



Cofinanciado por
la Unión Europea

MÓDULO 09

ALFABETIZACIÓN MEDIÁTICA Y SEGURIDAD EN LÍNEA

DIGITAL RURAL EUROPEAN ART
AND MEMORY



Socios del proyecto



Project DREAM
Digital Rural European Art and Memory
2025-1-SK01-KA210-ADU-000360122



Cofinanciado por
la Unión Europea

Información del proyecto:

DREAM - Digital Rural European Art and Memory
2025-1-SK01-KA210-ADU-000360122

Financiado por la Unión Europea. Sin embargo, las opiniones y posturas expresadas son responsabilidad exclusiva del/de los autor/es y no reflejan necesariamente las de la Unión Europea ni las de SAAIC. Ni la Unión Europea ni la entidad financiadora se hacen responsables de ellas.



Cómo usar este libro electrónico

Puedes leer este material antes, durante o después de la sesión. Cada sección presenta un concepto y lo relaciona con una actividad práctica. Las actividades están diseñadas para personas adultas principiantes. No requieren conocimientos técnicos avanzados. El objetivo es desarrollar buenos hábitos: detenerse antes de compartir, comprobar las fuentes, proteger las cuentas, revisar la privacidad y pedir ayuda cuando sea necesario.

El módulo también incluye una sección de Aprender jugando. No se trata de un apéndice, sino de una parte práctica del módulo en la que los participantes aplican la teoría mediante breves retos de toma de decisiones inspirados en cuestionarios reales sobre alfabetización mediática y ciberseguridad.

Al final del módulo, los participantes completan una actividad integrada: analizan un contenido en línea, comprueban su fiabilidad y preparan un breve plan de seguridad en línea.



Sagrada Família, España

INFORMACIÓN DEL MÓDULO

 Número de módulo 09	 Nivel Principiante
 Tema Seguridad en línea y alfabetización mediática	 Formato Aprendizaje híbrido
 Duración 3 horas	 Salida principal Plan de seguridad en línea

Acerca de este módulo

Este libro electrónico acompaña al Módulo 9 de DREAM, dedicado a la alfabetización mediática y la seguridad en línea. Su objetivo es ayudar a los participantes a utilizar los medios digitales con mayor conciencia, protegerse en línea y tomar mejores decisiones al leer, compartir o publicar información.

La alfabetización mediática no consiste únicamente en detectar noticias falsas. Incluye comprender quién creó un mensaje, por qué se creó, cómo llega hasta nosotros, qué evidencias lo respaldan, qué emociones activa y qué riesgos pueden surgir cuando lo compartimos. La seguridad en línea está relacionada con todo ello. Una persona capaz de evaluar la información también necesita proteger sus cuentas, reconocer estafas, gestionar su privacidad, responder ante comportamientos dañinos y saber dónde pedir ayuda.

En el contexto de DREAM, este módulo favorece la participación digital, el trabajo relacionado con el patrimonio cultural y los proyectos comunitarios. Los participantes pueden utilizar plataformas en línea para compartir historias locales, imágenes, vídeos, modelos o recursos educativos. Deben hacerlo de forma crítica, segura y respetuosa.



Objetivos de aprendizaje

- Comprender qué significan la alfabetización mediática y la seguridad en línea en la vida digital cotidiana.
- Distinguir entre hechos, opiniones, interpretaciones, publicidad y manipulación.
- Evaluar fuentes en línea mediante comprobaciones básicas de credibilidad.
- Reconocer la desinformación involuntaria, la desinformación deliberada, el contenido clickbait y la manipulación emocional.
- Comprender cómo los algoritmos, los influencers y las plataformas sociales pueden influir en lo que ven las personas.
- Aplicar hábitos básicos de verificación de hechos antes de compartir información.
- Proteger las cuentas mediante contraseñas seguras, gestores de contraseñas y autenticación multifactor.
- Reconocer riesgos habituales en línea, como el phishing, el smishing, las tiendas falsas, la suplantación de identidad y las estafas.
- Utilizar recursos como INCIBE y Have I Been Pwned para mejorar la seguridad en línea.
- Practicar la alfabetización mediática y la seguridad en línea mediante retos gamificados con situaciones, elecciones, retroalimentación y reflexión.
- Preparar una lista de comprobación sencilla sobre seguridad en línea a nivel personal o de proyecto.

Índice

1. ¿Qué es la alfabetización mediática?	3
2. Por qué es importante la alfabetización mediática para DREAM	5
3. Hechos, opiniones, interpretaciones y publicidad.....	7
4. Cómo nos llega la información en línea	9
5. Desinformación, información errónea y manipulación	11
6. Hábitos de evaluación de fuentes y verificación de datos	12
7. Imágenes, vídeos y contenido generado por IA.....	14
8. Privacidad, huella digital y datos personales	16
9. Conceptos básicos de seguridad en línea: cuentas, contraseñas y dispositivos	18
10. Recomendaciones del INCIBE y recursos de ayuda de confianza	20
11. «Have I Been Pwned» y comprobaciones de fugas de datos.....	21
12. Seguridad de los archivos compartidos: Telegram, descargas directas y archivos comprimidos	23
13. Estafas en línea, phishing e ingeniería social.....	26
14. Ciberacoso, discurso de odio y participación respetuosa.....	28
15. Publicaciones seguras para proyectos comunitarios y patrimoniales	30
16. Aprender jugando: retos de alfabetización mediática y ciberseguridad	32
17. Actividad final	34
18. Consejo sobre bienestar digital	36
19. Glosario básico.....	37
20. Cierre del módulo	38
Bibliografía	39

1. ¿Qué es la alfabetización mediática?

