Ficha de la formación CDI

|  |  |
| --- | --- |
| **Título** | Cómo identificar información incompleta y noticias falsas en línea en un contexto cultural relevante |
| **Área formativa** | *Please select one or more of the following:*

|  |  |
| --- | --- |
| Seguridad en línea | X |
| Alfabetización cultural y mediática |  |
| Transacciones económicas |  |
| Protección de datos personales |  |
| Indentidad digital y reputación online |  |

 |
| **Palabras clave** | seguridad en línea, seguridad en línea, contexto cultural, noticias falsas, información incompleta |
| **Realizado por** | Community Development Institute, CDI |
| **Idioma** | Castellano |
| **Objetivos / metas / resultados de aprendizaje** |
| Al final de este módulo, adquirirá conocimientos sobre el reconocimiento de noticias falsas e información faltante, así como la seguridad en línea en un contexto cultural.El módulo consta de cuatro unidades que brindan información relacionada con el tema en diferentes secciones. Las diferentes actividades y agradecimientos se apoyan con ejemplos para una mejor comprensión del material, fotos explicativas y enlaces útiles para ampliar tus conocimientos sobre el tema.Los usuarios tendrán la oportunidad de conocer la seguridad en línea en un contexto cultural, así como la seguridad en línea. Las posibles amenazas de seguridad en línea se presentarán a través de explicaciones de los diferentes tipos de amenazas como malware, phishing, ataques de contraseña, etc.Los usuarios podrán:● Comprender el significado de seguridad y protección en línea.● Marcar la diferencia entre noticias falsas, información errónea e información incompleta. ● Usar diferentes consejos con respecto a la seguridad en línea en el contexto cultural |
| **Descripción**  |
| Las tecnologías digitales han revolucionado todos los aspectos de nuestras vidas. Han impactado en las cadenas de valor de todas las industrias culturales y creativas no solo en lo que respecta al proceso creativo y su ejecución, sino también en lo que se refiere a la elaboración de una obra o producto de arte y su promoción, distribución, comercialización y venta.Esta unidad de aprendizaje enseñará a los estudiantes digitales tardíos a detectar posibles estafas fraudulentas que podrían encontrar en la web mientras usan o buscan recursos culturales. Esta unidad proporcionará ejemplos específicos de estafas comunes relacionadas con recursos culturales, como venta de entradas falsas, intentos de phishing después de realizar un pedido en línea, etc. También brindará los puntos clave para identificar recursos culturales seguros en línea.En la era actual de tecnología, las noticias falsas y la información incompleta son parte de la circulación diaria y la información en línea. Se presentará a los usuarios cuál es el significado de noticias falsas e información incompleta, cómo reconocer noticias falsas y la importancia de diferenciar entre noticias falsas e información faltante. Fomentar la capacidad de reconocer y protegerse de la información incompleta y las noticias falsas es la unidad que proporciona información y contenido con respecto a la capacidad de los usuarios para protegerse en línea. Se proporcionan consejos y trucos junto con ejemplos y fotografías útiles. |

|  |
| --- |
| **Contenidos dispuestos en 3 niveles** |
| **1. INTRODUCCIÓN****2. CONTENIDO****Unidad 1: ¿Qué es la seguridad en línea?**1.1 Seguridad en línea y seguridad en línea, significado1.2 Seguridad en línea en contenidos culturales**Unidad 2: Las mayores amenazas a su seguridad en línea**2.1 Tipos de amenazas de seguridad en línea● software malintencionado● Hombre en el medio MITM “Men in the middle”● suplantación de identidad● Ataques de contraseña**Unidad 3: Identificar la información incompleta, la información errónea, la desinformación y las noticias falsas en el contexto cultural**3.1 ¿De dónde vienen las noticias falsas?3.2 Cómo reconocer noticias falsas, información errónea, desinformación e información faltante en el contexto cultural.**Unidad 4: Protéjase de las amenazas de seguridad en línea**4.1 Protéjase mientras está en línea4.2 Consejos para la seguridad en línea en un contexto cultural**5. CONCLUSIÓN****Módulo: Cómo identificar información incompleta y noticias falsas en línea en un contexto cultural relevante.**1. **INTRODUCCIÓN**

