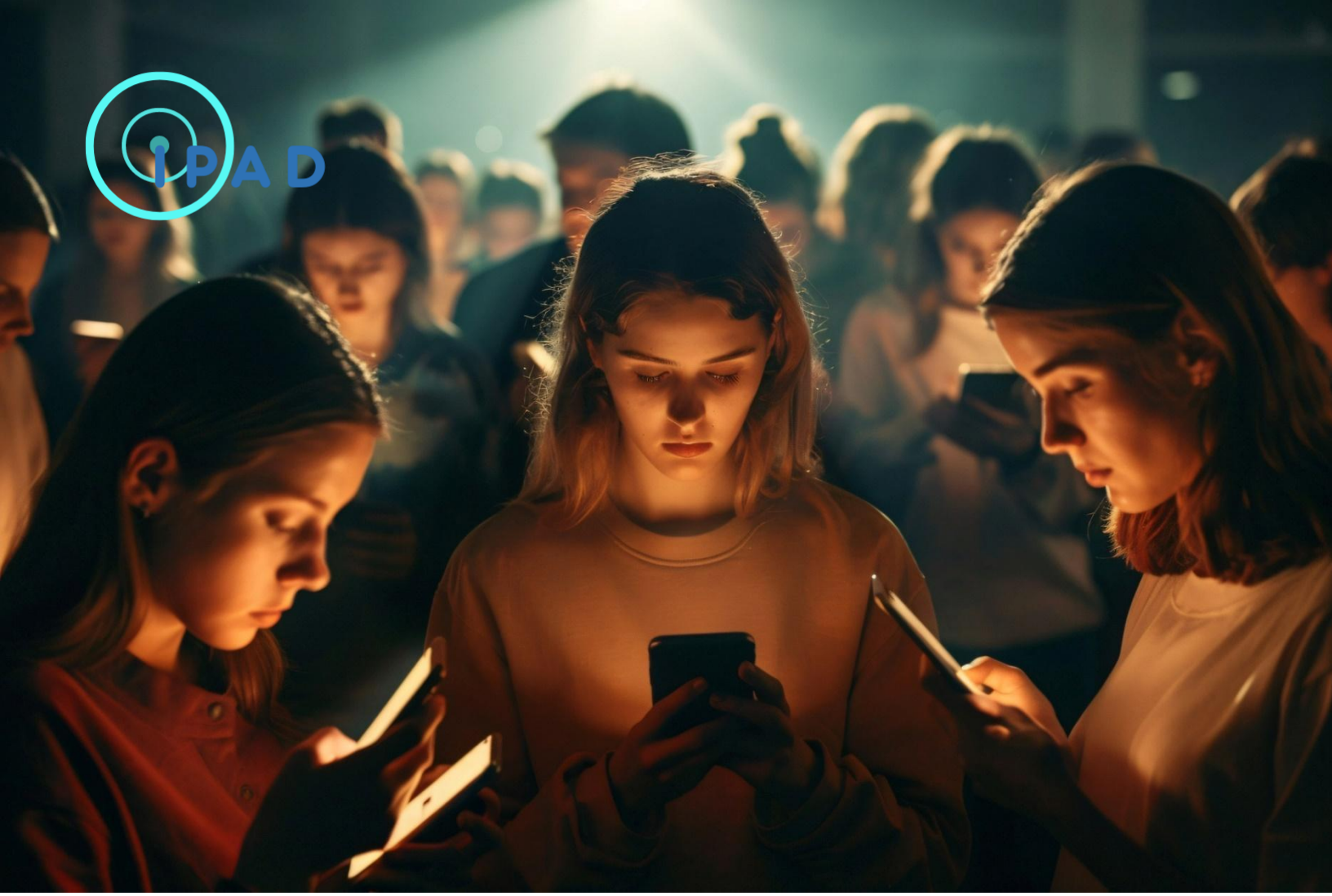

Guía de actividades prácticas y métodos de evaluación del proyecto IPAD.

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados son, sin embargo, exclusivamente los de los autores y no reflejan necesariamente los de la Unión Europea ni los de la Agencia Ejecutiva en el ámbito Educativo, Audiovisual y Cultural (EACEA). Ni la Unión Europea ni la EACEA se hacen responsables de ellos. Número de proyecto 2023-1-ES01-KA220-ADU-000152665

Cofinanciado por la Unión Europea

ÍNDICE

INTRODUCCIÓN

La Guía de actividades prácticas y herramientas de evaluación del IPAD se ha elaborado como un recurso integral para **los educadores de adultos que trabajan con familias** en el ámbito de **la educación digital, la alfabetización en redes sociales y la seguridad en Internet**. Este documento integra un conjunto de **actividades formativas innovadoras** diseñadas para mejorar las competencias digitales de los adultos, dotándoles de los conocimientos necesarios para navegar por el mundo online de forma segura y responsable.

Esta guía consolida **las actividades prácticas** y **las herramientas de evaluación** desarrolladas en colaboración por los socios del proyecto como parte del plan de estudios IPAD. Las actividades se estructuran en seis unidades clave, cada una de las cuales aborda un aspecto fundamental de **la alfabetización en redes sociales y la seguridad en Internet para las familias y sus hijos**. Estas unidades proporcionan a los educadores ejercicios listos para usar, metodologías atractivas y estrategias de evaluación para **evaluar el progreso del aprendizaje** y **adaptar los enfoques de enseñanza** en función de las necesidades de los participantes.

Estructura y uso

Cada unidad de esta guía está estructurada de la siguiente manera:

1. **Título**: nombre de la actividad práctica.
2. **Objetivos de aprendizaje**: Descripción de los objetivos vinculados a la unidad asignada y sus resultados de aprendizaje. Cada actividad incluye al menos dos objetivos de aprendizaje.
3. **Descripción detallada**: Instrucciones paso a paso sobre cómo llevar a cabo la actividad, incluyendo:
    - Duración
    - Preparación previa necesaria (por ejemplo, planificación)
    - Descripción del proceso (diferentes pasos o fases)
    - Recomendaciones metodológicas, si procede
4. **Recursos útiles**: Enlaces a información adicional, directrices pedagógicas, estudios de investigación, normativas y herramientas que apoyan la implementación de la actividad.
5. **Material necesario**: una lista de los recursos necesarios, como ordenadores, acceso a Internet, gráficos, aplicaciones u otros materiales. Se incluyen hojas de actividades, plantillas e imágenes cuando es necesario.
6. **Herramientas de evaluación**: estrategias para medir el impacto de la actividad en el progreso del aprendizaje de los participantes. Estas herramientas incluyen:
    - Evaluación cualitativa: preguntas estratégicas, observación de los participantes, pequeños debates, informes escritos, demostraciones y evaluaciones basadas en tareas.
    - Evaluación cuantitativa: preguntas de opción múltiple, ejercicios de emparejamiento, afirmaciones verdaderas/falsas, actividades para rellenar los espacios en blanco y listas de verificación.

Destinatarios

Esta guía está dirigida principalmente a **educadores, formadores y facilitadores de adultos** que trabajan con familias para **promover un uso seguro y responsable de las tecnologías digitales**. Sirve como un conjunto de herramientas prácticas para guiar los debates sobre **el pensamiento crítico, la ciberseguridad, la privacidad en línea, la netiqueta y la mediación parental**. Mediante el uso de estos materiales, los educadores pueden capacitar a los adultos para **que comprendan los riesgos digitales, apoyen las experiencias en línea de sus hijos y desarrollen una cultura de ciudadanía digital responsable**.

Cómo utilizar esta guía

Al integrar la **base de datos digital en línea, las bases teóricas y pedagógicas y el curso de aprendizaje en línea**, la **plataforma de materiales de aprendizaje abierto en línea IPAD** ofrece un **ecosistema completo de recursos educativos**. Los educadores pueden utilizar estas herramientas **de forma individual o combinada** para crear **experiencias de aprendizaje atractivas y eficaces** para adultos y familias.

Los educadores pueden implementar actividades prácticas, como ejercicios independientes, o integrarlas en **sesiones de formación estructuradas**. Las herramientas de evaluación proporcionadas pueden utilizarse para **realizar un seguimiento del progreso de los alumnos** y **adaptar las actividades** en función de sus niveles de alfabetización digital. Tanto si se utiliza en **entornos educativos formales como informales**, este documento ofrece un **enfoque** flexible y **eficaz para reforzar las habilidades digitales** de las familias.

UNIDAD 1.

MEJORAR LA ALFABETIZACIÓN EN REDES SOCIALES Y EL PENSAMIENTO CRÍTICO

1.1: El reto de la verificación de datos: detectar la desinformación

Objetivos de aprendizaje

- Aplicar estrategias de pensamiento crítico para evaluar la credibilidad y fiabilidad de las fuentes en línea.
- Identificar sesgos, información errónea y noticias falsas, y emplear estrategias de verificación.
- Desarrollar autonomía en el fomento de una actitud crítica hacia la información en línea.

Descripción detallada

DURACIÓN: 60 minutos

PREPARACIÓN:

1. Reúna una mezcla de artículos de noticias reales y falsos en línea, publicaciones en redes sociales y anuncios.
2. Prepare una hoja de trabajo para la verificación de datos que incluya preguntas clave sobre credibilidad, fuentes y sesgos.
3. Asegúrese de tener acceso a herramientas de verificación de datos (por ejemplo, Snopes, FactCheck.org, Google Reverse Image Search).

DESCRIPCIÓN DEL PROCESO:

PASO 1. Introducción (10 min):

- Explique brevemente la importancia del pensamiento crítico en la alfabetización digital.
- Presente las tácticas comunes de desinformación (clickbait, deepfakes, estadísticas engañosas).

PASO 2. Actividad en grupo (30 min):

- Divida a los participantes en pequeños grupos.
- Proporcione a cada grupo una mezcla de noticias **reales y falsas** de .
    - https://docs.google.com/document/d/1Xz2wC5Re3D5S3nT-rjxxn-IwKBaqWeoB/edit
- Pídales que analicen los artículos utilizando la **hoja de trabajo de verificación de datos**, verificando las fuentes, comprobando las URL y utilizando herramientas de verificación de datos.
    - https://docs.google.com/document/d/1LBF2j8UZZk1ANKBlUgOi-s4-syqgdb5N/edit
- Los grupos presentan sus conclusiones y justifican sus decisiones.

PASO 3. Debate y reflexión (20 min):

- Facilite un debate sobre los retos encontrados.
- Haga hincapié en la importancia de **verificar los datos antes de compartir** contenidos.

RECOMENDACIONES METODOLÓGICAS:

✓ Anime a los participantes a **justificar su razonamiento** en lugar de limitarse a hacer conjeturas.
✓ Utilice **ejemplos del mundo real** para que la actividad resulte atractiva.
✓ Promueva **la colaboración y el debate en equipo**.

