InSET | Educación a Distancia
Instituto Superior de Enseñanza Técnica

Comunicación y Tecnología

Tecnicatura Superior en Ciencia de Datos e Inteligencia Artificial

PROFESORA
Alzaga, Julieta

2022
Primer cuatrimestre

Clase N° 9: Ciencia y tecnología.

Bienvenidos y bienvenidas a la clase N° 9 de Comunicación y Tecnología de la Tecnicatura Superior de Ciencia de Datos e Inteligencia Artificial. En esta clase revisaremos Ciencia y tecnología: perspectivas, tensiones y dilemas, donde abordaremos los principales problemas en torno a internet que tienen que ver con la seguridad y la privacidad. Continuaremos desarrollando esta temática la próxima clase también.

Los objetivos de la clase son:

- Reconocer las ventajas y desventajas de las nuevas tecnologías de seguridad.
- Reconocer los procesos criptográficos por los cuales pasan los datos sensibles de los cibernautas o usuarios.

Privacidad de la información

A fines de los ‘90 cuando Internet se consolidaba como una herramienta de conexión con el mundo para todos y todas, se desencadenaba una revolución silenciosa: el acceso gratuito a los servicios de internet. **Tim Berners-Lee**, conocido por ser el padre de la World Wide Web ya que estableció la primera comunicación entre un cliente y un servidor usando el protocolo HTTP en diciembre de 1990, afirmaba que la red es para conectar a la humanidad.

En el año 2008 en una conferencia Berners-Lee explicó que él trabajaba en la web 3.0 semántica que busca un acceso más sencillo a los datos, haciendo la búsqueda de información más simple al basarse en los significados de lo que se transmite. Eso hace también que se unifiquen los contenidos y sea más fácil trasladar la información entre dispositivos. Allí dijo: "las cosas cambiarán mucho en internet. Ya no hablamos de documentos web, ni de sitios web, sino de gente web. La web es la humanidad conectada por la tecnología"[1]. Sin embargo vemos cómo ese intercambio para acceder a información tiene un precio y es el de brindar información sobre nosotr@s mismos.

Todo lo que expresamos y mostramos en las redes sociales, nuestros pensamientos y deseos, son tipificados y comercializados en grandes bases de datos que utilizan los gobiernos, las empresas de productos o servicios y las grandes corporaciones como Google. Cada vez que enviamos un mail por Gmail, Google registra las palabras clave y las integra en su base de datos vinculada a esa cuenta, lo que aumenta así la nube de etiquetas para una persona para saber más sobre ella y ofrecerle información y publicidad vinculada a sus gustos y deseos.

Existe una frase famosa que dice que el producto online no es el contenido, el producto son los ojos que miran el contenido, el tiempo destinado.

Internet fue creado por científicos e informáticos altamente calificados con fines académicos que buscaban extender el horizonte de conocimiento mediante la comunicación entre ámbitos académicos, científicos,

[1] Extracto de la entrevista a TVE Informe Semanal. Tim Berners-Lee: "La web es la humanidad conectada por la tecnología"

gubernamentales, entre otros. La aplicación de la WWW con una interfaz amigable, intuitiva y multimedia, internet adquirió masividad y fue transformándose, siendo cada vez más omnipresente y vigilante.

Es por este motivo que algunos de los principales referentes de Silicon Valley comenzaron a "arrepentirse" de los productos que crearon, a tomar conciencia de lo que estaban haciendo con las redes sociales, a reconocer que se les había "ido de las manos" y a denunciar la manipulación. Muchos de los ex responsables de Facebook, Twitter, Google e Instagram, entre otros, participan del documental "El dilema de las redes sociales" (*The social dilemma*, 2020: Netflix) en donde exponen cuáles son las estrategias de monetización y comercialización para que el usuario permanezca en la pantalla.