Las tecnologías digitales han revolucionado todos los aspectos de nuestras vidas. Han impactado en las cadenas de valor de todas las industrias culturales y creativas no solo en lo que respecta al proceso creativo y su ejecución, sino también en lo que se refiere a la elaboración de una obra o producto de arte y su promoción, distribución, comercialización y venta. A medida que continúa el cambio digital, cada vez más artistas, cineastas, productores, músicos, etc., distribuyen sus productos digitalmente. Al final de este módulo, adquirirá conocimiento y reconocimiento de información falsa nueva y faltante, así como seguridad en línea en un contexto cultural.En un mundo en el que se produce un ataque de piratas informáticos aproximadamente cada 39 segundos, la seguridad en línea ya no puede tomarse a la ligera. De lo contrario, todos sus datos personales podrían estar en peligro.Pero, ¿qué es la seguridad en línea, para ser exactos? ¿Qué tipo de amenazas hay en la web y qué puede hacer para protegerse de ellas? Una amenaza a la seguridad en línea se refiere a cualquier posible ataque malicioso que busca acceder ilegalmente a los datos, interrumpir las operaciones digitales o dañar la información. Ahora más que nunca, el contenido cultural es ampliamente accesible y también está abierto a amenazas en línea, la difusión de información faltante, información errónea, desinformación y noticias falsas podría dañar la experiencia de una persona mientras disfruta e informa sobre un espectáculo o evento cultural.**Unidad 1: ¿Qué es la seguridad en línea?****Sección 1.1 Explicación de la seguridad en línea y estar online seguro**La seguridad en Internet consiste en una variedad de tácticas de seguridad para proteger las actividades y transacciones realizadas en línea a través de Internet. Estas tácticas están destinadas a proteger a los usuarios de amenazas como la piratería en sistemas informáticos, direcciones de correo electrónico o sitios web. La seguridad en Internet es un aspecto específico de conceptos más amplios como la ciberseguridad y la seguridad informática, centrándose en las amenazas y vulnerabilidades específicas del acceso en línea y el uso de Internet.La **seguridad en línea** protege a las personas que usan Internet de cualquier daño a través de la concientización, la educación, la información y la tecnología. Seguridad en línea es ser consciente de la naturaleza de las posibles amenazas que podría encontrar mientras realiza actividades a través de Internet, estas podrían ser amenazas de seguridad, proteger y administrar sus datos personales en línea y evitar contenido dañino o ilegal.**Sección 1.2 Seguridad en línea en contenidos culturales**Las tecnologías digitales han revolucionado todos los aspectos de nuestras vidas, y la cultura no es una excepción. Han impactado en las cadenas de valor de todas las industrias culturales y creativas no solo en lo que respecta al proceso creativo y su ejecución, sino también en lo que se refiere a la elaboración de una obra o producto de arte y su promoción, distribución, comercialización y venta. Algunos procesos de producción son exclusivamente digitales y la tecnología tiene un enorme potencial para hacer la cultura accesible a todos, democratizando tanto el consumo como la implicación en la creación cultural.Al mismo tiempo, las instituciones culturales, como museos, archivos, bibliotecas y emisoras de cine, televisión y música han estado digitalizando sus colecciones en un esfuerzo por preservarlas y hacerlas más accesibles. A veces, la digitalización es un paso necesario, como en el caso de las películas analógicas, que ya no se pueden proyectar en su forma original, ya que los cines están equipados únicamente con tecnología digital.Una gran cantidad de contenido cultural digital está disponible en línea de forma gratuita, por una tarifa o ilegalmente. Tal disponibilidad y abundancia de contenido cultural y las diversas formas de consultarlo en línea traen nuevos desafíos y oportunidades para interrumpir la seguridad en línea de una persona por diversos medios. Por lo tanto, es importante en esta era digital estar informado y conocer las amenazas a su seguridad en línea y cómo protegerse mientras accede a contenido cultural en línea.