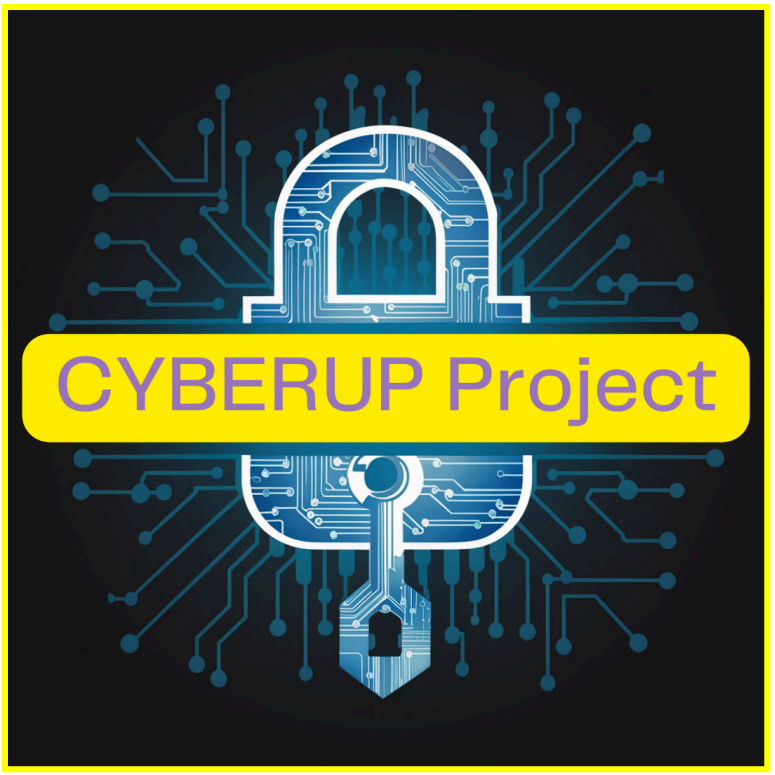


Proyecto Erasmus+ "Cybersecurity literacy to empower seniors towards safe Digitalisation"

2023-1-CY01-KA210-ADU-000150806

Guía para el Uso Seguro y Responsable de Internet para Formadores de Educación de Adultos

TABLA DE CONTENIDOS

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

1. Introducción del proyecto Erasmus + CYBERUP

El proyecto Erasmus+ CYBERUP (2023-1-CY01-KA210-ADU-000150806) tiene como objetivo principal desarrollar conocimientos, actitudes y habilidades digitales aplicadas a la ciberseguridad en personas mayores para un uso más eficiente e inclusivo de las tecnologías digitales más comunes en las personas mayores de 60 años. años con bajas habilidades digitales.

El uso generalizado de la tecnología en la actualidad, acelerado por la pandemia de COVID-19, aumenta la importancia del acceso a los dispositivos digitales y a Internet, y de adquirir las habilidades digitales necesarias para participar en la sociedad pero, sobre todo, para hacer un uso seguro y equitativo de las nuevas tecnologías. y evitar convertirse en víctima de un delito cibernético. El uso generalizado de la tecnología en todos los ámbitos de la vida también ha generado riesgos importantes, como la desinformación, el uso indebido de datos personales y la posible traducción de la brecha digital en una brecha de aprendizaje, lo que genera mayores desigualdades.

Estos avances refuerzan la necesidad de prestar más atención a las habilidades digitales, especialmente para las personas mayores, y de fomentar las habilidades cívicas. Los ciberataques y la ciberdelincuencia están aumentando en toda Europa y se están volviendo cada vez más sofisticados. Esta tendencia seguirá empeorando en el futuro.

Este proyecto pretende dar respuesta a las necesidades de la transformación digital en términos de alfabetización en ciberseguridad para garantizar una transición digital segura tanto en la educación como en la sociedad. El principal objetivo de este proyecto es desarrollar conocimientos, actitudes y habilidades digitales aplicadas a la ciberseguridad en personas mayores para un uso más eficiente e inclusivo de las tecnologías digitales más comunes en personas mayores de 60 años con bajas habilidades digitales.

Objetivos específicos:

- Proporcionar a los formadores una herramienta que les ayude a promover el aprendizaje permanente en habilidades digitales y ciberseguridad en el ámbito de la educación de adultos.

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

- Promover la alfabetización digital en términos de ciberseguridad para las personas mayores para evitar amenazas digitales y reducir la brecha de habilidades en ciberseguridad.
- Sensibilizar sobre la necesidad y la importancia de empoderar a las personas mayores hacia una transformación digital más segura y justa.

Los objetivos del proyecto están vinculados a las prioridades establecidas de la siguiente manera:

- Erasmus Digital+. Este proyecto tiene como objetivo responder a las necesidades de la transformación digital en términos de alfabetización en ciberseguridad para garantizar una transición digital segura también en la educación y la sociedad.

- La creación o ampliación de un acceso a itinerarios de mejora de capacidades para adultos con un bajo nivel de capacidades. El proyecto tiene como objetivo abordar las necesidades del principal grupo objetivo (personas adultas mayores de 60 años con bajas habilidades digitales) en términos de seguridad digital y empoderarlos hacia una transformación digital más inclusiva a través de una formación personalizada sobre alfabetización en ciberseguridad.

- Ampliar y desarrollar las competencias de educadores y profesores. El proyecto tiene como objetivo apoyar la promoción e implementación de la ciberseguridad en la educación de adultos (a través de la guía metodológica para formadores) como aspecto fundamental para ayudar a lograr una transición más justa y segura en la educación digital actual.

1.1 Perfil e investigación del participante

El primer paso del proyecto es la creación de la “Guía para el uso seguro y responsable de Internet para formadores en educación de adultos”. Esta guía contiene, por un lado, información relevante sobre la situación actual de las personas mayores en cuanto a sus habilidades digitales y de ciberseguridad en los países socios, así como los nuevos retos a los que se enfrentan. Por otro lado, contiene información, recursos y métodos para ayudar a los formadores a aplicar y promover la ciberseguridad como parte del aprendizaje permanente en el campo de la educación de adultos.

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

El análisis de necesidades informa sobre actitudes y necesidades relacionadas con las habilidades digitales aplicadas a la ciberseguridad en personas mayores para un uso más eficiente e inclusivo de las tecnologías digitales más comunes en personas mayores de 60 años con bajas habilidades digitales. Los perfiles de los participantes se basan en personas mayores de 60 años, de ambos países implicados en el proyecto, Chipre y España. Este grupo de población se ha digitalizado en gran medida en los últimos dos años, precisamente por su uso cada vez más constante de herramientas tecnológicas tras los años de pandemia de covid-19, aumentando el riesgo de convertirse en un blanco fácil para los ciberdelincuentes que se aprovechan de ellas. de su vulnerabilidad. La metodología seguida en este informe de estudio se basa en un cuestionario con un grupo focal basado en el grupo objetivo con 10 preguntas para recopilar la información necesaria para la creación de esta guía metodológica para cada país involucrado en el proyecto Erasmus+, Chipre y España.

El informe surge de haber hecho primero uno individual para cada país y a través de este informe juntamos una fase de investigación de necesidades bibliográficas y la fase práctica, habiéndose utilizado los dos grupos focales. Cada uno se centra en un 54,5% de personas mayores de España y un 45,5% de personas mayores de Chipre con 15 participantes. hombres y mujeres, con edades comprendidas entre 60 y 95 años. El 70% tenía entre 60 y 67 años en España y Chipre. Pero también éramos personas mayores de 70, 80 y también 90 años.

1.2 . Recopilación de datos y resultados.

El grupo seleccionado de seniors seleccionados de ambos países implicados, Chipre y España, con un Grupo de estudio de 15 personas por país, se ha digitalizado en gran medida en los últimos dos años, precisamente por su uso cada vez más constante de herramientas tecnológicas en a raíz de los años de la pandemia de covid-19, aumentando el riesgo de convertirse en un blanco fácil para los ciberdelincuentes que se aprovechan de su vulnerabilidad. Este grupo poblacional creció en una generación en la que estas tecnologías no existían y tienen miedo de usarlas, lo que los hace aún más vulnerables en términos de seguridad digital.

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

En primer lugar, los perfiles de los participantes se basan en personas mayores de 60 años de ambos países involucrados. Respondieron al informe el 54,5% de personas mayores de España y el 45,5% de Chipre. La edad puede cruzarse con otros factores socioeconómicos, como los ingresos, la educación y la ubicación geográfica, lo que influye en las disparidades en la alfabetización digital y el acceso a la tecnología. La identificación de barreras específicas por edad para la inclusión digital puede informar políticas e iniciativas destinadas a reducir la brecha digital y promover el acceso equitativo a los recursos y oportunidades digitales para personas de todas las edades.

En general, la consideración se centró en la alfabetización digital, conocimientos valiosos sobre cómo las habilidades, actitudes y comportamientos digitales son una necesidad para el grupo objetivo de este proyecto, para enfrentar el desafío cognitivo de adquirir nuevas habilidades y habilidades; y en segundo lugar, favorece su autonomía y bienestar emocional ya que la tecnología rompe las barreras de la soledad y el aislamiento, pero también para integrarse en la nueva era digital, promover la inclusión digital, mejorar la alfabetización digital y abordar las diversas necesidades y preferencias de los individuos a lo largo de su vida. En cuanto a la edad, la mayoría de los encuestados tenían entre 60 y 67 años en España y Chipre. Pero hay personas mayores de 70, 80 y también 90 años. también.

Los socios del proyecto, Connecting Dots de Chipre e Inercia Digital de España, entregaron un cuestionario con 10 preguntas implementadas en un formulario de Google que se distribuyó a 15 partes interesadas en Chipre y 15 partes interesadas en España. A continuación mostramos la explicación de los resultados de cada una de las preguntas del cuestionario. Con él pretendemos tener una mejor visión y comprensión del uso real que las personas mayores de 60 años hacen de las tecnologías, y el uso digital en su vida diaria, y así encontrar y diseñar mejor una futura guía de uso y seguridad digital.

Han sido los facilitadores y personal de nuestras organizaciones quienes han podido recapitular las respuestas a las preguntas que iban mencionando. Su accesibilidad a la hora de distribuirlos ya que se pueden compartir fácilmente a través de un enlace y pueden completarse desde cualquier dispositivo conectado a Internet, ya sea ordenador, teléfono móvil o tablet; y la recogida automática de respuestas que Google almacena directamente en una hoja de cálculo, facilitando así el análisis de los datos recogidos durante la investigación.

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

El grupo objetivo de la fase de investigación expresó el uso diario de dispositivos digitales como teléfonos inteligentes, ordenadores y tablets.

- **Necesidad uno:** uso de dispositivos digitales: eso muestra una proporción significativa de participantes que utilizan dispositivos digitales a diario, lo que indica un alto nivel de compromiso con la tecnología en su vida diaria. Dado que casi la mitad de los participantes utilizan dispositivos digitales todos los días, se subraya el papel integral que desempeña la tecnología en la sociedad moderna.
- **Necesidad dos:** el uso básico implica que el grupo objetivo puede utilizar principalmente plataformas de redes sociales para funciones fundamentales como navegar, ver contenido o publicar publicaciones ocasionales, sin utilizar ampliamente funciones avanzadas ni participar en actividades interactivas y participativas como crear contenido, establecer contactos o unirse. comunidades en línea. Esto sugiere distintos niveles de alfabetización en medios sociales entre los usuarios, y algunos potencialmente necesitan apoyo u orientación para aprovechar las plataformas de medios sociales de manera más efectiva.
- **Necesidad tres:** comunicación digital. El grupo objetivo de la investigación, en su mayoría, conoce los conceptos básicos. Los resultados se refieren a las habilidades en el uso de redes sociales como Facebook, Twitter o Instagram, que se indican con regularidad y son muy básicas.
- **Necesidad cuatro:** confianza. Los talleres, tutoriales y materiales educativos personalizados pueden ayudar a las personas mayores a mejorar sus habilidades y confianza para organizar y administrar archivos digitales de manera más efectiva.
- **Necesidad cinco:** uso diario para la vida moderna. El hecho de que casi un tercio de los participantes acceda a Internet a diario pone de relieve el papel omnipresente de Internet en la vida moderna. El acceso diario a Internet se ha vuelto esencial para diversas actividades, incluida la educación y las transacciones en línea, pero, por supuesto, la comunicación, la recuperación de información y el entretenimiento, que es un uso importante para la mayoría de los encuestados, como querían dejar claro.