Recursos útiles

- Snopes: sitio web de verificación de datos
- FactCheck.org: verificación de noticias políticas
- Búsqueda inversa de imágenes de Google: identificación de imágenes manipuladas

Material necesario

- Muestras de noticias impresas o digitales (Anexo I)
- Hoja de trabajo para la verificación de datos (Anexo II)
- Dispositivos conectados a Internet para la verificación

Herramientas de evaluación

(Todas las herramientas de evaluación a las que se hace referencia en este documento se recogen y desarrollan en el documento *Herramientas de evaluación IPAD*)

- Lista de verificación para la autoevaluación: los participantes evalúan su capacidad para identificar noticias falsas.
- Comentarios del debate en grupo: evaluar el razonamiento y la argumentación.
- Cuestionario de opción múltiple sobre indicadores de desinformación.

ANEXO I: EJEMPLOS DE NOTICIAS REALES Y FALSAS

NOTICIAS REALES

1. **La NASA confirma la presencia de agua en la Luna (2020)**

   📌 **Titular:** *La NASA confirma la presencia de agua en la superficie iluminada de la Luna*
   🔗 **Fuente:** NASA, revistas científicas

   📰 **Resumen:** En 2020, la NASA confirmó la presencia de moléculas de agua en la superficie iluminada por el sol de la Luna utilizando el telescopio SOFIA. Este descubrimiento tiene implicaciones para la futura exploración lunar.

   ✅ **¿Por qué es real?** Publicado por una organización científica creíble (la NASA), verificado por múltiples fuentes de prestigio y respaldado por investigaciones.

2. **La OMS declara la COVID-19 pandemia mundial (2020)**

   📌 **Titular:** *La Organización Mundial de la Salud declara la COVID-19 pandemia mundial*

   🔗 **Fuente:** Organización Mundial de la Salud (OMS), CDC, sitios web gubernamentales

   📰 **Resumen:** El 11 de marzo de 2020, la OMS declaró oficialmente la COVID-19 como pandemia debido a su rápida propagación mundial, instando a los países a implementar medidas de salud pública.

   ✅ **¿Por qué es real?** Informado por las principales organizaciones sanitarias y agencias de noticias, ampliamente cubierto con datos de apoyo de fuentes oficiales.

3. **El telescopio James Webb captura las primeras imágenes de galaxias lejanas (2022)**

   📌 **Titular:** *El telescopio espacial James Webb de la NASA envía las primeras imágenes impresionantes del universo*

   🔗 **Fuente:** NASA, BBC, National Geographic

   📰 **Resumen:** En julio de 2022, la NASA publicó las primeras imágenes a todo color del telescopio espacial James Webb, que revelan las vistas más profundas y detalladas del universo jamás vistas.

   ✅ **¿Por qué es real?** Verificado por la NASA y por investigaciones revisadas por pares, ampliamente cubierto por organizaciones de noticias fiables.

NOTICIAS FALSAS

1. **Bill Gates planea implantar microchips en las vacunas contra la COVID-19**

📌 **Titular:** *Bill Gates admite que las vacunas contra la COVID-19 implantarán microchips de rastreo en las personas*

🔗 **Fuente:** Publicaciones virales en redes sociales, blogs conspirativos

📰 **Resumen:** Una afirmación ampliamente difundida afirmaba que Bill Gates y la OMS planeaban utilizar las vacunas contra la COVID-19 para implantar microchips de rastreo en los seres humanos.

❌ **¿Por qué es falsa?**

- No hay pruebas científicas que respalden esta afirmación.
- Malinterpretación de la financiación de Gates para la investigación de vacunas.
- Rechazada por organizaciones sanitarias (OMS, CDC).
- Verificado por Snopes y Reuters.

2. **El 5G causa los síntomas de la COVID-19**

📌 **Titular:** *Un nuevo estudio demuestra que las redes 5G son la verdadera causa de la COVID-19*

🔗 **Fuente:** Sitios web marginales, afirmaciones virales en las redes sociales

📰 **Resumen:** Algunos teóricos de la conspiración afirmaron que la tecnología 5G, y no un virus, era la causa de los síntomas de la COVID-19.

❌ **¿Por qué es falso?**

- La COVID-19 está causada por el virus SARS-CoV-2, según han confirmado las organizaciones sanitarias mundiales.
- El 5G es una tecnología de comunicación inalámbrica que **no** tiene **ningún efecto biológico sobre el sistema inmunitario**.
- Verificado por la OMS, los CDC y científicos independientes.

3. **El Gobierno prohibirá el dinero en efectivo y obligará a todo el mundo a utilizar moneda digital**

📌 **Titular:** *El Gobierno de EE. UU. anuncia que el dinero en efectivo se prohibirá en 2025 y que todo el mundo deberá utilizar moneda digital*

🔗 **Fuente:** Sitios web sensacionalistas, blogs de desinformación

📰 **Resumen:** En publicaciones virales en las redes sociales se afirmaba falsamente que los gobiernos planeaban eliminar por completo el dinero en efectivo y obligar a todos los ciudadanos a utilizar únicamente transacciones digitales.

❌ **¿Por qué es falso?**

- Ninguna declaración oficial del Gobierno ni de las instituciones financieras respalda esta afirmación.
- Las economías siguen dependiendo del dinero físico.
- Verificado y desmentido por los reguladores financieros.

ANEXO II: EJEMPLO DE HOJA DE TRABAJO PARA LA VERIFICACIÓN DE DATOS

1. Información básica

- Título de la noticia: _____
-
- Fecha de publicación: _____
- Autor (si está disponible): _____

2. Evaluación de la fuente

✅ **Comprueba la credibilidad de la fuente.**

Pregunta	Sí	No	Notas/Justificación
¿La fuente es una organización conocida y de buena reputación (por ejemplo, BBC, Reuters, OMS, NASA)?	☐	☐	
¿La URL del sitio web parece legítima (por ejemplo, .gov, .edu, .org, sitios web de noticias importantes)?	☐	☐	
¿Puede encontrar la misma noticia publicada por varias fuentes fiables?	☐	☐	
¿El sitio web tiene una página clara «Acerca de nosotros» o de contacto?	☐	☐	

🔍 **Compruébelo utilizando sitios web de verificación de datos:**

- Snopes
- FactCheck.org
- Reuters Fact Check
- Búsqueda inversa de imágenes de Google

3. Análisis del contenido y el lenguaje

✅ **Analiza cómo está redactado el artículo.**

Pregunta	Sí	No	Notas/Justificación
¿El titular utiliza un lenguaje sensacionalista o cargado de emotividad?	☐	☐	

Pregunta	Sí	No	Notas/Justificación
¿Hay afirmaciones impactantes sin pruebas que las respalden?	☐	☐	
¿El artículo se basa en fuentes anónimas o carece de credenciales del autor?	☐	☐	
¿Se proporcionan estadísticas/datos? En caso afirmativo, ¿se citan de una fuente fiable?	☐	☐	
¿El artículo incluye imágenes manipuladas, gráficos engañosos o falsificaciones profundas?	☐	☐	

4. Proceso de verificación de datos

✅ **Utilizar estrategias de verificación para confirmar o desmentir la afirmación.**

Pregunta	Sí	No	Notas/Justificación
¿Realizó una búsqueda en Google para comprobar si había artículos similares de fuentes fiables?	☐	☐	
¿Utilizó la búsqueda inversa de imágenes de Google para verificar las imágenes?	☐	☐	
¿El artículo proporciona enlaces a fuentes fiables (estudios científicos, informes oficiales)?	☐	☐	

5. Veredicto final

Basándote en tu verificación de los hechos, ¿crees que esta noticia es:

☐ Real (creíble y verificada)
☐ Falsa (engañosa, carece de credibilidad)
☐ Poco clara (necesita más verificación)

📢 **Explica tu razonamiento:**

6. Preguntas para reflexionar

1. ¿Cuáles fueron los principales indicios que hicieron que la noticia pareciera falsa o creíble?

2. ¿Cómo ayudaron las herramientas de verificación de datos a comprobar la veracidad de la noticia?

3. ¿Por qué es importante verificar los hechos antes de compartir contenido en línea?

1.2 Análisis de contenido en redes sociales: contenido digital seguro frente a contenido digital perjudicial

Objetivos de aprendizaje

1. Diferenciar entre contenido digital educativo y perjudicial para menores.
2. Identificar las tácticas publicitarias y sus efectos en los niños y adolescentes.
3. Promover un comportamiento responsable en el intercambio de contenidos en los espacios en línea.

Descripción detallada

DURACIÓN: 60 minutos

PREPARACIÓN:

1. Recopilar capturas de pantalla de **contenidos de redes sociales** (publicaciones educativas, anuncios dirigidos a niños, contenidos nocivos o engañosos).

2. Prepare una **hoja de criterios de evaluación de** que cubra:

- **Idoneidad para la edad**
- **Fiabilidad de las fuentes**
- **Impacto emocional e intención**

3. Garantizar el acceso a **las plataformas de redes sociales** para realizar análisis en directo.

DESCRIPCIÓN DEL PROCESO:

PASO 1. Introducción (10 min):

- Explicar **cómo las redes sociales influyen en las percepciones y los comportamientos.**
- Analizar las técnicas publicitarias más comunes y su impacto en los jóvenes.

PASO 2. Análisis en grupo (30 min):

- Dividir a los participantes en pequeños grupos.
- Proporcione **diferentes ejemplos de redes sociales** (educativas, engañosas, publicidad dirigida, contenido violento o inapropiado).
- Los grupos utilizan la **hoja de criterios de evaluación** para evaluar la seguridad del contenido.
- Cada grupo presenta sus conclusiones y justifica sus calificaciones.

PASO 3. Debate y reflexión (20 min):

- Comparen perspectivas y debatan **por qué el contenido puede ser engañoso o perjudicial.**
- Elaborar **directrices para educadores y familias** sobre cómo identificar **contenidos digitales seguros.**

RECOMENDACIONES METODOLÓGICAS:

✓ Anime a los participantes a **considerar la manipulación emocional** en los anuncios publicitarios.
✓ Utilice **ejemplos de la vida real** para mejorar la participación.
✓ Facilite un **debate** abierto **sobre las cuestiones éticas** en la creación de contenidos digitales.

Recursos útiles

- Common Sense Media: evaluación de los contenidos digitales para niños
- MediaSmarts: recursos sobre alfabetización digital
- Ad Decoder: comprensión de las técnicas publicitarias

Material necesario

- Capturas de pantalla de diversos contenidos de redes sociales
- Hoja de criterios de evaluación
- Dispositivos conectados a Internet para la revisión de contenidos en directo

Herramientas de evaluación

(Disponible en el documento *Herramientas de evaluación IPAD*)

- Evaluación mediante lista de verificación: los participantes evalúan la idoneidad del contenido utilizando criterios establecidos.
- Debate basado en escenarios: los grupos debaten casos reales de contenido engañoso.
- Breve reflexión escrita: los participantes resumen las conclusiones clave sobre la alfabetización en redes sociales.