**Unidad 2: Las mayores amenazas para su seguridad en línea** **Sección 2.1 Tipos de amenazas a la seguridad en línea**Una amenaza a la seguridad en línea se refiere a cualquier posible ataque malicioso que busca acceder ilegalmente a los datos, interrumpir las operaciones digitales o dañar la información.Hay docenas de amenazas de seguridad en línea en Internet, por lo que decidimos centrarnos en las más peligrosas y comunes.Malware:El malware es software malicioso, como spyware, ransomware, virus y gusanos. El malware se activa cuando un usuario hace clic en un enlace o archivo adjunto malicioso, lo que conduce a la instalación de software peligroso que, una vez activado, puede:● Bloquear el acceso a componentes clave de ntwork (ransomware)● Instalar software dañino adicional● Obtener información de forma encubierta mediante la transmisión de datos desde el disco duro (spyware)● Interrumpir piezas individuales, lo que hace que el sistema no funcione.**Man in the Middle, MITM “Hombre en medio”:**Una amenaza de hombre en el medio (MITM) ocurre cuando los actores maliciosos se insertan en una transacción de dos partes. Después de interrumpir la transacción, pueden filtrar y robar datos. La amenaza MITM se realiza a menudo cuando un visitante utiliza una red Wi-Fi pública no segura. Los actores maliciosos se interponen entre el visitante y la red, y luego usan el malware mencionado anteriormente para instalar software y usar datos de manera maliciosa.**Suplantación de identidad “phishing”:**Los ataques de phishing utilizan comunicaciones falsas, como un correo electrónico, para engañar al receptor para que lo abra y siga las instrucciones que contiene, como proporcionar un número de tarjeta de crédito. El objetivo es robar datos confidenciales como tarjetas de crédito e información de inicio de sesión o instalar malware en la máquina de la víctima.**Ataques de contraseña:**Con la contraseña correcta, un actor malicioso tiene acceso a una gran cantidad de información. La ingeniería social es un tipo de ataque de contraseña que se define como "una estrategia que se basa en gran medida en la interacción humana y, a menudo, implica engañar a las personas para que rompan las prácticas de seguridad estándar".Otros tipos de ataques de contraseña incluyen acceder a una base de datos de contraseñas o adivinar directamente.**Unidad 3: Identificar la información faltante, la información errónea, la desinformación y las noticias falsas en el contexto cultural**Ahora, más que nunca, el contenido cultural es ampliamente accesible y está abierto a amenazas en línea, la difusión de información faltante, información errónea, desinformación y noticias falsas podría dañar la experiencia de una persona mientras disfruta e informa sobre un evento o espacio cultural.**Sección 3.1 ¿Qué significa noticias falsas, información errónea y desinformación?****Las noticias falsas** son información elaborada a propósito, sensacionalista, cargada de emociones, engañosa o totalmente inventada.Hay dos tipos de noticias falsas: 1. Historias que no son ciertas. Estas son historias completamente inventadas diseñadas para hacer que las personas crean algo falso, para comprar un determinado producto o para visitar un determinado sitio web.2. Historias que tienen algo de verdad, pero que no son 100 por ciento precisas. Nuevamente, esto puede ser deliberado, para convencer a los lectores de cierto punto de vista, o puede ser el resultado de un error inocente.El término desinformación se refiere a información que es falsa o inexacta y, a menudo, se difunde ampliamente con otros, independientemente de la intención de engañar. Si bien la información errónea es información falsa que se crea y difunde independientemente de la intención de dañar o engañar, la **desinformación** es un tipo de información errónea que se crea para ser deliberadamente engañosa. Ambos formularios pueden compartirse ampliamente, independientemente de si el que comparte sabe que la información es incorrecta.Las plataformas de redes sociales permiten que casi cualquier persona publique sus pensamientos o comparta historias con el mundo. El problema es que la mayoría de las personas no verifican la fuente del material que ven en línea antes de compartirlo, lo que puede llevar a que las noticias falsas se propaguen rápidamente. Al mismo tiempo, se vuelve más difícil identificar la fuente original de las noticias, lo que puede dificultar la evaluación de su precisión.**Sección 3.2 Cómo reconocer noticias falsas, información errónea, desinformación e información incompleta en el contexto cultural**¿Cómo detectar noticias falsas, información errónea, desinformación e información incompleta? Hágase las siguientes preguntas y haga lo siguiente:**● ¿Quién lo escribió? Verifique el nombre del autor. ¿Está disponible el nombre o falta?** La mayoría de los autores que dedican tiempo a un artículo bien investigado probablemente tendrán su nombre adjunto.**● ¿Cuáles son sus calificaciones?