➔ **Recomendaciones:**

- La serie documental de 4 capítulos La revolución virtual (*The virtual revolution*, 2010) de la BBC y The Open University, conducida por Aleks Krotoski.
- El documental El dilema de las redes sociales (*The social dilemma*) Dir. Jeff Orlowski, 2020, Netflix.
- El ensayo Internet se rompió. Los arrepentidos de la tecnología de Axel Marazzi en *Anfibia*.

Si bien pensamos en internet como una enorme oportunidad de acceso a información que nos permite obtener mayor conocimiento humano, además debemos considerar que su principal función en la actualidad es el *marketing* y el comercio. De la misma manera la vigilancia masiva y la manipulación de información no deja de crecer.

El mismo Berners-Lee, en marzo de 2019 cuando internet cumplió 30 años, escribió una carta en la que expresó: "mientras la Web creó oportunidades, dando voz a grupos marginados y haciendo más fácil nuestra vida, también creó oportunidades para los estafadores, dio voz a los que proclaman el odio e hizo más fácil cometer todo tipo de crímenes"[2].

La identidad digital y la seguridad informática

Marta Peirano, periodista española especializada en tecnología y activista, en la charla TEDxMadrid "¿Por qué me vigilan, si no soy nadie?" dice que:

> "Cometemos tres errores. El primero es infravalorar la cantidad de información que producimos cada día; el segundo es despreciar el valor de esa información, y el tercero es pensar que nuestro principal problema es una agencia distante y superpoderosa que se llama NSA[3]" (Peirano, 2015).

➔ Marta Peirano en TEDxMadrid: ¿Por qué me vigilan, si no soy nadie?

A partir de esto plantea de qué manera nuestros celulares con georreferenciación permiten llevar a cabo una vigilancia precisa y continua sobre nuestros movimientos, contactos y actividades, ya sean de ocio, laborales como políticas. De la misma manera, se registra nuestra actividad digital en el ciberespacio.

A este registro virtual se lo conoce como **huella digital** que es la suma de los rastros que dejamos en la web a partir de lo que compartimos, publicamos y lo que los demás publican sobre nosotros, pero también sobre nuestras interacciones, es decir qué decimos y cómo nos expresamos. Este conjunto de datos conforman nuestra identidad digital en donde se almacena información sobre quiénes somos, dónde vivimos, qué lugares frecuentamos, dónde estamos, cuáles son nuestros gustos y preferencias. Incluso aunque borremos información, fotos y videos, todo va dejando huellas.

Según el sitio de Argentina.gob.ar la huella digital está compuesta por:

- **Datos públicos:** los datos de la obra social, cuit o cuil, declaraciones de impuestos, domicilios en las facturas de servicios, resúmenes de tarjetas de crédito, cargos, becas, resultados de sorteos, resoluciones judiciales.
- **Datos publicados por otros:** fotos, posteos de amigos, familiares, clubes o espacios de pertenencia en redes sociales.

[2] Texto completo en WebFoundation.org 30 years on, what's next #ForTheWeb?
[3] La Agencia de Seguridad Nacional es una agencia de inteligencia a nivel nacional del Departamento de Defensa de los Estados Unidos, bajo la autoridad del Director de la Inteligencia Nacional.

- **Datos generados por nosotres:** posteos, comentarios, fotos en redes sociales y foros. Formularios que completamos, contenidos que compartimos en plataformas como currículum, perfiles en redes de contactos u otros contenidos como listas de reproducción y videos favoritos.

¿Para qué se usan los datos recopilados de nuestra huella digital?

Las empresas usan los datos de las huellas digitales para crear "perfiles" de usuarios y vender estos datos a otras empresas como potenciales consumidores de sus productos.

Los proveedores de servicios de Internet, las plataformas y las redes que brindan servicios para navegar intercambian información de los perfiles de sus clientes y estadísticas sobre sus transacciones. Las huellas digitales son procesadas por personas y por robots e inteligencias artificiales que forman parte del complejo sistema donde se comparten y monetizan los datos. Podríamos decir entonces que Internet en realidad es una gran industria económica y financiera sobre todo.

