PT 2 – PROGRAMA EDUCATIVO PR.I.S.C.I.LL.A PARA JÓVENES CON D.I.

Módulo 3: Posibles riesgos en el uso de las redes sociales

Documento creado por: INTRAS

Número de proyecto: 2023-2-RO01-KA220-YOU-000174271

Financiado por la Unión Europea. Los puntos de vista y las opiniones que se expresan son sin embrago solo del autor(es) y no reflejan necesariamente las de la Unión Europea o de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Tanto la Unión Europea como la EACEA no se hacen responsables de ello.

Co-funded by the European Union

PROGRAMA EDUCATIVO PR.I.S.C.I.LL.A PARA JÓVENES CON D.I.	
Módulo 3: Posibles riesgos en el uso de las redes sociales	
Resumen del módulo	En este módulo aprenderás sobre los riesgos que puedes correr al utilizar las redes sociales. Estos riesgos incluyen el ciberacoso (cuando la gente es mala contigo en Internet), el grooming (cuando un adulto se hace pasar por alguien de tu edad y te engaña para que compartas fotos o participes en actividades íntimas) y el phishing (cuando alguien intenta robar tu identidad o tus contraseñas). También aprenderás a detectar estos riesgos y a mantenerte seguro en las redes sociales.
Resultados de aprendizaje del módulo	Cuando termines este módulo, serás capaz de: 1.Entender qué son el ciberacoso, el grooming y el phishing. 2.Reconocer las situaciones en las que pueden darse estos riesgos. 3.Aprender consejos y medidas para mantenerse a salvo de estos riesgos.
Principios educativos adoptados	Este módulo está diseñado para ayudarte a: ● Asumir riesgos positivos utilizando los medios sociales de forma segura. ● Sentir que controlas tus acciones online. ● Aumentar tu independencia en el uso de las redes sociales.

Número de proyecto: 2023-2-RO01-KA220-YOU-000174271

Financiado por la Unión Europea. Los puntos de vista y las opiniones que se expresan son sin embrago solo del autor(es) y no reflejan necesariamente las de la Unión Europea o de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Tanto la Unión Europea como la EACEA no se hacen responsables de ello.

Co-funded by the European Union

	● Tomar decisiones seguras con confianza.
Contenidos del módulo	En los módulos anteriores hemos aprendido que las redes sociales son un espacio lleno de posibilidades. Es un entorno donde podemos descubrir información interesante, compartir nuestros pensamientos y sentimientos sobre distintos temas y conectar con personas que comparten nuestros intereses. Sin embargo, es importante recordar que el mundo online también tiene sus riesgos. Para disfrutar de las redes sociales de forma segura, debemos conocer estos riesgos y aprender a protegernos de ellos. De este modo, podremos sacar el máximo partido de nuestras experiencias en línea sin correr riesgos. Ahora te presentaremos algunos de los riesgos más comunes: el ciberacoso, el grooming y el phishing. **¿Qué es el ciberacoso?** El ciberacoso se produce cuando alguien utiliza las redes sociales o las plataformas en línea para enviar mensajes malintencionados, publicar comentarios hirientes o difundir rumores. Los ciberacosadores suelen esconderse tras cuentas falsas. **Ejemplos de ciberacoso:** ● Alguien comenta tu foto: «¡Qué raro estás! No le gustas a nadie». ● Un grupo de personas envía mensajes desagradables en un chat de grupo, haciéndote sentir excluido o molesto, por ejemplo: «Ignorémosla y no la dejemos formar parte del grupo nunca más.»

Número de proyecto: 2023-2-RO01-KA220-YOU-000174271

Financiado por la Unión Europea. Los puntos de vista y las opiniones que se expresan son sin embrago solo del autor(es) y no reflejan necesariamente las de la Unión Europea o de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Tanto la Unión Europea como la EACEA no se hacen responsables de ello.