La alfabetización mediática es la capacidad de acceder, comprender, evaluar, crear y compartir mensajes mediáticos de forma responsable. Se aplica a noticias, publicaciones en redes sociales, vídeos, imágenes, podcasts, resultados de búsqueda, publicidad, sitios web y contenidos generados por IA. Una persona con alfabetización mediática no se cree todo de inmediato, pero tampoco lo rechaza todo automáticamente. La clave está en plantear mejores preguntas: ¿quién lo ha creado?, ¿qué pruebas se aportan?, ¿qué falta?, ¿a quién beneficia? y ¿qué debería comprobar antes de compartirlo?

La alfabetización mediática también implica comprender que los mensajes mediáticos están contruidos. Un titular, una fotografía, la elección musical, el estilo de edición o una miniatura pueden influir en lo que pensamos sobre un tema antes incluso de leer los detalles.



Conceptos clave

Alfabetización mediática: la capacidad de acceder, comprender, evaluar, crear y compartir contenidos mediáticos de forma crítica y responsable.

Fuente: la persona, organización, publicación, sitio web u otro origen del que procede la información o el contenido mediático.

Mensaje: la idea principal, la información o la impresión que una pieza de contenido mediático comunica a su audiencia.

Evidencia: información utilizada para respaldar una afirmación o declaración, como hechos, datos, documentos, fotografías, conocimientos de expertos u otro material verificable.

Audiencia: las personas a las que un mensaje mediático pretende llegar o a las que probablemente llegue.

Propósito: la razón por la que se creó un mensaje mediático, por ejemplo, para informar, explicar, persuadir, entretener, promocionar algo o animar a las personas a actuar.



Tarea práctica

Elige una publicación en línea y responde:

- ¿quién la creó?
- ¿qué intenta hacerte pensar o hacer?
- ¿qué evidencias aporta?

Pequeño consejo: No te limites a preguntarte si un mensaje es cierto; pregúntate cómo intenta influir en ti.

2. Por qué es importante la alfabetización mediática para DREAM

Los alumnos de DREAM pueden utilizar herramientas digitales para documentar el patrimonio local, publicar los resultados de los proyectos, compartir materiales de formación o participar en comunidades en línea. Estas actividades requieren confianza y responsabilidad. Cuando un proyecto comunitario publica contenido en línea, este pasa a formar parte del entorno informativo. Un crédito de imagen erróneo, una afirmación exagerada, una estadística engañosa o una publicación insegura pueden dañar la credibilidad.

La alfabetización mediática ayuda a los alumnos a convertirse en mejores participantes, no solo en mejores consumidores. Aprenden a buscar, comparar, interpretar, crear y compartir con cuidado.

En el ámbito de la cultura y el patrimonio, la alfabetización mediática también protege el contexto. Una historia, un objeto o una imagen no deben separarse de su significado ni utilizarse de forma que confundan al público.



Conceptos clave

Participación digital: Participar en espacios digitales aportando información, ideas, conocimientos o contenidos, en lugar de limitarse a recibir información.

Memoria comunitaria: Las historias, fotografías, experiencias, tradiciones y conocimientos a través de los cuales una comunidad recuerda y comprende su pasado.

Credibilidad: El grado en que una información o un contenido puede considerarse fiable. La credibilidad se refuerza mediante la precisión, el uso de fuentes fiables, una atribución correcta y la transparencia sobre posibles incertidumbres.

Contexto: La información de fondo necesaria para comprender algo correctamente, como quién lo creó, de dónde y de cuándo procede, qué representa y por qué es importante.

Publicación responsable: Comprobar el contenido antes de compartirlo y tener en cuenta la precisión, las fuentes, los permisos, la privacidad, la atribución y los posibles efectos sobre las personas o la comunidad implicadas.



Tarea práctica

Enumera tres tipos de contenido que un proyecto DREAM podría publicar en línea y un riesgo para cada uno.

Pequeño consejo: un buen proyecto digital no solo es visible, sino que también inspira confianza.

3. Hechos, opiniones, interpretaciones y publicidad

Un hecho puede contrastarse con pruebas. Una opinión expresa un punto de vista. Una interpretación explica lo que algo puede significar. La publicidad intenta persuadir a la gente para que compre, haga clic, se suscriba o apoye algo. Los contenidos en línea suelen mezclar estas categorías. Un vídeo puede incluir hechos, opiniones personales, productos patrocinados y narraciones emotivas. Una publicación en redes sociales puede parecer información, pero en realidad funciona como promoción. Los alumnos deben practicar cómo separar la afirmación de la emoción. Si un mensaje dice que algo es impactante, urgente u obvio, el lector debe preguntarse de todos modos qué pruebas lo respaldan.



Conceptos clave

Hecho: Una afirmación que puede comprobarse y respaldarse con evidencias fiables.

Opinión: Un punto de vista, creencia o juicio personal. Una opinión puede basarse en hechos, pero no puede demostrarse del mismo modo que una afirmación factual.

Interpretación: Una explicación de lo que puede significar una información, un acontecimiento, una imagen o una fuente. Distintas personas pueden interpretar el mismo material de manera diferente, por lo que el razonamiento y las evidencias que sustentan una interpretación deben quedar claros.

Publicidad: Contenido creado para promocionar un producto, servicio, organización o actividad y animar a las personas a realizar una acción concreta, como comprar, visitar o registrarse.