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

- **Necesidad sexta:** Interés por el aprendizaje y participación en el mismo. Comprender las razones detrás de la renuencia a participar en programas de alfabetización digital puede contribuir al desarrollo de iniciativas más efectivas e inclusivas destinadas a promover la inclusión digital y empoderar a las personas mayores para que aprovechen la tecnología para el enriquecimiento personal, la conectividad social y el aprendizaje permanente. Se pueden ofrecer estrategias para aumentar la participación en relación con los beneficios prácticos de las habilidades de alfabetización digital para los grupos de personas mayores y abordar conceptos erróneos o preocupaciones sobre la tecnología.
- **Necesidad siete:** Uso de las redes sociales. A los participantes en la investigación les gustaría saber mejor cómo utilizar las redes sociales y una variedad de aplicaciones disponibles en los teléfonos inteligentes para ver fútbol en vivo, pagar en línea, etc. El interés en mejorar las habilidades en las redes sociales resalta la importancia de la socialización y la conectividad en línea. para personas mayores. Los participantes están interesados en mantenerse conectados con amigos y familiares, interactuar con comunidades de interés y acceder a información y entretenimiento.
- **Necesidad ocho:** falta de acceso. Cuando se trata de tener acceso a recursos de apoyo para mejorar sus habilidades digitales destacan varias consideraciones importantes como la falta de acceso a recursos específicamente diseñados para ayudarles a mejorar sus habilidades digitales y la ciberseguridad para sentirse cómodos usándolos. Esto podría incluir el desarrollo real de la presente Guía.

2. Seguridad en Internet

A través de esta guía, se presenta la oportunidad de conocer más sobre las necesidades y desafíos que los adultos mayores están enfrentando actualmente en los países socios, adquirir un conocimiento más profundo sobre ciberseguridad y aprender cómo aplicarlo en la comunidad de adultos mayores para ayudarlos a formar parte de la transición digital de una manera más

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

participativa, pero sobre todo, de una manera segura y responsable. Para lograrlo, es importante situar a los formadores como transmisores de todo el conocimiento, habilidades y comportamientos que promuevan la alfabetización en ciberseguridad y aseguren la seguridad digital de la población mayor.

La seguridad en internet y el uso de la tecnología son temas cada vez más relevantes, especialmente para los adultos mayores. A medida que la tecnología se convierte en una parte integral de nuestras vidas diarias, es importante que todas las personas, incluidos los adultos mayores, estén informadas y protegidas.

Las habilidades digitales para el trabajo y la vida son una de las principales prioridades en la agenda política europea. La estrategia de habilidades digitales de la UE y las iniciativas políticas relacionadas tienen como objetivo mejorar las habilidades y competencias digitales para la transformación digital.

El Marco de Competencias Digitales para la Ciudadanía, también conocido como DigComp, proporciona un lenguaje común para identificar y describir áreas clave de competencias digitales. Es una herramienta a nivel de la UE para mejorar la competencia digital de los ciudadanos, ayudar a los responsables políticos a formular políticas que apoyen el desarrollo de la competencia digital y planificar iniciativas de educación y formación para mejorar las competencias digitales de grupos específicos. Este marco de referencia nos ayudará a crear esta metodología para los adultos mayores, ya que es un marco que define los componentes clave de la competencia digital en diferentes áreas, como articular las necesidades de información, localizar y recuperar datos, información y contenido digital, juzgar la relevancia de la fuente y su contenido, identificar necesidades y problemas, y resolver problemas conceptuales y situaciones problemáticas en entornos digitales para los adultos mayores, incluyendo herramientas digitales para innovar procesos y productos y mantenerse al día con la evolución digital.

Es crucial proporcionar educación y concienciación sobre la seguridad en internet y el uso de la tecnología a los adultos mayores. Esto incluye enseñarles sobre la importancia de las contraseñas seguras, cómo reconocer y evitar estafas en línea, cómo proteger su información personal y cómo usar de manera segura las redes sociales y otras plataformas en línea. Los adultos mayores deben ser conscientes de la importancia de proteger su información personal en línea, como los números de seguridad social, los números de tarjetas de crédito y las contraseñas.

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

2.1. Alfabetización Digital

La alfabetización digital se refiere a la capacidad de utilizar las tecnologías digitales de manera efectiva y crítica. Implica no solo el conocimiento técnico sobre cómo usar dispositivos y software, sino también la capacidad de evaluar, analizar y crear información digital de manera responsable. Según Jones (2020), es una competencia esencial en la sociedad contemporánea, y en este caso específico para los grupos de personas mayores que son inmigrantes digitales, donde las tecnologías digitales están omnipresentes en casi todos los aspectos de la vida diaria, el trabajo y la educación. Para los adultos mayores, es crucial facilitar la participación activa en la sociedad digital, permitiéndoles involucrarse en debates públicos, acceder a servicios gubernamentales y participar en la economía digital, pero también promover la inclusión social que reduce la brecha digital, asegurando que todos, independientemente de su edad, tengan las mismas oportunidades para acceder y beneficiarse de las tecnologías digitales.

Hay varios aspectos sobre la alfabetización digital que deben considerarse, tales como:

Habilidades técnicas, el conocimiento básico de cómo operar dispositivos como ordenadores, tablets y teléfonos inteligentes, así como el uso de software y aplicaciones.

En el contexto de la era digital, estas habilidades a menudo se relacionan con el uso de tecnología y software. Habilidades técnicas comunes incluyen:

- Programación y Codificación: Comprensión de lenguajes como Java, HTML, JavaScript.
- Administración de Sistemas: Gestión de sistemas operativos (Windows, Linux).
- Redacción Técnica: Documentación de procesos, creación de manuales de usuario, redacción de informes técnicos.
- Habilidades Informáticas Básicas: Operación de un ordenador, uso de sistemas operativos, gestión de archivos y carpetas.

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

- Competencia en Internet: Uso efectivo de motores de búsqueda, comprensión de URLs y navegación por sitios web.
- Herramientas de Comunicación: Uso de correo electrónico, mensajería instantánea, herramientas de videoconferencia (Zoom, Skype).
- Alfabetización en Redes Sociales: Comprensión de plataformas de redes sociales, gestión de configuraciones de privacidad, creación de contenido.

Integración de Habilidades Técnicas y Alfabetización Digital

Tanto las habilidades técnicas como la alfabetización digital son fundamentales en la fuerza laboral actual y en la vida cotidiana. Por ello, debemos incorporar tanto la formación técnica como los programas de alfabetización digital en el currículo educativo y fomentar el aprendizaje continuo y el desarrollo profesional a través de cursos en línea, talleres y certificaciones. Establecer políticas organizacionales que promuevan el uso responsable de la tecnología y la mejora continua de habilidades, así como desarrollar programas comunitarios para mejorar la alfabetización digital entre diversos grupos de edad y contextos socioeconómicos. Además, es esencial garantizar el acceso a la tecnología necesaria y a los recursos para el aprendizaje y la aplicación de tanto las habilidades técnicas como la alfabetización digital.

Al combinar habilidades técnicas con alfabetización digital, los individuos no solo pueden realizar tareas específicas de manera más efectiva, sino también navegar por el mundo digital de manera responsable y crítica.

Comprensión de la Información: Capacidad para buscar, evaluar y gestionar la información en línea de manera efectiva y crítica. Esto incluye reconocer fuentes fiables y detectar información falsa o sesgada. La comprensión de la información digital implica entender, interpretar y analizar críticamente la información proveniente de fuentes digitales. A medida que los medios digitales se convierten en la fuente principal de información para muchos, desarrollar estas habilidades es esencial para navegar por el mundo digital de manera efectiva y responsable. Debemos seguir los siguientes pasos para una comprensión completa:

- Primer paso: Evaluar la credibilidad y confiabilidad de las fuentes digitales, incluyendo sitios web, blogs y redes sociales. Identificar la autoría, la fecha de publicación y la intención detrás del contenido digital.

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

Cofinanciado por la Unión Europea

- Segundo paso: Evaluar la precisión y validez de la información encontrada en línea.
- Tercer paso: Reconocer sesgos, propaganda y desinformación en los medios digitales.
- Cuarto paso: Comprensión contextual, que implica interpretar la información digital dentro de su contexto más amplio, incluyendo perspectivas culturales, sociales e históricas, entendiendo cómo el contenido digital puede estar influenciado por su plataforma y audiencia.

Al desarrollar habilidades de comprensión de la información digital, las personas pueden navegar por las complejidades del mundo digital, tomar decisiones informadas y participar plenamente en la sociedad moderna.

Actuar de manera ética y responsable en el entorno digital, respetando las normas de conducta y las leyes relacionadas con el uso de las tecnologías digitales.

En resumen, la alfabetización digital es una competencia fundamental en el mundo moderno, que no solo mejora la capacidad de las personas para usar tecnologías, sino que también potencia su capacidad para participar de manera plena y efectiva en la sociedad digital. Promover y mejorar la alfabetización digital es esencial para crear una sociedad más equitativa.

Uno de los problemas más graves son las posibles violaciones de la ética de los datos (Knight, 2015). La ética de los datos se refiere al uso de datos de acuerdo con los deseos de las personas cuyos datos están siendo recopilados.

Las organizaciones enfrentan una creciente presión para manejar los datos de los consumidores de manera responsable y transparente. Por lo tanto, deben prestar atención a las cuestiones relacionadas con el uso de datos, la ética digital y la tecnología de privacidad. De hecho, las organizaciones no solo deben comprender los problemas éticos detrás de la recopilación de datos y el entorno regulatorio actual, sino que también deben implementar de manera proactiva un plan y práctica de ética de los datos.

El segundo factor es la normalización creciente de la recopilación de datos de la actividad en línea. Los usuarios generan datos cuando compran, utilizan motores de búsqueda o interactúan en redes sociales. Los datos pueden recopilarse de manera ética, como cuando los consumidores voluntariamente proporcionan su información a los minoristas. Sin embargo, la mayoría de las

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

veces, terceros sin una relación directa con los usuarios recopilan datos en línea a través de cookies u otras fuentes. Esta es una práctica éticamente cuestionable.

Algunas leyes están del lado de la protección del ciudadano/consumidor. Por ejemplo, bajo el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, las empresas deben obtener el consentimiento explícito de una persona para recopilar sus datos para cada propósito en el que se utilicen. Los sujetos de datos también pueden retirar su consentimiento en cualquier momento.

En otras partes del mundo, el panorama regulatorio de la privacidad de datos está en un estado similar de agitación. Dadas las leyes de privacidad dispares y las diferencias históricas y culturales entre los países, un enfoque unificado es poco probable. Sin embargo, la mayoría de los países comparten algunos elementos clave de protección de datos. Estos incluyen restricciones en las transferencias transfronterizas de datos personales, notificaciones en caso de una violación de datos y derechos de acceso y corrección individuales.

2.2. Comunicación online

La comunicación en línea efectiva es esencial en la era digital actual, ya sea para interacciones personales, colaboraciones profesionales o propósitos educativos. Para comprender los procesos, debemos hablar sobre los diferentes aspectos de la comunicación digital. La comunicación en línea se refiere al intercambio de información e ideas a través de plataformas digitales, que incluyen correos electrónicos, mensajería instantánea, videoconferencias, redes sociales y otros canales en línea.

Existen diferentes tipos de comunicación digital:

- Comunicación Sincrónica: Interacción en tiempo real, como videollamadas, chats en vivo y seminarios web.
- Comunicación Asincrónica: Respuestas diferidas, como correos electrónicos, publicaciones en foros y vídeos grabados.

Según el tipo de comunicación, nos enfocamos en criterios de selección:

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

- Propósito: Determinar el propósito de la comunicación, que podría ser una conversación informal, una reunión formal, un proyecto colaborativo, etc.
- Audiencia: Considerar las preferencias y capacidades técnicas de la audiencia.
- Evaluación de funciones: Evaluar características como el intercambio de archivos, videoconferencias, compartir pantalla e integración con otras herramientas.
- Seguridad: Asegurarse de que la plataforma ofrezca medidas de seguridad robustas para proteger la información sensible.

