Estudiante 3.0

Cómo participar de manera segura y responsable en los entornos digitales

Lorena A. Montbrun, Daniela B. Solivellas,
Sandra E. Angeli y Mauricio N. Boarini

UniRío editora

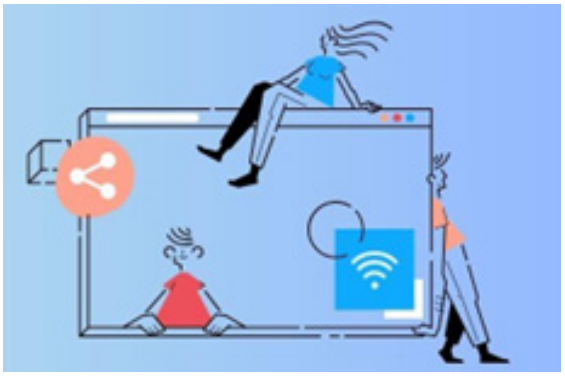
Colección PASAPALABRAS

Serie
Competencias
para la vida universitaria

ISBN 978-987-688-682-6
e-book

Estudiante 3.0

Cómo participar de manera segura y responsable en los entornos digitales.



Introducción

Cada vez más las tecnologías digitales forman parte de nuestro día a día. Navegar por internet, realizar un posteo en redes sociales, mirar un video o jugar en línea puede ser una de tus actividades más frecuentes. Pero, ¿has pensado que cada vez que interactuamos en las redes dejamos datos e información disponible? ¿Cómo podemos reconocer si lo que se comparte por las redes es una información falsa o verdadera? ¿Cómo podemos protegernos para interactuar con los medios digitales de manera segura? ¿Cómo hacer un uso responsable de las aplicaciones con Inteligencia Artificial para hacer la tarea? Estos interrogantes y otros más nos desafían a adquirir habilidades para ser un ciudadano digital responsable, crítico y participativo en el ciberespacio.

En este material didáctico te proponemos 4 recorridos para revisar algunos conceptos, estrategias y reflexionar sobre lo que podés hacer como ciudadano/a digital para desarrollar interacciones en línea empáticas, respetuosas, responsables y seguras.

Los temas sobre los que te planteamos trabajar tienen que ver con la construcción de tu identidad en las redes y la gestión de tu huella digital; las medidas de cuidado y prevención en el uso de las redes y las comunicaciones que establecemos a través de las tecnologías; las estrategias para analizar y validar la confiabilidad de la información que accedemos a través de las tecnologías digitales. Además un primer acercamiento sobre la Inteligencia Artificial, qué es, sus posibilidades y riesgos en general y cómo hacer un uso responsable y ético de la misma.

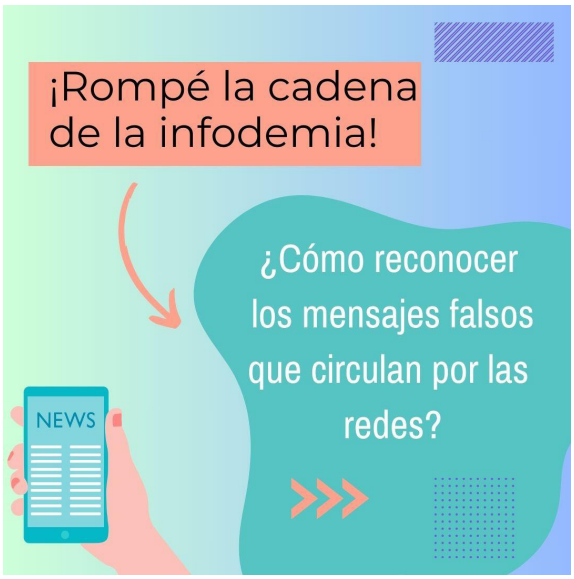
Podrás recorrer este material libremente, en diferentes momentos, y en el orden que desees. Allí encontrarás explicaciones, links a recursos y algunas actividades cuya resolución te permitirá revisar la comprensión de los temas vistos. Una vez que hayas abordado los 4 temas del material y resuelto las actividades te proponemos como cierre realizar una actividad de metacognición.

¿Listo para comenzar? Avancemos entonces.

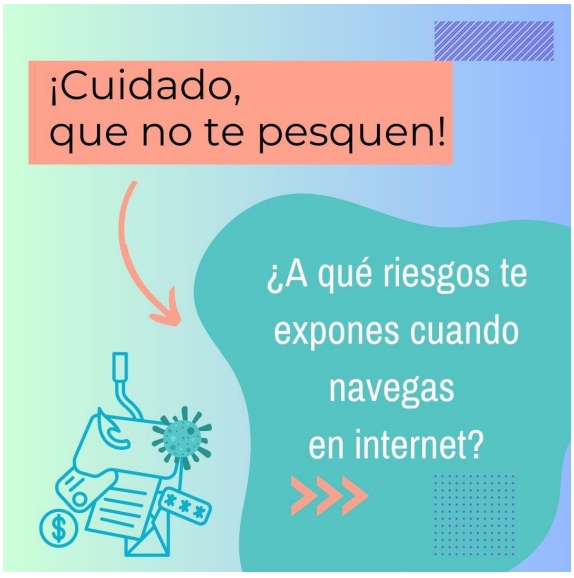
A continuación podés hacer click sobre cada tema para ir de manera directa a la sección correspondiente.



Tema 1: En cada “Clic”, un Rastro



Tema 2: Rompé la cadena de la Infodemia



Tema 3: ¡Cuidado, que no te pesquen!



Tema 4: Descubre el poder de la IA

Tema 1: En cada "Clic", un Rastro

La Huella Digital

Cada vez que haces un "clic", das un "me gusta" en las redes sociales, o cuando usas una aplicación desde tu celular, computadora o cualquier dispositivo conectado a Internet, dejás información personal. Los datos o rastros que genera tu actividad en la internet crean lo que se conoce hoy como "huella digital".

Te presentamos algunas acciones que construyen tu Huella Digital.

- Realizar búsquedas en Internet: Los sitios web que visitas, y las páginas que sigues en redes sociales forman parte de tu historial de navegación en línea.
- Ingresar a sitios con Usuario y Contraseña: Tu nombre de usuario, contraseñas y direcciones de correo electrónico asociadas a cuentas en línea también son parte de tu huella digital.
- Interactuar en Redes Sociales: Los comentarios, publicaciones y fotos que compartes en redes sociales son rastros que dejas a diario.
- Compartir tu ubicación: La ubicación activa en tu celular permite saber qué lugares frecuentas.
- Escuchar música o ver videos: La música que escuchas o las películas que ves en plataformas Streaming se registran y hacen que otros sepan de tus gustos personales.
- Comprar por Internet: Adquirir productos en tiendas "on line" habla de tus preferencias y permite registrar tus consumos.
- Chatear o enviar mensajes a personas: Cuando te comunicas con otras personas por medio de aplicaciones das a conocer con quién te relacionas.

Seguramente en este momento se te ocurren otras cosas que realizas a diario y que hablan de vos. En general todas las acciones que haces en línea dejan rastros que crean tu huella digital en Internet.

Si visualizas el siguiente video titulado Microaprendizaje: ¿Qué es la huella digital? publicado por el Portal Educar podrás aprender más sobre este tema



Captura de pantalla del video en portal Educar
https://www.youtube.com/watch?v=fb506ebswb8&t=6s

A continuación, teniendo en cuenta lo que viste en el video te invitamos a pensar la respuesta a la siguiente pregunta

1.1 ¿Cuáles de las siguientes situaciones que ocurren a diario en las redes, consideras que podrían ser producto de tu huella digital en Internet?

- El diario La Nación publica en su sitio web una columna con información referida a los consumos problemáticos de los adolescentes.
- Recibimos una oferta de productos electrónicos mientras recorremos nuestro Instagram.
- Encontramos en nuestro correo electrónico las fechas de exámenes regulares del año en curso.
- Navegando en Internet encontramos una publicidad de un organismo del estado donde se comunica la habilitación de una ciclovía cerca de mi barrio.
- Recibimos una llamada de WhatsApp de un número desconocido.

Anteriormente te contamos qué acciones crean tu huella. Ahora te proponemos conocer qué programas automatizan la creación de esa huella.

Las Cookies. Nuestros datos al alcance de otras personas.

Las Cookies son pequeños programas con datos que se guardan en la computadora, celular o dispositivo conectado a Internet. Almacenan cierta información sobre el usuario, por ejemplo, su comportamiento de navegación. Cuando usas aplicaciones o visitas una web por primera vez, regularmente te aparecen mensajes para que aceptes sus Cookies.

Las Cookies de internet pueden tener diversas funciones, pero de forma general se puede decir que sirven para que el servidor, computadora donde se aloja un sistema, pueda identificar el equipo de un usuario y recuerde datos importantes, básicamente quién eres y qué has hecho durante el uso del mismo.

¿Cuáles son los tipos de Cookies más comunes?

Hoy la mayoría de navegadores permiten desactivar o activar las Cookies. También puedes borrarlas si no quieres que la información siga almacenada en el equipo. Sin embargo, eliminar algunas Cookies pueden limitar las posibilidades del usuario en una web o incluso impedirle el acceso. Por ello, es importante que sepas de manera general que existen distintos tipos de Cookies y que cumplen con diferentes funciones, entre ellas se encuentran las que guardan información sobre ingreso y autenticación de usuario cuando completas formularios o ingresas a algún servicio con usuario. De esta manera, podrás observar que tu usuario se recuerda para no tener que ingresarlo cada vez que hagas uso.

Por otra parte, las Cookies se usan para brindar seguridad, guardando la cantidad de intentos de acceso a una cuenta y bloqueando la misma cuando se acumulan cierto número de posibilidades.

Hoy los perfiles de usuarios a partir de la navegación web son generados por la información que envían los mismos usuarios web en forma de archivos cookies. Estos se utilizan para que las empresas envíen publicidad relacionada con sus intereses.

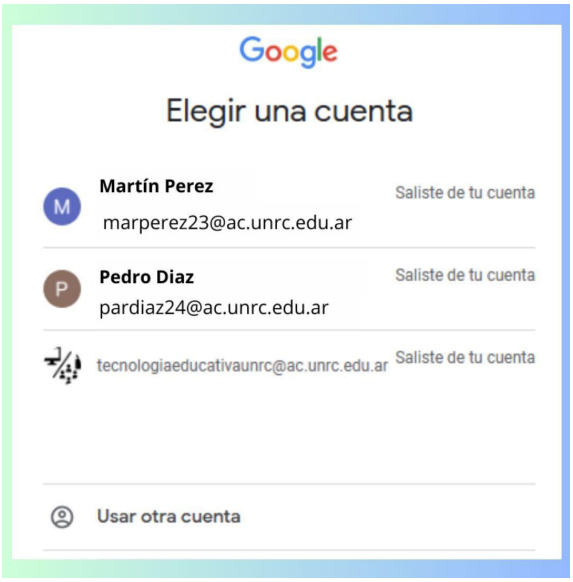
Como cierre de los expuesto, podemos decir que las Cookies no fueron creadas con el fin de perjudicar a los usuarios, sin embargo, muchos de los datos que se almacenan a partir de las mismas, son utilizados con otros fines.

Para repasar el tema, te proponemos que respondas la siguiente pregunta:

1.2 ¿En cuáles de las siguientes imágenes se visualiza la personalización de pantalla generada por Cookies?