Co-funded by the European Union

● Alguien te envía un mensaje privado diciendo: «Eres un estúpido. **“**Deja de publicar cosas en Internet”**.Consejos prácticos para evitar el ciberacoso**

1.No respondas. Si alguien te envía mensajes malintencionados, no respondas.
2.Guarda las pruebas. Haz capturas de pantalla de los mensajes o comentarios malintencionados para enseñárselos a un adulto de confianza.
3.Bloquea y denuncia. Utiliza las herramientas de la plataforma para bloquear al acosador y denunciar su comportamiento.
4.Habla con alguien de confianza. Comparte tus sentimientos con un padre, profesor o amigo.
5.Sé amable en Internet. Trata a los demás con respeto para crear un entorno online positivo.

¿Qué es el Grooming?

El grooming es cuando un adulto usa internet para manipular y engañar a un menor con el fin de obtener información personal, pedir fotos privadas o hacer que participe en conductas peligrosas. Los groomers suelen hacerse pasar por un amigo, alguien de tu edad o alguien que dice entenderte para ganarse tu confianza.

Ejemplos de Grooming

- Una persona en línea te envía mensajes amistosos y halagos, y te hace preguntas personales como: “¿Dónde vives?” o “¿Puedes mandarme una foto tuya?”

- Alguien te dice: “Me gusta mucho cómo te ves. Eres muy guapo/a. Mi tío tiene una agencia de modelos y puede hacerte famoso/a si me mandas

Número de proyecto: 2023-2-RO01-KA220-YOU-000174271

Financiado por la Unión Europea. Los puntos de vista y las opiniones que se expresan son sin embrago solo del autor(es) y no reflejan necesariamente las de la Unión Europea o de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Tanto la Unión Europea como la EACEA no se hacen responsables de ello.

Co-funded by the European Union

unas fotos tuyas."

Consejos prácticos para evitar el grooming

- **No compartas información personal.** Nunca des tu dirección, número de teléfono, nombre de tu escuela ni contraseñas.
- **Ten cuidado con las fotos.** No envíes tus fotos a personas que no conoces.
- **Confía en tus sentimientos.** Si alguien en internet te hace sentir incómodo/a, deja de hablarle.
- **Habla con un adulto de confianza.** Si tienes dudas sobre alguien en línea, cuéntaselo a un padre, profesor o cuidador.
- **Bloquea y reporta.** Usa la configuración de la plataforma para bloquear a la persona y reportar su comportamiento.

¿Qué es el Phishing?

El phishing es cuando alguien finge ser una persona o empresa de confianza para robar tu información, como contraseñas, datos de cuentas o dinero. Suelen usar correos electrónicos, mensajes o sitios web falsos para engañarte.

Ejemplos de Phishing

- Recibes un correo que parece de tu banco y dice: "Hay un problema con tu cuenta bancaria. Haz clic aquí para iniciar sesión."

Número de proyecto: 2023-2-RO01-KA220-YOU-000174271

Financiado por la Unión Europea. Los puntos de vista y las opiniones que se expresan son sin embrago solo del autor(es) y no reflejan necesariamente las de la Unión Europea o de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Tanto la Unión Europea como la EACEA no se hacen responsables de ello.

Co-funded by the European Union

- Te llega un mensaje que dice: “¡Has ganado un premio! Haz clic en este enlace para reclamarlo.”

Consejos prácticos para evitar el phishing

- **No hagas clic en enlaces desconocidos.** Si recibes un mensaje o correo de alguien en quien no confías, ignóralo y no hagas clic en ningún enlace.
- **Revisa al remitente.** Observa bien la dirección de correo o el nombre de usuario. Los mensajes falsos suelen tener errores de ortografía.
- **Protege tus contraseñas.** Nunca compartas tus contraseñas con nadie.
- **Desconfía de premios.** Si alguien dice que ganaste algo increíble pero suena raro o demasiado fácil, probablemente no sea real.
- **Usa sitios seguros.** Asegúrate de que el sitio web comience con “https://” y tenga el símbolo del candado.

Número de proyecto: 2023-2-RO01-KA220-YOU-000174271

Financiado por la Unión Europea. Los puntos de vista y las opiniones que se expresan son sin embrago solo del autor(es) y no reflejan necesariamente las de la Unión Europea o de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Tanto la Unión Europea como la EACEA no se hacen responsables de ello.