Plataformas populares que implican comunicación digital:

- Correos electrónicos: Gmail, Hotmail
- Mensajería instantánea: Slack, Microsoft Teams
- Videoconferencias: Zoom, Google Meet
- Herramientas de colaboración: Trello, Asana
- Redes sociales: Instagram, Facebook, WhatsApp, Twitter

Todas estas plataformas utilizan la comunicación digital para diferentes propósitos e involucran texto e imágenes que comunican de distintas maneras a la audiencia.

La ética en la comunicación en línea es crucial, ya que las plataformas digitales se vuelven cada vez más integrales en nuestras interacciones personales, profesionales y educativas. La comunicación en línea debe basarse en tratar a los demás con respeto, independientemente de las diferencias de opiniones, antecedentes o creencias, y evitar el uso de lenguaje inflamatorio, ataques personales o comentarios discriminatorios. Es importante ser transparente sobre tu identidad e intenciones al comunicarte en línea. Debes evitar prácticas engañosas, como usar identidades falsas o difundir desinformación, además de respetar la privacidad de los demás y no compartir información sensible sin su consentimiento.

En conclusión, al entender los diferentes tipos de comunicación en línea, elegir las plataformas adecuadas, adherirse a las mejores prácticas y mejorar

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

continuamente tus habilidades, podrás comunicarte de manera más efectiva y alcanzar tus metas personales y profesionales.

2.3. Identidad digital y huellas digitales

A. La **identidad digital** y las huellas digitales se refieren a la presencia y actividades en línea que las personas crean a medida que interactúan y participan en entornos digitales. La identidad digital es la representación de la identidad de una persona en línea. Incluye información personal, comportamiento en línea, interacciones y actividades a través de diversas plataformas digitales.

Componentes de la Identidad Digital:

- Información Personal: Nombre, edad, género, ubicación y otros detalles identificables compartidos en línea.
- Perfiles en Línea: Perfiles en redes sociales, perfiles en redes profesionales (como LinkedIn) y cuentas en varios sitios web.
- Comportamiento en Línea: Interacciones, publicaciones, comentarios, "me gusta", compartidos y contribuciones en diversas plataformas digitales.
- Activos Digitales: Contenido creado y compartido en línea, como fotos, videos, blogs y artículos.

La identidad digital influye en cómo las personas son percibidas en línea y puede afectar las oportunidades en educación, empleo e interacciones sociales. Es crucial para la gestión de la privacidad, la seguridad y la reputación en el ámbito digital.

B. La **huella digital** se refiere al rastro de datos que deja una persona a través de sus actividades en línea. Abarca todas las interacciones y contribuciones digitales realizadas en internet.

Tipos de Huellas Digitales:

- Huella Activa: Acciones intencionales, como publicaciones en redes sociales, comentarios, cargas e interacciones.

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

- Huella Pasiva: Datos recopilados sobre una persona a través de actividades en línea, como el historial de navegación, cookies y transacciones digitales.

Características de la Huella Digital:

- Permanencia: La información compartida en línea puede permanecer accesible y ser rastreable indefinidamente.
- Visibilidad: Las huellas digitales pueden ser visibles para otros, influyendo en cómo se percibe a las personas en línea.
- Impacto: Las huellas digitales pueden afectar la reputación, la privacidad y las oportunidades en educación, empleo y relaciones personales.

Para gestionar tu huella digital, debes seguir los siguientes pasos:

- Configuración de privacidad: Ajusta las configuraciones de privacidad en redes sociales y otras plataformas para controlar quién puede ver tu información.
- Piensa Antes de Compartir: Considera el impacto potencial de tus publicaciones y contribuciones antes de compartir en línea.
- Monitoreo y Limpieza: Revisa regularmente tu huella digital, elimina contenido desactualizado o irrelevante y gestiona tus perfiles en línea.
- Transparencia: Sé transparente sobre cómo se usa y comparte tu información personal en línea.
- Respeto: Respeta la privacidad de los demás, los derechos de propiedad intelectual y los límites digitales.
- Responsabilidad: Asume la responsabilidad de tus acciones en línea y de tu huella digital.

Comprender la identidad digital y las huellas digitales es esencial para navegar de manera efectiva en el entorno digital. Al entender primero el uso y las formas de comunicación en línea, puedes mejorar tu presencia en línea, proteger tu privacidad y construir una reputación digital positiva.

2.4. Privacidad y Seguridad

Privacidad en la comunicación digital se refiere al derecho de las personas a controlar la recopilación, el uso y la difusión de su información personal transmitida a través de canales digitales.

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

Preocupaciones clave en la privacidad de la comunicación digital:

- Recopilación de datos: Evitar la recopilación no autorizada de datos personales por parte de terceros.
- Compartición de datos: Controlar quién tiene acceso a la información personal y cómo se comparte.
- Consentimiento: Asegurarse de que las personas otorguen un consentimiento informado antes de que sus datos sean recopilados o utilizados.

Smith (2021) enfatiza la importancia de la ciberseguridad para proteger los datos sensibles. La **seguridad** en la comunicación digital se refiere a las medidas adoptadas para proteger la integridad, confidencialidad y disponibilidad de los datos transmitidos y almacenados en línea.

Preocupaciones clave:

- **Ciberataques:** Protección contra el acceso no autorizado, malware, phishing y otras amenazas cibernéticas. Los ciberataques son actividades maliciosas llevadas a cabo a través de canales digitales con la intención de comprometer sistemas informáticos, redes o dispositivos, y de robar, alterar o destruir datos. Estos ataques pueden tener graves consecuencias para individuos, empresas y organizaciones. Los más comunes son: **Malware**, software malicioso diseñado para infiltrarse o dañar un sistema informático sin el consentimiento del usuario. Algunos ejemplos incluyen virus, gusanos, ransomware y spyware. El impacto de los atacantes cibernéticos incluye la interrupción de operaciones, el robo de información sensible o la exigencia de pagos de rescate. **Phishing**, un ataque fraudulento que intenta obtener información sensible (como nombres de usuario, contraseñas, detalles de tarjetas de crédito) haciéndose pasar por una entidad confiable. Ejemplos comunes hoy en día incluyen correos electrónicos falsos, sitios web o mensajes que parecen legítimos pero están diseñados para engañar a los usuarios. El impacto incluye robo de identidad, pérdidas financieras y acceso no autorizado a cuentas. **Denegación de Servicio (DoS)**, otro ejemplo de ciberataque que implica abrumar una red, servidor o sitio web con una avalancha de tráfico para interrumpir sus operaciones normales. Las consecuencias incluyen inundar un servidor con solicitudes excesivas o coordinar ataques desde múltiples fuentes, lo que produce un impacto

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

directo en la interrupción del servicio, la pérdida de ingresos y daños a la reputación.

¿Cómo podemos mitigar los ciberataques?

- Implementar cortafuegos, software antivirus y sistemas de detección de intrusos para proteger contra malware y accesos no autorizados.
- Realizar capacitaciones en ciberseguridad para enseñar a los empleados y a las personas a reconocer intentos de phishing y otras tácticas de ingeniería social.
- Actualizar regularmente el software, sistemas operativos y aplicaciones para corregir vulnerabilidades y proteger contra amenazas de seguridad conocidas.
- Utilizar contraseñas fuertes y únicas, y habilitar la autenticación multifactor para agregar una capa adicional de seguridad al acceder a cuentas y sistemas.

Leyes de Protección de Datos:

Familiarízate con las regulaciones de protección de datos, como el GDPR (Reglamento General de Protección de Datos) en Europa. Asegúrate de cumplir con los requisitos legales relacionados con la recopilación, procesamiento y almacenamiento de datos.

En conclusión, la privacidad y la seguridad en la comunicación digital son esenciales para proteger la información personal, mantener la confianza y mitigar los riesgos asociados con las amenazas cibernéticas. Manteniéndose informado sobre las amenazas emergentes y priorizando las consideraciones éticas, las personas y las organizaciones pueden mejorar su resiliencia digital y proteger eficazmente la información sensible.

2.5 Recomendaciones para hábitos responsables

Hábitos responsables de ciberseguridad son esenciales para proteger la información personal y mantener la seguridad digital. Al implementar las siguientes prácticas recomendadas, los usuarios pueden mejorar significativamente su postura de ciberseguridad y ayudar a protegerse contra diversas amenazas cibernéticas.

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

- Usar contraseñas fuertes y únicas: Crea contraseñas complejas utilizando una combinación de letras (tanto mayúsculas como minúsculas), números y símbolos. Evita usar la misma contraseña en varias cuentas. Considera el uso de un administrador de contraseñas para llevar un registro de ellas y generar contraseñas seguras.
- Mantener el software actualizado: Actualiza regularmente los sistemas operativos, aplicaciones y software antivirus para protegerte contra las amenazas más recientes. Habilita las actualizaciones automáticas cuando sea posible.
- Ser cauteloso con las estafas de phishing: No hagas clic en enlaces ni abras archivos adjuntos en correos electrónicos o mensajes no solicitados. Verifica la autenticidad de las solicitudes de información personal.
- Asegurar tus dispositivos: Utiliza programas antivirus y antimalware. Protege tus dispositivos con una contraseña, PIN o método biométrico.
- Usar conexiones seguras: Evita usar Wi-Fi público para transacciones sensibles; si es necesario, usa una red privada virtual (VPN). Asegúrate de que los sitios web sean seguros (busca "https://" en la URL) antes de ingresar información personal.
- Limitar la compartición de información personal: Sé cauteloso con la cantidad y el tipo de información personal que compartes en línea. Revisa la configuración de privacidad en las plataformas de redes sociales y ajustala para obtener la máxima seguridad.

3 Actividades Prácticas:

Esta sección contiene 15 actividades prácticas divididas en los 4 temas principales de la guía: Alfabetización Digital, Comunicación Digital, Identidad Digital, Privacidad y Seguridad.

Cada actividad sigue la siguiente estructura: Nombre, Objetivo, Necesidades, Material necesario e Instrucciones para realizarla. Si es necesario, añadimos infografías o imágenes para ayudar al usuario a realizar la actividad o ejemplos en caso de que se requieran.

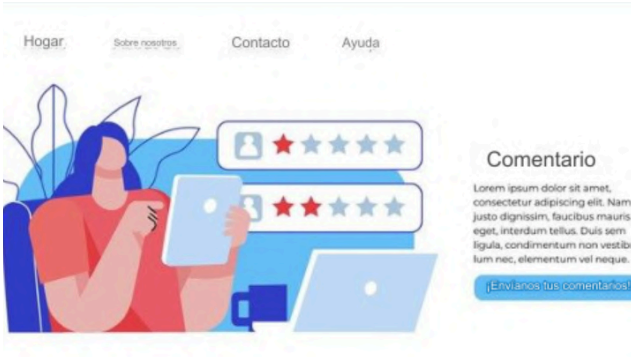
Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

Las imágenes utilizadas en esta sección provienen de capturas de pantalla de las páginas citadas para la actividad (Facebook, Google, etc.) y de imágenes creadas con IA a través de freepik.es, utilizadas legalmente como imágenes gratuitas.

El orden de las actividades puede ser alterado según tu conveniencia.

A: Alfabetización Digital

1: Actividad: "Evaluando Fuentes En Línea"



El objetivo de esta actividad es aprender a evaluar la credibilidad de las fuentes en línea. Basado en esto, las necesidades están relacionadas con el conocimiento de la investigación en línea con veracidad. Para realizar esta actividad, el material necesario será un ordenador o tableta con acceso a Internet. Esta actividad dura 40 minutos y debe realizarse en parejas.

La actividad consiste en una lista de sitios web que se te proporcionarán para que evalúes la fiabilidad, exactitud y sesgo de cada sitio. Los criterios pueden incluir la verificación de las credenciales del autor, el dominio del sitio web y la comparación de la información con fuentes confiables. Primero, verás un ejemplo.

Ejemplo:

www.cdc.gov

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

Los siguientes son ejemplos de la información que debes buscar en los sitios web para la actividad:

- Credenciales del autor: Los artículos e información suelen estar escritos por expertos en salud pública, epidemiología e investigación médica.
- Dominio del sitio web: .gov (sitio web oficial del gobierno, altamente confiable).
- Comparación de información: El CDC es una fuente primaria de información en salud pública y es ampliamente referenciada por otras fuentes reputadas.
- Sesgo y objetividad: Generalmente objetivo, enfocado en información basada en evidencias, aunque puede existir alguna influencia política dado que es una agencia gubernamental.

