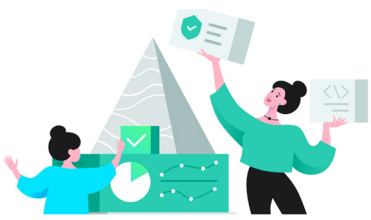
kaspersky

Por qué la ciberseguridad es importante en este curso escolar

Mientras los niños se preparan para el nuevo curso con lápices afilados y cuadernos recién estrenados, hay algo muy importante que a menudo se pasa por alto: la ciberseguridad. En una época en la que la educación es cada vez más digital, los alumnos dependen más que nunca de portátiles, tabletas, aplicaciones de mensajería y plataformas de aprendizaje online. Pero, junto con la comodidad del aprendizaje conectado, también crece la exposición a una gran variedad de amenazas online, que van desde el phishing, las estafas y las filtraciones de datos hasta el ciberacoso y el robo de identidad.

Para los padres, esto significa que la ciberseguridad ya no es opcional: es una parte fundamental de la preparación para la vuelta al cole. Igual que enseñas a tu hijo a cruzar la calle con seguridad o le preparas una comida saludable, también necesitas darle las herramientas y el conocimiento para desenvolverse en el mundo digital con confianza y precaución.

En esta guía te mostraremos los principales riesgos de ciberseguridad a los que tu hijo puede enfrentarse este curso y cómo puedes ayudarles a prevenirlos. Desde crear contraseñas seguras y configurar controles parentales hasta identificar estafas y hablar sobre el comportamiento en Internet, la Mochila Digital está aquí para ayudarte a ir un paso por delante y garantizar la seguridad digital de tus hijos.



Mundo online

Los estudiantes están más conectados que nunca: chatean con amigos en aplicaciones de mensajería, participan en foros de clase, utilizan herramientas de IA para completar tareas y exploran el mundo de Internet, tanto para estudiar como para divertirse. Pero junto a estas oportunidades de aprendizaje existen riesgos reales. El mundo online, aunque entretenido y lleno de posibilidades, también puede exponer a los niños a contenidos dañinos, estafas o situaciones de ciberacoso.

Ya no se trata solo del tiempo frente a la pantalla, sino de lo que ocurre durante ese tiempo. Los niños pueden sin saberlo, descargar malware disfrazado de herramienta educativa, interactuar con desconocidos que se hacen pasar por compañeros o compartir en exceso información personal que puede ser explotada. Incluso las plataformas diseñadas para aprender y colaborar no están exentas de amenazas.

Comprender estos peligros es el primer paso para proteger a tu hijo. En esta sección exploraremos las amenazas online más comunes a las que se enfrentan los niños en edad escolar, desde el phishing y las aplicaciones falsas hasta la ingeniería social y los contenidos inapropiados, y explicaremos cómo funcionan, por qué los menores son especialmente vulnerables y qué puedes hacer para ayudarles a mantenerse seguros.

Búsquedas seguras

Los buscadores no siempre distinguen entre contenido adecuado para menores y material adulto. Por eso, los niños necesitan tanto herramientas técnicas como habilidades de pensamiento crítico para desenvolverse en el mundo digital con confianza. Cuando se fomentan hábitos de búsqueda segura desde pequeños, no solo se evitan riesgos online, también se forman estudiantes más reflexivos, curiosos e independientes.

1. Usa filtros de contenido y controles parentales

Empieza activando los controles parentales en todos los dispositivos que use tu hijo: smartphones, tablets, ordenadores y televisiones inteligentes. La mayoría de los sistemas operativos (iOS, Android, Windows y macOS) incluyen funciones para bloquear páginas explícitas, restringir ciertos tipos de aplicaciones y filtrar los resultados de búsqueda. Además, plataformas como YouTube, Netflix o TikTok permiten activar modos “restringido” o “para niños” que limitan el acceso a contenido para adultos. Para un control más completo, puedes recurrir a herramientas como Kaspersky Safe Kids, que ofrecen filtrado de contenido en tiempo real, gestión del tiempo de pantalla y supervisión de aplicaciones. Estas soluciones ayudan a detectar material inapropiado que puede escaparse a los filtros estándar, sobre todo en los navegadores.

2. Desactiva la reproducción automática

La reproducción automática es una de las principales vías por las que los niños se topan con contenido inadecuado sin darse cuenta. En plataformas como YouTube o Netflix, un vídeo lleva a otro vídeo y, antes de darte cuenta, tu hijo puede estar viendo algo que no corresponde a su edad. Desactiva esta función siempre que sea posible, tanto en los ajustes como mediante extensiones de navegador si hace falta. Al hacerlo, el niño debe tomar la decisión consciente de hacer clic en el siguiente vídeo, lo que ralentiza el consumo, te da margen para intervenir y fomenta hábitos de consumo de contenidos más conscientes.

3. Enseña a tu hijo qué hacer cuando vea algo incorrecto

Ningún filtro es perfecto. Por eso es fundamental enseñar a los niños a reaccionar cuando algo no les resulta adecuado. Una regla sencilla es la respuesta en tres pasos: **Parar – Cerrar el contenido – Avisar a un adulto**. Hazles saber que no serán castigados por contártelo, aunque hayan hecho clic por error o por curiosidad. Refuerza la importancia de la sinceridad y la confianza. Incluso podéis acordar una “palabra clave digital” que tu hijo pueda usar cuando haya visto algo que le incomode y no sepa cómo expresarlo al momento.

4. Observa y habladlo juntos

El filtro más eficaz no es un software, **eres tú**. Dedica tiempo a ver programas, jugar o navegar con tu hijo. Esto no solo te permite supervisar lo que está viendo, también abre la puerta para hablar sobre valores, emociones y situaciones de la vida real. Puedes descubrir más sobre lo que buscan los niños en Internet en nuestro último informe sobre intereses infantiles.