Co-funded by the European Union

Casos hipotéticos **Introducción**	Explica a los participantes que van a escuchar/leer tres historias diferentes, cada una de las cuales presenta una situación que tuvo lugar en Internet. Estas historias están diseñadas para ayudarles a comprender algunos de los riesgos que pueden encontrar al utilizar las redes sociales e Internet. Después de leer cada historia, guía a los participantes en un debate haciéndoles preguntas específicas. Anímalos a que reflexionen sobre la situación, identifiquen los riesgos que conlleva y piensen en la mejor manera de responder de forma segura. El objetivo de esta actividad es ayudar a los participantes a reconocer los peligros en línea y a desarrollar estrategias para protegerse.
Caso hipotético 1	**El caso de Lucía** Lucia tiene 19 años y le gusta dibujar. A menudo comparte sus obras en las redes sociales. Un día, alguien le envía un mensaje: «¡Hola! Me encantan tus dibujos. Tienes mucho talento. ¿Podemos ser amigos?». Lucía se siente feliz y responde: «¡Gracias! Claro». Al cabo de unos días, la persona empieza a hacerle a Lucía preguntas personales como: «¿Dónde vives?» y «¿Puedes enviarme una foto tuya?». También le dicen a Lucía: «No le cuentes a nadie lo de nuestros mensajes: es nuestro secreto». **1.** ¿Qué podría pasar si Lucía comparte información personal con alguien que no conoce en Internet? a) Podrían utilizar la información para engañarla o hacerle daño. b) Que se convierta en su mejor amigo.

Número de proyecto: 2023-2-RO01-KA220-YOU-000174271

Financiado por la Unión Europea. Los puntos de vista y las opiniones que se expresan son sin embrago solo del autor(es) y no reflejan necesariamente las de la Unión Europea o de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Tanto la Unión Europea como la EACEA no se hacen responsables de ello.

Co-funded by the European Union

	c) Nada; compartir información personal siempre es seguro. **2.** ¿Qué debe hacer Lucía cuando la persona le pide una foto? a) Enviarla rápidamente para ser educada. b) Decir que no y bloquear a la persona. c) Preguntar a la persona para qué necesita la foto. **3.** Si Lucía se siente insegura ante esta situación, ¿cuál es el mejor paso que puede dar? a) Hablar con un adulto de confianza sobre los mensajes. b) Ignorar sus sentimientos y seguir hablando. c) Preguntar a sus amigos si les parece bien.
Caso hipotético 2	**El caso de Luca** Luca comparte una divertida foto suya en las redes sociales. Alguien comenta: «¡Pareces tonto!» y otras personas empiezan a reírse y a escribir cosas feas sobre él. Luca se siente molesto y no sabe qué hacer. Se pregunta si debería borrar su cuenta o responder enfadado a los comentarios. **1.** ¿Qué es lo primero que debe hacer Luca ante los malos comentarios? a) Ignorar los comentarios y hacer capturas de pantalla como prueba. b) Responder a los comentarios malintencionados.

Número de proyecto: 2023-2-RO01-KA220-YOU-000174271

Financiado por la Unión Europea. Los puntos de vista y las opiniones que se expresan son sin embrago solo del autor(es) y no reflejan necesariamente las de la Unión Europea o de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Tanto la Unión Europea como la EACEA no se hacen responsables de ello.

Co-funded by the European Union

	c) Borrar su cuenta inmediatamente. **2.** ¿Con quién debería hablar Luca si se siente herido por los comentarios? a) Un adulto de confianza, como un profesor, un padre o un cuidador. b) Con la persona que publicó los comentarios. c) Con nadie; debe guardárselo para sí mismo. **3.** ¿Cuál es una buena manera de que Luca afronte el ciberacoso en el futuro? a) Evita volver a compartir nada en Internet. b) Bloquear y denunciar a las personas que están siendo malas. c) Escribir un post largo explicando lo herido que se siente.
Caso hipotético 3	**El caso de Ana** Ana recibe un correo electrónico que parece de su tienda online favorita. El correo dice: «¡Enhorabuena! ¡Has ganado una tarjeta regalo de 50 euros! Haz clic aquí para conseguir tu premio». Ana está emocionada, pero no está segura de que sea real. Se da cuenta de que la dirección de correo electrónico tiene un aspecto extraño y de que el enlace no coincide con el sitio web de la tienda. 1. ¿Qué debe hacer Ana antes de hacer clic en el enlace?