Contenido patrocinado: Contenido que ha sido pagado o apoyado de otro modo por una empresa u organización. Debe identificarse claramente para que la audiencia pueda distinguirlo del contenido editorial o informativo independiente.

Evidencia: Información utilizada para respaldar o verificar una afirmación, como un documento oficial, una fotografía, un conjunto de datos, un registro, una fuente experta u otro material fiable.



Tarea práctica

Clasifica tres frases de un artículo en línea como hecho, opinión, interpretación o publicidad.

Pequeño consejo: Antes de reaccionar, identifica qué tipo de mensaje estás leyendo.

4. Cómo nos llega la información en línea

La gente no ve la información en línea de forma aleatoria. Los motores de búsqueda, las redes sociales, las plataformas de vídeo y los sistemas de recomendación deciden qué aparece primero, qué se repite y qué parece popular. **Los algoritmos** pueden ser útiles porque ayudan a filtrar enormes cantidades de contenido. Pero también pueden crear hábitos de información limitados, repetir puntos de vista similares y premiar el contenido emocional o extremo.

Los influencers, las comunidades en línea y el diseño de las plataformas también influyen en la atención que prestamos. Los «me gusta», las veces que se comparte, los comentarios, las notificaciones y las secciones de tendencias pueden hacer que un contenido parezca importante, incluso cuando no es fiable.



Conceptos clave

Algoritmo: Conjunto de reglas o cálculos que un sistema digital utiliza para procesar información y decidir qué contenido o resultados mostrar.

Recomendación: Contenido sugerido a un usuario en función de señales como la actividad previa, los intereses, la popularidad o las reglas de la plataforma.

Feed: Flujo de publicaciones, vídeos, noticias u otros contenidos que se actualiza continuamente y se muestra en una plataforma.

Influencer: Persona que ha creado una audiencia en línea y puede influir en aquello a lo que sus seguidores prestan atención, de lo que hablan, en lo que confían o en lo que compran.

Diseño de la plataforma: Forma en que está estructurada una plataforma digital, incluidos sus botones, notificaciones, diseño y funciones, que puede influir en cómo se comportan las personas y en lo que ven.

Atención: Capacidad mental limitada que las personas dedican a la información. Muchas plataformas digitales están diseñadas para atraer y mantener la atención durante el mayor tiempo posible.



Tarea práctica

Compara los primeros resultados sobre el mismo tema en dos plataformas.
¿Son similares o diferentes?

Pequeño consejo: lo que ves en Internet está seleccionado, no es neutral.

5. Desinformación, información errónea y manipulación

La desinformación es información falsa o inexacta que se comparte sin que necesariamente haya intención de causar daño. **La desinformación** es información falsa o engañosa creada o difundida deliberadamente para engañar.

La manipulación puede utilizar hechos reales de forma engañosa. Una publicación puede utilizar una imagen antigua, eliminar el contexto, exagerar una estadística, recurrir a un supuesto experto o presentar un único ejemplo como si demostrara una regla general.

El **«clickbait»** aprovecha la curiosidad, el miedo o la ira para que la gente haga clic. La manipulación emocional es poderosa porque, a menudo, la gente comparte el contenido sin comprobarlo cuando este confirma lo que ya sienten.



Tarea práctica

Busca un titular que utilice emociones intensas. Reescríbelo de forma neutral.

Pequeño consejo: una emoción intensa es una señal para tomarse un respiro, no para compartir más rápido.

Aprende jugando: después de esta sección, prueba el Reto 3, «Fake News Lab», de la sección 16. Convierte las técnicas de desinformación en una breve actividad de toma de decisiones.

6. Hábitos de evaluación de fuentes y verificación de datos

Una verificación básica de la fuente comienza con preguntas sencillas: ¿quién lo ha publicado, cuándo, dónde, con qué pruebas y con qué propósito? Si la fuente no está clara, la información debe tratarse con cautela. **La verificación cruzada** consiste en comparar la afirmación con otras fuentes fiables. Las instituciones oficiales, los medios de comunicación reconocidos, las fuentes académicas, las organizaciones especializadas y los organismos de verificación de datos pueden ser de ayuda, pero deben leerse siempre con espíritu crítico.

La verificación de datos no es solo cosa de periodistas. Cualquier persona puede adquirir pequeños hábitos: leer más allá del titular, comprobar la fecha, buscar la misma afirmación en otros sitios, examinar la URL, buscar la fuente original y evitar compartir capturas de pantalla sin contexto.



Conceptos clave

Fuente: La persona, organización, documento, sitio web u otro material del que procede la información.

Credibilidad: El grado en que una fuente o una información puede considerarse fiable en función de factores como la experiencia, la transparencia, la precisión y las evidencias.

Evidencia: Información que respalda o ayuda a verificar una afirmación, como documentos, datos, fotografías, registros, investigaciones u otras fuentes fiables.

Verificación cruzada: Comparar la misma afirmación o información con otras fuentes independientes para comprobar si la confirman, la contradicen o aportan contexto adicional.

Fuente original: La fuente más antigua o primaria de la que procede una información, imagen, cita, estadística o afirmación, en lugar de una republicación, resumen o copia posterior.

Verificación de hechos: El proceso de comprobar si una afirmación es correcta mediante el análisis de evidencias, la identificación de la fuente original y la comparación de información fiable.

Mini consejo: Si no puedes averiguar de dónde procede una afirmación, no contribuyas a su difusión.

