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

PR.I.S.C.I.LLA
Preventing Incident of Sexual Cyberbullying in Intellectual disability

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

Co-funded by the European Union

Project Nr: 2023-2RO01-KA220-YOU-000174271

1

Posibles riesgos al usar Redes Sociales

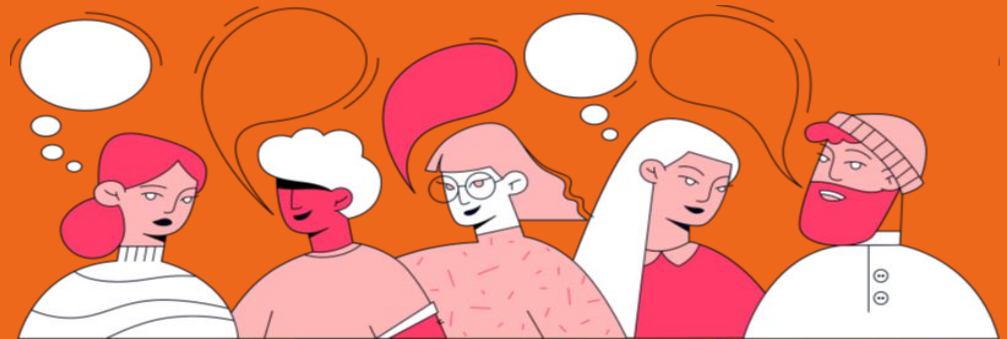



Resumen del módulo

En este módulo, aprenderás sobre los riesgos que pueden ocurrir al utilizar las redes sociales. Estos riesgos incluyen:

- **Ciberacoso**
- **Grooming**
- **Phishing**

También aprenderás a detectar estos riesgos y a mantenerte seguro cuando utilices las redes sociales.



Resultados de aprendizaje del módulo

Al final de este módulo, serás capaz de:

1. Entender qué son el ciberacoso, el grooming y el phishing.
2. Reconocer las situaciones en las que pueden producirse estos riesgos.
3. Aprender consejos y medidas para protegerte de estos riesgos.

Resumen del módulo

Este módulo está diseñado para ayudarte:

- Asume riesgos positivos utilizando las redes sociales de forma Segura
- Controla tus acciones en Internet
- Aumenta tu independencia en el uso de las redes sociales
- Tomar decisiones seguras con confianza

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.

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.

Grooming

Ocurre cuando un adulto utiliza Internet para manipular y engañar a un joven para que comparta información personal, envíe fotos privadas o adopte comportamientos inseguros.

Consejos para evitar el grooming

1. **No compartas información personal.** Nunca des tu dirección, número de teléfono, nombre de la escuela o contraseñas.
2. **Ten cuidado con las fotos.** No envíes tus fotos a gente que no conoces.
3. **Confía en tus sentimientos.** Si alguien en Internet te hace sentir incómodo, deja de hablar con él.
4. **Habla con un adulto de confianza.** Si no estás seguro de alguien en Internet, díselo a tus padres, profesor o cuidador.
5. **Bloquea y denuncia.** Utiliza la configuración de la plataforma para bloquear a la persona y denunciar su comportamiento.

Phishing

Ocurre cuando alguien se hace pasar por una persona o empresa de confianza para robar su información, como contraseñas, datos de cuentas o dinero. Suelen utilizar correos electrónicos, mensajes o sitios web falsos para engañarte.

Consejos para evitar el phishing

1. **No hagas clic en enlaces desconocidos.** Si recibes un mensaje o correo electrónico de alguien que no te inspira confianza, ignóralo y no hagas clic en los enlaces que contenga**.**
2. **Comprueba el remitente.** Fíjate bien en la dirección de correo electrónico o el nombre de usuario del remitente. Los mensajes falsos suelen tener pequeñas faltas de ortografía**.**
3. **Proteja sus contraseñas.** Nunca compartas tus contraseñas con nadie.
4. **Cuidado con los premios.** Si alguien te dice que has ganado algo increíble, pero te parece extraño o demasiado fácil, probablemente no sea real.
5. **Utiliza sitios web seguros.** Asegúrate de que el nombre del sitio web empieza por «https://» y muestra un candado.

2

Casos hipotéticos




Ahora leeremos tres situaciones en línea que te ayudarán a comprender algunos de los riesgos que puedes encontrar al utilizar las redes sociales e Internet.

Después de leer cada historia, reflexionaremos sobre la situación, identificaremos los riesgos que conlleva y pensaremos en la mejor manera de responder de forma segura.