UNIDAD 2.

ESTABLECIMIENTO DE LOS FUNDAMENTOS DE LA CIBERSEGURIDAD Y LAS MEDIDAS DE SEGURIDAD EN INTERNET

2.1 Taller sobre aspectos esenciales de la ciberseguridad para educadores de adultos

Objetivos de aprendizaje

1. Comprender los conceptos fundamentales de la ciberseguridad y por qué son esenciales para la seguridad personal y familiar en línea.
2. Reconocer e identificar las amenazas cibernéticas comunes, como el phishing, el malware y el ransomware, y su posible impacto.
3. Aprender las mejores prácticas para un comportamiento seguro en línea, incluyendo la creación de contraseñas seguras y la detección de intentos de phishing.
4. Capacitar a los educadores para que orienten a los adultos en la adopción de prácticas seguras en línea y la protección de datos confidenciales.

Descripción detallada

DURACIÓN: 1 hora

PREPARACIÓN:

Prepare un conjunto de ejemplos de correos electrónicos de phishing, enlaces y archivos adjuntos sospechosos para la demostración.

Configure dispositivos con acceso a Internet y ejemplos de configuraciones de seguridad en plataformas como el correo electrónico y las redes sociales.

Proporcione guías sobre la gestión de contraseñas, la detección de phishing y la configuración de seguridad a los participantes.

DESCRIPCIÓN DEL PROCESO:

Paso 1: Introducción a las amenazas cibernéticas (15 minutos)

Comience con una descripción general de las amenazas cibernéticas comunes (por ejemplo, phishing, malware, ransomware, ingeniería social) y cómo afectan a las personas y las familias. Discuta la importancia de los conceptos básicos de la ciberseguridad, incluidos los conceptos de huellas digitales y comportamiento seguro en línea.

Paso 2: Reconocer el phishing y otras amenazas (20 minutos)

Muestre ejemplos de correos electrónicos y mensajes de phishing. Oriente a los participantes para que detecten señales de alerta comunes (por ejemplo, URL sospechosas, lenguaje urgente, solicitudes de

información personal). Utilice una prueba de phishing simulada para que los participantes practiquen la identificación de posibles amenazas en un entorno controlado.

Paso 3: Configuración de los ajustes de seguridad (25 minutos)

Guíe a los participantes a través de la configuración de medidas de seguridad básicas en sus dispositivos. Esto incluye:

- Ajustar la configuración de privacidad y seguridad en las cuentas de redes sociales.
- Demostrar la configuración de la autenticación de dos factores.
- Revisar la configuración del software antivirus y la protección del cortafuegos. Anime a los participantes a aplicar estos ajustes en sus propios dispositivos y a hacer preguntas sobre funciones de seguridad específicas.

Paso 4: Reflexión y preguntas y respuestas (15 minutos)

Facilite un debate sobre los retos comunes en materia de ciberseguridad a los que se enfrentan las familias y las personas. Pida a los participantes que compartan cómo piensan integrar estas prácticas de seguridad en sus rutinas diarias. Responda a las preguntas pendientes y ofrezca orientación sobre otros recursos de ciberseguridad.

RECOMENDACIONES METODOLÓGICAS:

- ✓ **Utilice simulaciones interactivas**: cree un entorno seguro para simular la detección de phishing y la configuración de la seguridad.
- ✓ **Simplifique las explicaciones técnicas**: evite la jerga utilizando ejemplos cotidianos para explicar los conceptos de ciberseguridad.
- ✓ **Fomente la aplicación práctica**: asegúrese de que los participantes puedan seguir el ejemplo en sus propios dispositivos para ganar confianza.

Recursos útiles

Guía para la detección del phishing: guía ilustrada para identificar los intentos de phishing. https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

Tutorial en vídeo sobre la autenticación de dos factores: un breve vídeo sobre cómo configurar la autenticación de dos factores en las redes sociales. *https://www.youtube.com/watch?v=9T66xFMsUxo*

Recursos familiares sobre seguridad en línea: un recurso de ConnectSafely que ofrece consejos sobre seguridad y privacidad digitales adaptados al uso familiar, que abarca temas que van desde la seguridad de las contraseñas hasta las prácticas de navegación segura. https://www.connectsafely.org/safety-tips-advice/

Material necesario

- Dispositivos con acceso a Internet (ordenadores portátiles o tabletas)
- Ejemplos de correos electrónicos y mensajes de phishing
- Guías impresas sobre prácticas básicas de ciberseguridad

Herramientas de evaluación

(Disponibles en el documento *Herramientas de evaluación IPAD*)

- Cuestionario de conocimientos sobre ciberseguridad: los participantes completaron un breve cuestionario para evaluar su comprensión de los conceptos clave de la ciberseguridad, incluida la identificación de intentos de phishing y la configuración de los ajustes de seguridad.
- Hoja de trabajo de reflexión sobre ciberseguridad: Los participantes reflexionaron sobre lo aprendido identificando dos amenazas cibernéticas, describiendo una configuración de seguridad que aplicaron y enumerando un nuevo hábito de ciberseguridad que planean adoptar.
- Encuesta sobre el taller y el nivel de confianza: Los participantes proporcionaron comentarios sobre el taller y valoraron su nivel de confianza a la hora de gestionar amenazas de ciberseguridad y orientar a otras personas.

2.2 Taller de juegos de rol sobre ciberseguridad

Objetivos de aprendizaje

1. Identificar y analizar las características clave de los intentos de phishing, el malware y otras amenazas en línea.
2. Demostrar medidas prácticas para mitigar los riesgos de ciberseguridad, como habilitar la autenticación de dos factores y actualizar la configuración de privacidad.
3. Aplicar el pensamiento crítico para resolver retos de ciberseguridad del mundo real mediante escenarios de juego de roles.
4. Dotar a los educadores de las habilidades necesarias para enseñar a las familias y comunidades a reconocer y responder a las amenazas en línea.

Descripción detallada

DURACIÓN: 90 minutos

PREPARACIÓN:

Prepare casos prácticos o escenarios que destaquen los retos comunes de ciberseguridad, como los correos electrónicos de phishing, las contraseñas débiles o el software obsoleto, e imprima materiales que detallen las mejores prácticas para la configuración de la seguridad y la creación de contraseñas; además, asegúrese de que haya dispositivos con acceso a Internet disponibles para las actividades prácticas.

DESCRIPCIÓN DEL PROCESO:

PASO 1: Introducción (15 minutos):

Ofrezca una breve charla sobre los fundamentos de la ciberseguridad, las amenazas cibernéticas comunes, como el phishing, el ransomware y la ingeniería social, así como las mejores prácticas para crear contraseñas seguras y proteger las cuentas en línea.

PASO 2: Escenarios de juego de roles (40 minutos):

Divida a los participantes en pequeños grupos y asigne a cada uno un escenario, como un correo electrónico sospechoso de un remitente desconocido, una ventana emergente con una advertencia sobre malware o una filtración de datos en una escuela o lugar de trabajo. Los grupos representarán el papel de formadores en ciberseguridad y decidirán cómo identificar, mitigar y explicar los riesgos que conlleva a un público no experto. Anime a los participantes a aplicar las herramientas y prácticas que han aprendido, como identificar elementos de phishing en un correo electrónico, demostrar cómo actualizar la configuración de seguridad o instalar software antivirus, y explicar la gestión de contraseñas mediante aplicaciones o técnicas como la autenticación de dos factores.

PASO 3: Intercambio y comentarios (20 minutos):

Cada grupo presenta su escenario y su solución al resto de participantes, mientras que el facilitador ofrece comentarios constructivos y resuelve cualquier duda.

PASO 4: Reflexión y resumen (15 minutos):

Dirija un debate sobre cómo los participantes pueden aplicar estas soluciones en la vida real, centrándose en la divulgación comunitaria y la orientación a las familias.

RECOMENDACIONES METODOLÓGICAS:

- ✓ Céntrese en **las aplicaciones prácticas** de los conocimientos y habilidades en materia de ciberseguridad para garantizar su relevancia en la vida cotidiana de los participantes.
- ✓ Utilice métodos **de aprendizaje activo** (por ejemplo, juegos de rol) para que el contenido resulte atractivo y memorable.

Incluya **situaciones con las que las familias puedan identificarse**, reflejando cómo los educadores de adultos enseñarán a otros.

Recursos útiles

Manténgase seguro en línea: consejos de seguridad en Internet https://www.staysafeonline.org/

Cyber Aware: conceptos básicos de ciberseguridad https://www.ncsc.gov.uk/cyberaware

FTC: evite las estafas y el fraude https://consumer.ftc.gov/

Material necesario

- Dispositivos con acceso a Internet (ordenadores portátiles o tabletas).
- Guías impresas o digitales sobre prácticas de ciberseguridad, incluyendo la gestión de contraseñas y la configuración de la privacidad.
- Pizarra blanca o rotafolio para debates y presentaciones en grupo.

Herramientas de evaluación

(Disponibles en el documento *Herramientas de evaluación del IPAD*)

Herramienta de evaluación 1: Cuestionario sobre conocimientos de ciberseguridad. Un cuestionario evaluó la capacidad de los participantes para reconocer los correos electrónicos de phishing, comprender la autenticación de dos factores e identificar las mejores prácticas en materia de ciberseguridad.

Herramienta de evaluación 2: Cuestionario sobre la aplicación de la ciberseguridad. Los participantes respondieron a preguntas para demostrar sus conocimientos sobre la aplicación de medidas prácticas de ciberseguridad, como la habilitación de la autenticación de dos factores y la gestión de la configuración de privacidad.

Herramienta de evaluación 3: Hoja de trabajo de reflexión sobre ciberseguridad. Los participantes documentaron sus ideas enumerando las prácticas de ciberseguridad que aprendieron, describiendo los retos a los que se enfrentaron y detallando cómo planean educar a otros.

2.3 Taller de identificación y prevención de amenazas cibernéticas

Objetivos de aprendizaje de

1. Comprender las características y el impacto de las amenazas cibernéticas comunes, como el phishing, el malware y el ransomware.
2. Desarrollar habilidades prácticas para identificar y responder a las amenazas cibernéticas en situaciones reales.
3. Capacitar a los educadores para que orienten a los adultos en la aplicación de medidas preventivas, como hábitos de navegación seguros y supervisión proactiva de las amenazas.
4. Fomentar la confianza en el uso de herramientas como el software antivirus y los cortafuegos para mejorar la seguridad.

Descripción detallada

DURACIÓN: 1 hora

PREPARACIÓN:

Para preparar esta actividad, el facilitador debe recopilar y preparar ejemplos de amenazas cibernéticas comunes, como correos electrónicos de phishing, páginas de inicio de sesión falsas y ventanas emergentes de malware. Estos ejemplos se pueden imprimir o mostrar digitalmente para su análisis. Además, cree una guía sobre cómo configurar cortafuegos y utilizar eficazmente el software antivirus. Asegúrese de que los dispositivos con acceso a Internet estén configurados con entornos de demostración simulados o seguros para que los participantes puedan practicar la configuración de los ajustes de seguridad. Por último, proporcione folletos que resuman las mejores prácticas para identificar y prevenir las amenazas cibernéticas.