Aprende jugando: tras esta sección, prueba el Reto 3, «Fake News Lab», de *la sección 16*, y aplica los hábitos de verificación de fuentes antes de elegir una respuesta.

7. Imágenes, vídeos y contenido generado por IA

Las imágenes y los vídeos resultan convincentes porque parecen directos. Sin embargo, pueden estar editados, sacados de contexto, montados, generados por IA o reutilizados de otro suceso. Un hábito útil es **realizar una búsqueda inversa** de una imagen, comprobar si la misma foto apareció anteriormente, buscar incoherencias visuales y preguntarse si la fuente de la imagen es fiable.

El contenido generado por IA plantea nuevos retos. Los textos, las imágenes, las voces y los vídeos pueden imitar a personas reales o acontecimientos realistas. La respuesta no es el pánico, sino la verificación: comprueba el contexto, la fuente, las pruebas y si fuentes fiables informan sobre el mismo suceso.



Conceptos clave

Imagen editada: Una imagen que ha sido modificada después de haber sido tomada o creada.

Contexto: La información que rodea una imagen o un mensaje y que nos ayuda a comprender lo que realmente muestra o significa.

Búsqueda inversa: Una forma de buscar en Internet utilizando una imagen en lugar de palabras para comprobar en qué otros lugares aparece.

Deepfake: Una imagen, vídeo o audio falso o manipulado mediante inteligencia artificial para que pueda parecer o sonar real.

Contenido generado por IA: Texto, imágenes, vídeo o audio creados parcial o totalmente por inteligencia artificial.

Verificación: Comprobar si una información, una imagen o una afirmación es real, correcta y fiable.



Tarea práctica

Compara dos imágenes sobre el mismo tema e identifica qué contexto aporta u oculta cada una.

Mini consejo: una imagen realista no es lo mismo que una prueba fiable.

Aprende jugando: tras esta sección, prueba el Reto 2, «¿Real o IA?», de *la sección 16*. El reto pide a los alumnos que examinen las imágenes y los vídeos antes de confiar en ellos.

8. Privacidad, huella digital y datos personales

La **privacidad** significa controlar la información personal y comprender quién puede verla, almacenarla, utilizarla o compartirla. Una **huella digital** es el rastro que dejan las cuentas, las publicaciones, las fotos, los comentarios, las búsquedas, los datos de ubicación y los archivos compartidos.

Debes evitar publicar información sensible, como documentos de identidad, contraseñas, direcciones privadas, números de teléfono personales, información sanitaria o imágenes de otras personas sin su permiso. La configuración de privacidad es importante, pero no es mágica. Una publicación privada puede copiarse. Una publicación eliminada puede haberse guardado. Una carpeta compartida puede reenviarse. Un comportamiento prudente es más eficaz que confiar únicamente en la configuración.



Conceptos clave

Privacidad: Tener control sobre quién puede ver o utilizar información sobre ti.

Datos personales: Información que puede identificarte, como tu nombre, dirección de correo electrónico, número de teléfono o fotografía.

Huella digital: La información y los rastros que dejas cuando utilizas sitios web, aplicaciones o servicios en línea.

Consentimiento: Dar permiso de forma clara para que algo ocurra, por ejemplo, para que se comparta tu fotografía o información personal.

Visibilidad: Quién puede ver tu perfil, publicaciones, fotografías u otra información en línea.

Configuración: Opciones de una aplicación o sitio web que te permiten controlar aspectos como la privacidad, las notificaciones y quién puede ver tu contenido.



Tarea práctica

Revisa un perfil de redes sociales de ejemplo e identifica tres datos que no deberían ser públicos.

Pequeño consejo: comparte como si el contenido pudiera llegar más lejos de lo que esperas.

9. Conceptos básicos de seguridad en línea: cuentas, contraseñas y dispositivos

Muchos problemas de seguridad en línea comienzan con las cuentas. Una contraseña débil, una contraseña reutilizada o una cuenta de correo electrónico desprotegida pueden dar acceso a los atacantes a otros servicios. Entre los buenos hábitos básicos se incluyen el uso de contraseñas largas y únicas, guardarlas en un gestor de contraseñas, activar la autenticación multifactorial, actualizar los dispositivos, bloquear las pantallas y evitar descargas de origen desconocido.

Las copias de seguridad también son importantes. Si se pierde, se daña o se infecta un dispositivo, las copias de seguridad pueden proteger los archivos importantes. Para el trabajo en comunidad o en proyectos, las copias de seguridad deben estar bien organizadas y ser comprensibles, no improvisadas a última hora.



Conceptos clave

Gestor de contraseñas: Una herramienta que almacena tus contraseñas de forma segura para que no tengas que recordarlas todas.

Autenticación multifactor: Un paso adicional de seguridad que solicita algo más que una contraseña, por ejemplo, un código enviado a tu teléfono.

Actualización: Una versión más reciente de un programa que puede corregir problemas, mejorar la seguridad o añadir funciones.

Copia de seguridad: Una copia guardada de archivos importantes que puedes utilizar si los archivos originales se pierden o resultan dañados.

Seguridad del dispositivo: Las medidas que adoptas para proteger tu teléfono, tableta u ordenador frente al acceso no autorizado, la pérdida o el software malicioso.



Tarea práctica

Crea una lista de comprobación personal para la seguridad de tus cuentas sin escribir ninguna contraseña real.

Mini consejo: La cuenta de correo electrónico suele ser la llave maestra; protégela en primer lugar.