El objetivo de esta actividad es ayudarte a reconocer los peligros en línea y a desarrollar estrategias para protegerte.

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».

El caso de Lucía, debatamos

1. 1. ¿Qué podría pasar si Lucía comparte información personal con alguien que no conoce en Internet?

2. 2. ¿Qué debe hacer Lucía cuando la persona le pide una foto?

3. 3. Si Lucía se siente insegura ante esta situación, ¿cuál es el mejor paso que puede dar?

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.

El caso de Luca, debatamos

1. 1. ¿Qué es lo primero que debe hacer Luca ante los malos comentarios?

2. 2. ¿Con quién debería hablar Luca si se siente herido por los comentarios?

3. 3. ¿Cuál es una buena manera de que Luca afronte el ciberacoso en el futuro?

El caso de Ana

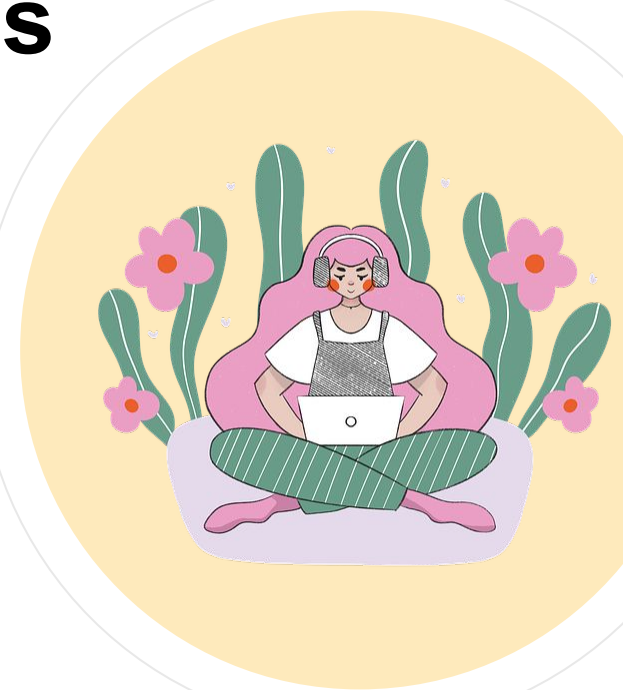
- Ana recibe un correo electrónico que parece de su tienda online favorita. El correo dice: «¡Enhorabuena! ¡Has ganado una tarjeta regalo de 50 euros! Haz clic aquí para conseguir tu premio». Ana está emocionada, pero no está segura de que sea real. Se da cuenta de que la dirección de correo electrónico tiene un aspecto extraño y de que el enlace no coincide con el sitio web de la tienda.

El caso de Ana, debatamos

1. ¿Qué debe hacer Ana antes de hacer clic en el enlace?

2. ¿Cuál es la señal de advertencia de que este correo electrónico puede ser falso?

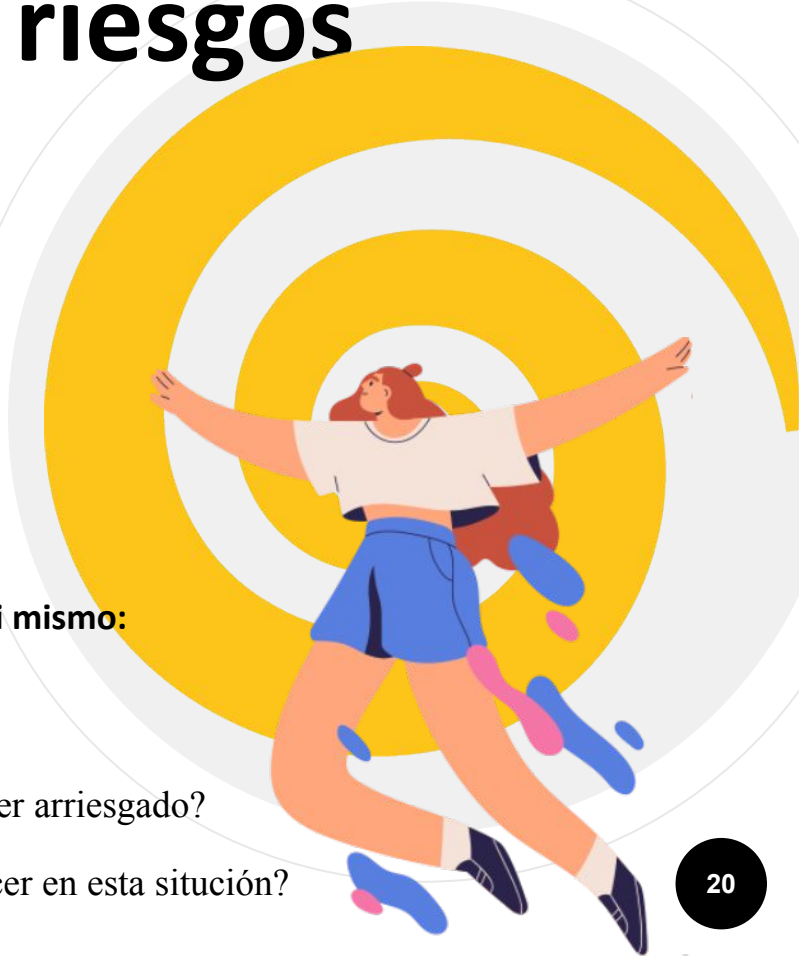
3. Si Ana cree que este correo electrónico es sospechoso, ¿qué debe hacer?