DESCRIPCIÓN DEL PROCESO:

PASO 1: Introducción a las amenazas cibernéticas (15 minutos):

El facilitador comienza la sesión con una breve charla en la que presenta las amenazas cibernéticas más frecuentes, como el phishing, el malware, el ransomware y los ataques de ingeniería social. Cada tipo de amenaza se explica con ejemplos reales para ilustrar su posible impacto en las personas y las familias. El facilitador hace hincapié en la importancia de reconocer estas amenazas a tiempo y adoptar medidas preventivas para mantenerse seguro en Internet.

PASO 2: Actividad de identificación de amenazas (20 minutos):

Los participantes se dividen en parejas y se les proporcionan ejemplos simulados de amenazas cibernéticas, como un correo electrónico sospechoso, una página de inicio de sesión falsa o un anuncio emergente que afirma que el sistema está infectado. Cada pareja analiza el ejemplo que se le ha asignado, identifica el tipo de amenaza que representa y anota los indicadores clave que señalan que se trata de una amenaz . A continuación, los participantes debaten las medidas que tomarían para evitar ser víctimas de la amenaza y documentan sus conclusiones.

PASO 3: Exploración de herramientas preventivas (15 minutos):

El facilitador muestra cómo configurar cortafuegos y utilizar software antivirus para detectar y bloquear amenazas. Se proporcionan instrucciones paso a paso para habilitar estas herramientas en dispositivos y plataformas comunes. A continuación, los participantes practican la aplicación de estas medidas en dispositivos o cuentas de demostración, con la orientación del facilitador para garantizar la precisión.

PASO 4: Reflexión y resumen (10 minutos):

La sesión concluye con un debate en grupo para abordar conceptos erróneos comunes sobre las herramientas de ciberseguridad y su eficacia. Los participantes comparten sus ideas y reflexionan sobre cómo pueden utilizar estas habilidades para educar a los adultos y las familias de sus comunidades. El facilitador anima a los participantes a seguir practicando y compartiendo medidas preventivas para fomentar una cultura de seguridad en línea.

RECOMENDACIONES METODOLÓGICAS:

- ✓ Utilice ejemplos cotidianos y cercanos de amenazas cibernéticas para ayudar a los participantes a comprender sus implicaciones prácticas.
- ✓ Incorpore actividades colaborativas, como el trabajo en grupo, fomente la participación y el aprendizaje entre pares, al tiempo que se genera confianza mediante la práctica con herramientas de seguridad.
- ✓ Proporcione materiales de seguimiento para garantizar que los participantes puedan seguir aprendiendo y enseñar eficazmente estas habilidades a otras personas.

Recursos útiles

Dominar el análisis de correos electrónicos de phishing: respuesta a incidentes https://www.youtube.com/watch?v=EjY26pq9yME

Ciberseguridad 101: cómo protegerse en Internet **https://www.youtube.com/watch?v=MuVswL8UN_I**

Centro de seguridad de Google: cómo protegerse en Internet **https://safety.google/**

Material necesario

- Ejemplos de amenazas cibernéticas, como correos electrónicos de phishing o sitios web falsos (impresos o digitales).
- Dispositivos con conexión a Internet para practicar la configuración de antivirus y cortafuegos.
- Folletos o guías sobre el uso de herramientas de ciberseguridad y la identificación de amenazas.

Herramientas de evaluación

(Disponibles en el documento *Herramientas de evaluación IPAD*)

Herramienta de evaluación 1: Cuestionario sobre amenazas cibernéticas. Un breve cuestionario para evaluar la comprensión de los participantes sobre las amenazas cibernéticas, como el phishing, y su capacidad para reconocer las señales de alerta clave.

Herramienta de evaluación 2: Hoja de trabajo de respuesta a amenazas. Los participantes analizan una amenaza cibernética simulada, describen sus indicadores clave y esbozan los pasos que darían para evitar convertirse en víctimas.

Herramienta de evaluación 3: Encuesta de opinión sobre el taller. Una encuesta para recabar opiniones sobre la relevancia de la sesión y medir la confianza de los participantes a la hora de identificar y responder a las amenazas cibernéticas .

UNIDAD 3 .

COMPRENDER EL ENTORNO EN LÍNEA DE LOS MENORES

3.1 Navegar por el mundo digital: cómo las redes sociales moldean nuestras vidas

Objetivos de aprendizaje

1. Los participantes adquirirán conocimientos prácticos sobre las plataformas de redes sociales más populares entre los menores (por ejemplo, TikTok, YouTube, Instagram, Snapchat) y comprenderán sus características, ventajas y riesgos.
2. Los participantes desarrollarán habilidades para analizar de forma crítica los hábitos digitales de los jóvenes e identificar estrategias para ayudar a los menores a navegar por estas plataformas de forma segura.

Descripción detallada

DURACIÓN: 90 minutos

OBJETIVO: Esta actividad tiene como objetivo ayudar a los participantes a comprender las características clave, el atractivo y los riesgos potenciales de las «cuatro grandes» plataformas de redes sociales (YouTube, TikTok, Instagram y Snapchat) entre los menores. Al explorar estas plataformas, los participantes obtendrán información sobre cómo ayudar a los menores a utilizarlas de forma responsable y segura.

PREPARACIÓN PREVIA: Prepare una presentación o un folleto que resuma las estadísticas y características clave de las «cuatro grandes» plataformas (YouTube, TikTok, Instagram y Snapchat).

Asegúrese de tener acceso a ordenadores o teléfonos inteligentes con conexión a Internet.

Cree una hoja de trabajo para que los participantes la rellenen durante la actividad. Estos son algunos de los títulos que podría incluir en la hoja de trabajo:

- Características principales de la plataforma asignada.
- Riesgos y beneficios potenciales.
- Estrategias para un uso responsable.
- Preguntas para la reflexión.

DESCRIPCIÓN DEL PROCESO:

Introducción (10 minutos):

Presente brevemente la actividad y sus objetivos. Explique que el objetivo es explorar las «cuatro grandes» plataformas para comprender mejor su atractivo para los menores y los riesgos asociados.

Comparta las estadísticas clave del informe del Pew Research Center (por ejemplo, las tendencias de uso de las plataformas entre los menores).

- Porcentaje de menores que utilizan cada plataforma.
- Tendencias en el consumo de contenidos (por ejemplo, vídeos cortos, retransmisiones en directo).
- Preocupaciones comunes (por ejemplo, ciberacoso, tiempo de pantalla, privacidad de los datos).

Intente centrarse en reforzar la importancia de abordar el debate con empatía y evitando en la medida de lo posible el lenguaje crítico.

Debate en grupo (20 minutos):

Divida a los participantes en pequeños grupos y asigne a cada grupo una de las «cuatro grandes» plataformas.

Pida a los grupos que debatan:

- ¿Qué características hacen que esta plataforma sea atractiva para los menores? Algunos ejemplos podrían ser el algoritmo de la plataforma, los elementos interactivos o la comunidad.
- ¿Qué riesgos potenciales plantea esta plataforma? Algunos ejemplos podrían ser la exposición a contenidos inapropiados, problemas de privacidad o efectos negativos sobre la salud mental.
- ¿Cómo pueden los adultos ayudar a los menores a utilizar esta plataforma de forma responsable? Algunos ejemplos podrían ser establecer límites saludables y educar sobre la configuración de la privacidad.

Exploración de la plataforma (30 minutos):

Cada grupo explorará la plataforma que se le haya asignado (a través de teléfonos inteligentes u ordenadores).

Los participantes deben identificar:

- Tipos de contenido populares: ¿qué es tendencia actualmente? (por ejemplo, memes, vlogs, retos).
- Configuración de privacidad y funciones de seguridad: ¿cómo protege la plataforma a sus miembros? (por ejemplo, configuración de control parental, funciones de denuncia).
- Ejemplos de la cultura de los influencers y su impacto: ¿cómo influyen los influencers en los comportamientos y las tendencias de los usuarios?

Presentaciones en grupo (20 minutos):

Cada grupo presenta sus conclusiones al resto del grupo.

Destacar las conclusiones clave, como los riesgos, los beneficios y las estrategias para un uso seguro.

Resumen y reflexión (10 minutos):

Facilite el debate en grupo sobre cómo se pueden aplicar los conocimientos adquiridos en situaciones reales (por ejemplo, conversaciones con menores, establecimiento de límites). Algunas preguntas para iniciar el debate son:

- ¿Cómo pueden los adultos iniciar conversaciones con menores sobre el uso de las redes sociales?
- ¿Qué límites o pautas podrían ser útiles?
- ¿Cómo pueden los adultos mantenerse informados sobre las características y los riesgos cambiantes de las plataformas?
- Distribuya una hoja de reflexión para que los participantes anoten sus principales aprendizajes.

Recomendaciones metodológicas:

Anime a los participantes a abordar la actividad con una mente abierta y a evitar el lenguaje crítico.

Haga hincapié en la importancia de la empatía y la comprensión al hablar de los hábitos digitales de los menores.

Recursos útiles

Informe del Pew Research Center (2023): Adolescentes, redes sociales y tecnología 2023

Common Sense Education: Plan de estudios sobre ciudadanía digital

Be Internet Awesome de Google: Plataforma de aprendizaje interactivo

Material necesario

- Ordenadores o teléfonos inteligentes con acceso a Internet.
- Proyector o pantalla para presentaciones.
- Folletos que resuman las características y estadísticas de la plataforma.
- Hojas de trabajo para debates y reflexiones en grupo.

Herramientas de evaluación

(Disponibles en el documento *Herramientas de evaluación del IPAD*)

Cuestionario posterior a la actividad: se encuentra en el documento Herramientas de evaluación.

Facilite el cuestionario a sus alumnos y repase con ellos las respuestas correctas (que se encuentran al final del documento) al final. Aproveche esta oportunidad para inculcar aún más los principios y teorías fundamentales discutidos a lo largo de la actividad práctica, pidiendo a los participantes que expliquen por qué una respuesta en particular es la «correcta», demostrando así las lecciones que han aprendido.

3.2 Mantener la resiliencia en línea: cómo lidiar con el ciberacoso y el acoso

Objetivos de aprendizaje

1. Los participantes aprenderán a identificar los signos del ciberacoso y el acoso en línea y comprenderán su impacto psicológico en los menores.

2. Los participantes desarrollarán estrategias prácticas para responder y prevenir el ciberacoso, incluyendo técnicas de comunicación empática e intervención.

Descripción detallada

Duración: 120 minutos

Objetivo: Esta actividad tiene como objetivo dotar a los participantes de los conocimientos y habilidades necesarios para identificar, abordar y prevenir el ciberacoso. A través del análisis de casos prácticos, juegos de rol y debates en grupo, los participantes aprenderán a apoyar a los menores que sufren acoso en línea y a desarrollar su resiliencia en los espacios digitales.