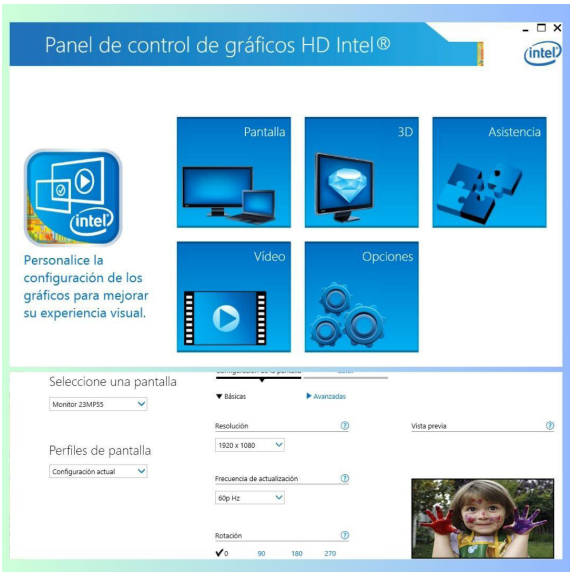
Ejecución de Antivirus



Ingreso a Correo Google



Anuncio en YouTube con una sesión de cuenta activa.



Configuración de pantalla de tu placa gráfica

¡Atención! Empresas atentas a tus rastros en la red

Vamos a hablar un poco sobre tu rastro en Internet, y mientras lo hacemos, vamos a preguntarnos: ¿A dónde van todos esos rastros? ¿Qué hacen con ellos?

Respuesta: La mayoría de estos datos son recopilados y utilizados por empresas comerciales.

En este punto es importante que tengas en cuenta este grupo de empresas Google, Apple, Meta-, Amazon y Microsoft. Estas empresas reúnen toda la información que compartimos en línea y la guardan en enormes bases de datos. Pero, ¿Qué hacen realmente con toda esa información? ¿A quién le importan nuestros datos? ¿Qué valor tendría nuestra información?

Nuestros datos importan porque sirven para hacer predicciones sobre nosotros mismos. En manos de estas empresas y de cualquier otra empresa, o incluso Estados, nuestra información se utiliza para predecir comportamientos y finalmente moldearlos. Utilizando algoritmos inteligentes se puede conocer mucho sobre nosotros, incluso más de lo que imaginamos. A veces, cuando descargamos aplicaciones o nos registramos en un sitio web, pensamos que no tiene consecuencia, pero en realidad estamos compartiendo información personal. Esto puede ser un problema, porque estamos exponiendo nuestra privacidad y permitiendo que algunas empresas conozcan demasiado sobre nosotros. Es como darles una llave para espiar nuestras vidas y usar esa información para su beneficio. A menudo, aceptamos los 'términos y condiciones' sin leerlos, y esto puede ser un error. Incluso nuestras fotos en redes sociales pueden revelar más de lo que pensamos sobre nuestras vidas. ¡Es importante estar conscientes de esto y cuidar nuestra privacidad en línea!"

Muchas veces al navegar por la web, comenzamos a recibir recomendaciones de productos y anuncios que parecen estar hechos a medida; ¡sorpresa! Sí, están hechos a medida. Esto puede suceder en nuestro correo electrónico personal, en Facebook, Instagram o incluso en los anuncios que aparecen en las páginas de internet.

Lo que ocurre es que nuestras actividades en línea, como lo que buscamos y hacemos en la web, son un tesoro. Las empresas usan esta información para predecir qué nos podría interesar y luego venden esas predicciones a otras empresas.



1.3 Para reflexionar sobre lo que expusimos te proponemos pensar y explicitar la respuesta a esta pregunta ¿Cuáles de los siguientes datos, vinculados a las acciones cotidianas que hacemos en las redes, crees que podrían ser tomadas por el grupo de empresas líderes en comunicaciones con el fin de dirigirnos sus anuncios comerciales?

- Los datos de la tarjeta de crédito utilizada para una compra “on line”.
- Tu ubicación cargada en una aplicación de pedidos en línea.
- Las búsquedas realizadas en un buscador sobre temáticas de tu interés.
- Tu usuario y contraseña de correo electrónico.
- Los videos vistos en YouTube.

La imposibilidad de borrar nuestra Huella Digital en Internet

Imagina que nuestra huella digital es como una huella que dejamos al caminar, pero en lugar de desaparecer con el tiempo, esta huella digital crece y nunca se borra. Esta huella incluye elementos como fotos, videos, comentarios en redes sociales, suscripciones y otros datos personales que dejamos en línea. Algunos de estos datos son sensibles, llegando a contar muchas cosas de nuestra vida personal. Lo que es complicado, una vez que algo se publica en Internet, es lo difícil de hacer que desaparezca por completo. Puedes borrarlo, dejarás de verlo, pero esa información brindada fue tomada y ya está circulando en la red. También puede ocurrir que terceros publiquen información y allí la gestión para borrar el contenido es aún más compleja.

Esto puede ser un problema cuando se trata de nuestro derecho a la privacidad. Si pedimos que se retiren ciertas publicaciones de la web y no sucede, esto puede ser una violación de nuestro derecho a que cierta información sea quitada de las redes. En otras palabras, nuestra privacidad y nuestro derecho a que se borre cierta información en línea pueden verse afectados cuando nuestros datos sensibles se comparten sin nuestro permiso.



Ahora, te invitamos a conocer algunos casos donde la imposibilidad de borrar información personal de la red ha llevado a la intervención de la justicia.

“Llevo 6 años luchando para que Google borre una información falsa sobre mí” - Ulrich Richter

“No busco dinero sino defender mis derechos” Natalia Denegri

Gestioná tu identidad digital, reduce tu huella.

Reducir tu huella digital no es algo simple y requiere en especial de un uso muy responsable y consciente de todos los servicios que brinda la Red. En este material brindamos algunas herramientas básicas para que puedas hacer un uso responsable y más cuidado. Finalmente queremos acompañar este objetivo con algunos consejos puntuales que puedas recordar fácilmente.

- Limita la cantidad de información personal que compartes en línea. Debes tener mucha precaución al publicar información personal como tu dirección postal o electrónica, número de teléfono, fecha de nacimiento o cualquier dato personal. Siempre que lo hagas, que sea de manera privada con el destinatario. No olvides que mucha información personal puede ser publicada de forma implícita por imágenes que compartes.

- Elimina tus cuentas inactivas. Si tienes cuentas en línea que ya no usas, es una buena idea eliminarlas para reducir tu huella digital.

- No aceptes cookies de sitios desconocidos.

- Navega de modo incógnito si no usas un dispositivo propio.

- Lee atentamente “El Contrato” (término y condiciones) que aceptas al instalar aplicaciones.



Chequear si tus respuestas fueron correctas consultando en el anexo en Claves de respuestas Tema 1

Tema 2: Rompé la cadena de la Infodemia

Desde que el director de la **Organización Mundial de la Salud** (OMS) en plena propagación del Covid 19, proclamara que "*no solo luchamos contra una epidemia, sino también contra una infodemia*", se comenzó a utilizar este término para referirse a la "sobreabundancia de información, alguna rigurosa y otra no, que hace que para las personas sea difícil encontrar recursos fidedignos y una guía de confianza cuando la necesitan". (OMS, 2020)

La cantidad excesiva de información sobre un problema o un tema puede dificultar encontrar la respuesta correcta. Además aumenta la propagación de noticias falsas o "fake news " que pueden provocar la estigmatización, la discriminación e incluso la violencia. Estas noticias se crean para generar mayores visitas en sitios web, desprestigiar, desinformar y manipular la opinión pública.

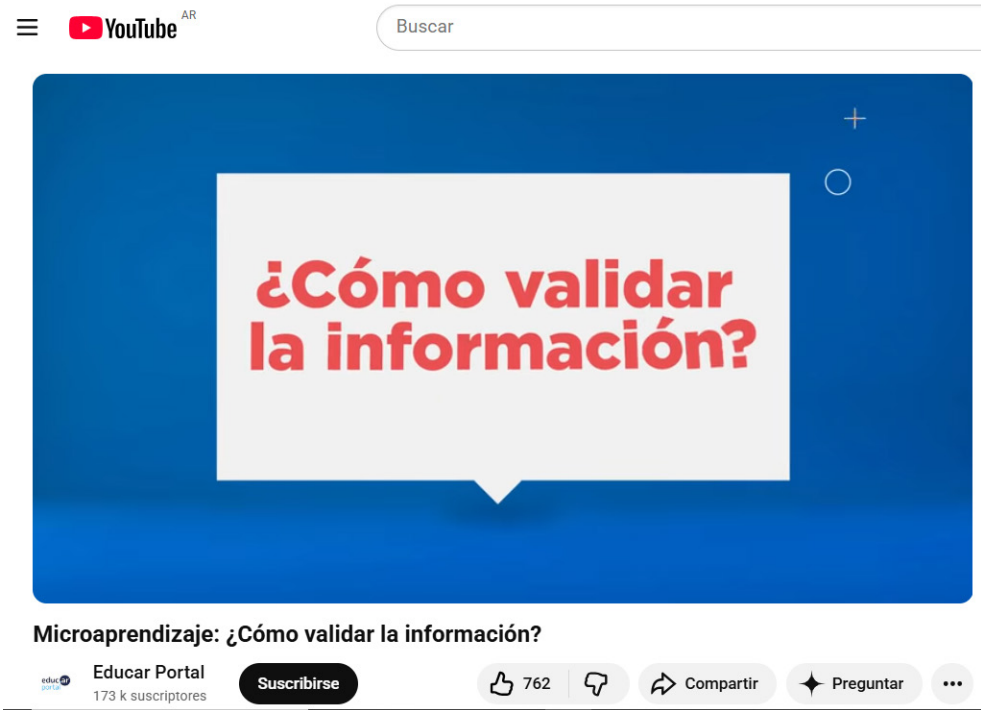
En el momento de buscar información por la web es necesario considerar criterios de validación y evaluación y así poder seleccionar el contenido correcto y adecuado a nuestros intereses y necesidades.

¿Con qué criterios podemos analizar si una información, noticia o mensaje que nos llega o encontramos en los medios digitales es verdadera o falsa?

- Comprobar las fuentes o el lugar de donde proviene la información o las noticias y sus autores.
- Estar alerta sobre los mensajes que nos llegan por las redes. Mantener una actitud crítica al recibir una información o mensaje.
- Leer el mensaje o la noticia completa antes de compartirla. No quedarse sólo con el título y la imagen.
- Si es una noticia verifica la fecha de publicación. En algunos casos se viralizan mensajes o informaciones que son de otros años.
- Observa bien la URL o dirección del sitio web porque se pueden hacer pasar por sitios verdaderos que tienen un nombre parecido. A veces una sola letra o símbolo distinto en la dirección implica un sitio o perfil falso.
- En los sitios web, considera también la calidad, la navegabilidad, la accesibilidad, la legibilidad y organización de la información.

Entonces, ¿cómo validar la información que circula por internet?

Visualiza el siguiente video titulado Microaprendizaje: ¿Cómo validar la información? realizado por el Portal Educar.



Captura de pantalla del video en portal Educar
https://www.youtube.com/watch?v=oBtjjDC4vS0

¿Qué hacer ante un mensaje o noticia dudosa o falsa?