10. Recomendaciones del INCIBE y recursos de ayuda de confianza

INCIBE, el Instituto Nacional de Ciberseguridad de España, es una referencia útil para la seguridad en línea en España. Ofrece orientación, recursos educativos y una línea de ayuda sobre ciberseguridad para ciudadanos, profesionales y organizaciones.

Los materiales de INCIBE para los ciudadanos abarcan temas prácticos como la navegación segura, las conexiones seguras, la configuración básica, los antivirus, los cortafuegos, las actualizaciones, las cuentas de usuario, las copias de seguridad, el cifrado, las contraseñas, el malware, el fraude en línea, el phishing, el smishing, el vishing, la privacidad, los dispositivos móviles y la inteligencia artificial. INCIBE resulta valioso porque traduce la ciberseguridad en acciones cotidianas. El objetivo no es convertirse en un experto técnico, sino saber qué hacer al recibir un mensaje sospechoso, proteger una cuenta, comprar por Internet o configurar un dispositivo.

Una sencilla lista de comprobación inspirada en INCIBE puede incluir:

- actualizar los dispositivos
- utilizar contraseñas únicas
- activar la autenticación multifactorial
- hacer copias de seguridad
- comprobar los enlaces antes de hacer clic
- Evita compartir los códigos de verificación
- Revisa la configuración de privacidad y pide ayuda si algo te parece sospechoso



Tarea práctica

Utiliza la lista de temas de INCIBE para elegir tres riesgos en línea y escribe una medida de prevención para cada uno.

Pequeño consejo: una buena seguridad en línea implica saber dónde pedir ayuda fiable.

11. «Have I Been Pwned» y comprobaciones de fugas de datos

«Have I Been Pwned» es un servicio que permite a los usuarios comprobar si una dirección de correo electrónico aparece en fugas de datos conocidas. También se puede utilizar para comprender por qué es peligroso reutilizar contraseñas. Una **fuga de datos** significa que se ha filtrado información de un servicio. Esto puede incluir direcciones de correo electrónico, nombres de usuario, contraseñas, números de teléfono u otros datos de la cuenta. Si se reutiliza una contraseña en varias cuentas, una sola fuga puede afectar a muchos servicios.

Los alumnos deben utilizar «Have I Been Pwned» con precaución. Pueden comprobar una dirección de correo electrónico, pero no deben introducir contraseñas reales y actuales en sitios web aleatorios. Para las contraseñas, deben utilizar gestores de contraseñas de confianza o herramientas de comprobación seguras y seguir las directrices oficiales. Si una dirección de correo electrónico aparece en una filtración, la respuesta debe ser serena y práctica: cambiar las contraseñas reutilizadas, hacer que cada contraseña sea única, habilitar la autenticación multifactorial, comprobar la actividad de la cuenta y estar alerta ante los mensajes de phishing.



Conceptos clave

Brecha de datos: Un incidente de seguridad en el que se accede a información privada o personal, o esta queda expuesta, sin permiso.

Correo electrónico expuesto: Una dirección de correo electrónico que ha aparecido en datos filtrados o robados y que puede ser conocida por los atacantes.

Reutilización de contraseñas: Utilizar la misma contraseña para más de una cuenta.

Relleno de credenciales: Un ataque en el que se prueban automáticamente direcciones de correo electrónico y contraseñas robadas en otros sitios web para comprobar si también funcionan allí.

Recuperación de cuenta: El proceso de volver a acceder a tu cuenta si olvidas tu contraseña o pierdes el acceso.



Tarea práctica

Simula un plan de respuesta ante una brecha de datos. ¿Qué harías si tu correo electrónico apareciera en una brecha de datos?

Mini consejo: Una alerta de filtración no supone el fin de la seguridad; es una señal para poner en orden tus cuentas.

12. Seguridad de los archivos compartidos: Telegram, descargas directas y archivos comprimidos

Muchos riesgos provienen de archivos compartidos fuera de los canales oficiales: grupos de Telegram, carpetas en la nube desconocidas, enlaces de descarga directa, foros, páginas de software pirateado o URL acortadas. Estas vías pueden ser legalmente cuestionables y técnicamente arriesgadas.

La recomendación más segura es evitar descargar archivos de fuentes de dudosa legalidad u origen poco claro. El software pirateado, las herramientas crackeadas, los instaladores desconocidos y los archivos protegidos con contraseña son formas habituales de distribuir malware.

Antes de abrir un archivo descargado, los alumnos deben plantearse algunas preguntas básicas:

¿Quién lo ha enviado?

¿Lo esperaba?

¿Tiene buena reputación la fuente?

¿Es legal el uso de este archivo? ¿Coincide el nombre del archivo con su contenido?

¿La extensión es sospechosa?

¿Me pide que desactive el antivirus o que active las macros?

Los archivos comprimidos como ZIP, RAR o 7Z no deben abrirse a ciegas. En primer lugar, comprueba la fuente, analiza el archivo con un antivirus, revisa la lista de archivos sin extraerlos si es posible y evita los archivos que contengan archivos ejecutables como .exe, .scr, .bat, .cmd, .msi, .apk o archivos de acceso directo sospechosos.

Si un archivo es importante pero no estás seguro de su fiabilidad, sigue unos pasos de análisis más seguros: comprueba la URL antes de descargarlo, escanea el archivo con un antivirus actualizado, compara los hash si la fuente oficial los proporciona y considera la posibilidad de utilizar servicios de análisis con múltiples motores, como VirusTotal, para

archivos o URL públicos que no sean privados. No subas archivos privados o confidenciales a servicios de análisis públicos.