Ahora, por favor revisen las páginas web para evaluar en parejas:

www.naturalnews.com

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

www.nytimes.com

www.snopes.com

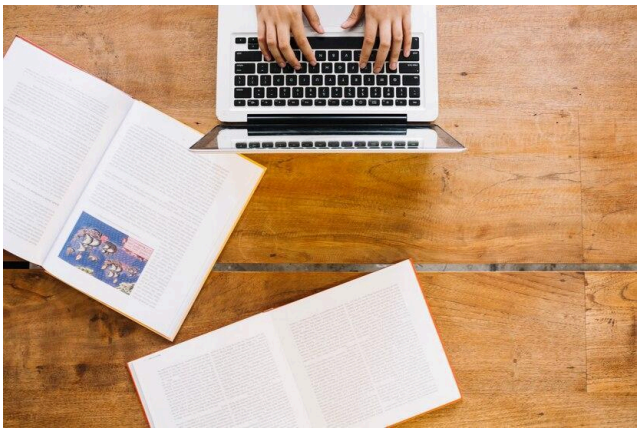
El siguiente paso es la evaluación: la siguiente lista de criterios de calidad ha sido creada como una guía para que puedas evaluar tantos aspectos como sea posible de las diferentes páginas web sugeridas:

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

- Verifica los antecedentes del autor: Busca información sobre las calificaciones, experiencia y otros artículos escritos por el autor. Los autores con títulos relevantes, experiencia profesional y un historial de reportes precisos son más creíbles.
- Dominios gubernamentales y educativos: Los sitios que terminan en .gov, .edu y organizaciones confiables con dominio .org son generalmente fiables.
- Dominios comerciales: Los sitios con dominios .com y .net requieren más escrutinio, ya que pueden ser propiedad de cualquier persona.
- Verifica si otros sitios reputables informan lo mismo.
- Sitios de verificación de hechos: Utiliza sitios como Snopes, FactCheck.org o PolitiFact para verificar afirmaciones.
- Identifica el sesgo: Analiza el lenguaje utilizado (¿es neutral o emocional?), el rango de perspectivas presentadas y las fuentes de financiamiento del sitio. Evalúa si el sitio proporciona puntos de vista equilibrados o promueve una agenda específica.

Después de discutir y revisar todos los sitios web, toma tus decisiones de acuerdo con los criterios, y toma notas, ya que en las actividades 2, 4 y 5 necesitarás esa primera investigación sobre los sitios web mencionados anteriormente.

2: Actividad: "Técnicas de Búsqueda Avanzada"



El objetivo de esta actividad es mejorar las habilidades de búsqueda en motores de búsqueda. Según esto, las necesidades son operadores de búsqueda avanzada (por ejemplo, comillas para frases exactas, signos menos para excluir términos) y herramientas de búsqueda específicas como Google

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

Scholar para artículos académicos. Para realizar esta actividad, el material necesario es un ordenador o tableta con conexión a internet.

Instrucciones: Utiliza operadores de búsqueda avanzada y Google Scholar para encontrar artículos académicos sobre los impactos del cambio climático en la biodiversidad o en otros temas que te interesen. Esta actividad dura 40 minutos.

El primer paso será formular una pregunta o tema de investigación específico relacionado con el cambio climático y la biodiversidad. Ejemplo: "¿Cómo afecta el cambio climático a la biodiversidad en las selvas tropicales?"

Ten en cuenta los siguientes consejos:

- Usa operadores de búsqueda avanzada: Comillas (" "): Busca frases exactas. Ejemplo: "impactos del cambio climático en la biodiversidad"
- Signo menos (-): Excluye términos para reducir los resultados. Ejemplo: impactos del cambio climático en la biodiversidad -marina
- Site: Limita tu búsqueda a dominios o sitios específicos. Ejemplo: site.google.com impactos del cambio climático en la biodiversidad
- Filetype: Si es necesario, especifica el tipo de archivo para documentos. Ejemplo: impactos del cambio climático en la biodiversidad filetype

Ahora es el momento de realizar la búsqueda utilizando Google Scholar (scholar.google.com) para llevar a cabo tu investigación.

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

Por favor, ingresa tu consulta de búsqueda refinada utilizando los operadores avanzados mencionados anteriormente. Luego, revisa los resultados de la búsqueda y evalúa la relevancia de cada artículo en función de los títulos, resúmenes y palabras clave. Verifica las citas y el número de veces que el artículo ha sido referenciado (si está disponible) para evaluar su impacto y relevancia. Haz clic en los enlaces para acceder a los artículos completos directamente desde Google Scholar o a través del acceso a la biblioteca de tu institución. Lee los artículos seleccionados cuidadosamente, enfocándose en la metodología, hallazgos y conclusiones relacionadas con los impactos del cambio climático en la biodiversidad. Después de completar los pasos, resume los puntos clave y conocimientos obtenidos de cada artículo. Por favor, mantén esta información disponible ya que la necesitarás para la siguiente actividad 3.

Aquí puedes encontrar una tabla con los aspectos de evaluación y un ejemplo:

Link	Título	Abstracto	Palabras clave
EJEMPLO https://www.science.org/doi/abs/10.1126/science.1131758	¿Cómo Afecta el Cambio Climático a la Biodiversidad?	El cambio climático es un factor crítico en la pérdida de biodiversidad, afectando ecosistemas y especies en todo el mundo. Este artículo revisa los impactos multifacéticos del cambio climático en la biodiversidad, con	Cambio Climático Biodiversidad Selvas Tropicales Incremento de la Temperatura Patrones de Precipitación Distribución de Especies Degradación del Hábitat Riesgo de Extinción

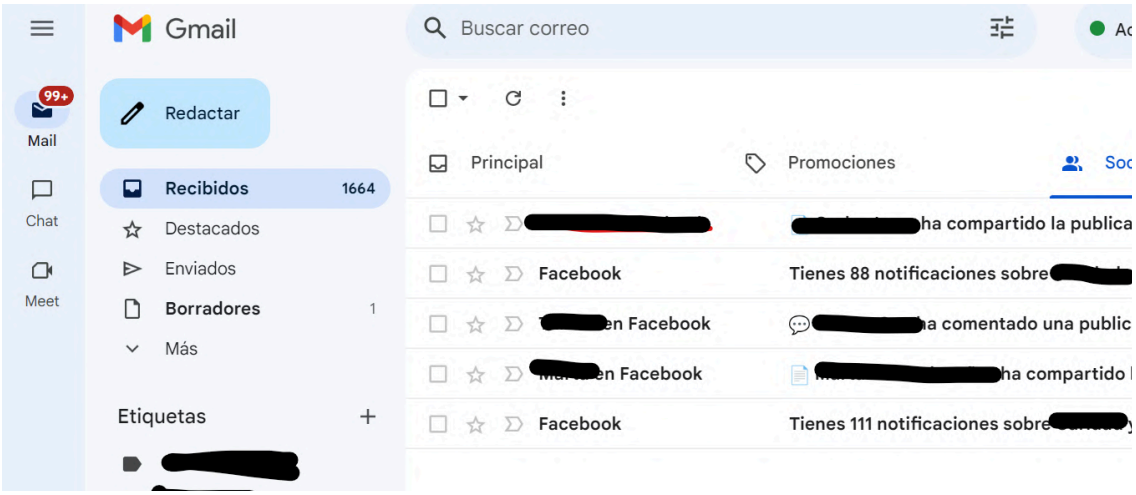
Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

		un enfoque en las selvas tropicales.	Esfuerzos de Conservación Disrupción del Ecosistema Enfermedades y Plagas Adaptación al Clima

3: Actividad: Proyecto de Colaboración Virtual

El objetivo de esta actividad es hacer uso de herramientas digitales para la colaboración, y las necesidades cubiertas son herramientas de colaboración como Google Docs. El propósito de la actividad es evaluar y practicar tu capacidad para comunicarse, compartir recursos y gestionar tareas de manera efectiva. Para realizar esta actividad, el material necesario son las actividades 1 y 2 de esta sección completadas, un ordenador y conexión a internet.

Ahora es el momento de realizar la actividad, que tomará 40 minutos. Utiliza Google Docs para colaborar con otros compañeros o colegas. Abre tu cuenta de Gmail y haz clic en la esquina superior derecha para encontrar Google Docs. Hay muchas formas de abrirlo, pero usemos esta manera sencilla:

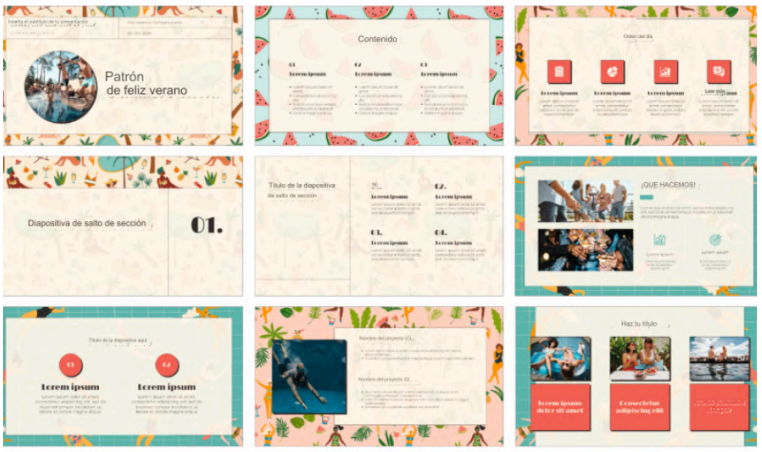


Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

El siguiente paso es que crees un nuevo documento. Todos, de manera individual en ordenadores separados, pueden agregar información al mismo tiempo. Por favor, utiliza la investigación y las notas de las Actividades 1 y 2.

Verás cómo puedes crear el mismo documento sin la necesidad de estar juntos en la misma habitación y usando el mismo ordenador. Puedes compartir el documento para que diferentes personas puedan agregar información simultáneamente. Las siguientes imágenes muestran las instrucciones para realizarlo correctamente.

4: Actividad: Presentación Multimedia



Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

El objetivo de esta actividad es desarrollar habilidades en la creación de presentaciones digitales. Cubre Alfabetización Digital y Comunicación Digital. Las necesidades cubiertas son un tema para presentar utilizando Google Slides, y el material necesario será un ordenador con conexión a internet. Esta actividad toma más de 1 hora para realizarla correctamente.

La presentación digital también puede realizarse con el uso de un complemento de IA como Slide AI, que puede mejorar tu presentación automatizando elementos de diseño, generando contenido y proporcionando recomendaciones inteligentes. La inteligencia artificial utilizada puede ayudar a generar viñetas o hechos clave sobre tu presentación.

Ahora es el momento de practicar. Utiliza el tema de las actividades anteriores 1, 2 y 3 para presentar utilizando Google Slides. Deberías incorporar texto, imágenes, videos y elementos interactivos para crear una presentación convincente. La siguiente imagen te ayudará a comenzar. Cuando puedas abrir las opciones de Google, busca Slides, haz clic y se abrirá para comenzar la creación:

Compila tus hallazgos en un informe o presentación que resuma el entendimiento actual sobre los impactos del cambio climático en la biodiversidad basado en la literatura académica. Puedes cambiar las imágenes, incluir, eliminar, duplicar, etc.

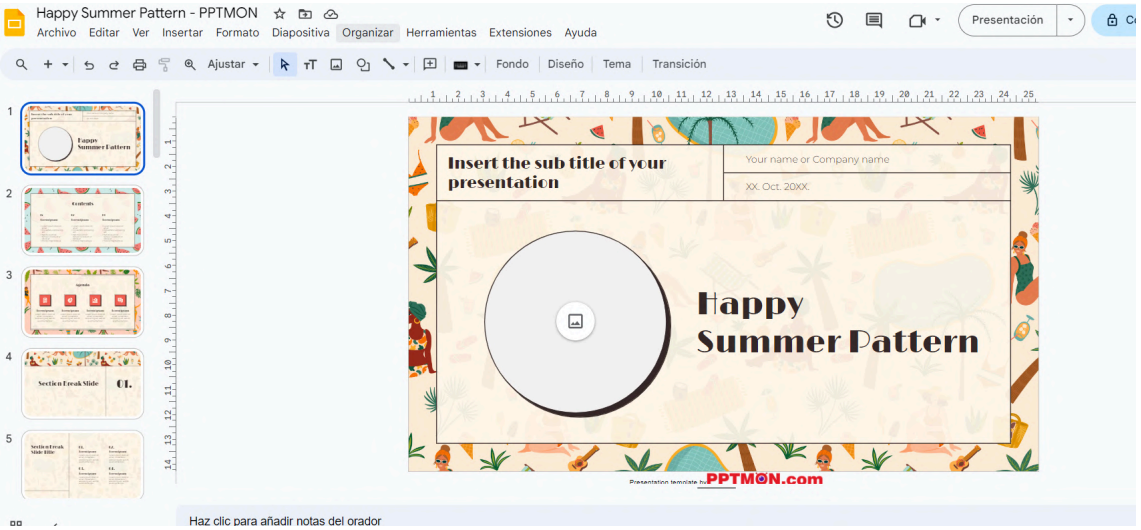
Por favor, asegúrate de incluir referencias a los artículos que utilizaste y discute cualquier punto de vista conflictivo o lagunas en la investigación.