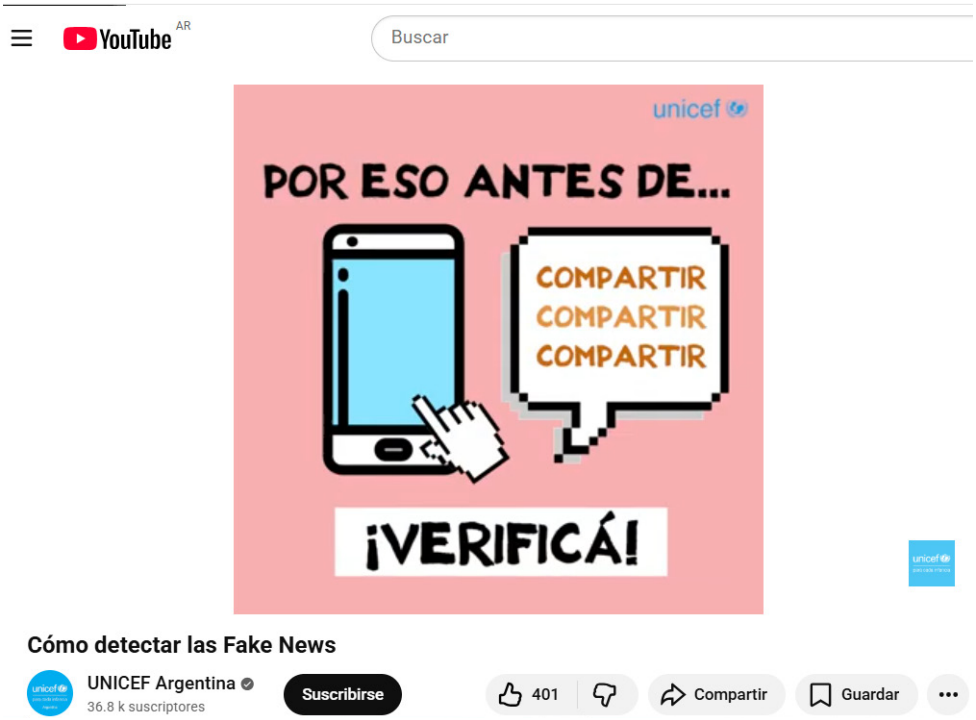
Lo primero a tener en cuenta es no compartir, reenviar o poner me gusta o alguna otra reacción. Cuando hacemos clic crece el valor económico de la publicación. Es importante siempre que aparece una noticia dudosa corroborar con una búsqueda en Google para ver si aparece en otros medios de comunicación.

Otra acción clave es llamar la atención a nuestros contactos si reenvían o comparten mensajes falsos.

También se puede recurrir a sitios especializados que se encargan de detectar noticias falsas. Es recomendable denunciar o realizar un reporte a la red social si han creado un perfil falso con tu identidad. Solo la persona cuya identidad se está suplantando puede realizarlos. Además, si reconoces un perfil falso de otra persona avísale para que pueda hacer la denuncia.

Es importante saber que cuando realizamos una consulta sobre un tema en los buscadores nos aparece un listado de sitios a enlaces donde podemos buscar las respuestas. Esto no significa que los datos sean correctos, verdaderos y confiables. Siempre hay que considerar las medidas de validación y evaluación de la información.

Para ampliar la información te invitamos a visualizar el siguiente video titulado Cómo detectar las Fake News realizado por UNICEF Argentina.



Captura de pantalla del video en UNICEF Argentina
https://www.youtube.com/watch?v=n_wtdAaY_hs

Ahora te proponemos que respondas las siguientes preguntas.

2.1. Luciana está cursando 6to año de la escuela secundaria. La profesora de Formación para la Vida y el Trabajo le ha pedido que busque información en internet sobre carreras universitarias que son de su interés. Luciana abre Google desde su celular y escribe "estudiar agronomía".

¿De acuerdo a los posibles resultados obtenidos, cuáles serían los sitios educativos confiables para encontrar información sobre la carrera elegida?

- https://www.quierouniversidad.com.ar/
- https://www.yahoraqueestudio.net/
- https://www.unl.edu.ar/carreras/ingenieria-agronomica
- https://www.unrc.edu.ar/
- https://www.unr4.edu.ar/

2.2 Es posible que Luciana en su primera búsqueda haya considerado la extensión del dominio de la dirección web.

Verdadero, con solo identificar la extensión es suficiente para reconocer que es un sitio confiable por ser educativo.

Falso, no solo pudo tener en cuenta la extensión de la dirección sino también las letras que no hayan sido cambiadas con el riesgo que sea un sitio clonado o falso.

2.3 Luciana decide ingresar al sitio web de la Universidad Nacional de Río Cuarto y consultar sobre el plan de estudios de la carrera de Ingeniería Agronómica. Cuáles son las variables en relación al contenido que permiten considerar al sitio como confiable.

- El reconocimiento de la institución a la que pertenece la información o contenido.
- La cantidad de contenido.
- La cantidad de videos e imágenes.
- La calidad y organización del contenido.
- La calidad, actualización, reconocimiento de la autoridad o institución y organización de los contenidos.

2.4 Siguiendo con su tarea, Luciana decide buscar información en internet sobre la salida laboral de un ingeniero agrónomo y qué tipo de actividades podría realizar en un futuro en su localidad o región. Del listado de páginas web que proporciona su búsqueda decide ingresar al sitio www.soyagronomo.net.cl. Allí encuentra información sobre qué hace un ingeniero agrónomo y un listado de los lugares donde puede trabajar. Siguiendo los criterios para validar y evaluar sitios web de acuerdo a la calidad de contenidos e intereses, ¿Qué debe tener en cuenta Luciana?

- Si el sitio web aparece en los primeros lugares de la lista.
- Si el sitio web brinda información clara, aunque no reconoce el responsable del sitio ni hay referencias sobre la fuente.
- La cantidad de imágenes llamativas que tiene el sitio.
- La dirección o dominio del sitio web.
- Realizar una búsqueda de la misma información en otros sitios para comparar resultados.

2.5 Según los criterios analizados ¿El sitio soyagronomo.net.br es el más pertinente según sus intereses y para la información que busca?

Sí No

2.6 Luciana al revisar sus redes sociales recibe el siguiente mensaje, ¿qué le haría suponer que es una noticia falsa?



- El poco texto que tiene.
- Los errores de ortografía.
- Los títulos llamativos.
- Que el enlace no funciona.
- Que no aparece un email.
- Que no se reconoce al autor.

2.7 ¿Qué debería hacer Luciana ante la aparición de esta noticia en sus redes sociales?

- Compartir con sus amigos para alertarle.
- Poner no me gusta.

✱ Comprobar la noticia con otras fuentes.

2.8 Para reflexionar ¿Te parece que la desinformación puede influir en la forma de pensar y actuar de las personas? ¿Como estudiante y ciudadano que interactúa en el mundo digital, cuáles son las habilidades y responsabilidades que deberías desarrollar y fortalecer?



Chequear si tus respuestas fueron correctas consultando en el anexo en Claves de respuestas Tema 2

Tema 3: ¡Cuidado, que no te pesquen!

¿Alguna vez te preguntaste cuáles son los riesgos a los que te expones cuando navegas por Internet? Detengámonos a pensar y reflexionar.

¿Puedes hacer un listado con tus ideas iniciales sobre las posibilidades de riesgo concretas? Te invitamos a que las registres a continuación:

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Ahora, nos introduciremos en la temática leyendo y accediendo a diferentes materiales que nos ayudarán a comprender y profundizar un poco más. ¡Empecemos!

Las palabras virus, correos spam, phishing entre muchas otras, se oyen con frecuencia. Lo mismo sucede con la mención a programas maliciosos y engaños fraudulentos. Todo suena amenazante y peligroso. Es cierto, pero es importante saber que existen formas de enfrentarse a este tipo de situaciones sin dejar de utilizar los beneficios de la web.

Todo lo que hacés en la web, tiene consecuencias. Una de las amenazas a la que estás expuesto al navegar o descargar aplicaciones, por ejemplo, es la instalación automática sin que ni siquiera te des cuenta, de software creado con el fin de robarte información personal de los dispositivos que habitualmente utilizas o bien dañar tus dispositivos. A este tipo de programas se los denomina Virus Informáticos.

¿Qué son entonces? son un tipo de software malicioso o **malware** que tiene como objetivo modificar el comportamiento de la computadora sin que nos percibamos de ello. Los virus pueden bloquear la computadora, observar el comportamiento del usuario e incluso robar su información.

Con los efectos que realiza un virus sobre tu dispositivo es posible que observes algún funcionamiento extraño de tu computadora. Como un virus no es otra cosa que un programa, su ejecución ocupará memoria, procesador y por consiguiente tu máquina estará más lenta.

Los virus llegan a tu computadora por acciones concretas que puedes realizar de manera involuntaria. Según el tipo de virus, llegan a causar desde algunas simples molestias hasta, consecuencias más graves como por ejemplo, robar contraseñas o datos, registrar pulsaciones de teclado, dañar archivos e incluso, tomar el control total de tu equipo. ¿Alguna vez te pasó que cuando estás trabajando con tu computadora te aparecen pantallas o ventanas poco usuales? o que de manera imprevista aparezcan, desaparezcan o se modifique el contenido de archivos? o que la computadora esté más lenta o que se reinicie el sistema por sí solo? Bueno, éstos son algunos de los indicadores que evidencian que algo extraño está sucediendo al interior de nuestro dispositivo tecnológico.

En la actualidad, los virus también pueden afectar tu teléfono celular. Debemos estar muy atentos.

Otros tipos de programas maliciosos son los denominados caballos de Troya o **troyanos** que tienen una funcionalidad, por ejemplo, un juego, pero además tienen una función oculta como capturar las claves que escribimos y mandarlas en un mensaje de correo electrónico a otra persona y los **gusanos** que se reproducen sin necesidad de que tengamos ningún tipo de interacción, por ejemplo atacando servicios de red vulnerables.

Seguramente te preguntarás ¿qué puedo hacer yo para proteger mis dispositivos de estos programas maliciosos? El siguiente video te permitirá conocer un poco más qué son, de qué manera se propagan y cómo podrías protegerte de ellos.



Captura de pantalla del video en portal Educar
https://www.educ.ar/recursos/150258/microaprendizaje-que-es-un-virus-informatico



Ahora te proponemos que respondas las siguientes preguntas.

3.1 ¿Cuáles son algunas formas en que se podrían propagar los virus informáticos?

- Mediante la descarga de un archivo adjunto.
- Cuando se reproduce un video.
- Con una notificación que te llega cuando estás navegando un sitio web oficial validado confiable seguro.
- A través de cualquier enlace que te envíen.
- Cuando recibimos un mail de un amigo o persona de confianza y su casilla de correo está verificada.
- Todos los mensajes de correo electrónico spam contienen virus.

¿Estás listo para continuar?

3.2 Avancemos seleccionando en la siguiente actividad, la/s afirmaciones que consideres correctas.

- Todos los programas que me permiten limpiar mi computadora son seguros.
- Todos los virus necesitan de algún tipo de acción personal sobre mi dispositivo para activarse.
- No todas las acciones que realiza un troyano en mi computadora son totalmente inofensivas.
- Los gusanos sólo pueden afectar a una computadora y no hay manera que se distribuyan a otras.
- Mientras estás jugando puede activarse un programa malicioso.

Hay otros riesgos a los que estamos expuestos por ejemplo cuando accedemos a nuestro correo electrónico. Lo analizaremos juntos a continuación: Seguramente has escuchado hablar de los Spam o inclusive has visto algunos en tu correo electrónico, dentro de una carpeta especial … ¿Te ha pasado?