Actividad: Detectar riesgos

En esta actividad, verás imágenes o escucharás historias breves sobre cosas que pueden ocurrir en Internet. Tu trabajo consiste en:

- Decide si la situación es arriesgada o segura.
- Decir por qué crees que es arriesgada.
- Explica qué harías para mantenerte a salvo.



Ejemplo

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?

Detectar riesgos: situaciones

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: 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?».

PR.I.S.C.I.LLA
Preventing Incident of Sexual Cyberbullying in Intellectual disability

Co-funded by the European Union

Reflexiones and conclusiones

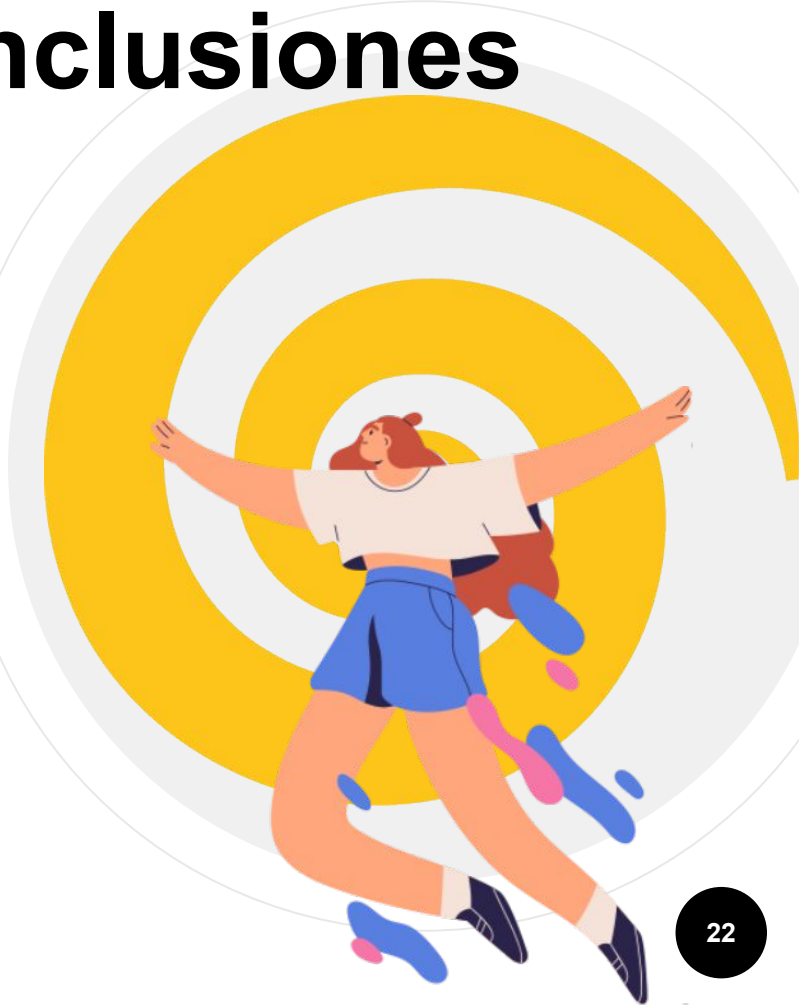
Después de terminar las escenas, tómate un tiempo para pensar en lo que has aprendido.

Pregúntate a ti mismo:

- ¿Qué riesgo te sorprendió más?
- ¿Cómo te sentiste al decidir qué hacer en cada situación?
- ¿Qué harías diferente la próxima vez que estés en línea?
- Comenta tus respuestas con el grupo o con tu profesor. Compartir tus ideas puede ayudarte a sentirte más seguro en Internet.