El máximo es de 9 diapositivas, incluyendo la portada, el índice al comienzo, y las referencias, saludos y detalles de contacto al final. La siguiente imagen es un ejemplo, algunas plantillas son gratuitas, encuentra aquí el tema "Happy summer".

Usa el ejemplo, encuentra aquí la plantilla:

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

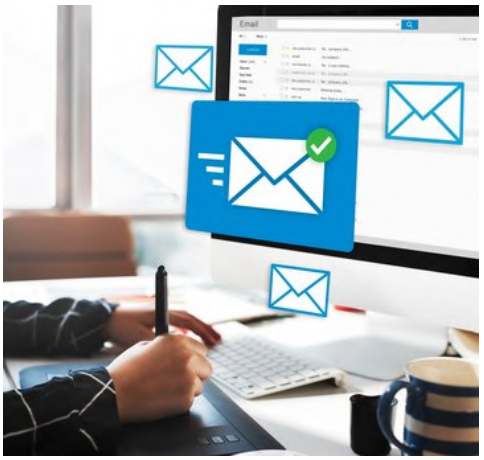
https://docs.google.com/presentation/d/1_7leG7vQNruGATabXvQm-4WqIAIlV8SX1KKWId8DTDY/template/preview



¡Ahora es el momento de prepararse en grupos de dos y presentarlo! ¡Buena suerte!

B: Comunicación Digital

1: Actividad: "Solicitar un Lugar"



El objetivo de la siguiente actividad es aprender a redactar un correo electrónico formal. Las necesidades cubiertas son, comunicación digital formal/informal para solicitar un lugar para una actividad. Según las necesidades, el material necesario para realizar la actividad será ordenadores

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

o tablets y dispositivos móviles, con acceso a Internet. Cuenta de correo electrónico activa para cada participante. Esta actividad tomará 20 minutos para realizarse.

Ahora es tiempo de practicar, primero tienes una sugerencia con algunos detalles. La estructura básica de un correo electrónico formal sería incluir saludos, cuerpo del mensaje y despedidas. Luego agrega el asunto con una línea de texto breve y clara que indique el propósito del correo.

Saludo Formal, como "Estimado/a [Nombre]." Después de esto puedes escribir el cuerpo, con información clara y directa sobre la solicitud. Para finalizar el correo, despídete de manera cortés, como "Atentamente" o "Saludos cordiales." Finalmente tu firma con nombre completo e información de contacto.

Ahora es tu turno. Aquí tienes un ejemplo:

Asunto: Solicitud de Lugar en la Clase de Baile

Estimado/a [Nombre del Instructor o Persona Responsable],

Le escribo para solicitar un lugar en la clase de baile que se impartirá los [días de la semana] a las [hora] en [lugar].

Me apasiona la danza y me encantaría tener la oportunidad de unirme a su clase para mejorar mis habilidades y disfrutar del ambiente.

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

Agradecería que me informara sobre la disponibilidad y los pasos a seguir para inscribirme.

Quedo a la espera de su respuesta.

Atentamente,

[Nombre completo]

[Teléfono de contacto]

[Correo electrónico]

Escritura Individual: Por favor, escribe tu propio correo utilizando la guía proporcionada.

Después de finalizar, el grupo revisará y dará retroalimentación. Los participantes intercambian correos electrónicos para revisarlos y proporcionar comentarios constructivos. Discutan en grupo los puntos fuertes y las áreas de mejora. Envía el correo a los participantes y envía el correo real a la persona a cargo de la clase de baile, o un correo de prueba a un instructor.

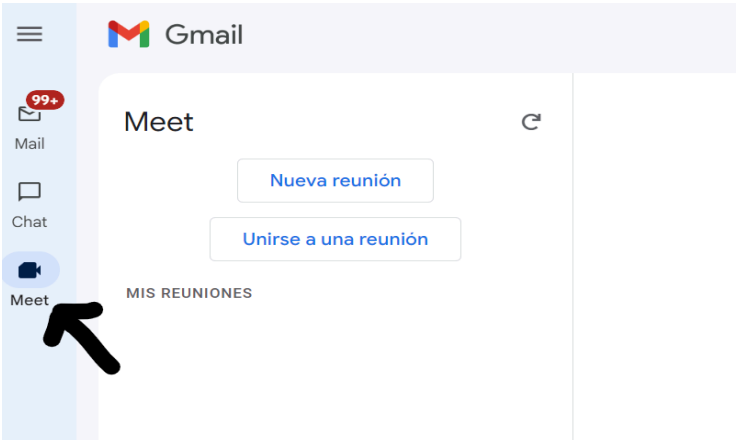
2: Actividad: "¿Podríamos tener una reunión?"

El objetivo de la actividad es aprender a crear, programar y unirse a una sesión en línea y familiarizarse con sus funciones básicas. Usaremos la opción más popular, aunque existen muchas: Google Meet. Las necesidades cubiertas son volverse cómodos con la creación y gestión de sesiones en Google Meet, lo

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

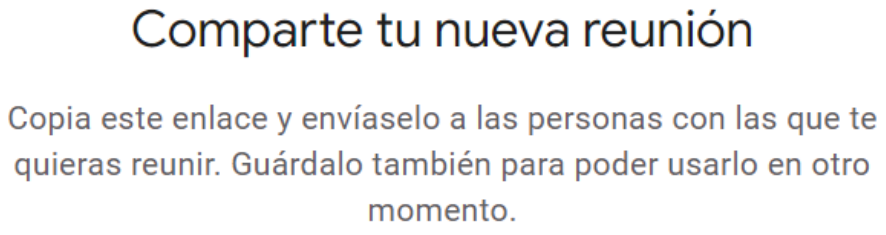
que les permitirá mantenerse conectados e involucrados en el mundo digital para comunicarse en línea. El material necesario son ordenadores o tablets con acceso a Internet y cuentas de Google para cada participante.

Ahora es tiempo de practicar, esta actividad tomará 30 minutos. Navega a Gmail y haz clic en el icono de 'Meet' ubicado en el panel izquierdo. Selecciona la reunión a la que deseas unirte y haz clic en 'Unirse ahora'.



Otra opción es crearla y ser el anfitrión, abre un navegador web y ve a Google Meet.

Haz clic en "Nueva reunión" y selecciona "Crear una reunión para más tarde" o "Iniciar una reunión instantánea" o la opción del Calendario de Google.

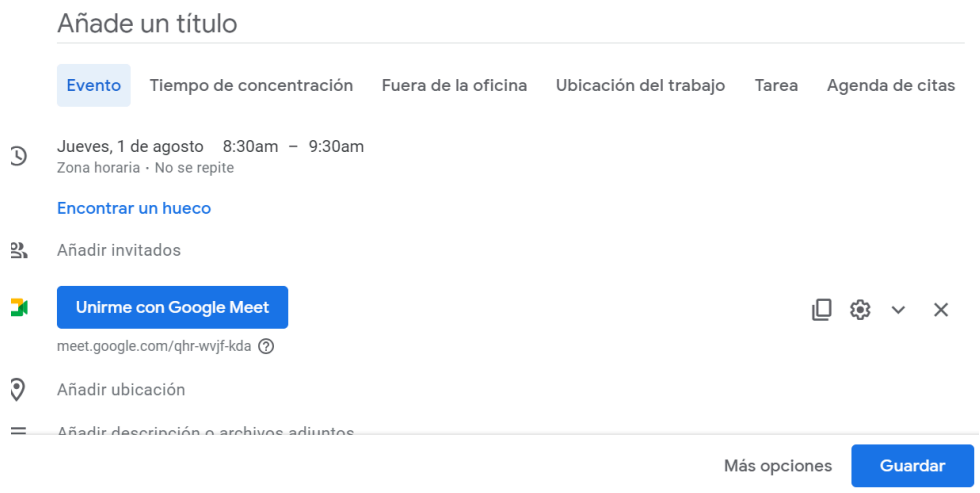


(Si tienes el enlace proporcionado, entonces copia el enlace directamente. Copia el enlace de la reunión proporcionado.)

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

Para unirse a una reunión de Google Meet sin una cuenta de Google, el participante debe recibir un enlace o código de conferencia del anfitrión de la reunión. Es importante destacar que estos usuarios no pueden iniciar una reunión por sí mismos. Además, solo pueden unirse a una reunión utilizando la versión de escritorio de Google Meet, ya que la aplicación móvil no es accesible sin una cuenta de Google.

Ahora es momento de crear tus propias sesiones de Google Meet siguiendo los pasos demostrados.



Programar una reunión en Google Meet: Abre Google Meet. Los participantes deben programar una sesión de Google Meet e invitar a 2 compañeros más de la clase.

Unirse a una sesión de Google Meet: Revisa la configuración de audio y video antes de unirte. Asegúrate de entender cómo silenciar/activar tu micrófono y cómo encender/apagar tu cámara. Familiarízate con la función de chat, compartir pantalla y cambiar el diseño.

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

En grupos de tres, practiquen reuniones en línea juntos. ¡Bien hecho!

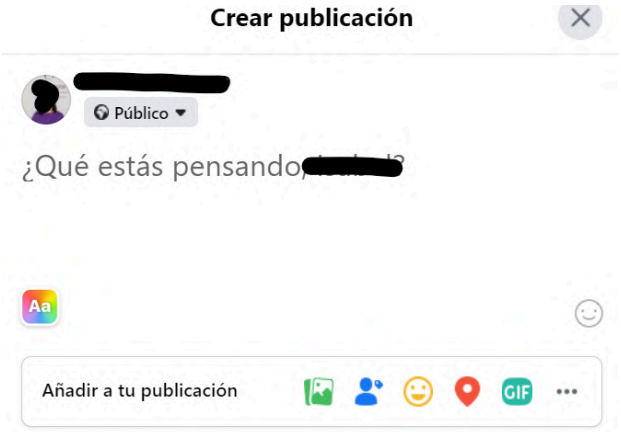
3. Actividad: “Compartiendo mi viaje”

El orden de las actividades puede ser alterado según tu conveniencia. En ese caso, te recomendamos realizar la actividad "Creación de Perfil" (Actividad 2) de la siguiente sección D: Identidad Digital. Después de crear tu perfil (si no tienes uno ya), deberías regresar a esta actividad.

El objetivo de esta actividad es aprender cómo nos comunicamos en las redes sociales. Para realizar la actividad, la necesidad cubierta es la capacidad de compartir información en las redes sociales con seguridad, y para llevarla a cabo, el material necesario será una conexión a internet, una ordenador portátil o tableta, y un perfil de Facebook. Para hacer una publicación con una foto, es posible editar la imagen desde Facebook antes de publicarla, así como etiquetar a una persona y agregar otros elementos.

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

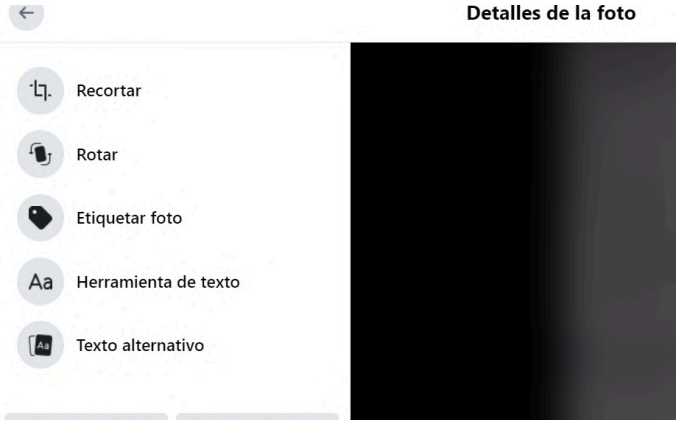
Cofinanciado por la Unión Europea



Para crear una publicación con foto en Facebook, deberás seguir estos pasos. Esta actividad tomará 30 minutos.