Es importante conocer cuáles son los correos spam sospechosos. Imagina una posible respuesta al siguiente interrogante:

Los correos electrónicos Spam ¿Ponen en riesgo nuestros dispositivos? Te invitamos a averiguarlo...

Un correo Spam, es un correo electrónico de distribución masiva y con contenido normalmente publicitario o malicioso, que se recibe sin haber sido solicitado y generalmente de remitentes desconocidos.

El correo electrónico de remitente desconocido, es el tipo más común de Spam. Si recibes un correo electrónico de alguien que no conoces y que nunca ha tenido ningún tipo de interacción con vos, es probable que sea Spam.

No todos los correos recibidos como Spam son peligrosos, pero es importante prestar especial atención a éstos y si tienen un archivo adjunto o enlace que generan alguna duda, lo mejor es evitar abrirlos. Generalmente, los servicios de correo disponen de una carpeta especial destinada a colocar de manera automática los correos que podrían ser Spam.

Existen algunos Spam verdaderamente peligrosos. Estos pueden contener información inapropiada o enlaces a sitios web maliciosos con la intención de robar información financiera, contraseñas, números de cuenta u otra información personal. Cuando nos solicitan como respuesta datos personales, claves o nos invitan a acceder a sitios desconocidos, es probable que estemos ante la presencia de un correo potencialmente peligroso, en ese caso lo mejor es no hacer lo que nos piden y borrarlo de nuestro buzón de correo, dado que en este caso podemos estar hablando de otro riesgo que se llama phishing y que abordaremos luego.

Mientras sea correo Spam que no te pida ningún dato personal o acceso a determinados sitios, no habría problemas más allá de llenar nuestro buzón de mensajes.



3.3 ¿Cuál/es de las siguientes situaciones podrían reflejar casos de Spam?

- Si iniciaste un proceso de autenticación y recibís un mensaje para la verificación de la cuenta de correo.
- Cuando recibes un correo en el que aparece publicidad de Mercado Libre
- Cuando te piden que confirmes por correo algún dato personal y el remitente no se corresponde con alguien que conoces.
- Cuando el correo recibido es de remitente desconocido y presenta un enlace para hacer el pago de alguna cuenta.
- Cuando se recibe un correo cuyo remitente es tu colegio y te informa las fechas de examen.

Hemos trabajado hasta aquí, con dos posibles riesgos, pero hay otros. Aprenderemos ahora acerca del phishing. Sigamos trabajando.

¿Te pescaron alguna vez? ¿A qué se denomina Phishing?

La palabra Phishing (del inglés fish: pescar) consiste en una forma de engaño mediante la cual se envía un mensaje de correo electrónico o de las redes sociales a una o varias personas, intentando convencerlas de que ingresen a sitios falsos que se asemejan a los legítimos, para obtener información confidencial como contraseñas, números de tarjetas de crédito o información bancaria.

Por lo general, intentan persuadirte con mensajes que suelen estar prolijamente redactados, que vienen a nombre de personas o empresas aparentemente reales pero que resultan ser remitentes engañosos, que utilizan la información recolectada para acciones delictivas.

En las comunicaciones digitales que nos envían, suelen crear sensación de urgencia o miedo: “tu cuenta será bloqueada”, “tienes un cargo pendiente”, etcétera, ya que, bajo presión, es más fácil que actuemos sin pararnos a pensar.

¿Cómo podemos hacer para protegernos del Phishing?

Dado que tanto los anuncios como los correos y las webs imitan a las auténticas, debemos tener siempre precaución cuando pensemos que estamos ante algo oficial y comprobar su autenticidad:

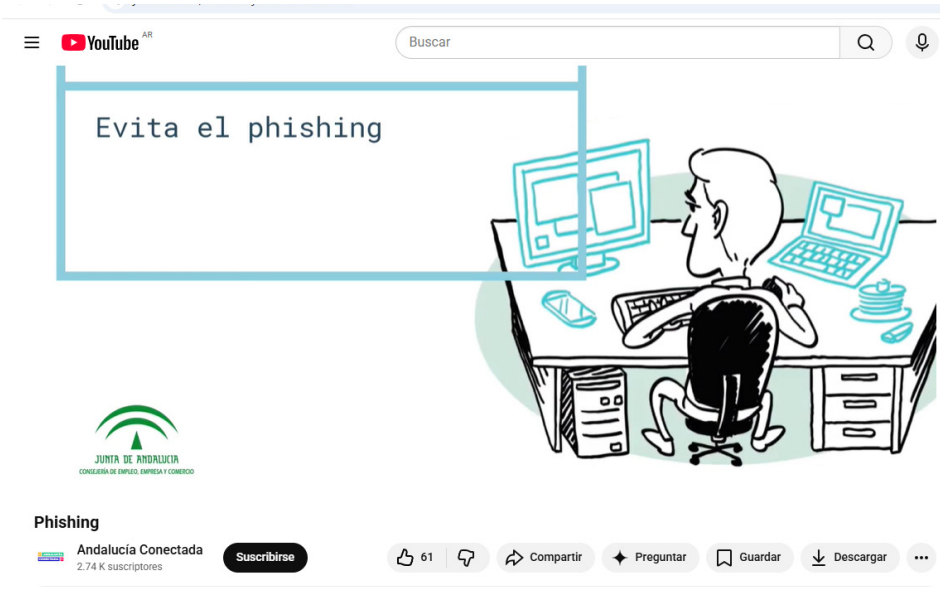
- Si es una página web, debemos comprobar que estamos ante una conexión segura y la dirección corresponde realmente con la que se supone que debe ser. Por ejemplo, si estamos en una página que debería ser de Amazon, pero vemos que su dirección es algo así <http://amazon.mark-soon.jp> es que estamos ante un fraude
- Los mensajes son urgentes y suelen requerir una acción inmediata.
- Nos piden datos bancarios o personales a través del correo, algo que nunca hacen las entidades bancarias.
- Se debe comprobar que el remitente de correo se corresponde con quién debe ser. Por ejemplo, un correo que debería ser de Google, pero en su lugar vemos que el remite es <google@googlemaildiv45.com> es que es falso.

Entonces, por favor, antes de proporcionar información o hacer clic en enlaces, verifica la legitimidad de la fuente a través de canales oficiales, no hagas clic en enlaces recibidos por email o mensajes de origen desconocido y no des nunca datos de tus cuentas (usuario y contraseña) por medio de correos o redes.

Profundizamos un poco más accediendo a ¿Qué es el phishing?

¿Qué te pareció la lectura del material? ¿Identificaste alguna situación personal en la cual puedes haber sido víctima de phishing?

¿Continuamos? Te invitamos a observar el siguiente video:



Captura de pantalla del video en Andalucía Conectada
https://www.youtube.com/watch?v=jlmBCYm6IZk&t=4s

Veamos ahora, cuál es la diferencia entre Correos Spam y Phishing.

La diferencia principal está en la intención y el riesgo:

Spam: Es correo no deseado enviado masivamente. Suele buscar publicidad, promocionar productos, generar visitas o saturar bandejas de entrada. Es correo denominado coloquialmente como “basura”.

Ejemplos comunes:

- Ofertas milagrosas
- Publicidad de casinos
- Promociones falsas o exageradas
- Suscripciones que nunca pediste

Molesta, pero no siempre busca robarte datos.

Phishing: Es un tipo de fraude diseñado para engañarte y robar información: contraseñas, tarjetas, códigos bancarios o acceso a cuentas. Normalmente imita a empresas reales como Google, Microsoft, Mercado Libre, bancos o redes sociales.

Ejemplos comunes:

- “Tu cuenta fue bloqueada, ingresá acá”
- “Tenés un paquete retenido”
- “Verificá tus datos bancarios urgente”
- Enlaces a páginas falsas casi idénticas a las reales
- Busca perjudicarte directamente.

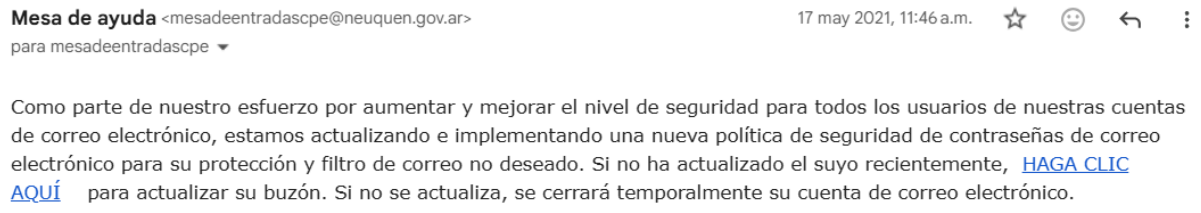
Una observación a tener en cuenta:

- **Muchos correos de phishing también son spam, porque llegan masivamente. Pero no todo spam es phishing.**
- **Si solo molesta probablemente sea un correo spam.**
- **Si pide datos, contraseña, pagos o urgencia posiblemente se trate de phishing.**

3.4 Te proponemos ahora, que analices cada una de las siguientes imágenes y especifiques si se trata de:

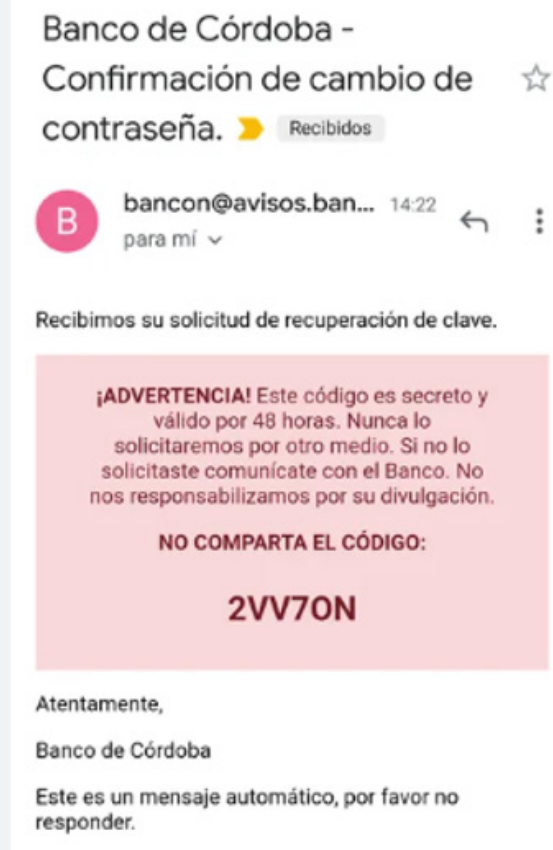
- correos spam
- phishing
- ambos riesgos a la vez
- ninguno de esos riesgos

Te pedimos que registres además, qué datos específicos de la imagen te permitieron determinar tu elección.


Mesa de ayuda <mesadeentradascpe@neuquen.gov.ar> 17 may 2021, 11:46 a.m.
para mesadeentradascpe

Como parte de nuestro esfuerzo por aumentar y mejorar el nivel de seguridad para todos los usuarios de nuestras cuentas de correo electrónico, estamos actualizando e implementando una nueva política de seguridad de contraseñas de correo electrónico para su protección y filtro de correo no deseado. Si no ha actualizado el suyo recientemente, HAGA CLIC AQUÍ para actualizar su buzón. Si no se actualiza, se cerrará temporalmente su cuenta de correo electrónico.