5. Revisa el historial del dispositivo —y mantenlo activo

Mantén habilitado el historial del navegador, el registro de visionados en YouTube y el uso de aplicaciones. No se trata de espiar, sino de asumir una responsabilidad compartida. Y lo más importante: si encuentras algo que no te gusta, no sobre reacciones ni regañes al niño de inmediato. Tómate un momento para entender qué ha ocurrido. Con el tiempo, a medida que tu hijo crezca, haga elecciones seguras de forma constante y pueda explicar por qué ciertos contenidos son adecuados o no, podrás ir reduciendo estas comprobaciones. El objetivo es ayudarle a construir hábitos digitales sólidos, de modo que la supervisión deje de ser necesaria y se sustituya por confianza, comunicación abierta y la capacidad del propio niño para afrontar los riesgos online.

Phishing y enlaces maliciosos

El phishing es una de las ciberamenazas más comunes a las que se enfrentan los niños en Internet. Suele consistir en un mensaje, página web o anuncio falso que engaña al usuario para que haga clic en un enlace malicioso, comparta datos personales o descargue software dañino. Como muchas veces parece "normal" (un aviso de premio, un archivo de tareas o una oferta de juego) los niños son especialmente vulnerables.

1. Enseña la regla de oro: "No hagas clic si no lo conoces"

Los niños suelen hacer clic con rapidez, sobre todo si reciben mensajes como "¡Has ganado un premio!" o "¡Skins gratis para Roblox!". Explícales que los ciberdelincuentes suelen hacerse pasar por alguien o algo conocido para engañar, igual que en las estafas del mundo real.

Pon ejemplos: mensajes falsos de "profesores" pidiendo contraseñas, ventanas emergentes diciendo que su dispositivo está infectado o anuncios que ofrecen "V-Bucks gratis". Hay que animarlos a preguntarse: ¿conozco a esta persona? ¿Es demasiado bueno para ser verdad? Si la respuesta es sí, no hagas clic. Mejor preguntar siempre a un adulto primero.

2. Muéstrales cómo es el phishing (de forma segura)

En lugar de limitarte a advertirles, enséñales ejemplos reales (o versiones seguras simuladas) de correos de phishing, páginas de inicio de sesión falsas o pop-ups fraudulentos. Señala las señales de alerta más comunes:
– Errores de ortografía
– Direcciones web extrañas
– Tono urgente ("¡Debes actuar ahora!")
– Peticiones de contraseñas o pagos

Realizar juntos un ejercicio de "encuentra la estafa" refuerza su capacidad de identificar estos intentos, igual que aprender a reconocer a un desconocido en la vida real.

3. Usa filtros antispam y opciones de navegación seguras

Configura el correo electrónico y el navegador de tu hijo con filtros de spam sólidos y protección contra phishing. Instala una solución de seguridad de confianza como Kaspersky Premium, que ofrece protección en tiempo real frente a intentos de phishing, anuncios maliciosos y descargas peligrosas. Estas herramientas bloquean muchas amenazas antes incluso de que tu hijo llegue a verlas.

4. Mantén las apps y los sistemas actualizados

Muchos ataques de phishing aprovechan fallos de seguridad en navegadores, aplicaciones o sistemas operativos desactualizados. Asegúrate de que las actualizaciones automáticas estén activadas en los dispositivos de tu hijo, así como en las apps de correo electrónico y navegadores. De esta forma, las vulnerabilidades pueden corregirse antes de que los ciberdelincuentes puedan explotarlas.

5. Enseña hábitos seguros de descarga

El phishing suele presentarse en forma de archivos maliciosos, sobre todo en contextos educativos y de videojuegos. Por ejemplo:
– Un “archivo de deberes” enviado por Discord
– Un “mod” de Minecraft de una página desconocid
– Un PDF recibido de un desconocido en WhatsApp

Explícales que solo deben descargar archivos de fuentes fiables, como profesores, webs oficiales o tiendas de aplicaciones verificadas. Establece una norma clara: si no están seguros, deben preguntar siempre a un adulto antes de descargar cualquier cosa.

6. Protege las cuentas de pago y de tiendas de apps

Muchas estafas buscan que los niños gasten dinero real por error, pidiendo datos de tarjeta de crédito “para reclamar un premio” o activando compras dentro de las aplicaciones sin querer. Configura todas las tiendas de apps y herramientas de pago para que requieran contraseña, biometría o aprobación parental antes de cualquier transacción. Además, revisa qué juegos y plataformas tienen guardada tu información de pago y elimínala o limita su uso siempre que sea posible.

7. Reporta y bloquea mensajes y cuentas sospechosas

Enséñales a denunciar anuncios falsos, mensajes fraudulentos o cuentas que suplantan identidad en cada plataforma que usen. Ya sea en TikTok, YouTube, Roblox o Instagram, todas ofrecen herramientas de denuncia. Anímales a utilizarlas incluso si el mensaje “parece una broma” o “probablemente no sea serio”. También deben aprender a bloquear y a no interactuar nunca con usuarios que envíen ofertas o enlaces sospechosos. Incluso responder con un simple “no, gracias” puede dar a los estafadores la confirmación de que la cuenta está activa y es vulnerable.

“Oversharing”

Hoy en día, niños y adolescentes crecen en un mundo donde compartir se ha vuelto algo natural: publicar selfies y vídeos, comentar cada momento de su vida o mostrar lo que hacen en tiempo real. Pero lo que para un menor puede parecer casual y divertido, puede convertirse en un grave riesgo de privacidad cuando información sensible llega a la audiencia equivocada.

El exceso de información (oversharing) no siempre parece peligroso. A veces es una foto de cumpleaños, un uniforme escolar, una etiqueta de ubicación o una conversación sobre los planes del fin de semana. Sin embargo, los pequeños detalles se acumulan, y los ciberdelincuentes, acosadores o desconocidos pueden utilizarlos para rastrear, manipular o dañar a un menor.

1. Configurar las cuentas juntos y revisar periódicamente la privacidad

Abrir una cuenta en redes sociales o en una app de mensajería debería ser siempre una actividad conjunta, especialmente para menores de 16 años. Siéntate con tu hijo y recorred juntos el proceso de registro. Así podrás entender cómo funciona la plataforma, establecer expectativas y configurar los ajustes de seguridad desde el principio.