Número de proyecto: 2023-2-RO01-KA220-YOU-000174271

Financiado por la Unión Europea. Los puntos de vista y las opiniones que se expresan son sin embrago solo del autor(es) y no reflejan necesariamente las de la Unión Europea o de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Tanto la Unión Europea como la EACEA no se hacen responsables de ello.

Co-funded by the European Union

	a) Comprobar si la dirección de correo electrónico y el enlace parecen reales y coinciden con el sitio web de la tienda. b) Hacer clic rápidamente antes de que se agote el premio. c) Responder al correo electrónico solicitando más detalles. 2. ¿Cuál es la señal de advertencia de que este correo electrónico puede ser falso? a) El correo electrónico le pide información personal. b) El mensaje está escrito en tono amistoso. c) El mensaje incluye el nombre de la tienda. 3. Si Ana cree que este correo electrónico es sospechoso, ¿qué debe hacer? a) Denuncia el correo como phishing y bórralo. b) Reenvía el mensaje a sus amigos para que comprueben si es real. c) Ignorar el mensaje, pero mantenerlo en su bandeja de entrada.
Material adicional	
Fuentes	

Actividad del módulo	
Nombre de la actividad	Detectar riesgos
Objetivos	Practicar la identificación de riesgos potenciales en diferentes escenarios en línea y discutir las acciones

Número de proyecto: 2023-2-RO01-KA220-YOU-000174271

Financiado por la Unión Europea. Los puntos de vista y las opiniones que se expresan son sin embrago solo del autor(es) y no reflejan necesariamente las de la Unión Europea o de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Tanto la Unión Europea como la EACEA no se hacen responsables de ello.

Co-funded by the European Union

	apropiadas que debemos tomar para mantenernos seguros.
Metodología de aprendizaje	Aprender haciendo, ejercicios prácticos y actividades interactivas
Duración de la actividad	30 minutos
Recursos necesarios	Tarjetas con escenarios Papel y bolígrafos si quieres escribir tus respuestas.
Instrucciones	En esta actividad, verás imágenes o escucharás historias breves sobre cosas que pueden ocurrir en Internet. Tu trabajo consiste en: 1. Decidir si la situación es arriesgada o segura. 2. Decir por qué crees que es arriesgada. 3. Explicar qué harías para mantenerte a salvo. **Ejemplo** Empecemos con un ejemplo sencillo para ayudarte a entender cómo funciona la actividad: Un desconocido te envía un mensaje diciendo: «¡Eres tan guay! ¿Podemos quedar?». Pregúntate a ti mismo: - ¿Es arriesgado? - ¿Porqué podria ser arriesgado? - ¿Qué debería hacer en esta situción? Respuesta:

Número de proyecto: 2023-2-RO01-KA220-YOU-000174271

Financiado por la Unión Europea. Los puntos de vista y las opiniones que se expresan son sin embrago solo del autor(es) y no reflejan necesariamente las de la Unión Europea o de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Tanto la Unión Europea como la EACEA no se hacen responsables de ello.

Co-funded by the European Union

	Sí, es arriesgado porque no conoces a la persona. Puede que no sea quien dice ser. Deberías ignorar el mensaje, bloquear a la persona y contárselo a un adulto de confianza. Ahora verás diferentes situaciones en Internet. Piensa detenidamente en cada una de ellas y responde a las siguientes preguntas: • ¿Es arriesgado o seguro? • ¿Por qué crees que es arriesgado o seguro? • ¿Qué harías para mantenerte a salvo? **Situación 1:** Alguien en línea dice: «Puedo ayudarte a conseguir muchos seguidores si me envías tu contraseña». **Situación 2:** Un amigo publica una foto divertida tuya sin preguntar antes. **Situación 3:** Alguien comenta en tu post: «Eres tan feo que todo el mundo te odia». **Situación 4:** Recibes un correo electrónico que dice: «¡Enhorabuena! ¡Has ganado 1.000 euros! Haz clic aquí para reclamar tu premio». **Situación 5:**

Número de proyecto: 2023-2-RO01-KA220-YOU-000174271

Financiado por la Unión Europea. Los puntos de vista y las opiniones que se expresan son sin embrago solo del autor(es) y no reflejan necesariamente las de la Unión Europea o de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Tanto la Unión Europea como la EACEA no se hacen responsables de ello.

