

Hoja de trabajo para la revisión de la seguridad de los jóvenes en Internet: Instrucciones

Esta ficha es una herramienta de evaluación estructurada diseñada para ayudar a padres, tutores, educadores o asistentes sociales a evaluar de forma sistemática la seguridad y el perfil de riesgo de una cuenta en línea concreta utilizada por un joven.

Se divide en tres áreas clave:

1. **Datos de la cuenta y ajustes técnicos:** recopila información identificativa (plataforma, nombre de usuario) y evalúa el nivel básico de seguridad Autenticación de Dos Factores (2FA), uso compartido de contraseñas, ajustes de privacidad.
2. **Interacción y características del contenido:** evalúa cómo se comunica el joven en la plataforma (voz, vídeo, mensajes privados) e indica problemas inmediatos relacionados con el contenido, como el acoso o las autolesiones.
3. **Indicadores de seguridad y riesgo:** una lista de verificación más amplia para determinar si se han implementado medidas de seguridad proactivas (tales como controles parentales, contratos de seguridad) e identificar “señales de alerta” en el comportamiento (aumento repentino del uso, contacto con personas desconocidas o preocupaciones relacionadas con el grooming).

Cómo utilizarlo

Se debe completar una hoja de trabajo independiente para cada plataforma principal que utilice el joven (por ejemplo, una para TikTok, otra para Instagram y otra para Roblox).

Paso 1: Recopilar información

- Siéntate con el joven y abran juntos la aplicación o la plataforma. Se recomienda encarecidamente realizar esto como una revisión colaborativa en lugar de una investigación secreta. Trabajar juntos en esto puede ayudar a generar confianza.

Paso 2: Rellena la sección “Cuenta”

- Rellena los espacios en blanco y marca las casillas correspondientes en relación con la configuración técnica.
- Comprobaciones fundamentales: revisa la configuración de privacidad (¿es realmente privada?), comprueba si la función de compartir la ubicación está activada y verifica si los mensajes privados y el chat de voz o vídeo están habilitados, ya que estas son las principales vías de riesgo.

Paso 3: Completa la sección “Indicadores de seguridad y riesgo”

Sé sincero al marcar estas casillas.

- Si marcas “Sí” en opciones como “aumento repentino del uso”, o en “nuevo amigo ‘importante’ en línea” o “contacto con personas desconocidas”, esto justifica una conversación y un seguimiento inmediatos.
- Si marcas “No” en “controles parentales activos” o en “contrato de seguridad en Internet y uso de datos”, es posible que debas tomar medidas inmediatas y proactivas...

Paso 4: Programar revisiones

- Este debe ser un proceso continuo, no un evento puntual aislado. Programa una revisión cada 90 días para asegurarte de que la configuración no ha cambiado y de que no han surgido nuevos riesgos. Siempre puedes revisar con más frecuencia si lo consideras necesario o si has detectado algún motivo de preocupación entre revisiones programadas.

Glosario

Término	Significado en lenguaje sencillo	Ejemplo
Autenticación de dos factores (2FA)	Un “cerrojo” o protección adicional para una cuenta. Aunque alguien robe la contraseña, no podrá acceder sin el código que se envía directo a tu teléfono.	Tras introducir la contraseña, la aplicación solicita un código de 6 dígitos que se envía al teléfono o al correo electrónico, o que se introduce desde una aplicación.
Correo electrónico/teléfono de recuperación	La información de contacto de “reserva” que se utiliza para volver a acceder a una cuenta si se olvida la contraseña o si un hacker la cambia.	Si un niño no puede acceder a su cuenta, se envía el enlace “Restablecer contraseña” a un correo electrónico o teléfono específico.
Compartir ubicación	Una función que utiliza el GPS para mostrar exactamente dónde se encuentra el dispositivo (y el joven) en un mapa a otros usuarios.	“Snap Maps” en Snapchat que muestra que el niño se encuentra actualmente en el parque local.
Controles parentales	Ajustes dentro de la aplicación o del dispositivo para limitar el tiempo o bloquear contenidos.	Configurar el “Tiempo de uso” en un dispositivo para desactivar todas las aplicaciones a las 9:00pm.

Término	Significado en lenguaje sencillo	Ejemplo
Software de supervisión	Aplicaciones de terceros que se instalan y que “vigilan” en busca de señales de alerta (palabras clave, fotos de desnudos, acoso) y te avisan.	Una aplicación que te envía una alerta porque ha detectado una conversación sobre “autolesiones” en un mensaje o una búsqueda.
Grooming	Cuando otra persona establece un vínculo emocional con un niño para reducir sus inhibiciones con el fin de abusar de él.	Otro “jugador” que le da a un niño moneda gratuita del juego y le dice: “No se lo digas a tus padres, no entenderían nuestra amistad”.
Sextorsión	Una forma de chantaje en la que alguien amenaza con difundir imágenes privadas o comprometedoras de un joven a menos que este le envíe más imágenes o dinero.	Alguien que se hace pasar por un compañero convence a una persona para que le envíe una foto o un vídeo y, a continuación, la amenaza con difundirlo a todo el colegio, sus amigos, sus padres, etc., a menos que le envíe dinero o más fotos o vídeos.
Violación de la cuenta	Cuando una persona no autorizada obtiene acceso a una cuenta (“ser hackeado”).	Un niño inicia sesión en su cuenta y descubre que toda su moneda del juego ha desaparecido y que su contraseña ha sido cambiada.

Consejo para padres: si no estás seguro de si un perfil es “privado” o “público”, prueba buscando el nombre de usuario de tu hijo en otro dispositivo en el que no hayas iniciado sesión. Si puedes ver sus fotos o su lista de amigos, es probable que la cuenta sea **pública**.