Los documentos también pueden ser peligrosos. Los archivos de Office con macros, los PDF de fuentes desconocidas, las facturas falsas y las carpetas comprimidas con ejecutables ocultos son métodos comunes de ataque . Un hábito seguro consiste en abrir los documentos en vista protegida, evitar habilitar las macros y utilizar fuentes oficiales siempre que sea posible.

En entornos de formación, la regla debe ser sencilla: utiliza sitios web oficiales, repositorios de confianza y fuentes legales. Si una plataforma o un archivo pide a los alumnos que eludan el pago, desactiven la protección, instalen herramientas desconocidas o ignoren las advertencias, no es adecuado para la formación.



Conceptos clave

Archivo comprimido: Un archivo que contiene uno o varios archivos empaquetados juntos, normalmente para facilitar su almacenamiento o envío. ZIP es un ejemplo habitual.

Archivo ejecutable: Un archivo que puede iniciar un programa o una instalación al abrirse, como un archivo .exe.

Malware: Software malicioso que puede dañar un dispositivo, robar información o acceder a él sin permiso.

Hash: Un valor digital que puede utilizarse para comprobar si un archivo ha sido modificado.

Antivirus: Software que ayuda a detectar, bloquear y eliminar software malicioso.

Descarga directa: Descarga de un archivo directamente desde un sitio web a tu dispositivo.

Software crackeado: Software que ha sido modificado ilegalmente para evitar pagar por él o eliminar las restricciones de licencia. También puede contener software malicioso.

Vista protegida: Un modo de seguridad que abre algunos documentos descargados con la edición desactivada hasta que decidas que el archivo es seguro.



Tarea práctica

Examina un ejemplo de descarga y decide si debes abrir el archivo, eliminarlo, analizarlo, verificarlo con el remitente o volver a descargarlo desde una fuente oficial.

Mini consejo: si un archivo procede de una fuente dudosa y te pide que confíes en él rápidamente, haz lo contrario: tómate tu tiempo y compruébalo.

Aprende jugando: tras esta sección, prueba el Reto 4, «Misión de descarga segura», de *la sección 16*. En él se practican decisiones sobre archivos de Telegram, descargas directas y archivos comprimidos.

13. Estafas en línea, phishing e ingeniería social

El **phishing** es una estafa que intenta que las personas revelen información o hagan clic en un enlace peligroso. El **smishing** utiliza SMS o aplicaciones de mensajería. El **vishing** utiliza llamadas telefónicas. La ingeniería social se vale de la confianza, la urgencia o el miedo para influir en el comportamiento.

Entre las señales de alerta más comunes se incluyen plazos urgentes, amenazas, premios, archivos adjuntos inesperados, solicitudes de códigos de verificación, instrucciones de pago extrañas, enlaces acortados y mensajes que presionan a las personas para que actúen rápidamente.

La respuesta más segura es tomarse un respiro. No utilices el enlace del mensaje. Ve directamente al sitio web o a la aplicación oficial, ponte en contacto con la organización a través de un canal conocido y nunca compartas contraseñas ni códigos de autenticación.



Conceptos clave

Phishing: Un mensaje o sitio web falso diseñado para engañarte y conseguir que reveles información personal, contraseñas o dinero.

Smishing: Phishing realizado mediante mensajes de texto o aplicaciones de mensajería.

Vishing: Phishing realizado mediante una llamada telefónica o un mensaje de voz.

Estafa: Un intento deshonesto de engañar a alguien, normalmente para robar dinero, información o acceso a una cuenta.

Ingeniería social: Manipular a las personas para que hagan algo inseguro, por ejemplo, compartir una contraseña o abrir un enlace malicioso.

Código de verificación: Un código temporal utilizado para confirmar tu identidad al iniciar sesión o realizar un cambio sensible en una cuenta.



Tarea práctica

Analiza tres mensajes sospechosos y señala las señales de advertencia.

Mini consejo: La urgencia es una de las herramientas más comunes del fraude en línea.

Aprende jugando: después de esta sección, prueba el Reto 1, «Detecta el phishing», en *la sección 16*. Sigue la misma lógica que los cuestionarios interactivos sobre phishing: analiza, decide y aprende de los comentarios.

14. Ciberacoso, discurso de odio y participación respetuosa

La seguridad en línea no es solo una cuestión técnica. También incluye cómo se tratan las personas entre sí. El ciberacoso, el acoso, el discurso de odio y la humillación pueden afectar gravemente al bienestar y a la participación. La participación respetuosa significa discrepar sin atacar, evitar la humillación pública, no compartir imágenes privadas, denunciar los comportamientos abusivos y apoyar a las personas que son objeto de estos ataques.

En proyectos educativos o comunitarios, los grupos deben acordar unas normas básicas antes de publicar o debatir en línea: quién puede comentar, quién modera, qué no es aceptable y cómo se gestionarán los problemas.



Conceptos clave

Ciberacoso: Utilizar herramientas digitales para herir, avergonzar o amenazar repetidamente a otra persona.

Acoso: Comportamiento no deseado que hace que una persona se sienta amenazada, incómoda o insegura.

Discurso de odio: Contenido que ataca o fomenta el odio contra personas por características como su origen, religión, género o identidad.

Moderación: El proceso de revisar contenidos y comportamientos en línea y aplicar las normas de la comunidad.

Denuncia: Utilizar las herramientas de una plataforma para alertarla sobre contenidos o comportamientos dañinos, abusivos o inapropiados.