** Si aparece el nombre del autor, averigüe quién es la persona y cuáles son sus credenciales**.****● Consulte la sección "Acerca de nosotros".** En la parte superior o inferior del sitio web, debe haber una sección llamada "Acerca de nosotros". Esta sección describe el propósito del sitio web.**● ¿El artículo le informa todos los aspectos del tema?** Los artículos de noticias deben proporcionarle datos desde varios puntos de vista.**● ¿El contenido coincide con el título del artículo**? Un título debe darte una idea de lo que trata todo el artículo, pero también puede usarse para persuadirte de que creas algo antes de leer el artículo.**● ¿Cuándo se publicó este artículo?** Es posible que los artículos más antiguos no contengan datos actualizados y que tengan enlaces rotos.**● ¿Se modificó o actualizó el artículo?** El contenido reutilizado o actualizado suele tener un descargo de responsabilidad al principio o al final del artículo.**● ¿Qué tan importante es la fecha?** La fecha le da una indicación de cuándo se publicó el artículo.**● ¿Parece correcta esta dirección web (URL)?** Escribir la dirección web incorrecta lo dirigirá a una página web que no tenía la intención de visitar. Puede llevarlo a una página con las amenazas de seguridad en línea mencionadas anteriormente.**● ¿Encontré esto en las redes sociales?** Las plataformas de redes sociales no son organizaciones de noticias. Estas son plataformas para que las personas creen y/o compartan contenido.**● ¿Encontré esto en un blog/sitio web?** Los blogs contienen contenido escrito de manera informal y administrado por un individuo o un grupo pequeño.Unit 4: Protecting yourself from online security threats **Sección 4.1 Protéjase mientras está en línea**Aquí hay algunas cosas que puede realizar mejor para protegerse mientras está en línea:**1. No use redes WiFi no seguras**Es mejor evitar cualquier red WiFi que no le solicite una contraseña y, en su lugar, simplemente use su propio plan de datos móviles.**2. Utilice un potente software antivirus**El software antivirus es su mejor apuesta para mantener su dispositivo a salvo de las infecciones de malware de las que hablamos. No deje que el nombre lo confunda: un programa antivirus lucha contra los virus, pero se dirige principalmente al malware (un virus es un tipo de malware). Asegúrese de mantener el programa actualizado y de ejecutar escaneos frecuentes, especialmente después de descargar archivos nuevos. De hecho, es mejor que no los abras sin escanearlos primero.**3. Utilice siempre una VPN en línea**Una VPN (red privada virtual) es un servicio en línea que puede usar para ocultar su dirección IP real y cifrar sus comunicaciones en línea. Es una de las mejores formas de mejorar su seguridad en línea y ocultar sus huellas digitales. Mientras se utilicen los métodos de encriptación adecuados, nadie podrá monitorear su tráfico en línea para ver lo que está haciendo en Internet.**4. Evite los intentos de phishing**Si recibe correos electrónicos o mensajes que afirman ser de alguien cercano a usted, su banco o la policía que le piden que descargue archivos adjuntos sospechosos, acceda a enlaces abreviados o comparta información confidencial, ignórelos. Póngase en contacto con el presunto remitente para averiguar la verdad. Intenta buscar en Google partes del mensaje que recibiste entre comillas. Si se trata de una estafa de phishing, es probable que obtenga resultados de otras personas hablando de recibir el mismo mensaje.**5. No mantengas el Bluetooth activado**Si bien Bluetooth tiene sus usos, mantenerlo encendido en todo momento es una apuesta arriesgada. En 2017, se descubrió un nuevo método de piratería de Bluetooth que afectó a millones de dispositivos al permitir que los piratas informáticos usaran la amenaza MITM Man in the Middle para obtener la información de su dispositivo. No lo estamos usando para mantener intacta su seguridad en línea.**6. Desactive los servicios de ubicación en sus dispositivos móviles**Los servicios de ubicación pueden ser realmente útiles, pero también pueden ser muy riesgosos, existe el hecho de que algunas aplicaciones podrían filtrar tu ubicación. Si eso sucede, no significa que estará en peligro inmediato. Aún así, su seguridad en línea se verá amenazada.