– Usar un apodo o solo el nombre de pila, evitando nombres completos que puedan vincularse a otros datos personales.
– Omitir cumpleaños, nombres de colegios o ciudades en biografías y perfiles públicos. Esta información puede servir a extraños para localizar o suplantar a tu hijo.
– Desactivar la geolocalización en los ajustes y hablar sobre la importancia de no publicar ubicaciones en tiempo real (por ejemplo: “¡En el parque [nombre del parque] ahora mismo!”).
– Restringir los comentarios o mensajes únicamente a “amigos” o personas que ambos conozcáis en la vida real.

2. Enseñar qué no se debe publicar

Los menores suelen subestimar cuánto revelan en lo que parece una publicación, historia o chat inocente. Divide la explicación en categorías y aclara por qué es arriesgado, no solo “porque lo digo yo”, sino porque puede usarse de forma indebida, malinterpretarse o manipularse.

Información personal

Nunca publiques ni envíes:
– Nombre completo
– Dirección o calle
– Número de teléfono, correo electrónico o contactos de los padres
– Nombre del colegio, número de aula o ruta del autobús
– Número de estudiante, notas, resultados de exámenes o contraseñas

Estos datos pueden servir para adivinar respuestas de seguridad, localizar vuestro domicilio o hacerse pasar por tu hijo en Internet.

Detalles de rutina

Evita compartir:
– Dónde está en ese momento
– Lugares a los que va todos los días
– Planes de viaje

Con esta información, un extraño puede rastrear patrones de movimiento y saber cuándo un menor está solo o desprotegido.

Información sensible

Tener cuidado con fotos y vídeos:
– En uniforme escolar con escudos o insignias visibles
– Dentro de casa mostrando la distribución, objetos de valor o pertenencias personales
– En ropa interior, bañador o pijama, incluso en tono de broma
– De otros menores sin su permiso

Una vez compartidas, pierdes el control de estas imágenes y pueden copiarse, volver a difundirse o usarse para acosar, y a menudo sin que el niño se dé cuenta.

3. Hablar sobre la huella digital y las consecuencias a largo plazo

Aunque una publicación desaparezca, Internet no olvida. Fotos borradas pueden haber sido capturadas, copiadas o archivadas. En el futuro, empresas, centros educativos o incluso equipos deportivos podrían revisar la presencia online de tu hijo, o alguien podría intentar avergonzarle con un post antiguo.

Explícaselo en positivo: “cada día estás construyendo tu identidad y reputación digital. Intenta que sea algo de lo que te sientas orgulloso”. Anímalos a compartir aficiones, logros, arte o mensajes amables, cosas que reflejen sus valores y personalidad de manera sana.

Blogging y streaming

Muchos niños aspiran a convertirse en creadores de contenido en redes sociales, y estudios muestran que el 33% de los jóvenes en España quiere dedicarse a ello y que el 10% lo está intentando. Para ellos, los creadores digitales se convierten en referentes, y el deseo de triunfar en Internet aparece incluso antes de la adolescencia. En este contexto, la implicación de los padres no solo es útil, sino esencial. Cuando los padres participan de forma activa —aprendiendo cómo funcionan las plataformas, configurando juntos la privacidad y la seguridad, y manteniendo conversaciones abiertas sobre límites— este viaje digital compartido convierte los riesgos potenciales en oportunidades de aprendizaje y permite que los niños exploren su creatividad con confianza.

1. Sé curioso, no crítico. Tu apertura es su red seguridad.

Cuando un niño dice "quiero empezar un blog" o "quiero ser YouTuber", es normal que surja preocupación, sobre todo pensando en trolls, estafadores o el exceso de exposición. Pero el paso más seguro no es prohibir, sino dialogar. Pregúntale por qué quiere hacerlo y qué tipo de contenidos quiere publicar. Este enfoque tiene dos ventajas clave: por un lado, demuestra que te tomas en serio sus intereses y generas confianza; por otro, te permite introducir de manera natural temas de seguridad como los ajustes de privacidad, los límites de contenido o cómo gestionar la atención online.

Para facilitar y hacer más amenas estas conversaciones, puedes empezar con recursos adaptados a edades tempranas. Por ejemplo, el Abecedario de la Ciberseguridad de Kaspersky, un libro gratuito para descargar que enseña a los niños las bases de la higiene digital de forma sencilla y divertida. Presenta conceptos clave de ciberseguridad con un lenguaje cercano e ilustraciones coloridas, ayudándoles a aprender a detectar fraudes, proteger sus datos y mantenerse seguros mientras exploran su creatividad online.

2. Busca regularmente su alias en Google

En cuanto tu hijo empiece a publicar bajo un seudónimo, es importante comprobar qué tan visible y rastreable es en Internet. Una forma sencilla es buscar su alias en Google con regularidad: su nombre de usuario, el título del blog o su cuenta de redes sociales. Observa qué aparece: ¿fotos personales, etiquetas de ubicación o comentarios que revelan más de la cuenta? ¿Alguien ha copiado su contenido o intentado suplantarle?

3. Alerta sobre colaboraciones falsas u ofertas sospechosas

A medida que los jóvenes blogueros ganan visibilidad, pueden empezar a recibir mensajes de supuestas marcas u otras cuentas que les ofrecen productos gratis, patrocinios u oportunidades de colaboración. Para un niño esto puede parecer un sueño hecho realidad, pero muchas veces es una estafa. Enséñales a tratar cualquier oferta inesperada con cautela. Las "colabs" falsas suelen llegar por mensajes directos o correos e incluyen enlaces a páginas de phishing diseñadas para robar credenciales, datos personales o incluso información bancaria. Algunos estafadores piden pagar "gastos de envío" por regalos falsos o intentan que los menores instalen aplicaciones maliciosas.

Ayúdales a identificar señales de alarma como mala ortografía o un tono urgente ("¡actúa ya!"), solicitudes de datos personales o contraseñas, enlaces sospechosos o webs poco fiables, o cuentas no verificadas que se hacen pasar por marcas conocidas.

En el caso de los menores, todas las interacciones "comerciales" deben ser gestionadas por los padres: leer los mensajes, valorar propuestas y responder a las solicitudes de colaboración. Hablad juntos sobre qué marcas son adecuadas y por qué algunas ofertas pueden ser peligrosas.