[Rectorado] Edición 1106 del semanario de la UNRC
prensa@rec.unrc.edu.ar
para Facayv, Faceco, Facexa, Fachum, facing, rectorado
inglés
español
Traducir mensaje
Estimados lectores,
Se adjunta la edición 1106 del semanario Hoja Aparte.
Cordiales saludos
Rectorado mailing list
Rectorado@listas.unrc.edu.ar
https://listas.unrc.edu.ar/mailman/listinfo/rectorado
Un archivo adjunto • Analizado por Gmail
Hoja Aparte
Se aprobó el calendario
hoja 1106.pdf



Banco de Córdoba - Confirmación de cambio de contraseña. Recibidos

B bancon@avisos.ban... 14:22
para mí

Recibimos su solicitud de recuperación de clave.

¡ADVERTENCIA! Este código es secreto y válido por 48 horas. Nunca lo solicitaremos por otro medio. Si no lo solicitaste comunícate con el Banco. No nos responsabilizamos por su divulgación.

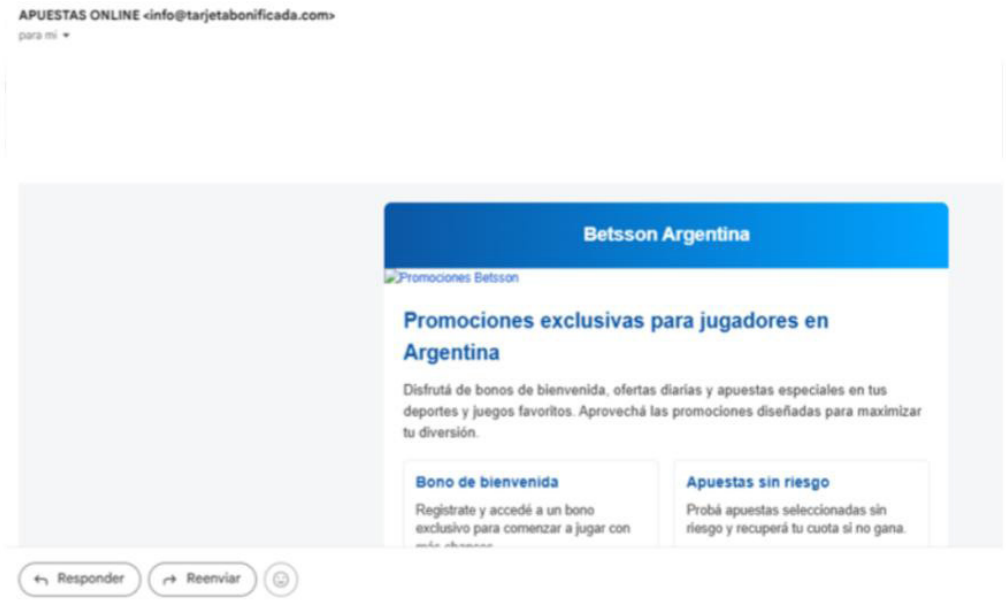
NO COMPARTA EL CÓDIGO:

2VV7ON

Atentamente,

Banco de Córdoba

Este es un mensaje automático, por favor no responder.



¿Estás listo para continuar? Veremos ahora otra forma mediante la cual podemos quedar expuestos y generarnos problemas con nuestra información personal y confidencial.

¡Cuidado con las contraseñas! ¿Cómo generar contraseñas fuertes?

Actualmente, casi toda la seguridad está basada en la elección de una buena contraseña. En la mayoría de servicios se accede escribiendo un nombre de usuario y una contraseña. Si la contraseña es fácil de averiguar, tenemos muchas posibilidades de que en un momento u otro alguien acceda a nuestros datos e incluso se haga pasar por nosotros.

Entonces podemos decir que la solicitud de una contraseña es una manera que tienen determinados sitios o aplicaciones para autenticarnos, es decir confirmar que somos nosotros y que estamos autorizados para acceder al mismo. Las contraseñas son privadas, personales, sólo vos debes saberlas, no se deben compartir, ni mostrar, ni dejar accesibles o a la vista de otros, ya que si caen en manos de personas con malas intenciones podrías quedar expuesto a riesgos, como por ejemplo el robo de identidad.

Por eso es muy importante que nunca compartas tus contraseñas, y que puedas definir contraseñas que sean fuertes, robustas, es decir difíciles de descifrar.

¿Cuándo podemos decir que una contraseña es fuerte? Cuando es difícil de adivinar o descifrar, lo que la hace más segura frente a intentos de acceso no autorizado. Las contraseñas fuertes suelen cumplir con ciertos criterios clave, que incluyen:

1. Longitud: Debe tener al menos 8 caracteres.
2. Combinación de caracteres: Debe incluir una mezcla de letras mayúsculas y minúsculas, números y caracteres especiales (como por ejemplo !, @, #, $, etc.).
3. Evitar información personal: No debe basarse en información personal que sea fácilmente deducible o que esté accesible, como nombres, fecha de nacimiento, nombres de mascotas, etc.
4. No utilizar secuencias obvias: Evitar secuencias sencillas, como “123456” o “qwerty”.
5. Única para cada cuenta: No debes usar la misma contraseña para múltiples cuentas. Si una contraseña se ve comprometida, las otras cuentas seguirán siendo seguras.



3.5 Te proponemos completar la siguiente tabla remarcando si cada una de las contraseñas es fuerte o débil según corresponda. Piensa en cada caso acerca de ¿Cuál crees que es más fácil de adivinar? ¿Cuál usaría mucha gente?¿Cuál parece más segura y por qué?

Contraseña	Fuerte	Débil
qwerty		
m%7oplñD		
1234678		
hola1234		
“!(cdFrety))		
aguanteracing		

¿Cómo mejorarías cada una de las contraseñas que identificaste como débiles?

.....

.....

.....



Chequear si tus respuestas fueron correctas consultando en el anexo en Claves de respuestas Tema 3

Tema 4: Descubre el poder de la IA

Seguramente en este último tiempo has escuchado o visto en diferentes situaciones el término IA o Inteligencia Artificial. Pero ¿Sabés qué es la IA y cómo funciona? ¿Conoces qué posibilidades ofrece? Te has detenido a pensar ¿Cuáles son los posibles riesgos que se pueden generar y cómo hacer un **uso ético** y responsable de la misma? Te invitamos a recorrer esta sección para introducirte en el tema y reflexionar al respecto. ¡Comencemos!

La inteligencia artificial está más presente de lo que pensamos.

Antes de avanzar tómate un momento para reflexionar sobre lo siguiente: ¿Qué te sugiere, en qué pensás cuando te dicen “IA” o “Inteligencia Artificial”? ¿Dónde crees que está presente la IA? ¿Has tenido contacto con la Inteligencia Artificial?

Registra a continuación lo que vos entendés y pensás. No esperamos una definición teórica, escríbelo con tus propias palabras.

Te proponemos ahora ver el video *Lo que YA sabes sobre Inteligencia Artificial*, en el que el *Youtuber Carlos Santana Vega* nos introduce en el mundo de la IA, nos da algunas pistas para comprender que tan presente está la IA en nuestras vidas y los avances que pueden venir en un futuro.



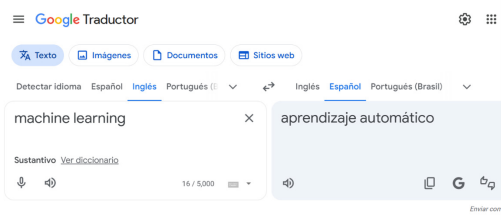
Captura de pantalla del video en YouTube

Para ver el video en el canal de YouTube hacé click sobre la imagen anterior o accedé al siguiente link: https://youtu.be/i1wGMQ3TjzA?si=DWpuRkodQ-AG3cv4

Qué bueno que sigues aquí!! ¿Pudiste ver el video? ¿Qué te pareció?

Ahora, teniendo en cuenta lo que hemos visto hasta aquí, te proponemos un primer desafío.

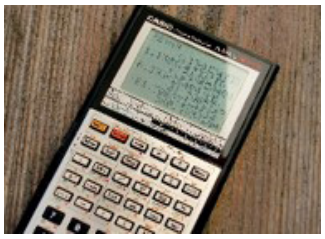
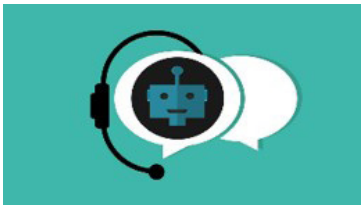
4.1 Podrías decir ¿En cuáles de estos productos tecnológicos crees que hay Inteligencia Artificial?



Traductor de Google



Puerta automática

Whatsapp	 Calculadora científica
 Auto inteligente	Recomendadores de contenidos como Netflix o Spotify
 Kit de robótica	 Chatbot
 Función de reconocimiento facial	 Enrutador de red

Si lo deseas puedes chequear si tus respuestas fueron correctas consultando el punto *Claves de respuesta para el tema 4* en el anexo.

Como habrás podido observar y reflexionar, la Inteligencia Artificial está cada vez más presente en nuestras vidas e interactuamos con aplicaciones o dispositivos que integran IA muchas veces sin darnos cuenta.

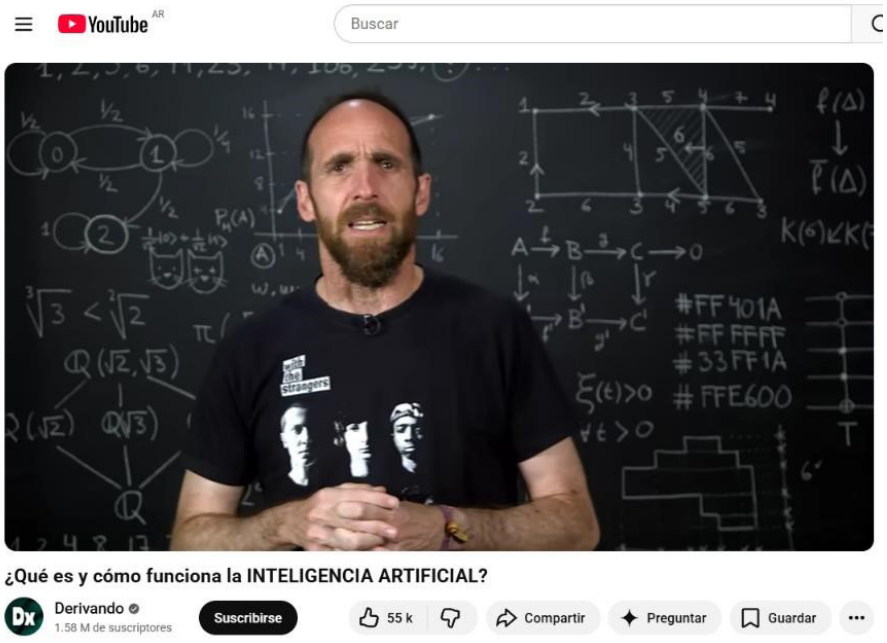
Pero entonces ¿Qué es la Inteligencia Artificial?

La Inteligencia Artificial es una disciplina del área de las Ciencias de la Computación que nació en 1956 como campo de conocimiento, investigación y desarrollo, ha atravesado diferentes estadios de evolución, cobrando mayor impulso y significatividad en estos últimos años a partir del exponencial crecimiento del poder computacional.