Co-funded by the European Union

	Estás en un chat de grupo en línea sobre tu videojuego favorito. Alguien en el chat pregunta: «¿Qué día cumples años? Queremos celebrarlo contigo». **Situación 6:** Recibes un mensaje de alguien que dice: «Buscamos gente para trabajar desde casa. Envía tu nombre, dirección y datos bancarios para empezar». **Situación 7:** Te haces una foto de grupo con tus amigos en un parque y quieres publicarla en las redes sociales. Uno de tus amigos dice que no quiere su foto en Internet. **Situación 8:** Un desconocido te envía un mensaje diciendo: «¡Eres tan guay y guapa! Me encantaría hablar más. ¿Puedes contarme más cosas sobre ti?». **Ejemplos de respuestas** Ejemplo de respuesta situación 1 ● Esto es arriesgado porque podrían usar tu contraseña para apoderarse de tu cuenta. ● Nunca debes compartir tus contraseñas con nadie. Bloquea a la persona y denúnciala. situación de respuesta de muestra 2 ● Esto podría ser arriesgado porque la foto podría avergonzarte o compartir información privada. ● Deberías pedirle a tu amigo que borre la foto y explicarle por qué es importante pedir permiso.

Número de proyecto: 2023-2-RO01-KA220-YOU-000174271

Financiado por la Unión Europea. Los puntos de vista y las opiniones que se expresan son sin embrago solo del autor(es) y no reflejan necesariamente las de la Unión Europea o de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Tanto la Unión Europea como la EACEA no se hacen responsables de ello.

Co-funded by the European Union

	Ejemplo de respuesta situación 3 ● Esto es ciberacoso porque el comentario es hiriente y podría herir tus sentimientos. ● Deberías hacer una captura de pantalla del comentario, bloquear a la persona y decírselo a un adulto de confianza Ejemplo de respuesta situación 4 ● Esto es arriesgado porque probablemente sea una estafa de phishing para robar tu información personal. ● Deberías eliminar el correo electrónico y denunciarlo como spam. Nunca hagas clic en enlaces de correos electrónicos como éste Ejemplo de respuesta situación 5 ● Esto es arriesgado porque compartir tu cumpleaños en un chat público puede conducir al robo de identidad o a contactos no deseados. ● Debes evitar dar detalles personales como tu cumpleaños completo en espacios públicos. Si alguien pregunta, di educadamente que no compartes información personal en línea. Ejemplo de respuesta situación 6 ● Esto es riesgoso porque probablemente sea una estafa diseñada para robar tu información personal o financiera. ● Deberías borrar el mensaje inmediatamente y denunciar al remitente. Nunca compartas información sensible como tu dirección o datos bancarios con personas que no conoces.

Número de proyecto: 2023-2-RO01-KA220-YOU-000174271

Financiado por la Unión Europea. Los puntos de vista y las opiniones que se expresan son sin embrago solo del autor(es) y no reflejan necesariamente las de la Unión Europea o de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Tanto la Unión Europea como la EACEA no se hacen responsables de ello.

Co-funded by the European Union

	Ejemplo de respuesta situación 7 ● Esto es seguro sólo si respetas los deseos de tu amigo y no publicas la foto. Ignorar su petición no sería seguro ni amable. ● Debes asegurarte de pedir permiso a todos los que aparecen en la foto antes de publicarla en Internet. Si alguien dice que no, elige otra foto o no la publiques. Ejemplo de respuesta situación 8 ● Esto es arriesgado porque los desconocidos que hacen cumplidos podrían estar intentando engatusarte o ganarse tu confianza por razones inseguras. ● No debes responder al mensaje. Bloquea a la persona inmediatamente y cuéntale lo sucedido a un adulto de confianza. **Reflexión** Después de terminar las situaciones, tómate un tiempo para pensar en lo que has aprendido. Pregúntate: ● ¿Qué riesgo te ha sorprendido más? ● ¿Cómo te sentiste al decidir qué hacer en cada situación? ● ¿Qué harás diferente la próxima vez que estés en línea? Habla con el grupo o con tu profesor sobre tus respuestas. Compartir tus pensamientos puede ayudarte a sentirte más confiado a la hora de mantenerte seguro en Internet.