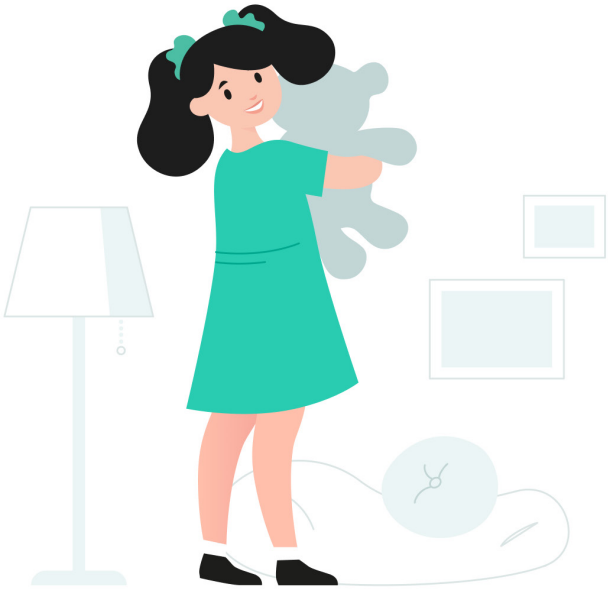
4. Hablar sobre los desconocidos online

A medida que tu hijo consigue una audiencia, puede atraer no solo seguidores, sino también personas con comportamientos inadecuados o manipuladores. Por desgracia, el grooming online es una amenaza real, sobre todo para creadores jóvenes, abiertos y confiados que comparten detalles de su vida. Explícale que no todas las personas que parecen amables en Internet tienen buenas intenciones. Los groomers suelen presentarse como "amigos de apoyo": alaban su contenido, ofrecen ayuda o dicen compartir intereses. Con el tiempo, pueden pedir datos personales, fotos privadas o intentar trasladar la conversación a plataformas menos seguras como chats privados, videollamadas o mensajería cifrada.

Enséñale a reconocer las señales de advertencia:

- Un desconocido que le escribe con frecuencia o de forma demasiado personal.
- Alguien que insiste en mantener el secreto ("no se lo digas a tus padres").
- Presión para compartir información privada o imágenes.
- Manipulación emocional basada en la culpa, los halagos o incluso amenazas.

Y lo más importante: asegúrate de que tu hijo sepa que siempre puede acudir a ti sin miedo a ser castigado.



IA y niños

La inteligencia artificial se está convirtiendo rápidamente en parte del mundo digital de tus hijos, desde chatbots y herramientas de escritura impulsadas por IA hasta juguetes inteligentes, motores de recomendación y tutores virtuales. Según un informe de Kaspersky, el interés por la IA entre los niños se duplicó en 2025. Aunque estas tecnologías pueden apoyar el aprendizaje y la creatividad, también plantean importantes cuestiones de privacidad, seguridad y ética. Como padre o madre, juegas un papel clave a la hora de guiar a tus hijos en esta nueva realidad.

1. Explica qué es la IA... y qué no lo es

Los niños suelen pensar que la Inteligencia Artificial (IA) es "solo un robot listo" o un amigo que lo sabe todo. Enséñale que la IA no "piensa" ni "siente": genera respuestas a partir de patrones de datos, no de emociones o intenciones. Esto es especialmente relevante para los más pequeños, que pueden crear lazos emocionales con avatares, chatbots o "amigos IA". Ayúdales a entender sus límites: la IA puede ser útil para hacer como punto de partida de ideas o para investigar, pero también se equivoca, puede mostrar sesgos o sonar muy segura incluso cuando no tiene razón. Anímales siempre a contrastar la información y a no darla por cierta automáticamente.

2. Habla de la privacidad al usar herramientas de IA

Muchas herramientas de IA recopilan grandes cantidades de datos personales, incluido lo que los niños escriben, preguntan o suben. Déjales claro que nunca deben compartir nombres reales, datos del colegio, fotos ni información sensible en estas plataformas. Revisad juntos las políticas de privacidad de cualquier aplicación o web basada en IA que quieran usar. Si la recopilación de datos no está clara o es excesiva, lo mejor es evitarla y buscar alternativas adaptadas a menores.

3. Pon límites al uso sin supervisión

Aunque parezca una actividad segura, usar IA sin supervisión puede exponer a los niños a contenidos dañinos o a desinformación, especialmente con herramientas abiertas como ChatGPT, bots de personajes o generadores de imágenes. Establece reglas claras:

- Pedir permiso antes de usar nuevas herramientas de IA.
- Usar la IA en espacios compartidos.
- Evitar plataformas que permitan interacción anónima.

Explícales que algunos modelos están entrenados con datos de todo Internet, incluido material inapropiado, y que incluso preguntas inocentes pueden dar respuestas inadecuadas.

4. Fomenta un uso ético, nada de atajos

La IA puede ser un atajo tentador para deberes, ensayos o trabajos creativos. Pero depender demasiado de ella puede perjudicar el pensamiento crítico y la creatividad. Habla con tu hijo sobre lo que es justo y lo que es hacer trampa al usar la IA. Una buena regla: **"Usa la IA para apoyar tu pensamiento, no para sustituirlo"**. Por ejemplo, está bien pedir ideas, definiciones o esquemas, pero no copiar respuestas completas ni presentar trabajos escritos por la IA como propios.

De esta forma, estarás fomentando la integridad digital desde una edad temprana.

5. Advierte sobre la descarga de software no oficial

En especial de programas que prometen herramientas "exclusivas" para hacer tareas o que aseguran "resolver cualquier problema al instante". Los ciberdelincuentes suelen disfrazar malware como aplicaciones educativas atractivas para que los estudiantes hagan clic en enlaces sospechosos.

Explícales que descargar desde webs no verificadas, plataformas de intercambio o enlaces en chats puede poner en riesgo el dispositivo, robar datos personales o incluso bloquearles las cuentas.

6. Ojo con los deepfakes y el engaño generado por IA

La inteligencia artificial ya puede crear imágenes, vídeos o voces falsas hiperrealistas, conocidas como deepfakes. Los niños pueden encontrarlas en TikTok, YouTube o en chats sin darse cuenta de que no son reales.