Científicos como John McCarthy, Marvin Minsky y otros sostienen que la IA busca lograr "la simulación con máquinas de las distintas facultades de la inteligencia, ya sea de la inteligencia humana, animal, vegetal, social o **filogenética**. Se parte de la suposición de que todas las funciones cognitivas, en especial el aprendizaje, el razonamiento, el cálculo, la percepción, la memorización e incluso el descubrimiento científico o la creatividad artística pueden describirse con una precisión tal que sería posible programar un ordenador para reproducirlas. Hace más de sesenta años que la IA existe y no ha habido nada que permita desmentir o demostrar de manera irrefutable esta especulación, que sigue siendo válida y fecunda." (Ganascia, Jean-Gabriel, 2021)

Podemos decir entonces que generalmente se utiliza el término IA para referenciar a aquellas aplicaciones o dispositivos que resultan novedosos por su complejidad, sofisticación y cuyo funcionamiento está asociado al análisis de enormes volúmenes de datos, a realizar predicciones, al procesamiento de lenguaje natural, al procesamiento automático de imágenes, a la generación automática de texto, imágenes, entre otros.

Para comprender un poquito más, sigamos avanzando de la mano del *Youtuber Eduardo Sáenz de Cabezón*, que en su video nos cuenta brevemente *¿Qué es y cómo funciona la Inteligencia Artificial?*



Captura de pantalla del video en Youtube

Para ver el video en el canal de YouTube hacé click sobre la imagen anterior o accedé al siguiente link: https://youtu.be/_tA5cinv0U8?si=YVe75naVxaej98Wy

¿Qué te pareció el video? ¿Pudiste entender mínimamente qué es la IA y cómo funciona?



4.2 Ahora te desafiamos por segunda vez. De acuerdo a lo que viste en el vídeo podrías identificar en la siguiente lista ¿Cuáles son las tareas propias de la inteligencia humana que los dispositivos con inteligencia artificial han logrado simular?

- Capacidad de cálculo
- Capacidad de memorizar datos
- Capacidad de sentir
- Capacidad de desarrollar estrategias para jugar y ganar
- Capacidad de aprender autónomamente
- Capacidad de crear
- Capacidad de tener autoconciencia
- Capacidad de reflexionar críticamente
- Capacidad de tomar decisiones
- Capacidad de aprender de sus errores



Si lo deseas puedes chequear si tus respuestas fueron correctas consultando el punto *Claves de respuesta para el tema 4* **en el anexo.**

Actualmente se asocia mucho la inteligencia artificial con el aprendizaje automático (o machine learning), entendiendo por ello al conjunto de técnicas mediante las cuales un **algoritmo** que tiene que realizar una tarea, es capaz de modificar su comportamiento de manera autónoma basándose en los datos que dispone para hacerla, en lo bien o mal que haya hecho esa tarea en situaciones pasadas, en lo bien o mal que le digan otros que ha hecho la tarea. De alguna manera esto se relaciona con la noción de entrenamiento, que forma parte de una de las etapas de desarrollo de tecnologías que utilizan IA.



4.3 Ahora un tercer desafío, teniendo en cuenta lo planteado en los videos que vimos, podrías indicar ¿Cuáles son los tipos de aprendizajes de los que se ocupa el campo del aprendizaje automático?

- Aprendizaje supervisado
- Aprendizaje remoto
- Aprendizaje significativo
- Aprendizaje no supervisado
- Aprendizaje por refuerzo
- Aprendizaje virtual
- Aprendizaje profundo
- Aprendizaje semi supervisado

Al igual que para los desafíos anteriores, puedes chequear si tus respuestas fueron correctas consultando el punto *Claves de respuesta para el tema 4* en el anexo.

Dicen que el ChatGPT "alucina" ¿Será posible?

Tal como vimos algunas de las potencialidades de la IA es la capacidad de procesamiento del lenguaje natural. Un ejemplo concreto de la aplicación de modelos de procesamiento de lenguaje natural y de técnicas de aprendizaje profundo es la creación del ChatGPT de la empresa OpenAI. Esta es una herramienta del tipo chatbot que puede producir textos similares a los que elabora una persona, y que interactúa de forma conversacional para simular que se está hablando con una persona real. ChatGPT fue entrenado con 570 GB de datos que incluyen páginas web, libros y otras fuentes, y alcanzó 100.000.000 de usuarios en 2 meses luego de su presentación.

> (...) "Gracias al aprendizaje automático, los modelos de lenguaje de gran tamaño, como ChatGPT, pueden llevar a cabo diversas tareas, como resumir, ampliar información, traducir textos, hacer predicciones, crear guiones, escribir código y generar discursos con gran precisión (Brown et al., 2020, Hernández Rizzardini et al., 2021). (...) Uno de los mayores desafíos de ChatGPT es que, aunque puede generar respuestas coherentes y a veces sorprendentes, estas respuestas pueden no ser precisas ni confiables. La falta de contexto y la naturaleza limitada del entrenamiento pueden llevar a respuestas erróneas o inapropiadas. El sesgo de los **datos de entrenamiento** también puede generar problemas de **sesgo** en las respuestas proporcionadas, lo que puede conducir a respuestas insensibles u ofensivas. Además, es importante tener en cuenta las limitaciones lingüísticas de ChatGPT, ya que se ha entrenado principalmente en inglés y su rendimiento en otros idiomas podría ser limitado. La falta de conocimiento del contexto y la comprensión profunda sobre temas éticos y morales también son factores limitantes que deben ser considerados al utilizar esta tecnología en el ámbito educativo." (Morales-Chan, M,)

Teniendo en cuenta lo antes planteado es posible ver que ChatGPT también puede tener puntos débiles, entre ellos la generación de respuestas falsas cuando no tiene suficiente información, o la creación de respuestas con estilo y estructura muy verosímil pero incorrectas, inventadas. En estas situaciones es que se dice que "ChatGPT Alucina". Por eso siempre que usamos este tipo de tecnología resulta fundamental conocer sobre el tema y/o poder corroborar con otras fuentes de información confiables las respuestas que nos da. Así que, si estás pensando en usar ChatGPT, recuerda esto que te contamos y toma medidas para hacer un uso responsable de esta tecnología.

Para ayudarte en ese sentido, te compartimos aquí un diagrama de flujo elaborado por *Aleksandr Tiulkanove* que puede ayudarte a decidir en qué situaciones puede ser apropiado utilizar esta herramienta y en cuáles no.

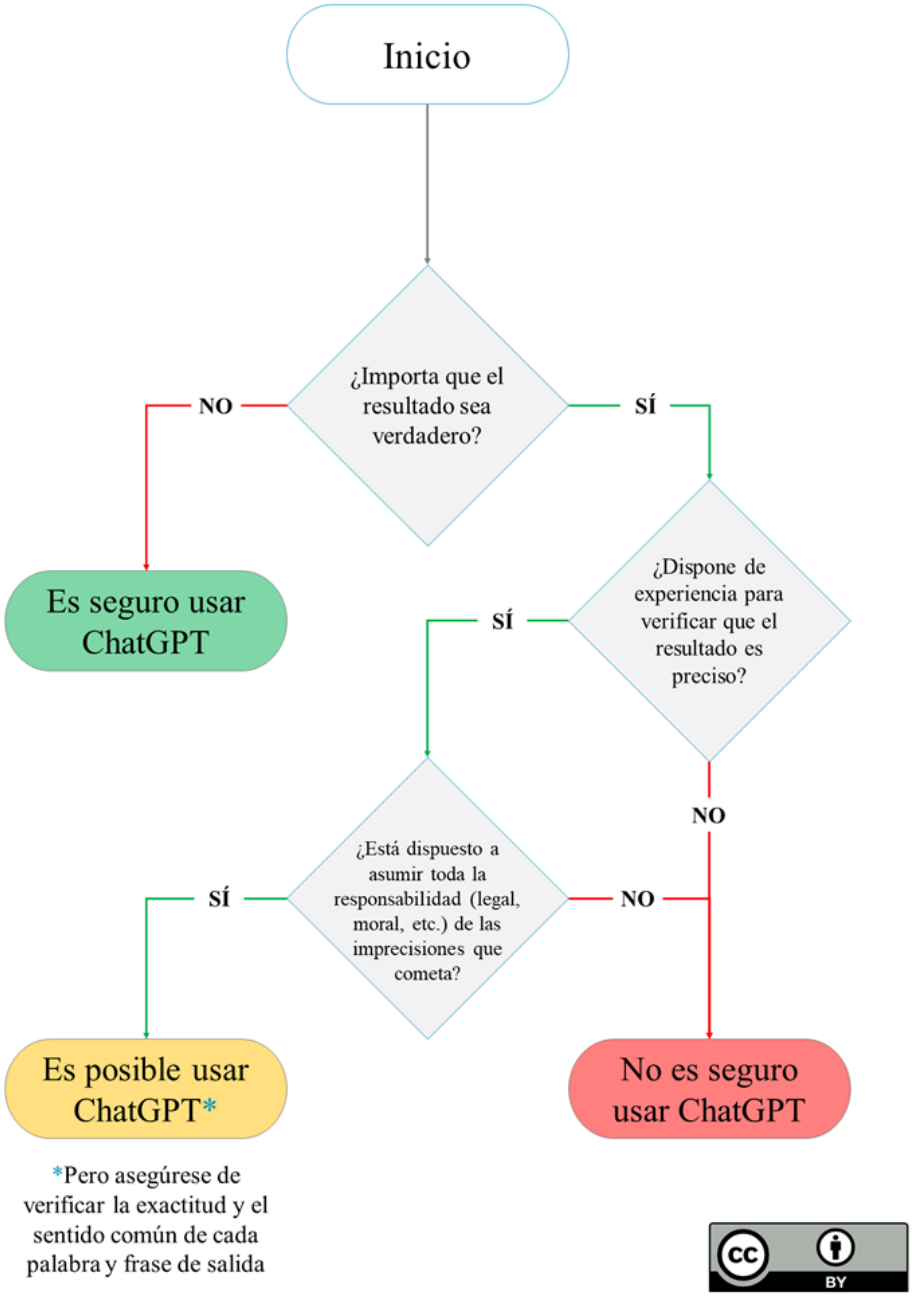


Diagrama de flujo elaborado por Aleksandr Tiulkanov, enero de 2023. Extraído del material de la UNESCO titulado ChatGPT e Inteligencia Artificial en la educación superior: Guía de inicio rápido.

Cabe aclarar que si bien el diagrama anterior, al igual que en otras definiciones o ejemplos, se presenta incluyendo como ejemplo sólo a ChatGPT, lo que se plantea allí debe ser considerado siempre que se utilice cualquier otra herramienta similar de IA generativa como por ejemplo Gemini, Claude, Copilot, Grock, DeepSeek, etc.



4.4 Ahora te proponemos un cuarto desafío, piensa en la siguiente situación. Tu profe de historia les pide que sean creativos y elaboren un guion para una obra de teatro que cuente con un poco de humor los hechos históricos de la declaración de la independencia. Uno de tus compañeros propone que usen el ChatGPT para hacer la tarea. ¿Cuál de las siguientes recomendaciones tendrías en cuenta para hacer un uso responsable y ético de esta tecnología?

- Contarle al profesor que queremos usar ChatGPT para hacer la tarea así nos orienta.
- No es necesario decir nada, los profesores no tienen forma de saber que usamos ChatGPT.
- Decir en el guion que ha sido creado utilizando IA.
- Contrastar con otras fuentes la veracidad de la información sobre los hechos históricos.
- Describir qué partes se han hecho con el ChatGPT y cuáles ha hecho nuestro grupo.
- No es necesario hacer nada, es una tecnología como cualquier otra de las que ya usamos.



De la misma manera que antes, puedes chequear si tus respuestas fueron correctas consultando el punto *Claves de respuesta para el tema 4* en el anexo.

¡Ya vamos llegando al final de este recorrido!