Recuerda

- Si algo te parece mal en Internet, confía en tus sentimientos.No compartas información personal ni contraseñas con desconocidos.Habla siempre con alguien de confianza si tienes dudas sobre una situación..



Juegos de rol

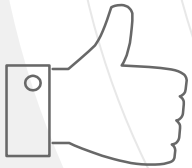
Practicarás cómo responder a diferentes riesgos online al representar situaciones en grupos pequeños. Esta actividad te ayudará a sentirte más seguro sobre qué hacer si enfrentas estos riesgos en la vida real.

Instrucciones

Trabajarán en pequeños grupos para representar diferentes situaciones. Cada grupo recibirá un escenario sobre un riesgo en línea. Una persona actuará como la persona que se enfrenta al problema, y los demás interpretarán distintos papeles, como el de un amigo, el de la persona que corre el riesgo o el de un adulto de confianza. Después de representar la situación, hablaremos de lo ocurrido y de cómo afrontarlo.

Situación 1

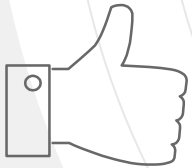
- Situación: Historia: Alguien en línea dice: "¡Tienes mucho talento! ¿Puedo ver más fotos tuyas? Prometo que no las compartiré con nadie".
- Roles:
- Persona a la que se le piden fotos.
- El extraño.
- Un adulto de confianza o un amigo con quien la persona habla para pedirle consejo.
- Pasos a seguir:



Negarse a enviar fotos.

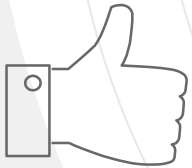
Bloquear al extraño. o Hablar con el adulto de confianza sobre lo que sucedió.

Situación 2



- Situación : 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:
- La persona que sufre el acoso.
- El acosador.
- Un adulto de confianza o un amigo con quien la persona habla.
- Pasos a seguir:
- No respondas a los comentarios malintencionados.
- Toma capturas de pantalla como prueba. Bloquea y denuncia al acosador.

Situación 3



- Situación : Recibes un correo electrónico que dice: “¡Felicitaciones! ¡Has ganado un teléfono nuevo! Haz clic en este enlace para reclamar tu premio”.
- Roles:
- La persona que recibe el correo electrónico.
- El estafador que envió este correo electrónico. Un amigo o un adulto de confianza que te da consejos.
- Pasos a seguir:
- No hagas clic en el enlace.
- Elimina el correo electrónico y denúncialo como spam.
- Habla con un adulto de confianza si no estás seguro.

Debate yConclusión

Debate

Después de haber representado el escenario, discutámoslo: :¿Qué hacía que la situación fuera arriesgada?

¿Qué hizo la persona para mantenerse a salvo?

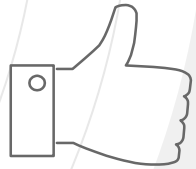
- ¿Qué sentiste al practicar esta situación?
- ¿Qué harías si esto te ocurriera en la vida real?
- :¿Qué hacía que la situación fuera arriesgada?

Conclusión

¡Has hecho un excelente trabajo practicando cómo manejar los riesgos en línea!

Recuerda

- Confía siempre en tus instintos: si algo te parece mal, probablemente lo sea.
- Bloquea y denuncia a quienes te hagan sentir incómodo.
- Habla con un adulto de confianza si no estás seguro de qué hacer.



Juego de clasificación de riesgos

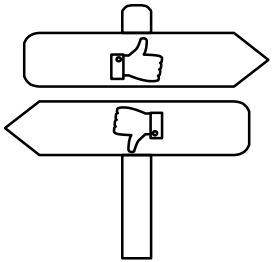
Practicarás la identificación de comportamientos en línea seguros y riesgosos clasificando los ejemplos en categorías "Seguro" o "arriesgado".

Trabajaremos en parejas o en pequeños grupos. Cada grupo recibirá tarjetas con ejemplos de acciones online. Su tarea consiste en colocar cada tarjeta en la categoría «Seguro» o «Riesgoso» en la pizarra o en la mesa.

Después de clasificar las tarjetas, discutiremos nuestras elecciones en grupo.

Juego de clasificación de riesgos

Ejemplo de tarjeta:
«Compartir tu nombre completo y dirección en tu perfil».¿Es seguro o arriesgado?
Respuesta: Arriesgado. Compartir información personal puede hacerte vulnerable.
Ahora te toca a ti.



Gracias

Co-funded by
the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.