¿Cómo se recopilan los datos de mi huella digital?

Los datos se recopilan a través de las *cookies* que son una cadena de letras y números, sin ningún significado intrínseco que un sitio web envía a su navegador web. Esta información permite a los proveedores de servicios de Internet vincular todas las acciones realizadas por un usuario y convertirlas en un hilo conectado.

Las *cookies* son necesarias para aumentar la usabilidad de Internet y también ayudan a que las transacciones individuales sean más seguras. Es por ello que no se puede navegar sin cookies y están en todos lados.

Las principales funciones de las cookies son:

- Llevar el control de usuarios: al ingresar a un sitio con usuario y contraseña se almacena una cookie para recordar esos datos y no ingresarlos cada vez, lo que relentizaría la navegación. Esto identifica a la tríada computadora-navegador-usuario.
- Conseguir información sobre los hábitos de navegación del usuario e intentos de *spyware* (programas espía) de agencias publicitarias u otros. Esto puede causar problemas de privacidad y es una de las razones por las cuales se ve con desconfianza a las *cookies*.

Marta Peirano concluye la charla diciendo que el principal problema es que la existencia misma de esa información, que generamos, nos hace vulnerables de maneras que no podemos ni imaginar en este momento. Por ello es importante proteger nuestros datos personales.

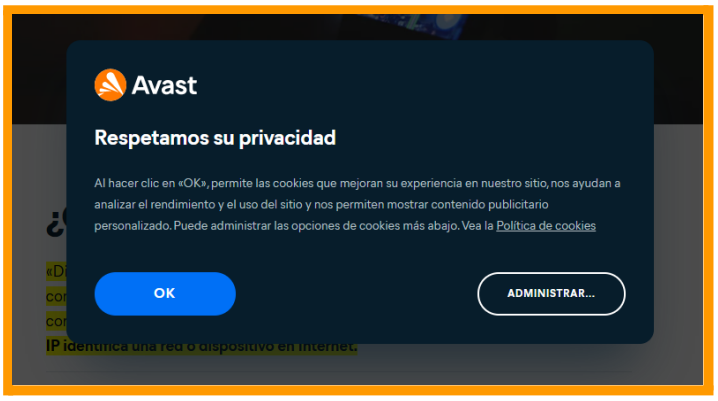
¿Cómo gestiono mi huella digital?

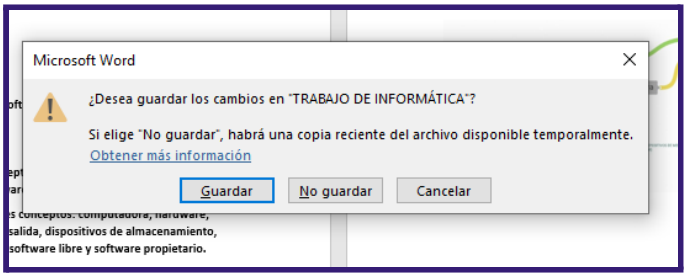
Generalmente los sitios avisan que están recolectando datos, por ello es importante leer esas advertencias y decidir autorizar las cookies de forma permanente o transitorias.

Otras estrategias de fácil aplicación es la de configurar la privacidad de las redes sociales para que no se exponga toda la información personal y navegar de modo incógnito para que no se guarden los datos e historial.

Como muestra la imagen debajo, tenemos una ventana emergente de una cookie, si observamos bien vamos a ver que tenemos dos botones: "OK" y "Administrar" los cuales poseen distintos aspectos. Al momento de diseñar un botón de un sitio web, siempre se va a destacar la opción que se le recomienda al usuario que ejecute, es por esto que inconscientemente aceptamos todas las cookies. Veamos un ejemplo simple y cotidiano en la actividad ofimática, cuando modificamos un documento en Word este nos va a recomendar con un botón resaltado en color azul que guardemos los cambios hechos para no perderlos.

Como usuarios podemos tomar el control y seleccionar el botón "Administrar cookies", donde vamos a activar solo las necesarias o rechazar todas.