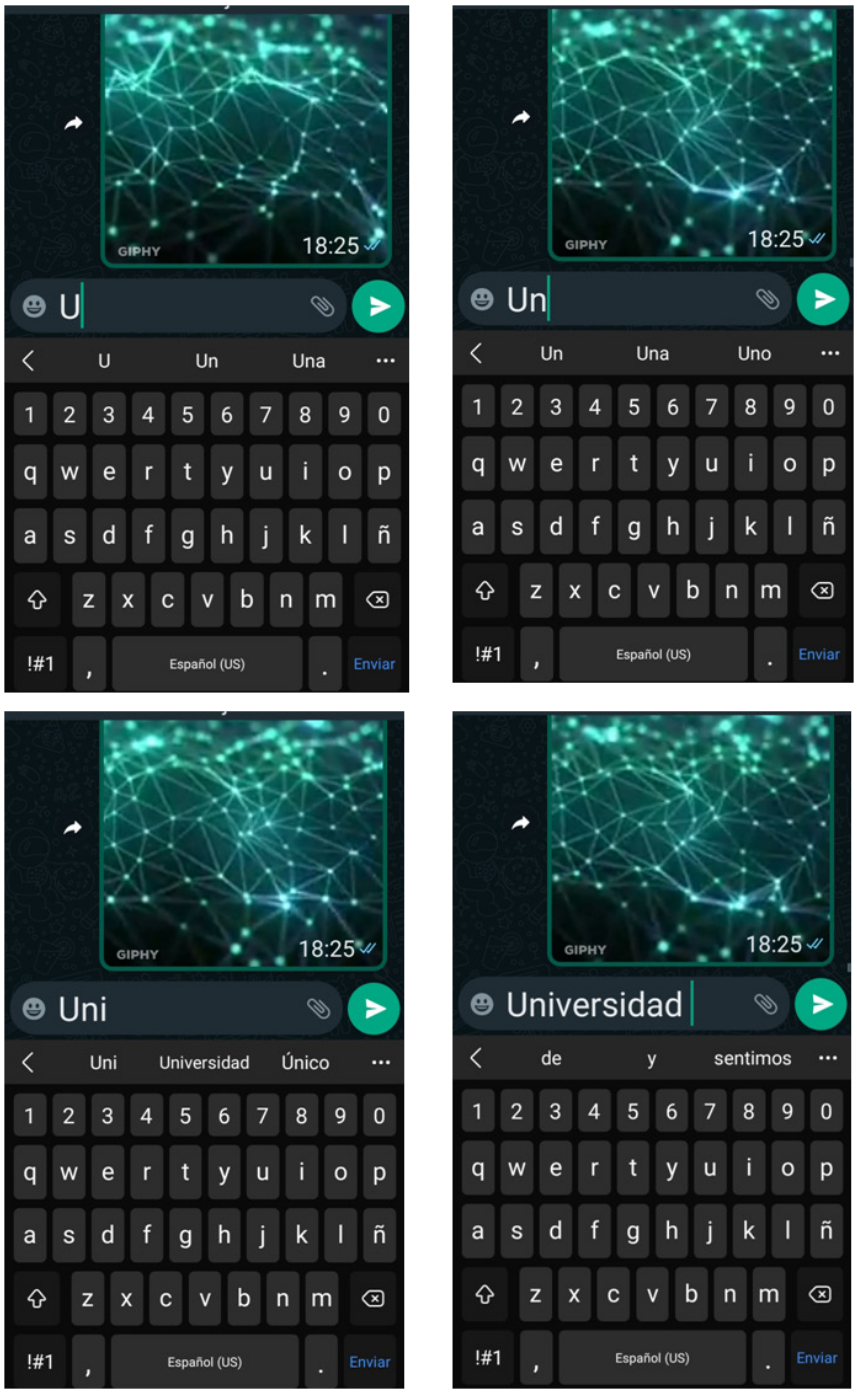
Como cierre te queremos invitar a realizar un experimento y relacionar algunos conceptos que estuvimos trabajando en esta sección. Para realizar el experimento necesitas un celular que tenga instalado WhatsApp y el **predictor de texto** activado.

¿Estás listo para realizar el experimento? Entonces, ¡manos a la obra!

Abre algún chat, y escribe la letra “U” y toma nota de todas las palabras que te sugiere el predictor de textos, luego ingresa la “n” y toma nota de las sugerencias, a continuación escribe la “i” y anota las palabras sugeridas, continua así repitiendo estas acciones por cada letra que falta completar de la palabra “universidad”. Puedes detenerte cuando te sugiera la palabra completa, presta atención y registra en qué letra te sugiere la palabra “universidad” y si seleccionas esa predicción que otras palabras te sugiere. Luego pídele a otra persona que con su propio celular haga el mismo experimento, registra las palabras que le sugiere al ingresar de a una por vez cada letra de la

palabra “Universidad”, y toma nota también en que letra le sugiere la palabra completa y que otras palabras sugiere al elegir esa palabra.

En la imagen siguiente puedes ver un ejemplo con el proceso que fuimos haciendo y del resultado que obtuvimos nosotros en el experimento.



Captura de pantalla del celular con la interacción generada en WhatsApp



4.5 Ahora, un quinto y último desafío, teniendo en cuenta estos tres resultados (el que te compartimos anteriormente, y los que obtuviste vos y la otra persona al hacer el experimento), reflexiona sobre lo siguiente.

¿En los 3 celulares WhatsApp sugirió las mismas palabras para cada letra ingresada? ¿Recomendó por primera vez la palabra completa "universidad" al ingresar la misma letra en los distintos celulares? ¿Por qué te parece que ocurre esto? ¿Qué necesita el predictor de textos de WhatsApp para hacer una predicción o recomendación? ¿Cómo crees que se relaciona esto que observaste en el experimento con las nociones de "Aprendizaje automático" y de "Datos de entrenamiento"?

Registra brevemente a continuación lo que pensaste, las ideas que se te ocurrieron.



De la misma manera que antes, puedes chequear si tus respuestas fueron correctas consultando el punto *Claves de respuesta para el tema 4* en el anexo.

Esperamos que este recorrido que compartimos te haya acercado un poquito a algunas nociones básicas relacionadas a la Inteligencia Artificial y a por qué es necesario tomar algunos recaudos al desarrollar, entrenar y utilizar tecnología de IA para poder hacerlo de manera responsable y ética. Esto fue sólo una pequeña introducción, hay un montón para seguir explorando y aprendiendo sobre este campo de conocimiento, si despertamos tu interés y curiosidad, te alentamos a conversar con tus profes para que puedan ayudarte y orientarte en el estudio de estos temas. Que nada te detenga en el camino de seguir aprendiendo un poquito más cada día!

Fuentes consultadas

Ganascia, Jean-Gabriel. (2021) Inteligencia artificial: entre el mito y la realidad. Citado en Octubre 2023. Disponible en: https://es.unesco.org/courier/2018-3/inteligencia-artificial-mito-y-realidad

Fundación Sadosky. (2023) ¿Qué necesita la IA para ser IA? Citado en Octubre 2023. Disponible en: https://curriculum.program.ar

Morales-Chan, Miguel A. (2023) Explorando el potencial de Chat GPT: Una clasificación de Prompts efectivos para la enseñanza. Citado en Octubre 2023. Disponible en: http://biblioteca.galileo.edu/tesario/handle/123456789/1348

Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura. (2023) ChatGPT e Inteligencia Artificial en la educación superior. Citado en Octubre 2023. Disponible en: https://unesdoc.unesco.org/ark:/48223/pf0000385146_spa

Organización Mundial de la Salud. Conferencia de Seguridad de Múnich, 15 de febrero de 2020. Múnich: OMS; 2020. Disponible en: Conferencia de Seguridad de Múnich (who.int). Disponible en https://www.who.int/es/director-general/speeches/detail/munich-security-conference

Real Academia Española. Diccionario de la lengua española. Consultado en Abril 2025. Disponible en: https://dle.rae.es/

Sitio web Argentina.gob.ar. ¿Cómo reconozco una noticia falsa en internet? Disponible en: https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/como-reconozco-una-noticia-falsa

Actividad metacognitiva

Finalmente te invitamos a reflexionar sobre cómo fue tu experiencia al interactuar con este material respondiendo a las siguientes preguntas:

1. ¿Te ayudó a cambiar tu forma de participar en el mundo digital? ¿Qué cambios has observado?
2. ¿Has logrado reconocer algunos riesgos a los que podés estar expuesto al interactuar con los medios digitales? ¿Cuáles?
3. Como ciudadano digital ¿Qué habilidades y responsabilidades crees que aún deberías seguir fortaleciendo?
4. ¿Qué consideras necesario cambiar en tu forma de utilizar la inteligencia artificial para hacer un uso responsable, ético y seguro?
5. ¿Te quedó alguna duda o surgieron inquietudes que no pudiste resolver con este material? ¿Cuáles?
6. ¿Cómo valoras este material?

Completá y enviá tus respuestas a la UNRC a través del siguiente formulario web:

https://forms.gle/6P3h51vtmp49EPtS8



Captura de pantalla del formulario web
https://forms.gle/6P3h51vtmp49EPtS8

Glosario

Cuenta Activa: Se define generalmente como aquella cuenta que ha realizado al menos una acción dentro de la plataforma en los últimos dos años, según el servicio digital al que se refiera.

Modo Incógnito: El modo incógnito (o navegación privada) se define como una función de los navegadores web que crea una sesión de navegación temporal aislada de la sesión principal.

Organización Mundial de la Salud (OMS): es el organismo de las Naciones Unidas (ONU) especializado en gestionar políticas de prevención, promoción e intervención en salud a nivel mundial. Fue fundada el 7 de abril de 1948 en Ginebra (Suiza) Actualmente lo integran 194 Estados Miembros distribuidos en más de 150 oficinas en todo el mundo.

Malware: También denominado "software malicioso". Es un término abarcador que describe cualquier programa o código malicioso que es dañino para los sistemas. El malware puede instalarse en tu computadora cuando navegas a través de sitios web no seguros, ves un sitio legítimo que muestra anuncios maliciosos, descargas archivos que contienen virus, instalas programas o aplicaciones de proveedores desconocidos, abres un archivo adjunto de correo malicioso.

Troyanos: Un troyano es un tipo de malware que se disfraza de software legítimo para engañar a los usuarios y lograr su instalación. A diferencia de los virus, no se autoreplican, pero crean "puertas ocultas" para robar información, espiar actividades, bloquear datos o tomar el control remoto del dispositivo infectado.

Gusanos: Un gusano informático es un tipo de malware que se autorreplica y propaga automáticamente a través de redes, sin necesidad de intervención humana o archivos anfitriones. A diferencia de los virus, los gusanos funcionan de manera independiente, consumiendo ancho de banda y recursos, lo que puede ralentizar o paralizar sistemas.

Conexión segura: Una conexión segura en informática es un enlace que garantiza la confidencialidad, integridad y autenticidad de los datos, generalmente mediante protocolos https. Evita que terceros intercepten o modifiquen información sensible. Se identifica con un candado en el navegador.

Uso ético: en este caso se refiere a hacer un uso correcto de la inteligencia artificial, respetando el conjunto de normas morales y valores que regulan el comportamiento de las personas.

Producto tecnológico: son aquellos servicios, sistemas, procesos, objetos, bienes creados por el ser humano a partir de conocimiento científico y técnico.