Preparación previa:

- Prepare estudios de casos o escenarios que describan casos de ciberacoso. Algunos ejemplos podrían ser los siguientes:
    - Un menor acosado en chats grupales.
    - Un adolescente que recibe comentarios vergonzosos sobre su físico en las redes sociales.
    - Un niño que es excluido o ridiculizado en comunidades de juegos en línea.
- **Nota:** Dado que se trata de un tema muy delicado, asegúrese de mantener un equilibrio entre situaciones realistas y evitables, sin caer en ejemplos demasiado gráficos o provocadores.

A continuación se muestra un ejemplo de un caso práctico adecuado para esta actividad:

Escenario:

Alex, un chico de 14 años, ha estado recibiendo comentarios desagradables en sus publicaciones de Instagram. Algunos compañeros de clase han creado una cuenta falsa para burlarse de su aspecto, y los comentarios son cada vez más hirientes. Alex ha empezado a evitar las redes sociales y parece retraído en la escuela.

Preguntas para el debate:

- ¿Qué señales indican que Alex está siendo víctima de ciberacoso?
- ¿Cómo se puede sentir Alex y cómo puede un adulto validar estas emociones?

- ¿Qué medidas inmediatas se pueden tomar para abordar la situación?
- ¿Qué estrategias a largo plazo pueden ayudar a Alex a desarrollar resiliencia y sentirse más seguro en Internet?

Crear una lista de recursos para denunciar el ciberacoso. Algunos ejemplos podrían ser herramientas de denuncia específicas de cada plataforma (por ejemplo, la función de denuncia de acoso de Instagram), líneas de ayuda nacionales (por ejemplo, Childline, Cyberbullying Research Center) o servicios de apoyo escolares o comunitarios.

Desarrolle un guion de juego de roles para que los participantes practiquen estrategias de intervención. Incluya indicaciones para escuchar con empatía, validar emociones y resolver problemas de forma colaborativa.

Además, recursos como folletos informativos podrían ser especialmente valiosos en esta actividad. Considere la posibilidad de incluir un breve texto introductorio sobre el desarrollo de la resiliencia, que abarque temas como el fomento de la comunicación abierta, la enseñanza de la alfabetización digital y el pensamiento crítico, y la promoción de métodos de autocuidado y regulación emocional.

Descripción del proceso:

Introducción (15 minutos):

Defina el ciberacoso y el acoso en línea utilizando ejemplos del mundo real (por ejemplo, ejemplos de artículos de prensa).

Discuta el impacto psicológico en los menores (los ejemplos podrían incluir ansiedad, depresión y problemas de autoestima, aislamiento social, deterioro académico o efectos a largo plazo en la confianza y la seguridad), así como la importancia de la empatía para abordar estas cuestiones.

Análisis de casos prácticos (30 minutos):

Dividir a los participantes en pequeños grupos y proporcionar a cada grupo un estudio de caso. Animar a los alumnos a tomar notas sobre cualquier punto interesante que surja durante sus debates.

Pida a los grupos que analicen el escenario e identifiquen:

- Señales de ciberacoso. ¿Cómo pueden los adultos reconocer cuándo un menor está siendo víctima de ciberacoso? (por ejemplo, cambios en el comportamiento, renuencia a usar dispositivos).
- Posibles repercusiones emocionales en la víctima. ¿Qué puede estar sintiendo la víctima y cómo pueden los adultos validar estas emociones?
- Estrategias de respuesta inmediatas y a largo plazo. ¿Qué medidas inmediatas se pueden tomar (por ejemplo, documentar el abuso, bloquear al acosador)? ¿Qué estrategias a largo plazo pueden ayudar (por ejemplo, desarrollar la resiliencia, buscar apoyo profesional)?

Actividad de juego de roles (40 minutos):

Los grupos representarán una conversación entre un adulto y un menor que ha sufrido ciberacoso.

Céntrate en escuchar con empatía (reconocer los sentimientos del menor sin interrumpir ni minimizar su experiencia), validar las emociones (utilizando frases como «Siento mucho que te haya pasado esto» o «No es culpa tuya») y desarrollar de forma colaborativa un plan de acción (por ejemplo, denunciar el abuso, buscar el apoyo de un adulto de confianza).

Debate en grupo (20 minutos):

Los grupos comparten sus experiencias con el juego de roles y debaten qué ha funcionado bien y qué se podría mejorar. Las preguntas para fomentar el debate podrían incluir:

- ¿Qué estrategias funcionaron bien durante el juego de roles?
- ¿A qué retos se enfrentaron los participantes y cómo se pueden abordar?
- ¿Qué conclusiones clave se pueden aplicar a situaciones de la vida real?

Destacar las estrategias clave para responder al ciberacoso, como documentar el abuso y denunciarlo a las plataformas, y buscar el apoyo de adultos o profesionales de confianza.

Resumen y reflexión (15 minutos):

Distribuya un folleto con consejos para desarrollar la resiliencia en los menores.

Pida a los participantes que reflexionen sobre cómo pueden aplicar estas estrategias en sus propios contextos.

Anime a los alumnos a reflexionar sobre las siguientes preguntas:

- ¿Qué has aprendido sobre cómo abordar el ciberacoso?
- ¿Cómo abordará las conversaciones con los menores sobre el acoso en línea?
- ¿Qué medidas puedes tomar para crear un entorno digital más seguro para los menores?

RECOMENDACIONES METODOLÓGICAS:

- ✓ Haga hincapié en la importancia de crear un entorno seguro y sin prejuicios para que los menores compartan sus experiencias.
- ✓ Anima a los participantes a practicar la escucha activa y evita dar lecciones durante los juegos de rol.

Recursos útiles

StopBullying.gov: Recursos sobre ciberacoso

Common Sense Education: Kit de herramientas contra el ciberacoso

NSPCC (Reino Unido): Recursos sobre seguridad en línea

Material necesario

- Folletos con casos prácticos.
- Guiones para juegos de rol.
- Folletos con consejos para desarrollar la resiliencia.
- Acceso a ordenadores o teléfonos inteligentes para investigar herramientas de denuncia.

Herramientas de evaluación

(Disponibles en el documento *Herramientas de evaluación IPAD*)

Cuestionario posterior a la actividad: se encuentra en el documento Herramientas de evaluación.

Realice el cuestionario con sus alumnos y repase con ellos las respuestas correctas (que se encuentran al final del documento) al final de la actividad. Aproveche esta oportunidad para reforzar los principios y teorías fundamentales que se han tratado a lo largo de la actividad práctica, pidiendo a los participantes que expliquen por qué una respuesta concreta es la «correcta» y demuestren así lo que han aprendido.

3.3 Seguridad en línea para menores: uso inteligente y seguro de Internet

Objetivos de aprendizaje

1. Los participantes aprenderán a enseñar a los menores conceptos clave de alfabetización digital, como la privacidad en línea, la seguridad de los datos y el comportamiento ético.
2. Los participantes desarrollarán herramientas y actividades prácticas para mejorar las habilidades de alfabetización digital de los menores, como la creación de contraseñas seguras y el reconocimiento de intentos de phishing.

Descripción detallada

Duración: 90 minutos

Objetivo: Esta actividad tiene como objetivo mejorar la comprensión de los participantes sobre los conceptos de alfabetización digital y dotarles de herramientas prácticas para enseñar estas habilidades a los menores. A través de talleres interactivos y debates en grupo, los participantes aprenderán sobre los riesgos en línea, las mejores prácticas de ciberseguridad y las estrategias para desarrollar la alfabetización digital de los jóvenes.

Preparación previa: Prepare una presentación sobre los conceptos de alfabetización digital, incluyendo:

- Cifrado: cómo protege los datos y garantiza la privacidad.
- Cookies: su finalidad y cómo gestionarlas.
- Higiene cibernética: mejores prácticas para mantenerse seguro en línea (por ejemplo, actualizar el software, evitar enlaces sospechosos).

Elabore un folleto con consejos para mejorar la alfabetización digital. Algunos temas sugeridos que se pueden tratar son la creación de contraseñas seguras y únicas, el reconocimiento de los intentos de phishing y la gestión de la configuración de privacidad de las redes sociales.

Descripción del proceso:

Introducción (10 minutos):

Defina la alfabetización digital y su importancia en el entorno online moderno. Defina algunos de los ejemplos más comunes de riesgos online, como:

- Phishing: intentos fraudulentos de robar información personal.
- Violaciones de datos: acceso no autorizado a datos confidenciales.
- Malware: software diseñado para interrumpir o dañar dispositivos.

Taller interactivo (40 minutos):

Actividad 1: Comprobador de la seguridad de las contraseñas

- Los participantes crearán y probarán contraseñas utilizando una herramienta en línea.
- Se presentará la importancia de las contraseñas seguras y únicas, así como de la autenticación de dos factores (2FA). Algunos consejos para crear contraseñas seguras son:
    - Utilizar una combinación de letras, números y símbolos.
    - Evitar palabras o frases comunes.
    - Utilizar un gestor de contraseñas para almacenar y generar contraseñas.

Actividad 2: Detectives de correos electrónicos de phishing

- Presente a los participantes ejemplos de correos electrónicos de phishing y pídales que identifiquen las señales de alerta.
- Discuta las tácticas comunes utilizadas por los estafadores, tales como:
    - Lenguaje urgente o amenazante.
    - Direcciones de remitentes o enlaces sospechosos.
    - Solicitudes de información personal o financiera.
- Comparta estrategias para evitar los intentos de phishing, como verificar los datos del remitente y evitar hacer clic en enlaces desconocidos.

Debate en grupo (20 minutos):

Divida a los participantes en pequeños grupos y pídales que hagan una lluvia de ideas sobre cómo enseñar a los menores sobre la alfabetización digital. Las preguntas para guiar el debate podrían incluir:

- ¿Cómo podemos hacer que los conceptos de alfabetización digital resulten atractivos para los menores?
- ¿Qué actividades o herramientas pueden ayudar a los menores a comprender los riesgos en línea?
- ¿Cómo podemos animar a los menores a practicar una buena higiene cibernética?

Los grupos compartirán sus ideas con el grupo en general.

Resumen y reflexión (20 minutos):

Distribuya un folleto con consejos y recursos sobre alfabetización digital. Aquí tiene una plantilla de ejemplo que puede utilizar como inspiración:

Consejos de alfabetización digital

1. Cree contraseñas seguras:

- Utilice una combinación de letras mayúsculas y minúsculas, números y símbolos.
- Evite utilizar información personal (por ejemplo, fechas de nacimiento, nombres).
- Considere la posibilidad de utilizar una frase de contraseña (por ejemplo, «¡A mi perro le encanta jugar!»).