Bienestar: Sentirse seguro, equilibrado y cómodo al utilizar tecnologías digitales.



Tarea práctica

Escribe cinco normas de convivencia para mantener un espacio de proyecto en línea seguro.

Pequeño consejo: un espacio digital seguro necesita normas, moderación y cuidado.

15. Publicaciones seguras para proyectos comunitarios y patrimoniales

Al publicar contenidos comunitarios o patrimoniales, los alumnos deben tener en cuenta el consentimiento, el contexto y la privacidad. Una foto de una persona, un lugar privado o una historia comunitaria puede requerir permiso antes de ser compartida. La publicación segura también implica comprobar los derechos de los medios, citar la fuente, evitar pies de foto engañosos y proteger a las personas vulnerables o la información cultural sensible.

Antes de publicar, el equipo del proyecto puede realizar una breve revisión: ¿Está clara la fuente? ¿Está clara la licencia? ¿Aparecen las personas con su consentimiento? ¿Revela el contenido datos privados? ¿Podría malinterpretarse la historia sin contexto?



Conceptos clave

Consentimiento: Permiso claro de una persona antes de utilizar o compartir su imagen, historia, voz o información personal.

Atribución: Reconocer a la persona o fuente que creó o proporcionó el contenido.

Contexto: La información de fondo que ayuda a las personas a comprender correctamente una historia, imagen, objeto o tradición.

Seguridad de la comunidad: Garantizar que el contenido publicado no exponga a personas, lugares o comunidades a riesgos innecesarios.

Sensibilidad hacia el patrimonio: Tratar el patrimonio cultural con cuidado y respeto, especialmente cuando incluye recuerdos personales, tradiciones, lugares sagrados o información sensible de la comunidad.

Revisión antes de publicar: Una comprobación final antes de compartir contenido para asegurarse de que sea correcto, respetuoso, esté debidamente atribuido y sea seguro publicarlo.



Tarea práctica

Revisa el borrador de una publicación sobre un elemento del patrimonio local e identifica qué debería comprobarse antes de publicarla.

Pequeño consejo: Publicar de forma responsable protege tanto al público como a la comunidad representada.

16. Aprender jugando: retos de alfabetización mediática y ciberseguridad

Esta sección convierte los conceptos de alfabetización mediática y seguridad en línea en breves retos de toma de decisiones. Los alumnos practican cómo detectar el phishing, el contenido generado por IA, la desinformación y los archivos peligrosos a través de escenarios realistas con retroalimentación inmediata.

El objetivo es el aprendizaje basado en la práctica. Los alumnos no solo leen consejos, sino que toman decisiones, comparan indicios, reciben explicaciones y reflexionan sobre lo que harían en la vida real.

Puntuación sugerida: cada reto incluye de 3 a 5 situaciones. Los alumnos reciben 1 punto por cada decisión acertada y 1 punto extra cuando son capaces de explicar la señal de alerta o el paso de verificación. Al final, pueden obtener una insignia sencilla: «Verificador cuidadoso», «Detective de fuentes», «Detector de imágenes generadas por IA» o «Guardián de la ciberseguridad».

Reto 1: Detecta el phishing. Los alumnos examinan correos electrónicos, mensajes SMS, mensajes directos o mensajes al estilo de Telegram. Analizan el remitente, el enlace, el tono, la urgencia, los archivos adjuntos, las solicitudes de códigos y si el mensaje les pide que utilicen un canal inseguro. Inspiración: Cuestionario sobre phishing de Google/Jigsaw (<https://phishingquiz.withgoogle.com/>). Ejemplo de decisión: hacer clic en el enlace, ignorarlo, denunciarlo o ir directamente a la página web oficial.

Reto 2: ¿Real o IA? Los alumnos analizan imágenes, vídeos cortos o capturas de pantalla y deciden si el contenido es real, generado por IA, editado o carece de contexto. Buscan inconsistencias visuales, manos o textos extraños, reflejos poco naturales, falta de fuente, imágenes antiguas reutilizadas como si fueran acontecimientos nuevos y si fuentes fiables confirman la afirmación. Inspiración: «Detect Fakes» de la Universidad Northwestern (<https://detectfakes.kellogg.northwestern.edu/>), los juegos de alfabetización digital «Deepfakes Tracker» (<https://deepfakestracker.org/digital-literacy-games/>), «Real or AI» (<https://whichoneisreal.com/real-or-ai/>) y «Sightengine AI or Not» (<https://sightengine.com/ai-or-not>).

Reto 3: Laboratorio de noticias falsas. Los alumnos analizan titulares, publicaciones o artículos breves e identifican la manipulación emocional, las pruebas poco sólidas, la falsa autoridad, los titulares sensacionalistas, la falta de contexto, los planteamientos conspirativos o las estadísticas engañosas. Inspiración: Bad News Game (<https://www.getbadnews.com/>), los juegos de Inoculation Science (<https://inoculation.science/inoculation-games/>), NewsFeed Defenders y ABC Fake News Game. Ejemplo de decisión: compartir, guardar para más tarde, consultar otra fuente, reescribir de forma neutral o rechazar por ser poco fiable.

Reto 4: Misión «Descarga segura». Los alumnos se enfrentan a situaciones realistas de intercambio de archivos: un archivo ZIP en un grupo de Telegram, un enlace de descarga directa, un archivo RAR protegido con contraseña, un instalador pirateado, una factura en PDF, un acceso directo oculto dentro de un archivo comprimido o un archivo de una carpeta en la nube desconocida. Deben decidir si abrirlo, borrarlo, escanearlo, verificarlo con el remitente, comprobar la URL, comparar un hash o descargarlo de una fuente oficial.