Filogenética: parte de la biología que se ocupa de las relaciones de parentesco entre los distintos grupos de seres vivos. Relativo al origen y desarrollo evolutivo de las especies, y en general, de las estirpes de seres vivos.

Algoritmo: conjunto finito y ordenado de acciones u operaciones que posibilita dar solución a un problema.

Datos de entrenamiento: conjunto de información en distintos formatos (textos, imágenes. audios, videos, números, etc) que se utiliza para enseñar a un modelo de aprendizaje automático (machine learning) a reconocer patrones, hacer predicciones o generar contenido.

Sesgo: Error sistemático en el que se puede incurrir cuando al hacer muestreos o ensayos se seleccionan o favorecen unas respuestas frente a otras.

Predictor de texto: es una herramienta tecnológica para asistir en la escritura, que funciona sugiriendo palabras probables a partir de la detección de las letras a medida que el usuario las teclea en un dispositivo.

Anexo

Claves de respuestas para el Tema 1

1.1

Recibimos una oferta de productos electrónicos mientras recorremos nuestro Instagram.

Navegando en Internet encontramos una publicidad de un organismo del estado donde se comunica la habilitación de una ciclovía cerca de mi barrio.

Recibimos una llamada de WhatsApp de un número desconocido.

1.2

Ingreso a Correo Google.

Anuncio en YouTube con una sesión de cuenta activa.

1.3

Tu ubicación cargada en una aplicación de pedidos en línea.

Las búsquedas realizadas en un buscador sobre temáticas de tu interés.

Los videos vistos en YouTube.

Claves de respuestas para el Tema 2: Rompé la cadena de la infodemia

2.1

https://www.unl.edu.ar/carreras/ingenieria-agronomica

https://www.unrc.edu.ar/

2.2

Falso

2.3

La calidad, actualización, reconocimiento de la autoridad o institución y organización de los contenidos.

2.4

La dirección o dominio del sitio web.

Realizar una búsqueda de la misma información en otros sitios para comparar resultados.

2.5

No. El sitio web pertenece a otro país.

2.6

Los errores de ortografía.

Los títulos llamativos.

Que no se reconoce al autor.

2.7

Comprobar la noticia con otras fuentes.

Claves de respuestas para el Tema 3: ¡Cuidado, que no te pesquen!

3. 1

Mediante la descarga de un archivo adjunto ejecutable que hace cambios en tu computadora

Al acceder a un sitio web desconocido por medio de un enlace que te envía por correo un remitente extraño

3.2.

No todas las acciones que realiza un troyano en mi computadora son totalmente inofensivas.

3.3.

Cuando recibes un correo en el que aparece publicidad de Mercado Libre

Cuando te piden que confirmes por correo algún dato personal y el remitente no se corresponde con alguien que conoces.

Cuando el correo recibido es de remitente desconocido y presenta un enlace para hacer el pago de alguna cuenta.

3.4

- Imagen 1: Spam y Phishing
- Imagen 2: Ninguno de los riesgos
- Imagen 3: Phishing
- Imagen 4: Spam

Claves de respuestas para el Tema 4: Descubre el poder de la IA

4.1 Desafío 1

Podrías decir ¿En cuáles de estos productos tecnológicos crees que hay Inteligencia Artificial?

Los sistemas predictivos que recomiendan música, videos, que sugieren texto, que responden a preguntas como un humano, o que traducen, que hacen reconocimientos de imágenes, entre otros ejemplos, utilizan el potencial de la IA. Si seleccionaste estas respuestas has podido reconocer dispositivos y aplicaciones que utilizan IA en su desarrollo. ¡MUY BIEN!

Una puerta automática, la calculadora científica, un kit de robótica, o un enrutador de red son desarrollos tecnológicos que procesan cierta información que toman por diferentes dispositivos entrada (sensores de movimiento, teclado, puertos y cables) y realizan una acción, tienen un determinado comportamiento pero que ha sido definido, programado con anterioridad. A la base de estos dispositivos no hay simulación

de comportamiento humano inteligente, porque no son sistemas predictivos, no hay procesamiento de lenguaje natural, no hay aprendizaje automático por parte del dispositivo. Si seleccionaste alguna de estas opciones tu respuesta no es del todo correcta. ¡CUIDADO!

4.2 Desafío 2

De acuerdo a lo que viste en el vídeo podrías identificar ¿Cuáles son las tareas propias de la inteligencia humana que los dispositivos con inteligencia artificial han logrado simular?

Tareas que los seres humanos son capaces de hacer tales como calcular, memorizar datos, aprender autónomamente, jugar y ganar, crear, tomar decisiones, aprender de los errores, son capacidades que la IA actualmente ya está logrando simular con mayor o menor presión, Si elegiste todas estas opciones, respondiste. correctamente. ¡MUY BIEN!

Por el momento la IA no ha podido imitar la capacidad humana de reflexionar críticamente, de considerar el contexto, de sentir como un ser humano, de tener autoconciencia. Si elegiste alguna de estas opciones tu respuesta no es totalmente correcta. ¡ATENCIÓN!

4.3 Desafío 3

Teniendo en cuenta lo planteado en los videos que vimos, podrías indicar ¿Cuáles son los tipos de aprendizajes de los que se ocupa el campo del aprendizaje automático?

El campo del aprendizaje automático se ocupa del aprendizaje supervisado, semi supervisado, no supervisado, por refuerzo, y profundo. Si elegiste estas opciones tu respuesta es correcta. ¡MUY BIEN!

Si en cambio incluiste como parte de tu respuesta aprendizaje virtual, aprendizaje significativo, o aprendizaje remoto, estos no son conceptos que se relacionen directamente al campo de la IA y del aprendizaje automático actualmente. ¡CUIDADO!

4.4 Desafío 4

Piensa en la siguiente situación. Tu profe de historia les pide que sean creativos y elaboren un guion para una obra de teatro que cuente con un poco de humor los hechos históricos de la declaración de la independencia. Uno de tus compañeros propone que usen el ChatGpt para hacer la tarea. ¿Cuál de las siguientes recomendaciones tendrías en cuenta para hacer un uso responsable y ético de esta tecnología?

Hacer un uso responsable y ético del ChatGpt o de cualquier otra herramienta de IA generativa para realizar tareas de la escuela o de la universidad, implica ser conscientes de todo lo que está detrás de la IA, de cómo funciona, aclarando siempre que se han utilizado esas tecnologías, que has generado con la IA y cuál ha sido tu aporte, recordando citar siempre las fuentes. Si tu respuesta ha incluido estas opciones, entonces

estás pensando en actuar correctamente. ¡MUY BIEN!

Si engañas al profesor haciéndole creer que hiciste un trabajo, pero que en realidad fue realizado por una herramienta de IA, por otra persona, o que copiaste, al igual que si no identificas las citas, de alguna manera estás mintiendo y faltando a la integridad académica. Además, hoy en día existen herramientas automáticas para identificar si un trabajo fue copiado o fue realizado por la IA, y si tu docente decide utilizarlas podrías estar en problemas. Si tu respuesta ha sido en este sentido, no vas por buen camino. ¡CUIDADO!

4.5 Desafío 5

Ahora, un quinto y último desafío, teniendo en cuenta estos tres resultados (el que te compartimos anteriormente, y los que obtuviste vos y la otra persona al hacer el experimento), reflexiona sobre lo siguiente.

¿En los 3 celulares WhatsApp sugirió las mismas palabras para cada letra ingresada? ¿Recomendó por primera vez la palabra completa “universidad” al ingresar la misma letra en los distintos celulares? ¿Por qué te parece que ocurre esto? ¿Qué necesita el predictor de textos de WhatsApp para hacer una predicción o recomendación? ¿Cómo crees que se relaciona esto que observaste en el experimento con las nociones de “Aprendizaje automático” y de “Datos de entrenamiento”?

Seguramente con el experimento habrás podido notar que para poder hacer una sugerencia el predictor de texto necesita cierta información de entrada y que las predicciones que ofrece cada celular pueden variar, de acuerdo a lo que escribe con más frecuencia el dueño del celular. Esto se relaciona con el aprendizaje automático que va haciendo la aplicación en la medida que la usamos.

Estudiante 3.0 : cómo participar de manera segura y responsable en los entornos digitales /
Lorena A. Montbrun ... [et al.]. - 1a ed. - Río Cuarto : UniRío Editora, 2026.
Libro digital, PDF - (Pasatextos. Serie Competencias para la vida universitaria)

Archivo Digital: descarga y online
ISBN 978-987-688-682-6

1. Materiales Didácticos. 2. Universidades Públicas. 3. Material Auxiliar para la Enseñanza. I. Montbrun, Lorena A.
CDD 378.17344678

2026 © *UniRío editora*. Universidad Nacional de Río Cuarto
Ruta Nacional 36 km 601. (X5804) Río Cuarto – Argentina
Tel.: 54 (358) 467 6309
editorial@ac.unrc.edu.ar . www.unirioeditora.com.ar

Primera Edición: setiembre de 2026 . ISBN 978-987-688-682-6

Coordinadores: Pablo Pizzi, Celina Martini, Sebastián Ruiz, Carolina Roldan, María Luisa Ledesma

Este obra está bajo una Licencia Creative Commons Atribución 2.5 Argentina.
http://creativecommons.org/licenses/by/2.5/ar/deed.es_AR

Uni. Tres primeras letras de "Universidad". Uso popular muy nuestro; la Uni.
Universidad del latín "universitas" (personas dedicadas al ocio del saber), se contextualiza para nosotros en nuestro anclaje territorial y en la concepción de conocimientos y saberes construidos y compartidos socialmente.
El río. Celeste y Naranja. El agua y la arena de nuestro Río Cuarto en constante confluencia y devenir.
La gota. El acento y el impacto visual: agua en un movimiento de vuelo libre de un "nosotros".
Conocimiento que circula y calma la sed.

Consejo Editorial

Facultad de Agronomía y Veterinaria
Prof. Virginia Mac Loughlin y Prof. Andrea del Valle Rivarola

Facultad de Ciencias Económicas
Prof. Clara Sorondo

Facultad de Ciencias Exactas, Físico-Químicas y Naturales
Prof. Laura Dalerba y Prof. Clarisa Bionda

Facultad de Ciencias Humanas
Prof. José Di Marco y Prof. Claudio Asaad

Facultad de Ingeniería
Prof. Marcelo Alcoba y Prof. Martín Broglia

Biblioteca Central Juan Filloy
María Eugenia Somaré y Sandra Murúa

Secretaría Académica
Prof. Pablo Pizzi y Prof. Gabriel Carini

Equipo Editorial

Secretaria Académica: *Pablo Pizzi*

Director: *Gabriel Carini*

Equipo:
José Luis Ammann, Maximiliano Brito, Ana Carolina Savino, Lara Oviedo, Roberto Guardia, Marcela Rapetti y Daniel Ferniot

e-book

Estudiante 3.0

Cómo participar de manera segura y responsable en los entornos digitales

Lorena A. Montbrun, Daniela B. Solivellas,
Sandra E. Angeli y Mauricio N. Boarini

Serie Competencias para la vida universitaria

Colección PASATEXTOS

El presente material forma parte de una serie de cuadernillos que se inscriben en la Colección Pasatextos. Esta colección reúne materiales didácticos destinados a favorecer los procesos de enseñanza y aprendizaje en el nivel de grado; y adquiere un valor estratégico en la consolidación de políticas académicas orientadas al acompañamiento de las trayectorias estudiantiles.

ISBN 978-987-688-682-6

UniRío editora | Universidad Nacional de Río Cuarto | Secretaría Académica