Enséñales a identificar señales de alerta:

- Movimientos extraños de los ojos o labios desincronizados en los vídeos.
- Rostros demasiado perfectos o con aspecto robótico.
- Intentos de manipulación emocional, como noticias falsas o estafas con famosos.

Fomenta un escepticismo saludable: «que lo veas no significa que sea real». Muéstrales ejemplos y desmiéntelos juntos: así conviertes la experiencia en un ejercicio de pensamiento crítico

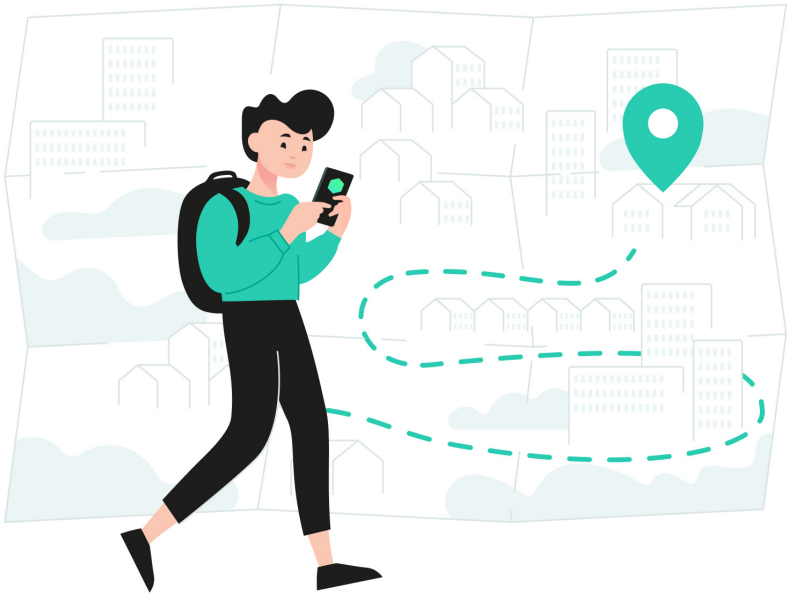
Mundo offline

Con el inicio del nuevo curso escolar, los niños suelen empezar a pasar más tiempo solos, ya sea yendo a pie al colegio, usando el transporte público, asistiendo a actividades extraescolares o estudiando en la biblioteca o en sus habitaciones. Esta independencia es un paso importante: les ayuda a ganar confianza, desarrollar habilidades para tomar decisiones y aprender a desenvolverse en el mundo que les rodea.

Pero a medida que asumen más responsabilidades, también aumenta su exposición a riesgos en el mundo real, muchos de los cuales tienen consecuencias digitales. La ciberseguridad no es algo que ocurra solo online, empieza con las elecciones cotidianas en el mundo offline.

En esta sección veremos cómo los padres pueden ayudar a los niños a crear hábitos seguros en espacios públicos, proteger su vida digital cuando están en movimiento y comprender que la conciencia en el mundo real es tan importante como las reglas sobre el tiempo frente a la pantalla.

Desde la seguridad física en el camino al colegio, hasta el uso responsable de redes Wi-Fi públicas o el cuidado de los dispositivos en la mochila, estas lecciones preparan a los niños para moverse por el mundo con confianza y precaución.



Seguridad física

Aunque la ciberseguridad suele centrarse en aplicaciones, dispositivos y redes, la seguridad en el mundo real desempeña un papel igualmente importante a la hora de proteger a tu hijo. Los niños en edad escolar son cada vez más autónomos: van solos al colegio, usan el transporte público o pasan tiempo fuera sin supervisión adulta. Estos momentos cotidianos también tienen implicaciones digitales: un dispositivo perdido, una contraseña en voz alta o un smartwatch sin protección pueden abrir la puerta a amenazas online.

1. Enséñales normas de seguridad para caminar y desplazarse

Asegúrate de que tu hijo conoce las reglas básicas de seguridad vial: cruzar siempre por pasos de peatones, respetar los semáforos, caminar por las aceras y nunca tomar atajos por callejones o zonas desconocidas. Estas reglas pueden parecer obvias, pero los niños menores de 12 años se distraen con facilidad, sobre todo si llevan auriculares o miran una pantalla mientras caminan.

Explícale la importancia de mantenerse alerta y sin dispositivos cerca de las carreteras o en espacios públicos. Ponte tú mismo como ejemplo: guarda el móvil en los cruces, mira a ambos lados y quítate los auriculares al caminar con tu hijo. Cuando ven que los adultos practican hábitos seguros, es más probable que los imiten.

2. Usa sistemas de rastreo GPS y check-ins

Valora utilizar herramientas de seguridad con GPS, como Kaspersky Safe Kids, para supervisar en tiempo real la ruta de tu hijo. Muchas aplicaciones permiten configurar alertas de geovalla: recibirás una notificación si tu hijo sale de un área definida o toma un desvío inesperado.

No se trata de espiar, sino de tranquilidad y seguridad. Sé transparente: explícale por qué utilizas la herramienta y estipula registros regulares por llamada o mensaje. Enséñale cómo contactar contigo rápidamente en caso de emergencia y practicad juntos qué hacer si se siente inseguro en el camino.

Para los padres, también es fundamental proteger la cuenta de rastreo: activa la autenticación en dos pasos, utiliza una contraseña única y revisa periódicamente los dispositivos conectados para garantizar que los datos de ubicación se mantienen privados.

3. Protege los dispositivos fuera de casa

Los niños suelen llevar smartphones, smartwatches, tabletas o portátiles. Son objetivos valiosos tanto para el robo como para la exposición de datos. Enséñales a mantener los dispositivos apagados, guardados y fuera de la vista cuando no los usen, y a no dejarlos nunca desatendidos, ni siquiera "solo un segundo". Configura códigos de bloqueo, activa funciones de borrado remoto (como Buscar mi iPhone o Encontrar mi dispositivo) y realiza copias de seguridad del material escolar en la nube. Así, incluso si el dispositivo se pierde o lo roban, la información seguirá protegida.

4. Precaución con el Wi-Fi público

Las redes Wi-Fi públicas, ya sea en colegios, cafeterías, aeropuertos o transporte público, pueden parecer prácticas, pero suelen conllevar serios riesgos de seguridad. Estas redes rara vez están cifradas, lo que significa que los ciberdelincuentes pueden interceptar los datos que tu hijo envía y recibe, incluidos inicios de sesión, mensajes e incluso fotos.