Desde el navegador se puede activar Do not Track que justamente inhabilita el seguimiento, pero es el proveedor del servicio el que acepta,

por lo tanto no es un bloqueo. También se pueden configurar alertas de Google sobre nuestro nombre, por ejemplo, para que no existan datos personales innecesarios en la web.

Ingresando en https://www.google.com/alerts inicias sesión en tu cuenta de Google o Gmail > Selecciona crear un alerta sobre un término > Crear alerta

Además se pueden denunciar páginas y sitios que exponen información personal sin consentimiento, es decir que están incumplimientos la Ley de Protección de Datos Personales.

➔ Denunciar incumplimientos de Protección de Datos Personales

¿Qué son los datos biométricos?

La biometría es un método tradicional de la identificación de las personas, las huellas dactilares es el ejemplo más práctico. Últimamente el interés por esta tecnología fue en aumento principalmente por dos razones: la necesidad creciente de la identificación de las personas de manera inequívoca tanto en el ámbito público como privado, debido al incremento del delito basado en la usurpación de identidad, la segunda razón sería la facilidad y rapidez que brinda al al momento de autenticar la identidad de una persona. Es decir, que cumplen con los tres pilares de seguridad informática mencionados en la clase anterior, aún así, se estudió que puede llegar a existir una situación riesgosa como la obtención del dato biométrico (huella digital) por otra persona ajena a esa información realizando el proceso inverso al de captura y almacenamiento.

Las huellas digitales tienen rasgos únicos conocidos como minucias, que son las que se reconocen al momento durante el proceso de captura, luego se codifican y almacenan. Se estima que una huella dactilar reconstruida a partir de la plantilla de minucias es efectiva en por lo menos el 90% de los casos. Casos como estos, en el que una base de datos de huellas dactilares fuera hackeada, accedida sin autorización, divulgada a terceros o utilizada para con fines maliciosos de cualquier tipo podría traerle daños al usuario primero, porque se trata de datos personales, únicos e irrepetibles para la persona humana a quien pertenecen y segundo, que para un usuario es posible, con menor o mayor dificultad, cambiar su contraseña tradicional pero es imposible cambiar su huella digital.

➔ Microaprendizaje: ¿Qué es la huella digital?
➔ Argentina.gob.ar ¿Qué es la huella digital en Internet?

Marta Peirano concluye la charla diciendo que el principal problema es que la existencia misma de esa información, que generamos, nos hace vulnerables de maneras que no podemos ni imaginar en este momento. Por ello es importante proteger nuestros datos personales.

Seguridad informática

Cuando nos referimos a seguridad primero lo relacionamos a virus, *malware* y niveles de encriptación. Sin embargo, la dimensión de seguridad abarca más aspectos como: gestionar el uso de datos, definiendo políticas de gobernanza a nivel global y definiendo quién puede acceder a qué información.

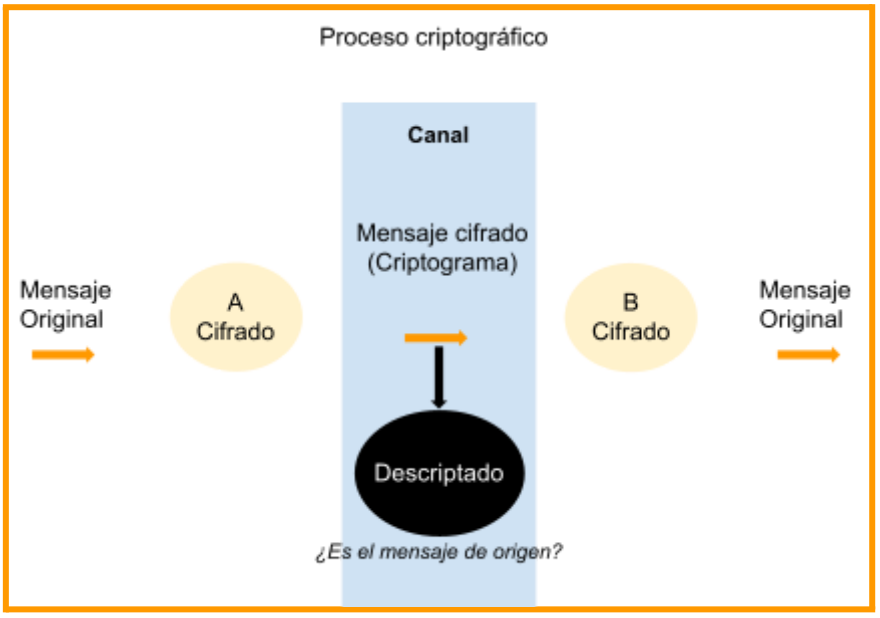
➔ Recomendamos este video con advertencias y sugerencias Así de fácil es robar tus datos privados del teléfono móvil | Filo.Tech