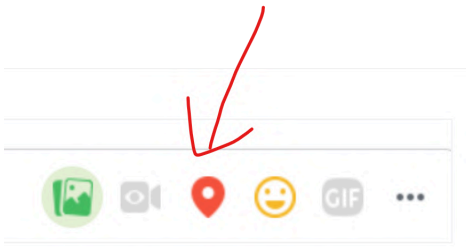
Primer paso: Inicia sesión en Facebook. En el espacio que dice "¿Qué estás pensando?", haz clic en Foto/Video. Selecciona la foto que deseas subir a la publicación. (Ten en cuenta que debes usar fotos de personas que ya te hayan dado su consentimiento para publicarlas, y trata de no publicar fotos de rostros de niños). En cualquier caso, puedes practicar con una foto que tomaste en tu último viaje, sin personas involucradas. Si deseas editar la foto, haz clic en el pequeño ícono con el pincel que dice: Editar foto. Las siguientes imágenes te ayudarán.

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.



Desde la ventana de edición es posible: agregar un filtro, etiqueta, añadir texto, recortar la foto y añadir emojis. Después de editarla, haz clic en Guardar. Para agregar una emoción o actividad relacionada con la foto, haz clic en Sentimiento/actividad.

Elige la ubicación relacionada con la publicación que estás haciendo. Por ejemplo, si subes una foto de tu viaje, puedes elegir la opción de Ubicación y añadir el lugar.



¡¡¡¡¡Haz click en COMPARTIR!!!!! ¡Tu publicación está lista! ¡Enhorabuena!

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

C: Identidad Digital

1. Actividad: "Mapea tu Huella Digital"

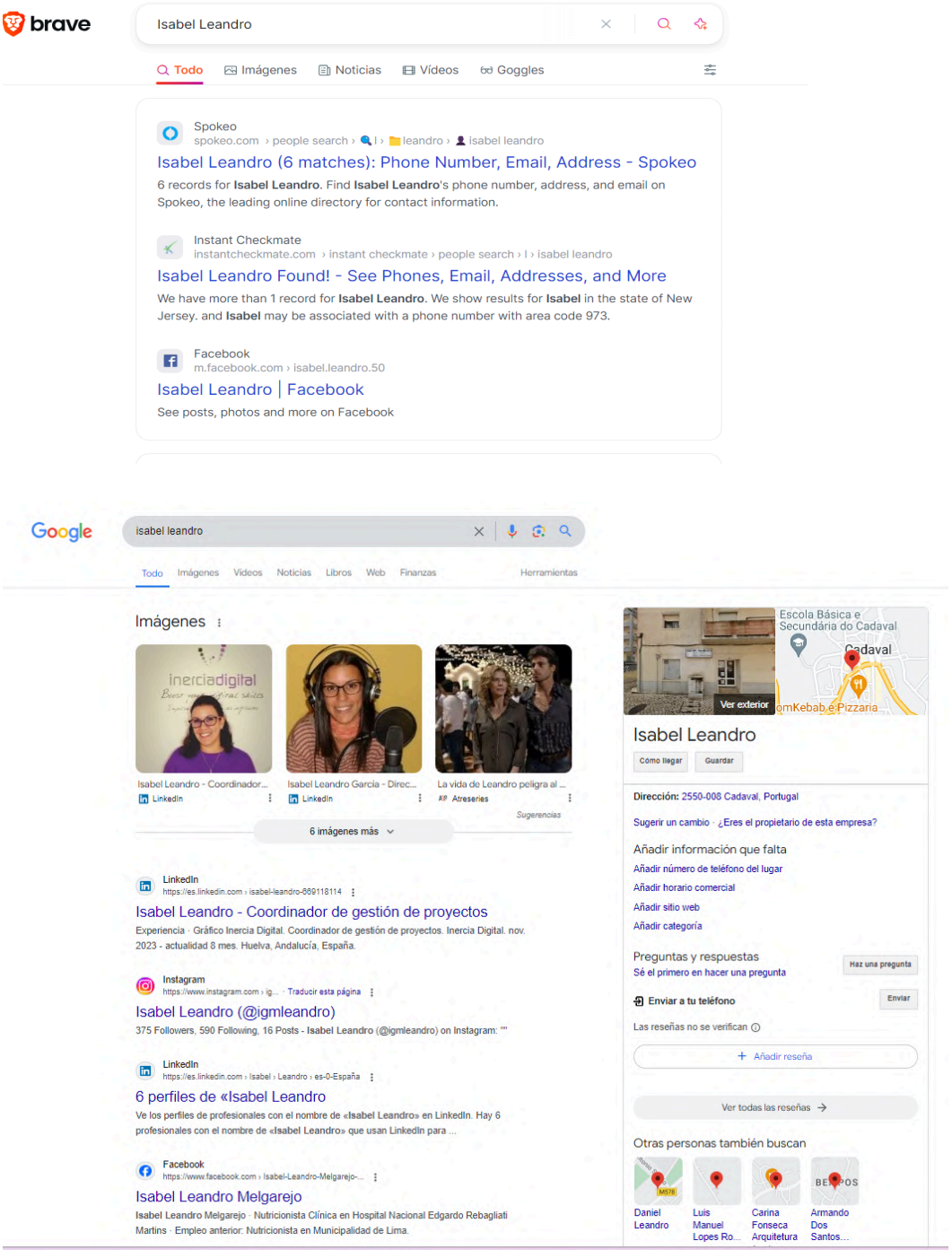
El objetivo de la siguiente actividad es comprender qué información está disponible públicamente sobre uno mismo en línea. La necesidad cubierta es la concienciación sobre la huella digital y la importancia de proteger la información personal. Para realizarla, los materiales necesarios serán ordenadores/tablets con acceso a internet, proyector/pantalla, papel y bolígrafos.

Ahora es momento de practicar, esta actividad tomará 20 minutos. Cada vez que usas Internet, dejas un rastro de información conocido como tu huella digital. Una huella digital crece de muchas maneras: por ejemplo, cuando publicas en redes sociales, te suscribes a un boletín, deja una reseña online o compras online.

Pide a los participantes que busquen sus nombres en varios motores de búsqueda. Usa los motores de búsqueda para verificar tu huella digital. Introduce tu nombre en los motores de búsqueda. Incluye tu nombre y apellido, y cualquier variación en la ortografía. Si cambiaste tu nombre, busca tanto el nombre actual como el anterior. Podemos utilizar: Brave, Google, Yahoo. Las siguientes figuras son ejemplos con el nombre: Isabel Leandro.

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

Cofinanciado por la Unión Europea



Toma nota de la información personal que encuentres. Revisar los resultados de la búsqueda te dará una idea de qué información sobre ti está disponible

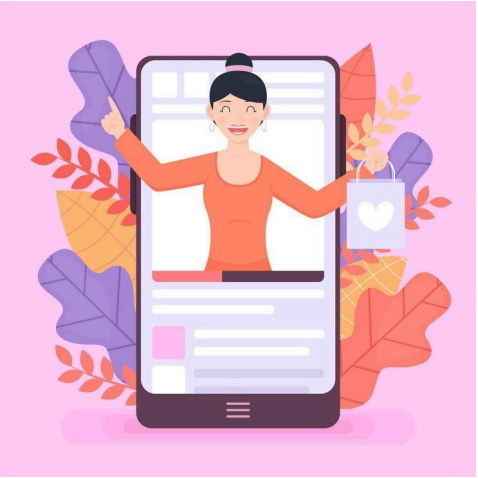
Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

públicamente. Si alguno de los resultados te muestra de manera negativa, puedes contactar al administrador del sitio para ver si pueden eliminarlo. Configurar Google Alerts (o cualquier otro motor de búsqueda que uses habitualmente) es una forma de monitorear tu nombre. Revisa la configuración de privacidad de tus redes sociales y asegúrate de que estén en un nivel con el que te sientas cómodo. Elimina cuentas inactivas para minimizar tu exposición a posibles filtraciones de datos. Usa contraseñas fuertes y asegúrate de utilizar diferentes contraseñas robustas para cada cuenta. Sé consciente de tus acciones en línea. Es importante ser consciente de tus acciones en línea y cómo pueden afectar tu huella digital.

Discute en pequeños grupos. ¿Cuántas veces aparece tu nombre real y está relacionado con qué? ¿Hay alguna página con la que no estés relacionado?

Discute cómo podría ser utilizada esta información por otros y la importancia de gestionar la propia huella digital. La huella digital es el rastro de datos que dejas cuando usas Internet. Es importante ser consciente de la importancia de tu huella digital, cómo se utiliza, y tomar medidas para proteger tu privacidad y seguridad en línea.

2. Actividad: "Creación de un Perfil"



El objetivo de esta actividad es desarrollar una presencia en línea (perfil). Las necesidades cubiertas son evaluar la completitud y coherencia de los perfiles creados. El material necesario será una ordenador o tableta con conexión a Internet.

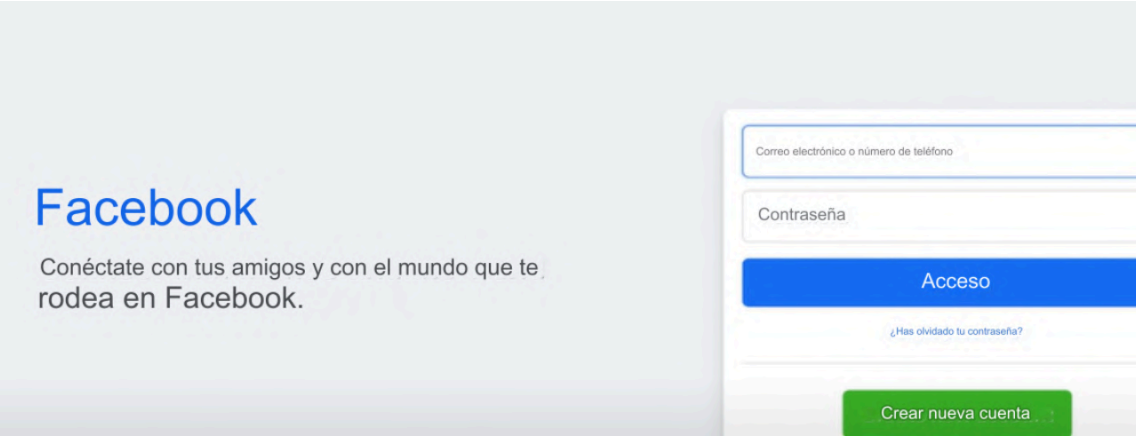
Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

Ahora es momento de practicar, esta actividad tomará 30 minutos. Crea o actualiza tus perfiles de Facebook o perfiles equivalentes. Esto incluye escribir un titular atractivo, un resumen, listar experiencias laborales, educación, antecedentes, habilidades y obtener recomendaciones. Luego, sigue algunas páginas que te interesen. Completa tanto como sea posible tu perfil y prepara las fotos que deseas subir. Aquí tienes algunos consejos, como usar una contraseña segura. No la compartas. Ten cuidado con la información que compartes. Puedes usar "Soporte de Facebook" para cualquier pregunta.

Encuentra aquí un enlace muy útil que podría ayudarte a evaluar la seguridad de la contraseña y que puede ser útil en el proceso de esta actividad:

https://password.kaspersky.com/es/

Las siguientes imágenes te ayudarán a encontrar la información para realizar la actividad. Primero, abre la página de Facebook y haz clic en "Crear una cuenta".



Entonces, completa la información requerida:

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

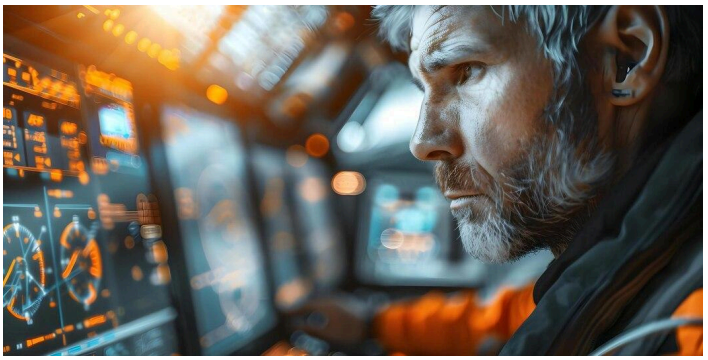
Recibirás un e-mail con un código que debes introducir.