Número de proyecto: 2023-2-RO01-KA220-YOU-000174271

Financiado por la Unión Europea. Los puntos de vista y las opiniones que se expresan son sin embrago solo del autor(es) y no reflejan necesariamente las de la Unión Europea o de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Tanto la Unión Europea como la EACEA no se hacen responsables de ello.

Co-funded by the European Union

	Conclusión Has hecho un gran trabajo detectando riesgos y pensando en cómo mantenerte seguro en Internet. Recuerda: ✔ Si algo te parece mal en Internet, confía en lo que sientes. ✔ No compartas información personal o contraseñas con gente que no conoces. ✔ Habla siempre con alguien de confianza si no estás seguro de alguna situación.

Actividad del módulo	
Nombre de la actividad	Juegos de rol
Objetivos	Practicarás cómo responder a diferentes riesgos online al representar situaciones en grupos pequeños. Esta actividad te ayudará a sentirte más seguro sobre qué hacer si enfrentas estos riesgos en la vida real. Aprenderás: ✔ Cómo responder a los riesgos comunes en línea. ✔ Cómo tomar decisiones inteligentes y seguras cuando algo parece estar mal. ✔ Cómo pedir ayuda cuando la necesitas.
Metodología de aprendizaje	Juegos de rol

Número de proyecto: 2023-2-RO01-KA220-YOU-000174271

Financiado por la Unión Europea. Los puntos de vista y las opiniones que se expresan son sin embrago solo del autor(es) y no reflejan necesariamente las de la Unión Europea o de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Tanto la Unión Europea como la EACEA no se hacen responsables de ello.

Co-funded by the European Union

Duración de la actividad	30-40 minutos
Recursos necesarios	● Tarjetas con las situaciones o hojas impresas con los escenarios. ● Un espacio seguro para que los grupos pequeños practiquen juegos de rol.
Instrucciones	Trabajarán en grupos pequeños para representar distintas situaciones. Cada grupo recibirá una situación sobre un riesgo en línea. Una persona actuará como la persona que enfrenta el problema y los demás desempeñarán diferentes roles, como un amigo, la persona riesgosa o un adulto de confianza. Después de representar la situación, hablaremos sobre lo que sucedió y cómo manejarlo. Situación 1 ● Historia: Alguien en línea dice: "¡Tienes mucho talento! ¿Puedo ver más fotos tuyas? Prometo que no las compartiré con nadie". ● Roles: o Persona a la que se le piden fotos. o El extraño. o Un adulto de confianza o un amigo con quien la persona habla para pedirle consejo.

Número de proyecto: 2023-2-RO01-KA220-YOU-000174271

Financiado por la Unión Europea. Los puntos de vista y las opiniones que se expresan son sin embrago solo del autor(es) y no reflejan necesariamente las de la Unión Europea o de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Tanto la Unión Europea como la EACEA no se hacen responsables de ello.

Co-funded by the European Union

	● Pasos a seguir: o Negarse a enviar fotos. o Bloquear al extraño. o Hablar con el adulto de confianza sobre lo que sucedió. Situación 2 ● Historia: Alguien comenta en tu publicación: "Esto es tan tonto. ¿Por qué te molestas?". Otras personas comienzan a darle Me gusta al comentario y también escriben cosas malas. ● Roles: o La persona que sufre el acoso. o El acosador. o Un adulto de confianza o un amigo con quien la persona habla. ● Pasos a seguir: o No respondas a los comentarios malintencionados. o Toma capturas de pantalla como prueba. o Bloquea y denuncia al acosador. Escenario 3 ● Historia: Recibes un correo electrónico que dice: “¡Felicitaciones! ¡Has ganado un teléfono nuevo! Haz clic en este enlace para reclamar tu premio”.

Número de proyecto: 2023-2-RO01-KA220-YOU-000174271

Financiado por la Unión Europea. Los puntos de vista y las opiniones que se expresan son sin embrago solo del autor(es) y no reflejan necesariamente las de la Unión Europea o de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Tanto la Unión Europea como la EACEA no se hacen responsables de ello.