Desde la identificación y el acceso a nuestros dispositivos tenemos a disposición el uso del DNI electrónico, las tarjetas de identificación electrónica, la huella dactilar digitalizada, la identificación biométrica, entre otras, que a veces no tienen éxito por factores externos como la falta de capacitación al usuario y/o una interfaz que no cumple con los requisitos de usabilidad básicos, pero son recomendados para proteger nuestros equipos e información.

Por otro lado, para acceder a ciertas app o sitios web debemos proporcionar datos sensibles y personales que también debemos proteger. En primer lugar es importante tener en cuenta que no debemos proporcionar información que pueda poner en riesgo nuestra privacidad o la de nuestra familia. En segundo lugar, siempre hay que leer la política de privacidad de redes y recursos digitales. Por otro lado, es importante conocer algunos sistemas de seguridad informática como la criptografía y la gestión de la huella digital.

Criptografía

Del término *criptología*, que significa estudio de lo oculto, se dividen dos grandes ramas que son la **criptografía** y el **criptoanálisis**. La primera, se ocupa del cifrado de mensajes en clave y del diseño de criptosistemas. La segunda, se trata de descifrar los mensajes en clave, rompiendo así el criptosistema.



El proceso de la figura se explica de la siguiente forma:

A y **B** son el *emisor* y el *receptor* de un determinado mensaje.

A, *transforma* el mensaje original en un mensaje cifrado mediante un proceso de cifrado controlado por una clave, que se envía por un canal público.

B, *recibe* y *transforma* ese criptograma en el mensaje original con el previo conocimiento de la clave.

Este proceso puede ser *interceptado* por un enemigo criptoanalista que lleva a cabo un labor de desencriptado.

Un buen sistema criptográfico será aquel que ofrezca un descifrado sencillo, pero un desencriptado imposible o muy difícil. Y además, esto lo podemos relacionar con el enfoque actual de la criptografía que es mantener comunicaciones seguras y a la vez cumplir con tres propósitos:

- ★ **Confidencialidad**: para que el mensaje sea visto por aquellos que tienen que ver la información.
- ★ **Autenticidad**: para asegurar la identidad del destinatario y remitente.
- ★ **Integridad**: para que el mensaje enviado por el emisor sea el mismo que reciba el receptor.

Entonces la **criptografía** se va a definir como el *arte de escribir como clave secreta o modo enigmático*, sin embargo actualmente se convirtió en una técnica más que un arte ya que esta proviene de tiempos clásicos donde el tamaño del mensaje a ocultar no se compara con el número de datos que se procesan actualmente. Los antecedentes de la criptografía

comienzan principalmente por cuestiones militares, religiosas y comerciales; veamos algunos ejemplos:

- Los sacerdotes egipcios utilizaron la **escritura hierática** (jeroglífica) que claramente no era comprensible para el resto de la población.