**7. Use bloqueadores de scripts en sus navegadores**Los bloqueadores de scripts son extensiones del navegador que puede usar para asegurarse de que los sitios web a los que accede no ejecuten scripts y complementos no autorizados en segundo plano que puedan comprometer su seguridad en Internet. No lo olvide: algunos scripts pueden ser tan peligrosos que pueden controlar su navegador, mientras que otros pueden ejecutar redireccionamientos o anuncios de phishing, o incluso extraer criptomonedas usando su CPU.**8. Mantenga su sistema operativo actualizado**No instalar las actualizaciones más recientes en su sistema operativo puede dañar seriamente su seguridad en línea. Porque los actores malintencionados pueden aprovechar las vulnerabilidades potenciales en su beneficio, vulnerabilidades que podrían haberse solucionado con la última actualización.**9. Considere el uso de aplicaciones de mensajería y correos electrónicos cifrados**Si realmente desea asegurarse de que sus comunicaciones en línea sean seguras, puede intentar usar las diferentes aplicaciones para enviar mensajes. Esa función de encriptación realmente poderosa.En cuanto a los correos electrónicos, es lo mismo, busque en línea diferentes aplicaciones y qué tipo de seguridad ofrecen.**10. Usa contraseñas seguras**Tener contraseñas poderosas para sus cuentas es extremadamente importante, pero encontrar una realmente buena es más fácil decirlo que hacerlo.Si necesita ayuda, pero aquí están las ideas principales:1. Use espacios si está permitido.2. Solo use contraseñas largas. Lo ideal es no ceñirse a una sola palabra.3. No utilices palabras del diccionario como contraseña.4. Usa letras mayúsculas y minúsculas y mézclalas al azar.5. Use símbolos (como $, % o \*) en su contraseña.6. Incluya números en su contraseña.7. Intente convertir su contraseña en una oración completa.8. Invierta algunas palabras que usa en la contraseña (en lugar de "silla" use "riahc").9. Además, trate de no usar la misma contraseña para todas sus cuentas. Es mejor usar contraseñas diferentes, o al menos variaciones de su contraseña principal.**4.2 Consejos para la seguridad en línea en un contexto cultural**Gracias a Internet, existen varias formas para que los consumidores obtengan entradas para un próximo evento. La desventaja es que también hay muchas trampas que los consumidores deben evitar. Hacer clic en el enlace incorrecto o confiar en el sitio web incorrecto podría generar un boleto falso y la pérdida de fondos.**Aquí hay algunos consejos sobre cómo estar seguro en línea, con un ejemplo específico de compra de boletos en línea para un evento cultural:****• Compra directamente en el lugar siempre que sea posible.** Muchos agentes oficiales de venta de entradas ahora también ofrecen opciones de venta secundarias. No haga clic en correos electrónicos o anuncios en línea; un truco común de estafa de boletos es crear una dirección web que sea similar a una empresa conocida.**• Considere su fuente.** Conozca la diferencia entre un corredor de boletos profesional (un revendedor legítimo y acreditado), un revendedor de boletos (un vendedor de boletos no regulado y sin licencia) y un estafador que vende boletos fraudulentos.**• Conozca la política de reembolso.** Debe comprar boletos solo de un revendedor de boletos que proporcione detalles claros sobre los términos de la transacción. Los vendedores deben revelar al comprador, antes de la compra, la ubicación de los asientos representados por los boletos, ya sea oralmente o por referencia a un plano de asientos; y, si los boletos no están disponibles para el acceso inmediato del comprador, informar cuándo se enviarán los boletos o cuándo estarán disponibles para su retiro.**• Utilice métodos de pago que vengan con protección.** Siempre use una tarjeta de crédito, para que tenga algún recurso si los boletos no son los prometidos. Las tarjetas de débito, las transferencias bancarias o las transacciones en efectivo son riesgosas; si las entradas son fraudulentas, lo más probable es que no puedas recuperar tu dinero. • **Tenga cuidado con los anuncios**. Cuando busca boletos en línea en la web, a menudo aparecerán anuncios de boletos baratos. Utilice el buen juicio; algunos de estos anuncios serán estafas de boletos, especialmente si los precios son bajos.**• Si no está seguro, verifique sus entradas.** Haga una visita al lugar donde se llevará a cabo el evento. Presente su entrada al servicio de atención al cliente y ellos pueden verificar si su entrada es legítimo y mostrarle cómo saber si una entrada es falsa.1. **CONCLUSIÓN**