Reflexión

¿Qué señal de advertencia estuviste a punto de pasar por alto y qué hábito te ayudará a detectarla la próxima vez?

Mini consejo: un buen reto debe parecer una decisión real, no una prueba de memoria.

17. Actividad final

La actividad final combina la alfabetización mediática y la seguridad en línea. Los alumnos eligen un contenido en línea relacionado con la cultura, la tecnología, las noticias locales o la vida comunitaria y lo analizan antes de decidir si debe compartirse.

Hoja de análisis

Título o tema	
Plataforma	
Creador	
Fecha	
Afirmación principal	
Pruebas	
Lenguaje emocional	
Verificación de la fuente	
Segunda fuente	
Posible falta de contexto	
Decisión final	

Ficha de seguridad

Datos personales implicados	
Riesgos para la privacidad	
Señales de alerta de estafa	
Medidas de seguridad de la cuenta	
Riesgos relacionados con la descarga de archivos	
¿Podrían ser de ayuda las recomendaciones de INCIBE?	
¿Sería útil «<i>Have I Been Pwned</i>» para comprobar si he sido víctima de una filtración de datos?	

Mini consejo: La mejor herramienta de seguridad en línea es pararse a pensar antes de actuar.

18. Consejo sobre bienestar digital



Consejo de bienestar digital

Haz que tu pantalla sea más cómoda

Una pantalla demasiado brillante, un texto demasiado pequeño o una postura incómoda pueden hacer que las actividades digitales resulten más cansadas de lo necesario.

Prueba esto: Ajusta el brillo de la pantalla, aumenta el tamaño del texto si es necesario y coloca el dispositivo de forma que puedas utilizarlo cómodamente. Cambia de postura o estira si llevas mucho tiempo sentado.

Pregunta de reflexión: ¿Hay algún pequeño cambio que podría hacer que utilizar tu teléfono u ordenador resulte más cómodo?

19. Glosario básico

Algoritmo: sistema que selecciona o clasifica contenidos según unas reglas y datos.

Ciberacoso: comportamiento dañino y repetido llevado a cabo a través de herramientas digitales.

Fuga de datos: exposición de datos personales o de una cuenta de un servicio.

Huella digital: rastro de información que deja una persona en Internet.

Desinformación: información falsa o engañosa difundida deliberadamente con el fin de engañar.

Verificación de datos: proceso de contrastar una afirmación con pruebas y fuentes fiables.

Hash: huella digital que se utiliza para comparar si un archivo coincide con una versión esperada.

Have I Been Pwned: servicio que permite comprobar si una dirección de correo electrónico aparece en fugas de datos conocidas.

INCIBE: Instituto Nacional de Ciberseguridad de España, una referencia de confianza y un recurso de ayuda en materia de ciberseguridad.

Alfabetización mediática: capacidad para acceder, comprender, evaluar, crear y compartir contenidos mediáticos de forma responsable.

Desinformación: información falsa o inexacta que puede compartirse sin intención de causar daño.

Autenticación multifactorial: protección de la cuenta que requiere un paso de verificación adicional.

Phishing: mensaje fraudulento diseñado para robar información o hacer que los usuarios hagan clic en enlaces peligrosos.

RAR/ZIP/7Z: formatos de archivo comprimido que pueden contener uno o varios archivos.

Privacidad: control y protección de la información personal.

Fuente: persona, organización o plataforma que publica información.

20. Cierre del módulo

La alfabetización mediática y la seguridad en Internet son habilidades cotidianas. Ayudan a las personas a participar en Internet sin ser pasivas, descuidadas o fácilmente manipulables. El módulo ha demostrado que una participación digital responsable requiere tanto pensamiento crítico como medidas prácticas de protección. Los alumnos deben verificar la información, proteger sus cuentas, respetar a los demás y publicar con cuidado.

Tras este módulo, los alumnos deberían ser capaces de pararse a pensar antes de compartir algo, evaluar una fuente, reconocer los riesgos habituales, utilizar recursos de ayuda fiables, practicar mediante pequeños retos y crear una sencilla lista de comprobación de seguridad para uso personal o en proyectos.

Pequeño consejo: Piensa de forma crítica, actúa con seguridad y comparte de forma responsable.

Bibliografía

Comisión Europea. (22 de junio de 2026). *Alfabetización mediática*. Forjando el futuro digital de Europa. <https://digital-strategy.ec.europa.eu/en/policies/media-literacy>

Comisión Europea. (23 de junio de 2026). *Lucha contra la desinformación en línea*. Forjando el futuro digital de Europa. <https://digital-strategy.ec.europa.eu/en/policies/online-disinformation>

Grizzle, A., Wilson, C. y Gordon, D. (Eds.). (2021). *Ciudadanos con alfabetización mediática e informacional: ¡Piensa de forma crítica, haz clic con prudencia!* UNESCO. <https://www.unesco.org/en/articles/media-and-information-literate-citizens>

Instituto Nacional de Ciberseguridad. (s. f.). *Ciudadanía*. Consultado el 28 de agosto de 2026, en <https://www.incibe.es/ciudadania>

Richardson, J. y Milovidov, E. (2022). *Manual de educación para la ciudadanía digital: Estar en línea, bienestar en línea, derechos en línea* (ed. de 2022). Ediciones del Consejo de Europa. [Publicación del Consejo de Europa](#)