2. Reconozca los signos comunes del phishing:

- Comprueba que la dirección de correo electrónico del remitente no contenga inconsistencias.
- Busque errores ortográficos y gramaticales.
- Evite hacer clic en enlaces o descargar archivos adjuntos de fuentes desconocidas.

3. Practique una buena higiene cibernética:

- Actualice el software y los dispositivos con regularidad.
- Utilice software antivirus y active los cortafuegos.
- Ten cuidado al compartir información personal en línea.

4. Enseñe a los menores sobre alfabetización digital:

- Utilice actividades interactivas (por ejemplo, juegos, concursos) para que el aprendizaje sea divertido.
- Fomente conversaciones abiertas sobre los riesgos y la seguridad en Internet.
- Dé ejemplo de buenos hábitos digitales y comente sus propias experiencias.

Pida a los participantes que reflexionen sobre cómo pueden incorporar estos conceptos en su trabajo con menores, comprometiéndose a realizar un cambio positivo que puedan integrar en sus contextos profesionales en el futuro. Anime a los alumnos a reflexionar sobre preguntas como: ¿Qué ha aprendido sobre la alfabetización digital y la seguridad en Internet? ¿Cómo incorporará estos conceptos en su trabajo con menores? ¿A qué retos podría enfrentarse y cómo podría abordarlos?

Recomendaciones metodológicas:

Utilice ejemplos del mundo real para que los conceptos resulten cercanos y atractivos.

Anime a los participantes a pensar de forma creativa sobre cómo enseñar estos conceptos a los menores.

Recursos útiles

Be Internet Awesome de Google: plataforma de aprendizaje interactivo

Common Sense Education: Lecciones de alfabetización digital

Norton Security: consejos para la seguridad en línea

Material necesario

- Ordenadores o teléfonos inteligentes con acceso a Internet.
- Folletos sobre conceptos de alfabetización digital.
- Acceso a herramientas en línea (por ejemplo, verificador de la seguridad de contraseñas, cuestionario sobre phishing).

Herramientas de evaluación

(Disponibles en el documento *Herramientas de evaluación del IPAD*)

Cuestionario posterior a la actividad: se encuentra en el documento Herramientas de evaluación.

Facilite el cuestionario a sus alumnos y repase con ellos las respuestas correctas (que se encuentran al final del documento) al final. Aproveche esta oportunidad para inculcar aún más los principios y teorías fundamentales discutidos a lo largo de la actividad práctica, pidiendo a los participantes que expliquen por qué una respuesta en particular es la «correcta», demostrando así las lecciones que han aprendido.

UNIDAD 4 .

NAVEGACIÓN POR LA CONFIGURACIÓN DE PRIVACIDAD Y SEGURIDAD

4.1 Taller de sensibilización sobre la privacidad para familias

Objetivos de aprendizaje

1. Comprender el concepto de huellas digitales y cómo afectan a la reputación y la privacidad en línea.
2. Aprender medidas prácticas para configurar los ajustes de privacidad en las redes sociales y las plataformas digitales con el fin de proteger la información personal y familiar.
3. Identificar los posibles riesgos para la privacidad relacionados con el exceso de información compartida, especialmente en lo que respecta a los menores, y aprender estrategias para prevenir estos riesgos.
4. Desarrollar habilidades para orientar a las familias sobre cómo supervisar y gestionar sus propias huellas digitales para una presencia en línea más segura.

Descripción detallada

DURACIÓN: 1 hora

PREPARACIÓN:

Los educadores preparan los materiales, incluyendo perfiles de muestra para diversas plataformas de redes sociales (por ejemplo, Facebook, Instagram) y directrices sobre la configuración de la privacidad para diferentes dispositivos (teléfonos inteligentes, ordenadores, tabletas).

Configurar ordenadores o tabletas con acceso a Internet y cuentas de demostración de prueba para practicar el ajuste de la configuración de privacidad.

DESCRIPCIÓN DEL PROCESO:

PASO 1: Introducción (10 minutos):

Comience hablando sobre las huellas digitales y su importancia. Explique cómo las actividades en línea contribuyen a la identidad digital de una persona.

PASO 2: Demostración interactiva (20 minutos):

Guíe a los participantes a través de la configuración de los ajustes de privacidad en una o dos plataformas populares (por ejemplo, Facebook, Instagram).

Muestre cómo ajustar la configuración para controlar quién puede ver las publicaciones, la información personal y la ubicación.

PASO 3: Ejercicio de simulación (20 minutos):

Presente situaciones de la vida real en las que la configuración de privacidad evita posibles problemas, como el robo de identidad o el exceso de información compartida sobre menores.

Anime a los participantes a debatir y ajustar la configuración de privacidad para abordar cada escenario.

PASO 4: Reflexión y preguntas y respuestas (10 minutos):

Facilite un debate sobre cómo las familias pueden mantener juntas la privacidad y la seguridad digitales. Responda a cualquier pregunta y anime a los participantes a aplicar estos ajustes en casa.

RECOMENDACIONES METODOLÓGICAS:

- ✓ Involucre a los participantes: Comience con un debate abierto para **involucrar a los participantes** preguntándoles sobre su comprensión actual y sus preocupaciones con respecto a la configuración de privacidad.
- ✓ Utilice demostraciones visuales: asegúrese de que cada paso de la configuración de los ajustes de privacidad se muestre visualmente en la pantalla para que resulte claro y accesible, especialmente para aquellos menos familiarizados con las plataformas digitales.
- ✓ Práctica: Siempre que sea posible, anime a los participantes a seguir los pasos en sus propios dispositivos, aplicando la misma configuración que el facilitador. Esta aplicación inmediata ayuda a reforzar el aprendizaje.
- ✓ Desglose los conceptos: simplifique los términos técnicos y la configuración de privacidad proporcionando explicaciones claras y cotidianas. Relacione la configuración con situaciones de la vida real, como explicar que restringir quién ve un perfil es similar a controlar quién entra en la casa de uno.
- ✓ Fomente el debate y la reflexión: anime a debatir abiertamente y a reflexionar sobre riesgos específicos, como compartir información excesiva sobre menores. Explique los riesgos en términos prácticos, mostrando cómo incluso la información aparentemente inofensiva puede ser utilizada de forma indebida.
- ✓ Sensibilidad cultural y necesidades de privacidad: aborde las diferentes necesidades de privacidad de las personas y las familias, haciendo hincapié en que cada hogar puede necesitar adaptar la configuración de acuerdo con sus valores únicos y su nivel de comodidad con las redes sociales.

Recursos útiles

La guía definitiva sobre cómo gestionar la configuración de privacidad de las redes sociales https://www.socialpilot.co/blog/social-media-privacy-settings-guide

Vídeo de YouTube: «Cuatro razones para preocuparse por su huella digital» - https://youtu.be/Ro_LlRg8rGg?si=AaT_HPKvAhbY7_Wp

La guía definitiva sobre cómo gestionar la configuración de privacidad en las redes sociales https://www.socialpilot.co/blog/social-media-privacy-settings-guide

Vídeo de YouTube: «Cuatro razones para preocuparse por tu huella digital» - https://youtu.be/Ro_LlRg8rGg?si=AaT_HPKvAhbY7_Wp

Material necesario

- Ordenadores o tabletas con acceso a Internet
- Instrucciones impresas sobre la configuración de privacidad de Facebook e Instagram
- Rotafolio o pizarra blanca para debatir los puntos clave

Herramientas de evaluación

(Disponible en el documento *Herramientas de evaluación IPAD*)

- Encuesta de autoevaluación: Pida a los participantes que valoren su nivel de comodidad con la configuración de privacidad antes y después del taller.
- Debate sobre comentarios: Concluya con un breve debate en grupo sobre la confianza que sienten los participantes a la hora de implementar estos ajustes en casa.

4.2 Análisis de la huella digital

Objetivos de aprendizaje

1. Comprender el concepto de huella digital y cómo las actividades en línea dan forma a la identidad digital de una persona.
2. Aprender métodos para analizar la propia huella digital e identificar posibles riesgos para la privacidad.
3. Capacitar a las familias para evaluar y gestionar de forma crítica sus huellas digitales, promoviendo interacciones en línea más seguras.

Descripción detallada

DURACIÓN: 45 minutos

PREPARACIÓN:

Los educadores preparan hojas de trabajo impresas en las que se enumeran las actividades típicas en línea (por ejemplo, publicaciones en redes sociales, compras en línea, compartir la ubicación) y su posible impacto en las huellas digitales.

Asegúrese de que los participantes tengan acceso a Internet para buscar sus nombres en línea como parte de la actividad.

DESCRIPCIÓN DEL PROCESO:

PASO 1: Introducción (10 minutos):

Comience hablando sobre qué es una huella digital y cómo las acciones cotidianas en línea contribuyen a ella.

Explique el impacto duradero de las huellas digitales en la reputación, la privacidad e incluso las perspectivas laborales.

PASO 2: Ejercicio de autoanálisis (20 minutos):

Reparta las hojas de trabajo y pida a los participantes que hagan una lista de sus actividades recientes en Internet o de sus huellas digitales (por ejemplo, publicaciones en redes sociales, comentarios en foros).

Indique a los participantes que busquen sus propios nombres en los motores de búsqueda y en las redes sociales para observar qué información es visible públicamente.

Anime a los participantes a evaluar sus hallazgos e identificar cualquier información inesperada o potencialmente sensible.

PASO 3: Reflexión y debate en grupo (15 minutos):

Dirija un debate en grupo sobre lo que han descubierto los participantes, sus sentimientos respecto a su huella digital y cómo podrían cambiar su comportamiento en línea.

Proporcione consejos sobre cómo gestionar y reducir las huellas digitales, como comprobar la configuración de privacidad y eliminar contenidos antiguos.

PASO 4: Reflexión y preguntas y respuestas (10 minutos):

Facilite un debate sobre cómo las familias pueden mantener juntas la privacidad y la seguridad digitales. Responda a cualquier pregunta y anime a los participantes a aplicar estos ajustes en casa.

RECOMENDACIONES METODOLÓGICAS:

- ✓ Fomente la franqueza y el respeto: asegure a los participantes que se trata de una actividad sin juicios y que solo deben compartir las ideas que se sientan cómodos discutiendo.
- ✓ Utilice ejemplos de la vida real: proporcione ejemplos reales de cómo las huellas digitales han afectado positiva o negativamente a las personas.
- ✓ Facilite la reflexión: utilice preguntas orientativas como «¿Cómo afecta esta información a su privacidad?» y «¿Qué cambios, si los hubiera, haría en su comportamiento en línea?».