La seguridad en línea en un contexto cultural más amplio es un tema muy interesante, ya que el contenido cultural está ampliamente disponible; también es el tema de las amenazas en línea.Las tecnologías digitales han revolucionado todos los aspectos de nuestras vidas. Han impactado en las cadenas de valor de todas las industrias culturales y creativas no solo en lo que respecta al proceso creativo y su ejecución, sino también en lo que se refiere a la elaboración de una obra o producto de arte y su promoción, distribución, comercialización y venta. A medida que continúa el cambio digital, cada vez más artistas, cineastas, productores, músicos, etc., distribuyen sus productos digitalmente.Al final de este módulo, adquirirá conocimientos sobre el reconocimiento de información falsa nueva y faltante, así como la seguridad en línea en un contexto cultural. Al utilizar los consejos y los ejemplos proporcionados como guía mientras está en línea, puede fomentar su seguridad en línea. Con amenazas de seguridad como malware, estafas, phishing, piratería y la difusión de información errónea y noticias falsas de desinformación que son cada vez más comunes hoy en día, la seguridad en línea se ha vuelto más importante que nunca.¿Seguridad en línea? El resultado final/puntos claveLa seguridad en línea representa las reglas que sigue, las acciones que realiza y los procesos que suceden para garantizar que esté seguro en Internet. Con las amenazas de seguridad (malware, estafas, phishing, piratería, etc.) cada vez más comunes hoy en día, la seguridad en línea se ha vuelto más importante que nunca.Por lo general, la mejor manera de asegurarse de estar seguro en línea es usar un programa antivirus sólido, una VPN confiable, contraseñas poderosas y bloqueadores de scripts (entre otras cosas).Las noticias falsas se refieren a falsedades deliberadas, o historias que contienen algo de verdad pero que no son completamente precisas, por accidente o por diseño.Algunas personas también afirman que las historias verdaderas son "noticias falsas/fake news", solo porque no están de acuerdo con ellas. Esto puede conducir al peligroso desconocimiento de consejos vitales.Las noticias falsas pueden tener un impacto negativo en los aspectos sociales y culturales de la sociedad, por lo que es crucial saber separar las noticias reales de las falsas y reconocer cuándo falta información, información errónea o desinformación. Puedes hacerlo siguiendo estos seis pasos:1. Desarrolle una mentalidad crítica.2. Verifique la fuente.3. Vea quién más está reportando la historia.4. Examine la evidencia.5. No tome imágenes al pie de la letra.6. Comprueba que "suena bien". |
| **Contenido en puntos claves** |
| ● El contenido cultural es ampliamente accesible en Internet y está abierto a amenazas en línea, la difusión de información faltante, información errónea, desinformación y noticias falsas podría dañar la experiencia de una persona mientras disfruta e informa sobre un espectáculo o evento cultural.● La seguridad en Internet consiste en una variedad de tácticas de seguridad para proteger las actividades y transacciones realizadas en línea a través de Internet.● Una amenaza a la seguridad en línea se refiere a cualquier posible ataque malicioso que busca acceder ilegalmente a los datos, interrumpir las operaciones digitales o dañar la información.● Seguridad en línea es ser consciente de la naturaleza de las posibles amenazas que podría encontrar mientras participa en actividades a través de Internet, estas podrían ser amenazas de seguridad, proteger y administrar sus datos personales en línea y evitar contenido dañino o ilegal. La Seguridad en Línea protege a las personas que realizan acciones en línea a través de la concientización, la educación, la información y la tecnología.● Hay docenas de amenazas de seguridad en línea en Internet, este módulo se enfoca en las más peligrosas y comunes, tales como: Malware; Hombre en el Medio MITM; Suplantación de identidad; Ataques de contraseña, etc.Los usuarios de Internet deben saber reconocer las noticias falsas, la información errónea, la desinformación y protegerse en consecuencia. Las noticias falsas pueden tener un impacto negativo en los aspectos sociales y culturales de la sociedad, por lo que es crucial saber cómo separar las noticias reales de las falsas. así como para reconocer cuando falta información, desinformación o desinformación. |
| **5 entradas del glosario** |