Enséñale una regla sencilla: nunca iniciar sesión en cuentas personales (como correo electrónico, banca o almacenamiento en la nube) con Wi-Fi público salvo que utilice una VPN de confianza. Una VPN cifra los datos que se transmiten, dificultando mucho que terceros puedan espiarnos.

5. Configura alertas para accesos o actividad sospechosa

Activa las **alertas de inicio de sesión** para recibir notificaciones si se accede a la cuenta desde una ubicación o dispositivo inusual. Estas alertas ayudan a detectar si alguien ha conseguido las credenciales a través de una sesión en Wi-Fi inseguro. Anima a tu hijo a informar de cualquier cosa extraña, como cierres de sesión inesperados o ventanas emergentes sospechosas, aunque no esté seguro de lo que ocurrió. Más vale prevenir que curar.

6. Cuidado con las conversaciones en público

Recuérdale que debe tener cuidado a la hora de compartir información personal (como dirección, contraseñas o planes de viaje) en lugares públicos. Si está al teléfono o usando una aplicación de mensajería, asegúrate de que no comparte datos privados en sitios donde otros puedan escucharlo fácilmente o mirar su pantalla. Esto es especialmente importante cuando viaja solo en autobuses, centros comerciales o actividades extraescolares. La privacidad digital empieza por ser consciente del entorno.

7. Planifica emergencias y practica los pasos

Proporciona a tu hijo información de contacto de emergencia y asegúrate de que sabe cómo actuar en caso necesario. ¿A quién debe llamar? ¿Dónde debe ir si se siente inseguro o se pierde? Practicad simulacros sencillos: teléfono perdido, quedarse fuera de casa, perder el autobús o presenciar un comportamiento sospechoso. Ensaya rutinas de respuestas tranquilas, sin pánico. El objetivo es reforzar la confianza y la preparación, no el miedo.

Seguridad financiera

A medida que los niños ganan independencia, sus hábitos financieros evolucionan al mismo tiempo que sus hábitos digitales. Desde comprar el almuerzo hasta hacer compras dentro de los juegos, hoy en día los menores gestionan dinero real a través de aplicaciones y plataformas online, muchas veces antes de comprender plenamente los riesgos que esto implica.

1. Establece límites de gasto claros

Empieza por definir una estructura básica de presupuesto para los gastos habituales de tu hijo:
- Material escolar
- Comida o dinero para el almuerzo
- Compras relacionadas con deportes o aficiones
- Entretenimiento (apps, juegos, suscripciones)

En lugar de controlar cada compra, habla en términos de porcentajes. Por ejemplo: “70% para gastos escolares, 20% para entretenimiento, 10% para ahorro”. Aprovecha la ocasión para introducir la educación financiera digital: explícales cómo las compras dentro de apps, las microtransacciones o las comisiones ocultas pueden agotar su saldo si no tienen cuidado.

2. Usa métodos de pago seguros

En lugar de darles dinero en efectivo (que puede perderse o sustraerse), otra opción son las tarjetas bancarias infantiles o monederos digitales con control parental. Muchas aplicaciones bancarias ofrecen funciones como:
- Límites de gasto
- Notificaciones de compra
- Historial de transacciones en tiempo real
- Bloqueo de ciertas categorías (por ejemplo, juegos o mercados online)

En paralelo, instala una solución de ciberseguridad que incluya navegación segura y protección de pagos. Así, cuando tu hijo compre en Internet (juegos o suscripciones), sus datos bancarios estarán cifrados y protegidos frente a keyloggers, páginas de pago falsas y ataques de intermediarios.

3. Protege dispositivos y cuentas financieras

Los niños quizá no entienden del todo la importancia de la seguridad de las cuentas, pero una contraseña débil o un dispositivo robado pueden exponer todas sus herramientas financieras y las tuyas. Como padre, puedes ayudar:

- Activando la autenticación en dos pasos (2FA) en todas las aplicaciones que gestionen dinero
- Usando un gestor de contraseñas que almacene credenciales de forma segura y permita acceso familiar si algo va mal
- Enseñando los principios básicos de una contraseña robusta: al menos 12 caracteres, nada de nombres o fechas de cumpleaños, y nunca reutilizarla en distintas plataformas

4. Habla sobre las ciberamenazas que afectan a los jóvenes

Los niños pueden pensar que las estafas solo afectan a adultos, pero en realidad los ciberdelincuentes suelen dirigirse a menores y adolescentes, que son más confiados y tienen menos experiencia.

Explica las formas más comunes de fraude financiero:
- Correos de phishing que se hacen pasar por un banco o tienda favorita
- Falsos sorteos que piden datos de la tarjeta
- Estafas de "amigo necesitado" en las que alguien pide dinero desde una cuenta hackeada
- Estafas dentro de juegos que ofrecen objetos "gratis" a cambio de credenciales

Enséñales a desconfiar de enlaces, ofertas y mensajes privados que transmiten urgencia ("¡Haz esto ahora o perderás tu cuenta!"). Anímalos a consultarte antes de introducir datos de pago en cualquier sitio online.

5. Controla suscripciones y cargos recurrentes

Muchas aplicaciones y plataformas, especialmente juegos, herramientas educativas y servicios de streaming, funcionan ahora con modelo de suscripción en lugar de compras únicas. Es fácil que los niños se apunten a una "prueba gratuita" que después genera cargos mensuales sin que se den cuenta.

Enséñales a:
- Pedir siempre permiso antes de iniciar una prueba gratuita
- Buscar configuraciones de "renovación automática" y aprender a cancelarlas
- Poner recordatorios en el calendario para las fechas de finalización de la prueba

Como padre, revisa el historial de compras de aplicaciones cada mes y comprueba regularmente el correo en busca de notificaciones de renovación ocultas. También puedes usar herramientas que detecten cargos recurrentes o envíen alertas por cada transacción.