Co-funded by the European Union

	● Roles: o La persona que recibe el correo electrónico. o El estafador que envió este correo electrónico. o Un amigo o un adulto de confianza que te da consejos. ● Pasos a seguir: o No hagas clic en el enlace. o Elimina el correo electrónico y denúncialo como spam. o Habla con un adulto de confianza si no estás seguro. Debate Después de que cada grupo haya representado su escenario, reúnanse en un grupo grande para debatir: ● ¿Qué hizo que la situación fuera arriesgada? ● ¿Qué hizo la persona para mantenerse a salvo? ● ¿Cómo se sintió al practicar esta situación? ● ¿Qué harías si esto te sucediera en la vida real? Conclusión ¡Has hecho un excelente trabajo practicando cómo manejar los riesgos en línea! Recuerda: ● Siempre confía en tus instintos: si algo te parece mal, probablemente lo esté.

Número de proyecto: 2023-2-RO01-KA220-YOU-000174271

Financiado por la Unión Europea. Los puntos de vista y las opiniones que se expresan son sin embrago solo del autor(es) y no reflejan necesariamente las de la Unión Europea o de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Tanto la Unión Europea como la EACEA no se hacen responsables de ello.

Co-funded by the European Union

	● Bloquea y denuncia a las personas que te hagan sentir incómodo. ● Habla con un adulto de confianza si no estás seguro de qué hacer.

Actividad del módulo	
Nombre de la actividad	Juego de clasificación de riesgos
Objetivos	Practicarás la identificación de comportamientos en línea seguros y riesgosos clasificando los ejemplos en categorías "Seguro" o "arriesgado".
Metodología de aprendizaje	Ejercicios prácticos y actividades interactivas
Time allocated for the Activity	20 minutos
Duración de la actividad	● Tarjetas con acciones en línea. ● Dos zonas etiquetadas: “Seguro” y “Riesgo” (en un tablero o mesa).
Instrucciones	¡Pongamos a prueba lo que has aprendido sobre los riesgos en línea! En esta actividad, verás ejemplos de cosas que la gente podría hacer en línea. Tu tarea es decidir si cada ejemplo es “seguro” o “arriesgado”. Trabajarás en parejas o en grupos pequeños. Cada grupo recibirá tarjetas con ejemplos de acciones en línea. Tu tarea es colocar cada tarjeta en la categoría “seguro” o

Número de proyecto: 2023-2-RO01-KA220-YOU-000174271

Financiado por la Unión Europea. Los puntos de vista y las opiniones que se expresan son sin embrago solo del autor(es) y no reflejan necesariamente las de la Unión Europea o de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Tanto la Unión Europea como la EACEA no se hacen responsables de ello.

Co-funded by the European Union

	“arriesgado” en el tablero o la mesa. Después de ordenar las tarjetas, analizaremos tus opciones como grupo. Probemos un ejemplo juntos: Ejemplo de tarjeta: "Compartir su nombre completo y dirección en su perfil". ¿Es seguro o arriesgado? Respuesta: arriesgado. Compartir información personal puede hacerte vulnerable. ¡Ahora te toca a ti! Estas son las tarjetas que debes ordenar: ● “Aceptar una solicitud de amistad de alguien que no conoces”. ● “Publicar una foto de tu pasatiempo favorito”. ● “Hacer clic en un enlace de un correo electrónico que dice que has ganado un premio”. ● “Bloquear a alguien que te envía mensajes malintencionados”. ● “Compartir tu número de teléfono en una publicación pública”. ● “Recibes una solicitud de amistad de alguien que no tiene foto de perfil ni publicaciones en su cuenta”. ● “Compartes una foto de tu libro favorito sin ningún otro detalle personal”. ● “Recibes un mensaje que dice: '¡Envíame tu ubicación para que podamos pasar el rato!' de alguien que no conoces”. ● “Publicas una foto del nombre de tu escuela en las redes sociales”.

Número de proyecto: 2023-2-RO01-KA220-YOU-000174271

Financiado por la Unión Europea. Los puntos de vista y las opiniones que se expresan son sin embrago solo del autor(es) y no reflejan necesariamente las de la Unión Europea o de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Tanto la Unión Europea como la EACEA no se hacen responsables de ello.