| **1) Seguridad en línea**La seguridad en Internet consiste en una variedad de tácticas de seguridad para proteger las actividades y transacciones realizadas en línea a través de Internet.**2) Navegar seguro**Seguridad en línea es ser consciente de la naturaleza de las posibles amenazas que podría encontrar mientras realiza actividades a través de Internet, estas podrían ser amenazas de seguridad, proteger y administrar sus datos personales en línea y evitar contenido dañino o ilegal. La Seguridad en Línea protege a las personas que realizan acciones en línea a través de la concientización, la educación, la información y la tecnología.**3) Contexto cultural**El contexto cultural está relacionado con la sociedad en la que se crían los individuos y cómo la cultura afecta el comportamiento. Incorpora valores que se aprenden y actitudes que se comparten entre grupos de personas. Incluye creencias, significados, costumbres, ideas, lenguaje, normas.Se refiere al significado simbólico, la dimensión artística y los valores culturales que se originan o expresan identidades culturales.**4) Noticias falsas/Fake News**Historias de noticias falsas, a menudo de naturaleza sensacionalista, creadas para ser ampliamente compartidas o distribuidas con el fin de generar ingresos, promover o desacreditar a una figura pública, movimiento político, empresa, etc.**5) Información incompleta**es información incompleta o inexacta que tiene como objetivo distraer la atención de la información precisa, causar confusión o cambiar el contexto de una oración, acción, actividad, etc. |
| **Bibliografía y referencias adicionales** |
| * <https://www.mindtools.com/pages/article/fake-news.htm>
* [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690570/EPRS\_BRI(2021)690570\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690570/EPRS_BRI%282021%29690570_EN.pdf)
* <https://www.researchgate.net/publication/336951206_Fake_news_Acceptance_by_demographics_and_culture_on_social_media>
* <https://en.unesco.org/sites/default/files/journalism_fake_news_disinformation_print_friendly_0.pdf>
* <https://www.nature.com/articles/s41586-021-03344-2>
* <https://www.kdd.org/exploration_files/8._CR.10.Misinformation_in_social_media_-_Final.pdf>
* <https://academicguides.waldenu.edu/library/fakenews/examples>
* [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690570/EPRS\_BRI(2021)690570\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690570/EPRS_BRI%282021%29690570_EN.pdf)
* [https://www.europarl.europa.eu/thinktank/en/document/EPRS\_BRI(2021)690570](https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI%282021%29690570)
* <https://en.wikipedia.org/wiki/Fake_news>
* <https://call-for-papers.sas.upenn.edu/cfp/2021/06/28/if-its-on-the-internet-it-must-be-true-the-socio-cultural-impact-of-fake-news>
* <https://www.frontiersin.org/research-topics/23019/the-psychology-of-fake-news-on-social-media-who-falls-for-it-who-shares-it-why-and-can-we-help-users>
* <https://researchguides.austincc.edu/c.php?g=612891&p=4258046>
 |
|  **Cinco preguntas de autoevaluación de opción múltiple** | 1) Un correo electrónico en su bandeja de entrada le pide que inicie sesión con una contraseña por alguna razón de seguridad. ¿Qué harías ?A. Nada, ignoraré el mensaje.B. Haré lo solicitado, es una razón de seguridadC. Me pondré en contacto con un experto en TI para obtener más información.**Correcta: A**2) Estás en un sitio web que vende entradas gratuitas para un evento cultural cerca de ti. Son gratuitas y solo solicitan parte de su información personal. ¿Qué harías ?A. Compraré las entradas e ingresaré mi información personal.B. Revisaré el sitio web para ver si es real y, si no lo es, informaré sobre el sitio.C. Compartiré el sitio para que otros también puedan obtener las entradas.**Correcta: B**3) Has realizado un recorrido virtual por un lugar cultural muy conocido. Notaste que faltaba información en uno de los sitios. ¿Qué harías?A. Llenaré el espacio vacío yo mismo.B. Informaré al guía virtual de este posible error.C. No haré nada.**Correcta: B**4) Está creando una cuenta en un sitio web y debe crear una contraseña. ¿Qué contraseña es la más segura?A. Su propio nombre.B. Una línea aleatoria de números y letras que podrías escribir en una hoja de papel para recordar.C. Su número de seguro social.**Correcta: B**5) ¿Mantiene su información personal segura cuando usa las redes sociales?1. Sí
2. No
3. No estoy seguro.

**Correcta: Opcional, todas son correctas.** |
| **Material relacionado** | Cómo identificar información faltante y noticias falsas en línea en un contexto cultural relevante \_PPT\_CDI |
| **Related PPT** |  |
| **Reference Link** |  |
| **Video en YouTube**  | <https://youtu.be/vPAW5j_L4-c><https://www.youtube.com/watch?v=0yL-k5nB65o> |