6. Vigila señales de robo de identidad

Si la información personal o financiera se ha visto comprometida, podrías notar:
- Compras inesperadas
- Bloqueos de cuentas o correos de restablecimiento de contraseña
- Notificaciones extrañas de plataformas que no usan

Usa herramientas de monitorización o alertas de crédito (cuando estén disponibles) para detectar actividad sospechosa lo antes posible. Enséñales a reconocer estas señales y a informarte de inmediato, en lugar de ignorarlas por miedo.

IoT y dispositivos inteligentes

Altavoces inteligentes, juguetes interactivos, relojes inteligentes, asistentes del hogar, tablets educativas... el Internet de las Cosas (IoT) se está convirtiendo rápidamente en parte de la vida cotidiana de los niños. Estos dispositivos hacen que el aprendizaje sea más interactivo, el entretenimiento más inmersivo y las tareas diarias más cómodas. Pero también generan nuevos riesgos de privacidad y ciberseguridad que muchas familias pasan por alto. Los dispositivos IoT están siempre encendidos, siempre conectados y, a menudo, escuchando. Esto genera una necesidad única de mantener una conciencia digital continua y control constante.

1. Supervisa el uso y elige dispositivos seguros

Al principio es fundamental observar cómo interactúa tu hijo con los dispositivos inteligentes. Ya sea un asistente de voz, un juguete conectado o una tablet educativa, mantente implicado en cómo se usa y qué funciones están activas.

Al elegir un dispositivo, fíjate en:
- Controles parentales integrados
- Opciones de configuración centradas en la privacidad
- Políticas claras sobre el uso de datos
- Posibilidad de silenciar micrófonos o desactivar la escucha cuando no se use
- Aprobación manual de nuevas funciones, apps o contactos

Siempre que sea posible, coloca los dispositivos inteligentes en zonas comunes como la cocina o el salón, nunca en los dormitorios, y considera limitar su uso sin supervisión.

2. Enseña las normas básicas de interacción segura

Los niños pueden humanizar a los asistentes de voz o juguetes inteligentes y empezar a hablarles como si fueran amigos de confianza. Por eso es crucial enseñarles los límites de una comunicación segura, sobre todo cuando el dispositivo está conectado a Internet.

Enséñales a:
- No compartir nunca nombres completos, números de teléfono, direcciones o datos del colegio
- No hablar sobre rutinas familiares, contraseñas o problemas personales
- Los asistentes de voz pueden “parecer amables”, pero no son personas ni espacios privados

Practica con ellos mediante juegos de rol sobre “qué está bien y qué no” decir en voz alta. Explícales que algunos juguetes inteligentes graban interacciones para mejorar su rendimiento, y por qué es importante tratarlos como extraños digitales.

3. Ajusta la privacidad y desactiva funciones innecesarias

Muchos dispositivos inteligentes vienen con configuraciones predeterminadas que priorizan la comodidad sobre la seguridad. Dedica tiempo a revisarlas con calma.

Acciones clave:
– Desactivar la subida automática de grabaciones de voz o la sincronización en la nube si es posible
– Desactivar la geolocalización salvo que sea estrictamente necesaria
– Borrar periódicamente el historial de interacciones o registros de voz
– Comprobar si se han activado funciones o “skills” de terceros sin tu consentimiento

4. Mantén el firmware actualizado y controla el acceso

Los dispositivos inteligentes desactualizados son más vulnerables a ciberataques. Asegúrate de que el firmware y el software estén siempre al día, ya sea manualmente o con actualizaciones automáticas de confianza.

Además:
– Limita qué cuentas y aplicaciones se conectan al dispositivo
– Usa contraseñas fuertes y únicas para los hubs inteligentes y las apps asociadas
– Revisa con frecuencia el historial de accesos o inicios de sesión si la plataforma lo permite
– Apaga micrófonos y cámaras cuando no se utilicen

Por ejemplo, televisores, altavoces o tablets inteligentes pueden ser puntos de entrada para accesos no autorizados si no se configuran correctamente.

5. Mantén viva la conversación

A medida que evolucionan los dispositivos inteligentes, también lo hacen los riesgos. Lo que hoy parece seguro mañana podría ser explotado. Crea una cultura en casa donde hacer preguntas y contar comportamientos extraños siempre esté permitido.

Pregunta cosas como:
– “¿Pasó algo raro mientras usabas el dispositivo?”
– “¿Te pidió que dijeras o hicieras algo?”
– “¿Respondió de una forma que te sorprendió o asustó? "

Estas preguntas ayudan a que tu hijo se mantenga alerta y te permiten detectar problemas potenciales a tiempo.

Recurso adicional
Checklist para el primer dispositivo

Tarde o temprano (la mayoría de) los padres acaban comprando a sus hijos su propio dispositivo electrónico. Según un informe de Kaspersky, el 61% de los niños recibe su primer dispositivo entre los ocho y los doce años y, quizá sorprendentemente, en el 11% de los casos se les da su propio teléfono móvil o tableta antes de cumplir los cinco. Es fundamental que los padres conozcan las pautas para introducir un dispositivo en la vida de sus hijos por primera vez.

Junto con la psicóloga clínica Dra. Saliha Afridi, Kaspersky ha elaborado una serie de recomendaciones tanto de ciberseguridad como psicológicas que los padres harían bien en tener en cuenta antes de regalar a sus hijos sus primeros gadgets tecnológicos.

¿Qué hacer antes de dar un dispositivo a un niño?

Configura una Cuenta Infantil antes de entregar el primer gadget a tu hijo. Ya sea un móvil o una tableta, es crucial garantizar que el dispositivo sea adecuado a su edad y seguro. Incluso si se trata de un regalo nuevo, prioriza siempre esta configuración. Una Cuenta Infantil actúa como salvaguarda en el dispositivo, evitando descargas de contenido para adultos o canciones con letras explícitas. Para obtener instrucciones detalladas sobre cómo crear una cuenta infantil, consulta nuestra guía para Android o la de iOS.

Instala todas las aplicaciones básicas que faciliten la comunicación o la geolocalización (como mensajería y mapas), además de aplicaciones educativas. Y no olvides configurar los ajustes de privacidad y confidencialidad en cada aplicación instalada, para que, por ejemplo, el niño no pueda ser localizado por desconocidos a través de su número de teléfono. Herramientas como Privacy Checker pueden ayudarte a personalizar la protección óptima en diferentes dispositivos y plataformas.