Co-funded by the European Union

	● "Tu amigo te dice que lo están acosando online y lo animas a hablar con un adulto de confianza". Respuestas de ejemplo: 1. “Aceptar una solicitud de amistad de alguien que no conoces”. Respuesta: arriesgado. Aceptar solicitudes de personas que no conoces puede ser peligroso porque podrían no ser quienes dicen ser. Asegúrate siempre de conectarte solo con personas en las que confíes. 2. “Publicar una foto de tu pasatiempo favorito”. Respuesta: seguro. Compartir tus intereses, como una foto de tu pasatiempo favorito, está bien siempre que no incluya detalles privados como tu ubicación o el nombre de la escuela. 3. “Hacer clic en un enlace de un correo electrónico que dice que has ganado un premio”. Respuesta: arriesgado. Es probable que se trate de una estafa de phishing. Hacer clic en el enlace podría dar a los estafadores acceso a tu información o dañar tu dispositivo. Elimina el correo electrónico y no hagas clic en el enlace. 4.“Bloquear a alguien que te envía mensajes malintencionados”. Respuesta: seguro. Bloquear a alguien que es malo contigo en línea es una forma inteligente de detener la negatividad. También es importante denunciar su comportamiento y contárselo a un adulto de confianza.

Número de proyecto: 2023-2-RO01-KA220-YOU-000174271

Financiado por la Unión Europea. Los puntos de vista y las opiniones que se expresan son sin embrago solo del autor(es) y no reflejan necesariamente las de la Unión Europea o de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Tanto la Unión Europea como la EACEA no se hacen responsables de ello.

Co-funded by the European Union

	5.“Compartir tu número de teléfono en una publicación pública”. Respuesta: arriesgado. Compartir tu número de teléfono en una publicación pública no es seguro porque cualquiera puede usarlo para ponerse en contacto contigo o averiguar tus datos personales. Mantén tu número de teléfono privado y compártelo solo con personas en las que confíes directamente. 6. “Recibes una solicitud de amistad de alguien que no tiene foto de perfil ni publicaciones en su cuenta”. Respuesta: arriesgado. Aceptar solicitudes de cuentas desconocidas o sospechosas puede dar lugar a interacciones inseguras. 7. “Compartes una foto de tu libro favorito sin ningún otro dato personal”. Respuesta: Seguro. Está bien compartir intereses generales sin revelar información privada. 8. "Recibes un mensaje que dice: '¡Envíame tu ubicación para que podamos pasar el rato!' de alguien que no conoces". Respuesta: Arriesgado. Compartir tu ubicación con desconocidos puede ser peligroso. 9. "Publicas una foto del nombre de tu escuela en las redes sociales". Respuesta: arriesgado. Compartir el nombre de tu escuela puede ayudar a desconocidos a averiguar dónde encontrarte.

Número de proyecto: 2023-2-RO01-KA220-YOU-000174271

Financiado por la Unión Europea. Los puntos de vista y las opiniones que se expresan son sin embrago solo del autor(es) y no reflejan necesariamente las de la Unión Europea o de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Tanto la Unión Europea como la EACEA no se hacen responsables de ello.

Co-funded by the European Union

	10. "Tu amigo te dice que lo están acosando en línea y lo animas a hablar con un adulto de confianza". Respuesta: Seguro. Apoyar a un amigo y ayudarlo a buscar ayuda es la acción correcta. Debate Después de ordenar las tarjetas, analiza tus respuestas con el grupo. ● ¿Todos estuvieron de acuerdo en qué acciones eran riesgosas? ● ¿Qué hizo que algunas acciones fueran más seguras que otras? ● ¿Cómo puedes recordar mantenerte a salvo en situaciones similares? Conclusión ¡Buen trabajo al ordenar los riesgos! Ahora sabes cómo identificar conductas seguras y riesgosas en línea. Recuerda, cuando tengas dudas, siempre pregunta a un adulto de confianza.

Número de proyecto: 2023-2-RO01-KA220-YOU-000174271

Financiado por la Unión Europea. Los puntos de vista y las opiniones que se expresan son sin embrago solo del autor(es) y no reflejan necesariamente las de la Unión Europea o de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Tanto la Unión Europea como la EACEA no se hacen responsables de ello.

Co-funded by the European Union