Una vez que hayas creado y abierto tu cuenta, puedes comenzar a subir las fotos de perfil y agregar tu información en las diferentes secciones, como intereses, antecedentes, etc.

¡Compártelo con compañeros y trata de hacer amigos!

3. Actividad 3: Estudio de Caso de Análisis

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.



El objetivo de esta actividad es aprender de ejemplos del mundo real sobre la gestión de la identidad digital para comprender estrategias efectivas y errores comunes. Las necesidades cubiertas son para los participantes que analizarán estudios de caso de figuras públicas o empresas que han gestionado con éxito o han dañado sus identidades digitales. Este análisis ayudará a los participantes a identificar estrategias clave, entender el impacto de la identidad digital en la reputación y aplicar estas lecciones a la gestión de su propia identidad digital. Para realizar la actividad, se necesitará un ordenador con acceso a Internet. La actividad tomará 25 minutos para realizarse.

Ahora es momento de practicar. Se presentará una variedad de estudios de caso que destacan tanto la gestión exitosa como la fallida de la identidad digital. Aquí puedes encontrar un caso positivo que muestra el uso estratégico de las redes sociales por parte de Taylor Swift, la participación de la NASA en Twitter, o la exitosa gestión de crisis de una empresa, como la respuesta de Tylenol al envenenamiento en la década de 1980.

https://www.rtve.es/noticias/20240529/taylor-swift-eras-tour-exito-empresarial-mundial/16118344.shtml


Taylor Swift, el éxito empresarial de una "maestra" del marketing: "Todo lo que toca se convierte en oro"

► La cantante estadounidense actúa dos días en Madrid por su gira 'The Eras Tour', considerada la más rentable de la historia
► Cada fan gasta más de 1.200 euros por concierto incluyendo la entrada, el viaje, comida y vestimenta, según un estudio

29.05.2024 | 07:40 horas Por RUTH DRAKE

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

Por otro lado, un caso negativo podría ser los tuits controvertidos de Elon Musk, la respuesta de United Airlines a los incidentes de remoción de pasajeros o la gestión inadecuada de una empresa ante una violación de datos.

https://elpais.com/economia/2017/04/11/actualidad/1491901519_801095.html


UNITED AIRLINES >

United Airlines se disculpa tras echar por la fuerza a un pasajero de un avión

La compañía vendió más billetes que plazas disponibles y pidió a cuatro voluntarios que bajasen de la aeronave

Después de leer los artículos y discutirlos, es momento de realizar la investigación y el análisis. Formen pequeños grupos y asignen a cada grupo un estudio de caso. Revisen con su grupo los antecedentes, una visión general del individuo o empresa y su presencia digital antes del incidente. Examinen el incidente y creen una descripción detallada del evento que impactó su identidad digital. Analicen los pasos tomados para gestionar la situación, incluyendo publicaciones en redes sociales, declaraciones públicas y otras comunicaciones digitales.

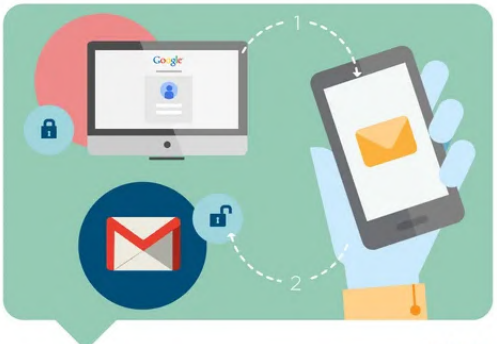
Luego, realicen una evaluación de los resultados de estas acciones sobre su identidad digital y reputación.

Finalmente, haremos una discusión en clase para comparar diferentes estrategias y resultados, y debatir cómo estas lecciones pueden aplicarse a sus propias identidades digitales.

D: Privacidad y Seguridad

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

1. Actividad: Reto de la Contraseña



El objetivo de la siguiente actividad es crear contraseñas fuertes y memorables y entender la importancia de la seguridad de las contraseñas. Las necesidades cubiertas son la capacidad de crear y gestionar contraseñas fuertes para mejorar la seguridad en línea. Para realizar la actividad, los materiales necesarios serán ordenadores/tablets, proyector/pantalla, papel y bolígrafos. Esta actividad tomará 20 minutos.

¿Qué hace que una contraseña sea fuerte? Los consejos incluyen números, letras mayúsculas, símbolos y tratar de no usar algunos detalles relacionados contigo. Para generar una contraseña fuerte, es importante equilibrar la seguridad con la facilidad de recordarla.

Ahora te mostramos dos métodos diferentes, el método 1, usa una frase fácil de recordar. Elige una frase significativa. Puede ser una frase de una canción favorita, un dicho popular o algo personal que sea fácil de recordar. Ejemplo: "En abril florecen mil flores" También acorta la frase, de modo que tomes la primera letra de cada palabra y las combines. Ejemplo: "Eafm"

Agrega números y símbolos: agrega algunos números y símbolos para aumentar la seguridad. Ejemplo: "Eafm2024#"

El segundo método 2 es usar palabras aleatorias. Selecciona palabras aleatorias y elige cuatro palabras que no estén relacionadas pero que sean fáciles de recordar. Ejemplo: "gato luna río mesa" combina palabras, junta las palabras y agrega un número y un símbolo. Ejemplo: "GatoLunaRioMesa!9"

Ahora encuentra consejos adicionales y asegúrate de usar una mezcla de letras mayúsculas y minúsculas. Evita la información personal. No uses información personal como fechas de nacimiento, nombres de familiares o direcciones. Usa un gestor de contraseñas: si la persona mayor tiene dificultad

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

Cofinanciado por la Unión Europea

para recordar múltiples contraseñas, un gestor de contraseñas puede ser una buena solución.

Ejemplos de contraseñas fuertes: (recuerda que puedes usar de nuevo el enlace que te proporcionamos para crear las contraseñas con verificación de seguridad:

https://password.kaspersky.com/es/

"C0nchaC4r4col!23"

"P3rro&Gat0_456"

"Happy*Birthday2024"

Estas contraseñas son relativamente fáciles de recordar pero lo suficientemente seguras. Crea tus propias contraseñas fuertes usando una mezcla de letras, números y símbolos. Discute las mejores prácticas para la gestión de contraseñas.

2. Actividad: "Encuentra el Phish"

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

El objetivo de la actividad es reconocer correos electrónicos de phishing y entender cómo responder a ellos. Las necesidades cubiertas son mejorar la capacidad de reconocer estafas de phishing y tomar las acciones apropiadas. Para realizar la actividad, se necesitan ejemplos de correos electrónicos de phishing. Esta actividad tomará 30 minutos para completarse.

En los correos electrónicos de phishing, los ciberdelincuentes a menudo solicitan la siguiente información: fecha de nacimiento, número de seguro social, número de teléfono, dirección de hogar, detalles de tarjetas de crédito, detalles de inicio de sesión, contraseña (u otra información necesaria para restablecer tu contraseña), también al hacer clic en un archivo adjunto, habilitar macros en un documento de Word, actualizar una contraseña, responder a una solicitud de amistad o contacto en redes sociales, conectarse a un nuevo punto de acceso Wi-Fi.

Ahora es momento de practicar, por favor revisa los siguientes ejemplos:

Ejemplo 1: Alerta Bancaria

Asunto: Urgente: Se requiere verificación de cuenta

Estimado/a Cliente,

Hemos detectado una actividad inusual en su cuenta y necesitamos que verifique su identidad para asegurar la seguridad de sus fondos. Por favor, haga clic en el enlace a continuación para verificar la información de su cuenta:

[Verificar Su Cuenta] http://santanderbank.com/rstcnn

Si no verifica en un plazo de 24 horas, se suspenderá su cuenta.

Gracias por su pronta atención a este asunto.

Atentamente,Equipo de Seguridad Bancaria

Ejemplo 2: Factura de una Empresa Conocida

Asunto: Pago de Factura Pendiente

Estimado/a [Tu Nombre],

Su factura del mes de julio está adjunta. Por favor, asegúrese de realizar el pago antes de la fecha de vencimiento para evitar cargos por retraso.

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

[Descargar Factura](http://PODIUM ENGINEERING LIMITED company.com/invoice)

Gracias-

Saludos cordiales,

Departamento de Facturación de PODIUM ENGINEERING LIMITED

Ejemplo 3: Notificación de Redes Sociales

Asunto: Nuevo Intento de Inicio de Sesión desde un Dispositivo

Hola [Tu Nombre],

Detectamos un intento de inicio de sesión desde un dispositivo desconocido. Si no fuiste tú, por favor asegure su cuenta haciendo clic en el enlace a continuación y actualizando la configuración de seguridad:

Asegurar Su Cuenta [http://facenonbooksocialmedia.com/security]

Gracias por mantener su cuenta segura.

Atentamente,

Equipo de Soporte de Facenonbook

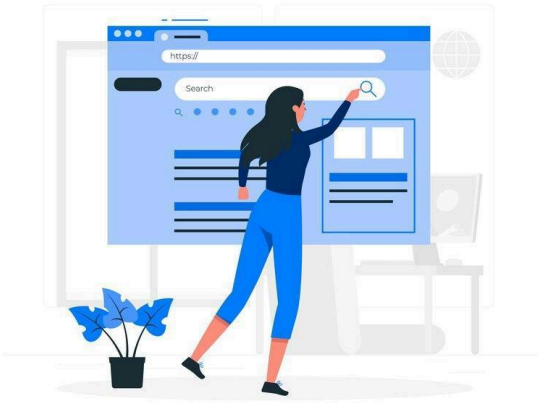
Ahora, por favor trabajen en parejas para identificar los indicadores de phishing. Discute y detecta los hallazgos en grupo. Encuentren la siguiente información en los correos electrónicos anteriores:

- Sentido de urgencia
- Enlace sospechoso
- Saludo genérico "Estimado/a Cliente"
- Amenazas de suspensión de cuenta
- Archivo adjunto o enlace no solicitado

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

- Nombre de empresa genérico o mal escrito
- Detalles de factura inusuales o desconocidos
- Alerta de seguridad no solicitada
- Enlace sospechoso
- Saludo genérico
- Errores gramaticales o de ortografía
- Reflexión para compartir consejos sobre cómo manejar correos electrónicos sospechosos.

3. Actividad: "A salvo o en peligro”



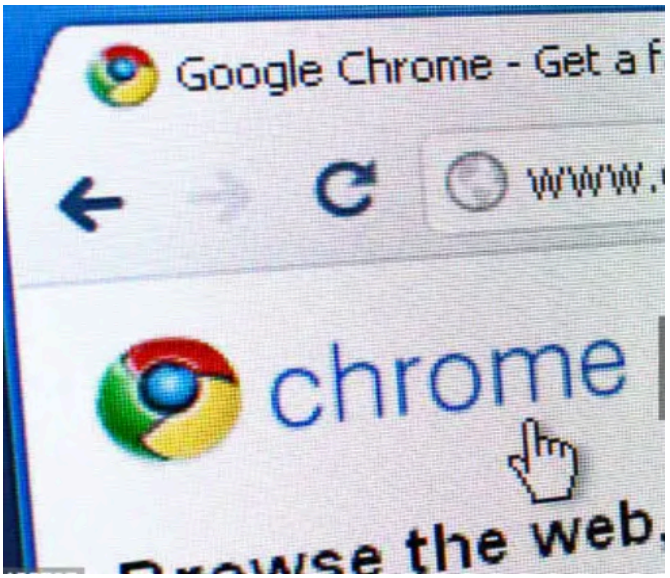
El objetivo es entender y practicar hábitos de navegación segura. La necesidad cubierta es el conocimiento de las prácticas de navegación segura para proteger la información personal en línea. Para realizar la actividad, se necesitan ordenadores/tablets, proyector/pantalla, papel y bolígrafos. Esta actividad tomará 25 minutos para completarse.

Configura tu navegador de manera segura: habilita la privacidad y seguridad en tu navegador, y evita la instalación de extensiones no confiables.

Revisa y sigue los siguientes pasos: Dividiremos al grupo en dos grupos. 1 CHROME y 2 MOZILLA.

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

El Grupo 1 usará Google Chrome.



Actualiza Chrome: Ve a Menú (tres puntos) > Ayuda > Acerca de Google Chrome y asegúrate de estar usando la versión más reciente.