Recuerda instalar también una app de control parental digital. Esto te permitirá seleccionar contenidos, supervisar cuánto tiempo dedica tu hijo a cada aplicación (y establecer límites si es necesario) y conocer su ubicación en todo momento.

¿Cómo introducir un nuevo dispositivo en la vida de un niño?

Explícale las funcionalidades del dispositivo, así como los posibles peligros, en el momento de regalárselo. Esta es una oportunidad ideal para explorar sus características y comprender también sus riesgos.

Cread juntos un conjunto de normas de uso familiar. En esta conversación es importante fomentar la comprensión y el consenso sobre las responsabilidades y expectativas vinculadas a la posesión de un dispositivo. Para hacer un uso saludable, estableced zonas y horarios libres de tecnología: por ejemplo, durante las comidas o antes de dormir. Reservad también momentos para aficiones sin pantallas como la lectura, los juegos al aire libre o los puzles, que sirven como alternativas beneficiosas al tiempo frente a la pantalla. Revisar y ajustar estas normas periódicamente, a medida que tu hijo crece y la tecnología avanza, será clave.

Y recuerda: a menos que un niño muestre un nivel adecuado de participación en actividades reales y en la socialización cara a cara, no conviene introducirle un smartphone o redes sociales. Una forma de "ganarse" un dispositivo es demostrar que es capaz de cumplir de manera regular y constante con lo que no se negocia: dormir bien, hacer ejercicio, cumplir con los deberes, socializar, comer sano y tener momentos de descanso consciente.

¿Cómo hablar con un niño sobre seguridad en Internet?

Fomenta una comunicación abierta desde el principio. Habla con tu hijo sobre sus experiencias online, asegurándote de que se sienta seguro compartiendo tanto lo positivo como lo negativo.

Mantente informado sobre las últimas tendencias digitales y amenazas, así como casos destacados de ciberacoso o filtraciones de datos. Comparte esta información con tu hijo de manera que la entienda. Puedes mantenerte al día de las últimas noticias de ciberseguridad a través de nuestro Blog.

Explícale la permanencia de las acciones en Internet. Todo lo que se comparte online permanece allí y puede afectar a su reputación y a sus oportunidades futuras. Los niños deben ser especialmente cuidadosos con la información que comparten sobre sí mismos: nunca dar su dirección, ubicación ni credenciales de acceso y contraseñas. Además, deben evitar usar su nombre real como usuario, ya que puede dar pistas a los ciberdelincuentes para encontrar otras cuentas en redes sociales. Ayúdalos a entender el concepto de privacidad y los riesgos de compartir demasiada información.

Enséñale también que aceptar solicitudes de amistad de personas que no conocen en la vida real no está bien. Es fundamental explicar que si alguien que no conocen insiste en pedirles información personal sobre ellos o sus padres, eso es motivo de preocupación. No deben sentir que son groseros o maleducados si ignoran una petición de amistad: en las redes sociales, igual que en la vida real, la privacidad es necesaria.

Con este tipo de conversaciones, educando sin confrontación, logras que tu hijo esté más dispuesto a acudir a ti cuando se encuentre con algo dudoso en Internet. Asegúrate de que mantenga una actitud de curiosidad y no de miedo o juicio. Tus reacciones marcarán la diferencia en lo abiertos que se sientan a compartir contigo en el futuro.

Una **aplicación de control parental digital** es también aquí una herramienta muy útil para supervisar sus búsquedas y actividades online, garantizando así una experiencia más segura.

¿Cuáles son los principales riesgos de los que debo hablar con mi hijo?

En la era digital, los niños son vulnerables a los ciberdelincuentes, a menudo porque no están familiarizados con los principios básicos de ciberseguridad ni con las tácticas de estafa más comunes. Es nuestro deber, como tutores, educarlos en estos temas antes de que caigan inadvertidamente en una trampa.

Por ejemplo, guíalos para identificar anuncios engañosos, encuestas falsas, loterías fraudulentas y otros esquemas que puedan poner en riesgo sus datos personales. Ayúdales a comprender que, aunque pueda resultar tentador descargar una película de Barbie antes de su estreno oficial, ofertas como esa suelen ser trampas de ciberdelincuentes para robar datos o incluso sustraer dinero de las tarjetas de sus padres. Una solución de seguridad fiable puede detectar y bloquear tanto sitios web de phishing como software malicioso

Inculca en tu hijo el hábito de ser crítico y cauteloso cuando esté online. Enséñale a detenerse antes de hacer clic en enlaces dudosos, adjuntos de correo desconocidos o mensajes de remitentes extraños. Hablad también sobre los permisos que deben tener las aplicaciones en sus dispositivos. Por ejemplo, no hay ninguna razón válida para que una aplicación de calculadora solicite acceso a la geolocalización.

Haz que las conversaciones sobre ciberseguridad sean más amenas e interesantes abordando el tema a través de juegos y otros formatos entretenidos. Lo más importante: dale la confianza de acudir siempre a un adulto de confianza cuando se enfrente a situaciones inquietantes o sospechosas en Internet.

¿Cómo comprobar que estás preparado?

Una vez que aparece un dispositivo en casa, la vida familiar inevitablemente se transforma, ya que el niño queda atraído por el mundo de Internet. En lugar de prohibirlo, es recomendable guiarlo hacia un comportamiento responsable online: bien utilizado, un dispositivo puede ayudar realmente a los niños a aprender y crecer. Sin embargo, esto solo es posible si saben cuándo y cómo alertar a sus padres sobre cualquier amenaza digital que encuentren, ya sea recibir mensajes extraños de adultos, solicitudes de información personal o páginas de phishing.

El aprendizaje, no obstante, es un proceso gradual y no garantiza perfección desde el principio. Los errores ocurrirán de forma natural: tu hijo puede descargar accidentalmente un malware, interactuar con personas sospechosas o tener dificultades con la gestión del tiempo frente a la pantalla. Aun así, tu papel como padre es brindar apoyo y ayuda en ese proceso de aprendizaje. Solo de esta forma podrás garantizar que tu hijo esté seguro en Internet.