Recursos útiles

Lista de verificación de la huella digital
https://www.fcps.edu/sites/default/files/media/forms/DigitalFootprintTipSheet.pdf

Gestiona tu huella digital para mantenerte seguro en Internet https://youtu.be/OaHVOKM-NjA?si=XkURFHTwvxyUnxU9

Material necesario

- Hojas de trabajo impresas con ejemplos de actividades en línea
- Ordenadores o tabletas con acceso a Internet
- Rotafolio o pizarra blanca para compartir las ideas del grupo

Herramientas de evaluación

(Disponibles en el documento *Herramientas de evaluación del IPAD*)

- Preguntas de reflexión: Pida a los participantes que respondan a preguntas sobre sus sentimientos y opiniones acerca de su huella digital.
- Hoja de trabajo de autoevaluación: una lista de verificación en la que los participantes pueden evaluar sus prácticas actuales en materia de huella digital y establecer objetivos de mejora.

- Encuesta posterior a la actividad: recopile comentarios sobre la actividad para comprender su impacto en la conciencia digital de los participantes.

4.3 Juego de roles sobre la configuración de la privacidad

Objetivo de aprendizaje

1. Aprender sobre la configuración de privacidad en diferentes plataformas mediante la exploración práctica basada en escenarios.
2. Adquirir habilidades para configurar los ajustes de privacidad con el fin de gestionar la visibilidad en línea y proteger la información personal.
3. Capacitar a los educadores de adultos para que orienten a las familias en la creación y aplicación de ajustes de privacidad eficaces para diversas plataformas digitales.

Descripción detallada

DURACIÓN: 1 hora

PREPARACIÓN:

Configurar cuentas de demostración en plataformas como Facebook, Instagram y WhatsApp para simular diversos ajustes de privacidad.

Prepare tarjetas de roles con diferentes perfiles de usuario (por ejemplo, un padre que comparte fotos familiares, un adolescente que se conecta con sus amigos, un profesional que establece contactos).

DESCRIPCIÓN DEL PROCESO:

PASO 1: Introducción (10 minutos):

Comience presentando la importancia de utilizar la configuración de privacidad para controlar la presencia digital y los tipos de configuración de privacidad disponibles en las distintas plataformas.

Explique la actividad de juego de roles y cómo ayudará a los participantes a comprender la configuración de privacidad en contextos del mundo real.

PASO 2: Actividad de juego de roles (30 minutos):

Divida a los participantes en grupos y asigne a cada grupo un perfil de usuario (por ejemplo, un padre, un adulto joven, un profesional).

Proporcione a cada grupo un escenario en el que deban configurar los ajustes de privacidad en una de las cuentas de demostración (por ejemplo, un padre que decide qué fotos familiares compartir, un adolescente que controla quién ve sus publicaciones).

Después de configurar los ajustes, cada grupo comparte su enfoque y el razonamiento que ha seguido para elegir los ajustes de privacidad.

PASO 3: Resumen y reflexión (20 minutos):

Facilite un debate sobre las experiencias del juego de roles, abordando los retos que encontraron los participantes y las soluciones que encontraron.

Debata cómo se pueden adaptar estos ajustes de privacidad a familias con diferentes necesidades y preferencias.

RECOMENDACIONES METODOLÓGICAS:

- ✓ Utilice escenarios realistas: cree personajes y escenarios que reflejen los retos habituales en la gestión de la privacidad para que la actividad resulte más cercana.
- ✓ Fomente la colaboración: permita que cada grupo debata sus ajustes y enfoques, promoviendo el aprendizaje entre compañeros y la diversidad de perspectivas.
- ✓ Proporcione ejemplos contextuales: comparta ejemplos prácticos de cómo la configuración de privacidad puede evitar el exceso de información compartida o limitar la exposición de datos, especialmente con los niños.

Recursos útiles

Cómo cambiar la configuración de privacidad en Instagram https://youtu.be/9T66xFMsUxo?si=MfxKza72nNehUwG4

Material necesario

- Cuentas de demostración en Facebook, Instagram y WhatsApp
- Tarjetas impresas con perfiles de usuarios y escenarios
- Pizarra para debatir ideas. Rotafolio o pizarra para compartir ideas del grupo.

Herramientas de evaluación

(Disponible en el documento *Herramientas de evaluación IPAD*)

- Hoja de trabajo para el análisis de escenarios: una hoja de trabajo con preguntas para evaluar la comprensión y la aplicación de la configuración de privacidad por parte de cada grupo.
- Formulario de comentarios sobre el juego de roles: después de la actividad, los participantes completan un formulario en el que reflexionan sobre su enfoque y lo que han aprendido.
- Sesión de reflexión en grupo: Facilite una breve sesión de comentarios en la que cada grupo comparta lo que ha aprendido de los enfoques de los demás grupos.

UNIDAD 5 .

NETIQUETA: PROMOVER LA PARTICIPACIÓN EN LA SOCIEDAD Y EL EMPODERAMIENTO

5.1 Análisis de las interacciones en línea

Objetivos de aprendizaje

1. Definir la netiqueta e identificar sus principios básicos.
2. Analizar diversas interacciones en línea (correos electrónicos, publicaciones en redes sociales, debates en foros) para identificar ejemplos de netiqueta adecuada e inadecuada.
3. Comprender las responsabilidades éticas en las interacciones digitales, incluyendo el respeto a la privacidad, la propiedad intelectual y las normas comunitarias.
4. Reconocer los riesgos comunes en línea asociados con la falta de netiqueta (por ejemplo, trolling, flaming, ciberacoso).
5. Desarrollar y articular estrategias para responder a las interacciones negativas en línea de manera respetuosa y constructiva.

Descripción detallada

DURACIÓN: 2,5 h (se puede repartir en dos sesiones)

PREPARACIÓN:

El educador debe preparar una amplia gama de escenarios de interacción en línea (al menos dos por cada grupo de tres alumnos). Estos deben incluir diversas plataformas (correo electrónico, redes sociales, foros) y abarcar diferentes niveles de gravedad en lo que respecta a las infracciones de la netiqueta. Prepare escenarios que ilustren diversos dilemas éticos relacionados con la comunicación en línea. Considere la posibilidad de utilizar ejemplos reales anonimizados o ejemplos ficticios cuidadosamente elaborados. Asegúrese de que los escenarios sean diversos en cuanto a la representación de edades, géneros y antecedentes culturales.

DESCRIPCIÓN DEL PROCESO:

PASO 1: Introducción (30 minutos)

Comience con un breve repaso de los principios básicos de la netiqueta. Utilice métodos interactivos, como un breve cuestionario o una sesión de lluvia de ideas, para involucrar a los participantes. Discuta la importancia de la netiqueta en la creación de comunidades en línea positivas.

PASO 2: Análisis de escenarios (60 minutos)

Divida a los participantes en grupos de 3-4 personas. Cada grupo recibirá un conjunto de escenarios. Cada escenario debe analizarse centrándose en:

- Identificación del tipo de comunicación en línea (correo electrónico, publicación en redes sociales, etc.).
- Identificación de cualquier infracción de la netiqueta presente.

- Explicación de por qué estas acciones violan los principios de la netiqueta, haciendo referencia al material de formación.
- Identificación de las posibles consecuencias de las acciones descritas.

PASO 3: Presentaciones y debate en grupo (30 minutos):

Cada grupo presenta su análisis de uno o dos escenarios. A continuación, se celebra un debate en clase para comparar los análisis, explorar diversas perspectivas y destacar diferentes interpretaciones.

PASO 4: Desarrollo de estrategias de respuesta (30 minutos):

Centrarse en escenarios que muestren interacciones negativas en línea. Los participantes trabajan en sus grupos para pensar en respuestas adecuadas y constructivas. Hacer hincapié en estrategias de comunicación respetuosas y asertivas. Guiar a los participantes para que consideren lo siguiente:

- Empatía: comprender la perspectiva de la otra persona.
- Claridad: expresar los puntos de vista de forma clara y concisa.
- Respeto: mantener un tono respetuoso, incluso cuando no se está de acuerdo.
- Asertividad: expresar opiniones sin ser agresivo.
- Resolución de problemas: centrarse en encontrar una solución que satisfaga a ambas partes.

PASO 5: Resumen y reflexión (30 minutos):

Facilite un debate en grupo para consolidar el aprendizaje. Aborde cualquier pregunta o inquietud pendiente. Pida a los participantes que reflexionen sobre sus propios hábitos de comunicación en línea e identifiquen áreas de mejora.

Recursos útiles

Netiqueta para niños www.youtube.com/watch?v=v1QFaFimVSk&t=18s

¿Qué es la netiqueta? www.youtube.com/watch?v=CWbtbycHZok

Material necesario

- Escenarios preparados (impresos o mostrados digitalmente)
- Pizarras blancas o rotafolios
- Rotuladores
- Notas adhesivas
- Ordenadores con acceso a Internet (si se utilizan herramientas de colaboración en línea).

Herramientas de evaluación

(Disponibles en el documento *Herramientas de evaluación del IPAD*)

Rúbrica de análisis de escenarios: rúbrica que evalúa la exhaustividad y precisión de los análisis grupales.

5.2 Creación de una guía de etiqueta en Internet para familias

Objetivos de aprendizaje

1. Adquirir una comprensión global de los principios de la netiqueta y su aplicación en diferentes contextos en línea (redes sociales, correo electrónico, juegos en línea, etc.).
2. Comprender la importancia del comportamiento ético en línea para las familias.
3. Desarrollar una guía de netiqueta práctica y fácil de usar, adaptada a las familias.
4. Comunicar información compleja de forma clara y concisa, adecuada para diferentes grupos de edad y niveles de alfabetización digital.
5. Asumir la responsabilidad del contenido de la guía, garantizando su precisión y reflejando las diversas dinámicas familiares.

Descripción detallada

DURACIÓN: 4 horas (se puede repartir en dos sesiones)

PREPARACIÓN:

Ninguna, salvo la recopilación de recursos y ejemplos para apoyar la actividad (por ejemplo, enlaces a guías de netiqueta existentes, artículos sobre comunicación familiar).

DESCRIPCIÓN DEL PROCESO:

PASO 1: Introducción y lluvia de ideas (30 minutos):

Comience con un debate sobre la importancia de establecer directrices claras de etiqueta en la red dentro de las familias. Haga una lluvia de ideas sobre los aspectos clave que deben incluirse en la guía de etiqueta en la red para familias (por ejemplo, uso de las redes sociales, juegos en línea, comunicación responsable, privacidad, prevención del ciberacoso).

PASO 2: Trabajo en grupo y creación de contenidos (90 minutos):

Divida a los participantes en grupos más pequeños y asigne a cada grupo una sección específica de la guía. Las secciones posibles incluyen:

- Mejores prácticas en redes sociales.
- Etiqueta en el correo electrónico y la mensajería.
- Directrices para los juegos en línea.
- Protección de la privacidad en línea.
- Cómo lidiar con los conflictos en línea.
- Prevención y respuesta al ciberacoso.

PASO 3: Refinamiento de la estructura y el contenido de la guía (60 minutos):

Debatir la estructura y el formato de la guía de etiqueta en Internet, garantizando la coherencia y la facilidad de comprensión. Cada grupo presenta su trabajo al grupo completo para recibir comentarios y perfeccionarlo. Debatir el uso de elementos visuales, como iconos o ilustraciones, para mejorar la comprensión.