Habilita Navegación Segura: Ve a Configuración > Privacidad y seguridad > Seguridad. Elige Protección mejorada en Navegación segura.

Bloquea Cookies de Terceros: Ve a Configuración > Privacidad y seguridad > Cookies y otros datos de sitios. Selecciona Bloquear cookies de terceros.

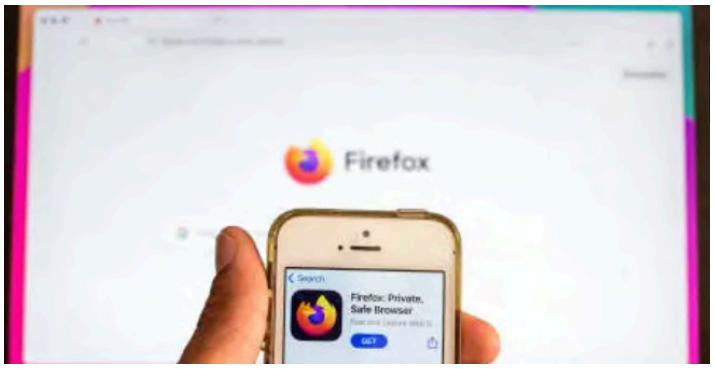
Habilita No Rastrear: Ve a Configuración > Privacidad y seguridad > Cookies y otros datos de sitios. Activa Enviar una solicitud de "No rastrear" con tu tráfico de navegación.

Borra Datos de Navegación: Ve a Configuración > Privacidad y seguridad > Borrar datos de navegación. Elige qué borrar (por ejemplo, historial de navegación, cookies, imágenes en caché) y selecciona Borrar datos.

El Grupo 2 usará Mozilla Firefox.

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

Cofinanciado por la Unión Europea



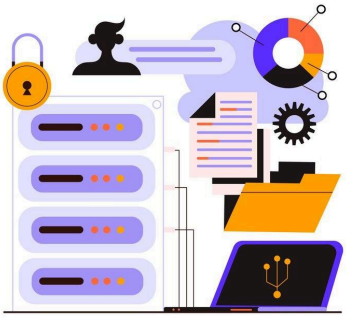
Actualiza Firefox: Ve a Menú (tres líneas) > Ayuda > Acerca de Firefox para buscar actualizaciones.

Habilita Protección de Rastreo Mejorada: Ve a Menú (tres líneas) > Configuración > Privacidad y Seguridad. Bajo Protección de Rastreo Mejorada, selecciona Estricto.

Bloquea Cookies: Ve a Configuración > Privacidad y Seguridad > Cookies y Datos de Sitios. Selecciona Administrar Excepciones para bloquear cookies específicas o Eliminar cookies y datos de sitios cuando se cierre Firefox.

Borra Datos de Navegación: Ve a Configuración > Privacidad y Seguridad > Cookies y Datos de Sitios.

4. Actividad: Revisión de Privacidad



El objetivo es comprender y gestionar la configuración de privacidad en las plataformas de redes sociales.

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

Las necesidades cubiertas son la capacidad de gestionar de manera efectiva las configuraciones de privacidad en las plataformas de redes sociales.

Para realizar la actividad, los materiales necesarios son ordenadores/tablets con acceso a Internet. Esta actividad tomará aproximadamente 25 minutos.

La importancia de las configuraciones de privacidad en las redes sociales. Revisar las preferencias es siempre el primer paso al usar redes sociales. Hoy en día, con la introducción de la IA, debes revisar y rechazar o elegir tus preferencias de seguridad y privacidad. Este paso es crucial para el uso futuro de tus perfiles en plataformas de redes sociales.

Configuraciones de privacidad en plataformas de redes sociales populares. Dividiremos al grupo en dos grupos: 1 Facebook, 2 Instagram. Ajusta tus configuraciones para mejorar la privacidad.

Antes de comenzar, ten en cuenta que Meta, la empresa matriz de Facebook e Instagram, ha anunciado su intención de usar los datos de los usuarios para entrenar sus sistemas de inteligencia artificial (IA) a partir del 26 de junio de 2024. A continuación se detallan los cambios y pasos para evitar que tus datos sean utilizados con este propósito. Meta usará todas las publicaciones, comentarios, audios y fotos compartidos en Facebook e Instagram, excepto los mensajes privados, para entrenar sus sistemas de IA.

Proceso para rechazar: debes:

- Entrar desde tu ordenador y hacer clic en la foto de perfil.
- Ir a “Configuración y privacidad” y seleccionar “Configuración”.
- Seleccionar “Política de privacidad” y luego “Derecho a Oponerse”.

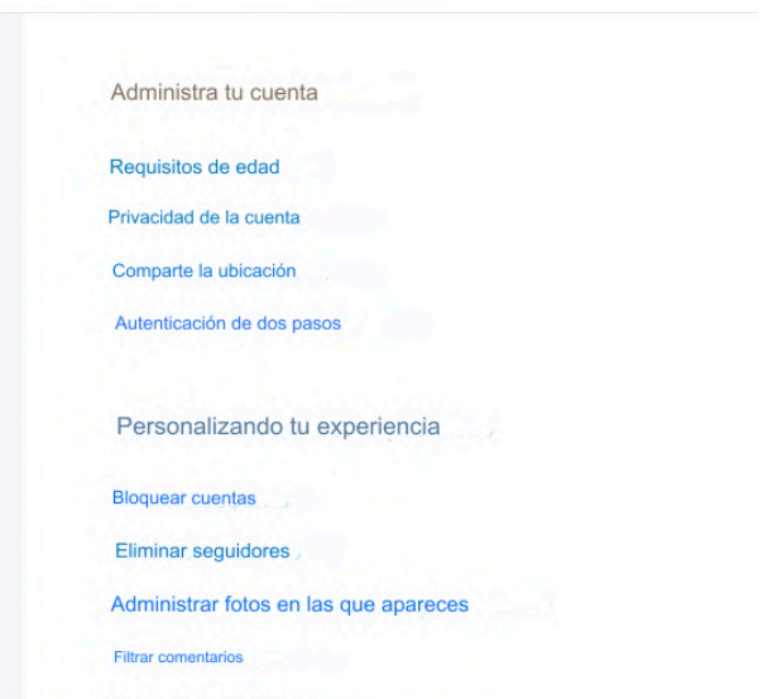
Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

- Rellenar un pequeño formulario especificando que no deseas que tus datos sean utilizados para entrenar la IA de Meta.

Grupo 1: Facebook

- Acceder a la Configuración de Privacidad: Haz clic en la flecha hacia abajo en la esquina superior derecha y selecciona Configuración y privacidad > Configuración.
- Revisión de privacidad: Ve a Configuración y privacidad > Revisión de privacidad.
- Sigue los pasos para revisar y ajustar configuraciones para publicaciones, información del perfil y más.
- Quién puede ver tus publicaciones: Ve a Configuración > Privacidad. Bajo Tu Actividad, elige quién puede ver tus futuras publicaciones y limita la audiencia para publicaciones pasadas.

Grupo 2: Instagram



Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

Acceder a Configuración de Privacidad: Ve a tu perfil y toca las tres líneas horizontales en la esquina superior derecha. Selecciona Configuración > Privacidad.

Cuenta Privada: Activa la opción de Cuenta Privada para que tus publicaciones sean visibles solo para los seguidores que apruebes.

Configuraciones de Historia: Bajo Privacidad > Historia, elige quién puede ver tus historias, responder a ellas y compartirlas.

Estado de Actividad: Bajo Privacidad > Estado de Actividad, desactiva Mostrar Estado de Actividad para ocultar tu estado en línea.

Fotos y Videos: Bajo Privacidad > Publicaciones, controla quién puede etiquetarte en fotos y videos y aprueba las etiquetas manualmente.

5. Actividad: "Hecho o Ficción"

El objetivo es desarrollar habilidades para evaluar críticamente la fiabilidad de la información en línea. Las necesidades cubiertas son la mejora de la

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

capacidad para evaluar críticamente la fiabilidad de la información en línea. Para realizar la actividad, los materiales necesarios son ordenadores/tablets, proyector/pantalla. Esta actividad tomará 30 minutos para completar.

El Código de Ética de la Sociedad de Periodistas Profesionales (SPJ) es un principio orientador para los periodistas, que enfatiza la importancia de la iluminación pública, precisión, imparcialidad y transparencia. El código consta de cuatro principios generales, que están respaldados por explicaciones adicionales y documentos de posición: https://www.spj.org/pdf/spj-code-of-ethics.pdf

- Mira este video: Ética 101: Los 5 Valores Centrales del Periodismo

Las noticias falsas pueden proliferar fácilmente, particularmente en tiempos de turbulencia política e inestabilidad. Echa un vistazo a los siguientes ejemplos de noticias falsas:

- Poner en Contexto un Video Viral de Biden: Un clip de 10 segundos de Joe Biden mostró una cita sin el contexto completo, lo que distorsionó su significado.
- Falsas Curaciones para el Coronavirus: Una receta que circulaba en las redes sociales afirmaba que el ajo curaba el coronavirus.
- Falsa Afirmación de que Wisconsin Contó Más Votos que los Votantes Registrados: Un rumor en redes sociales comparó incorrectamente el número de votantes registrados en 2018 con el número de votos emitidos en 2020.

Después de verificar la información y las noticias, pregúntate y discute en grupos de 3. Identificar noticias falsas requiere pensamiento crítico y escepticismo. Preguntas para determinar si una noticia es falsa o creíble:

- ¿Cuál es la fuente de la noticia?
- ¿Es de un medio de comunicación reputado y conocido, o de un sitio web desconocido?
- ¿Está identificado el autor y es creíble?
- ¿Tiene el autor un historial de informes fiables? ¿Puedes verificar sus credenciales?
- ¿La URL parece sospechosa?
- ¿El titular parece exagerado o está diseñado para provocar una respuesta emocional?
- ¿Hay errores de ortografía o gramática?

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

- ¿El contenido es lógicamente consistente y coherente?
- ¿La historia tiene sentido en su totalidad, o hay contradicciones y falacias lógicas?
- ¿El artículo cita fuentes creíbles?
- ¿Las afirmaciones están respaldadas por citas de expertos, declaraciones oficiales o enlaces a fuentes primarias?
- ¿Puedes encontrar la misma noticia reportada por otros medios reputables?
- ¿Hay enlaces incrustados que llevan a evidencia de apoyo?
- ¿Cuál es el propósito del artículo?
- ¿Busca informar con informes fácticos, o parece diseñado para engañar, entretener o promover una agenda específica?
- ¿El artículo incluye una fecha y hora de publicación?
- ¿La noticia evoca una fuerte reacción emocional?
- ¿Estás inclinado a creer la noticia porque se alinea con tus creencias existentes?
- ¿Son auténticas las imágenes y videos en el artículo?

Referencias y fuentes:

Arruda, W. (2019). *Digital you: Real personal branding in the virtual age*. Hoboken, NJ: Wiley.

Doorley, J., & Garcia, H. F. (2015). *Reputation management: The key to successful public relations and corporate communication* (3rd ed.). New York, NY: Routledge.

Van den Hurk, A. M. (2013). *Social media crisis communication: Preparing for, preventing, and surviving a public crisis*. Boston, MA: Pearson.

Smith, J. (2021). *Digital Literacy: Concepts, Strategies, and Practices*. Springer.

Jones, A. (2020). Teaching digital literacy in the classroom. En B. Brown & C. Davis (Eds.), *Advances in Digital Education* (pp. 45-67). Routledge.

Smith, J. (2020). *Cybersecurity Essentials*. Wiley.

Knight, Alison. "Data Analytics and the GDPR: Friends or Foes?" *Data Privacy Review* 8, no. 2 (2015): 123-145.

Garcia, M., & Lee, S. (2021). Current trends in cybersecurity. *Journal of Cybersecurity*, 5(2), 112-130. https://doi.org/10.1177/1234567890123456

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

Brown, C. (2023, Enero 15). Cyber threats on the rise. *New York Times*. https://www.nytimes.com/article/cyber-threats-rise.html

National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity*. https://www.nist.gov/cyberframework

Avery, J. (2020). The power of social media in crisis management. *Harvard Business Review*. https://hbr.org/

Digital Marketing Institute. (2021). Understanding digital reputation management. https://digitalmarketinginstitute.com/

Llopis, G. (2013). The role of personal branding in professional success. *Forbes*. https://www.forbes.com/

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.