PASO 4: Finalización, revisión y edición (30 minutos):

Recopile todas las contribuciones de los grupos en un documento unificado, asegurando la claridad, la coherencia y la precisión. Revise y edite la guía para que sea legible e inclusiva. Tenga en cuenta los distintos grupos de edad y niveles de alfabetización digital dentro de las familias.

PASO 5: Presentación (30 minutos):

Los grupos pueden presentar sus secciones de la guía. Esto permite la revisión por pares y destaca diferentes perspectivas y enfoques.

Recursos útiles

13 principios de netiqueta para empoderar a su hijo https://saferkidsonline.eset.com/uk/article/13-netiquette-principles-to-empower-your-child

Creación de una guía de medios para su familia https://educateempowerkids.org/creating-media-guideline-family-3

Netiqueta para niños www.youtube.com/watch?v=v1QFaFimVSk

La crianza de los hijos en la era digital: estrategias de crianza positiva para diferentes situaciones https://edoc.coe.int/en/children-and-the-internet/8316-parenting-in-digital-age-positive-parenting-strategies-for-different-scenarios.html

¿Qué es la netiqueta? Normas de comportamiento en Internet para niños www.youtube.com/watch?v=VflASFth8cg

Material necesario

- Papel grande o pizarra blanca para la lluvia de ideas y rotuladores
- Notas adhesivas
- Ordenadores con software de procesamiento de textos (se recomienda Google Docs o plataformas colaborativas similares)
- Impresoras (opcional)

Herramientas de evaluación

(Disponibles en el documento *Herramientas de evaluación IPAD*)

Cuestionario de autorreflexión

UNIDAD 6 .

MEDIACIÓN PARENTAL PARA UN MANEJO REFLEXIVO

6.1 Minimizar los riesgos de los niños en Internet y evitar daños mediante estrategias de mediación activas y restrictivas

Objetivos de aprendizaje

1. Analizar los principales riesgos para los niños en Internet y ofrecer recomendaciones para evitar daños.
2. Describir la necesidad de que los adultos se impliquen activamente en una comunicación abierta con sus hijos sobre sus experiencias en línea.
3. Asumir la responsabilidad de educar y apoyar a los padres para proteger a los menores mientras navegan por Internet.
4. Elaborar estrategias que los padres puedan implementar para garantizar un uso responsable y seguro de Internet por parte de sus hijos.

Descripción detallada

DURACIÓN: 1 hora y 30 minutos

Preparación previa: Imprima el folleto y córtelo por la mitad para realizar una lectura en grupo. Haga suficientes copias para que cada padre tenga una copia de la sección A y otra de la sección B.

En esta actividad práctica, los educadores de adultos presentarán a los padres dos tipos diferentes de estrategias de mediación que pueden seguir para minimizar los riesgos en línea para sus hijos. En primer lugar, se explorarán los riesgos a los que se enfrentan los niños cuando están en línea.

PASOS:

1. Comience la sesión presentando a los padres algunas estadísticas sobre el uso de Internet por parte de los niños, por ejemplo: Según la Comisión Europea, los jóvenes pasan más tiempo en línea que los adultos, con un 69 % de los jóvenes de entre 9 y 22 años que pasan una media de 3 horas al día en línea, y según un informe de Cybersafekids, una organización benéfica irlandesa, el 42 % de los niños de entre 8 y 12 años y el 62 % de los de entre 12 y 14 años no hablan con sus padres sobre su actividad en línea. Pida a los padres que reflexionen sobre los riesgos potenciales del mundo digital para los niños. Proporcione a los padres una hoja grande de papel y bolígrafos, y pídales que, en pequeños grupos, hagan una lluvia de ideas sobre los riesgos y anoten sus ideas en forma de diagrama de araña.

2. Pida a cada grupo que comparta sus ideas y organice un debate con todo el grupo sobre los distintos riesgos sugeridos.

3. Explique que va a presentar a los padres dos tipos diferentes de estrategias de mediación que pueden aplicar para proteger a sus hijos de los peligros de Internet. La mitad del grupo leerá sobre la mediación

activa y la otra mitad leerá sobre la mediación restrictiva. A continuación, se emparejarán con un compañero del otro grupo y compartirán todo lo que han aprendido y escucharán a su compañero hablarles sobre la estrategia que han leído. Una vez que lo hayan hecho, deben debatir las siguientes preguntas : 1/ ¿Ya utilizan estos enfoques de mediación? 2/ Si es así, ¿cuáles utilizan y qué hacen? ¿Qué impacto tiene? 3/ Si aún no utilizan estas estrategias, ¿qué estrategia cree que funcionaría mejor con sus hijos? 3/ ¿Cuál no funcionaría tan bien con sus hijos? ¿Por qué?

4. Reúna al grupo para un debate en grupo. Compartan lo que creen que funciona bien o funcionará bien y debatan los resultados de la aplicación de estas estrategias.

5. Para concluir, entregue a los padres una copia de los dos textos utilizados en la actividad para que se los lleven a casa. Pida a los padres que prueben algo nuevo que hayan aprendido hoy con sus hijos y que reflexionen sobre los resultados.

Recursos útiles

Los educadores de adultos pueden consultar el curso de aprendizaje electrónico del IPAD, Unidad de aprendizaje 6: Mediación parental para el manejo reflexivo (lecciones 1 a 3) y obtener allí información sobre los riesgos en línea para los niños (para la parte introductoria de la actividad) y la mediación activa y restrictiva (para la parte principal de esta actividad). Utilice esta información para crear dos textos que expliquen las diferentes estrategias de mediación.

Material necesario

- Los educadores de adultos deben preparar un folleto para: A) Mediación activa y B) Mediación restrictiva. Deben hacer suficientes copias para que los participantes reciban una copia de ambos, pero inicialmente los participantes solo deben recibir A o B para participar en la actividad de lectura en rompecabezas.
- Los participantes necesitarán una cartulina grande (una por cada tres) y rotuladores.

Herramientas de evaluación

(Disponibles en el documento *Herramientas de evaluación IPAD*)

Mantenga una breve conversación con los participantes después de la actividad. Hágales las siguientes preguntas para evaluar la actividad:

1/ ¿Conocía todos los riesgos potenciales para los niños en Internet antes de esta actividad? Si no es así, ¿qué ha aprendido?

2/ ¿Las estrategias de mediación activa y restrictiva eran nuevas para usted? ¿Qué ha aprendido y qué va a poner en práctica en su vida cotidiana a partir de ahora, o qué va a seguir haciendo si ya empleaba diversas estrategias para proteger a sus hijos de los peligros de Internet?

3/ ¿En qué medida ha sido eficaz esta actividad para enseñarle los riesgos potenciales de Internet para los niños y cómo proteger a sus hijos de cualquier daño?

6.2 Apoyar el uso seguro y responsable de la tecnología.

Objetivos de aprendizaje

1. Identificar los principales beneficios de los recursos y actividades en línea para el desarrollo de los niños.
2. Describir la necesidad de que los adultos se involucren activamente en una comunicación abierta con sus hijos sobre sus experiencias en línea.
3. Proporcionar recomendaciones sobre cómo responder a posibles conflictos.

Descripción detallada

Esta actividad debe ser impartida a los padres por educadores de adultos.

DURACIÓN: aproximadamente 1 hora y 30 minutos.

PASOS:

1. Repase los riesgos a los que están expuestos los niños en Internet. Haga un seguimiento de la tarea establecida en la actividad anterior, si procede. Pregunte a los padres cómo les ha ido con la implementación de estrategias de mediación activas y/o restrictivas. ¿Qué resultados han obtenido? Compartan experiencias.

2. Explique que esta actividad explorará los beneficios de estar en línea: aprendizaje en línea, aprendizaje de idiomas, juegos de matemáticas, comunicación, juegos, etc. Asigne a cada pequeño grupo/pareja de participantes una categoría, por ejemplo, aprendizaje de idiomas, o una de su elección. Cada grupo debe investigar las mejores aplicaciones y recursos en línea para ello y tomar notas. Después, todos presentarán sus conclusiones, lo que dará lugar a un debate con todo el grupo sobre recursos, aplicaciones, sitios web y consejos recomendados para mantenerse a salvo durante este tiempo (por ejemplo, restrictivo: desactivar la función de chat en los juegos en línea, para que nadie pueda ponerse en contacto con su hijo, y activo: la importancia de la comunicación abierta: debatir por qué no deben añadir como amigos a personas que no conocen y sugerir amablemente a su hijo que comente con usted las solicitudes de amistad que reciba, si las hay).

3. Destaque la importancia de la comunicación abierta: un estudio reveló que, si bien la mediación restrictiva puede reducir el tiempo que se pasa en línea y disminuir el riesgo potencial, es más probable que genere conflictos entre padres e hijos. Por lo tanto, para evitar conflictos, especialmente con los hijos mayores, la clave para tener una relación buena, abierta y honesta con su hijo es mantener conversaciones abiertas y sinceras con él de forma regular. Pida a los padres que reflexionen sobre lo siguiente: 1/ ¿Sé siempre lo que mi hijo ve, escucha o lee en Internet? 2/ ¿Hablo abiertamente con mi(s) hijo(s) sobre su uso de Internet? 3/ ¿Hablamos sobre lo que ve/lee/escucha? 4/ ¿Hablamos de ello con regularidad, cada vez? 5/ ¿Alguna vez su hijo se ha sentido molesto por algo en Internet? ¿Cómo

respondió usted? 6/ ¿Ha hablado con él sobre los riesgos y peligros de Internet y sobre cómo protegerse de ellos?

4. Concluya con un debate en grupo sobre las conclusiones clave de la sesión de hoy, en relación con los beneficios y los recursos recomendados, y cómo evitar conflictos: la importancia de una comunicación regular, abierta y honesta.

Recursos útiles

Véase la Unidad de aprendizaje 6: Mediación parental para un manejo reflexivo.

Material necesario

Los participantes necesitarán:

- acceso a Internet, a través de sus teléfonos o computadoras portátiles.
- papel y bolígrafos para tomar notas
- Las preguntas de autorreflexión pueden imprimirse en un folleto o escribirse en una pizarra blanca.

Herramientas de evaluación

(Disponibles en el documento *Herramientas de evaluación del IPAD*)

La evaluación consistirá en una autoevaluación de los participantes sobre la actividad.

1. He aprendido algunos recursos y herramientas útiles en línea que pienso mostrar a mis hijos para fomentar su desarrollo cuando están conectados.
2. Hablaré con mi hijo/a sobre sus actividades en línea de forma regular.
3. Supervisaré sus actividades y fomentaré un diálogo abierto y sincero.
4. Daré ejemplo y reduciré mi propio tiempo en línea/mirando mi teléfono.

Colaboración

Portada y contraportada
Imagen de freepik

Recursos innovadores de concienciación digital para padres sobre alfabetización en redes sociales y seguridad en Internet