- La **escitala espartana**: este método criptográfico se dio durante la guerra entre Atenas y Esparta. El historiador griego Plutarco, describe la escitala de la siguiente manera:

  "*La escitala era un palo o bastón en el cual se enrollaba en espiral una tira de cuero. Sobre esa tira se escribía el mensaje en columnas paralelas al eje del palo. La tira desenrollada mostraba un texto sin relación aparente con el texto inicial, pero que podía leerse volviendo a enrollar la tira sobre un palo del mismo diámetro que el primero*".

  Con este sistema los gobernantes pudieron transmitir sus instrucciones secretas a los generales de su ejército durante las campañas militares.

- El **cifrario de César**: este método fue utilizado en la Roma Imperial por Julio César. La técnica utilizada es un algoritmo de sustitución, uno de los más simples, que consiste en sustituir una letra por la situada tres lugares más allá en el alfabeto esto es la A se transformaba en D, la B en E y así sucesivamente.

Alfabeto original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto cifrado	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Luego de tener una referencia de los primeros sistemas criptográficos, veremos una explicación breve sobre otros conceptos técnicos de dos métodos criptográficos que tienen en cuenta el **tipo de clave.**

- **Sistemas de clave única o métodos simétricos:** son aquellos en los que los procesos de cifrado y descifrado se llevan a cabo con una única clave, la cual es compartida por el emisor y por el receptor. Es decir, que tanto para descifrar como para cifrar el mensaje, **vamos a utilizar la misma clave**.

  En el siguiente video se ofrece una explicación más gráfica:

  ➔ Sistema de cifra con clave secreta

- **Sistemas de clave pública o asimétrica:** son aquellos en los que los procesos de cifrado y descifrado son llevados a cabo por **dos claves distintas y complementarias**. Estas claves van a ser, una pública y otra privada. El mensaje lo ciframos con la clave pública del destinatario y este puede descifrar a continuación con su propia clave privada. La diferencia con el sistema anterior es que nadie necesita la clave privada de otro para poder enviar un mensaje en forma segura.

  En el siguiente video se ofrece una explicación más gráfica:

  ➔ Sistema de cifra con clave pública

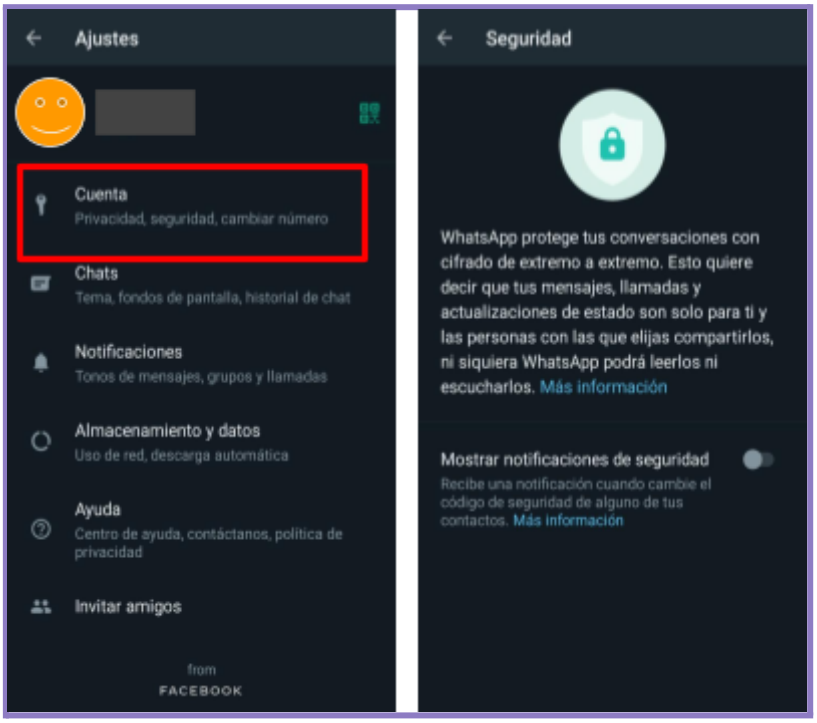
Los sistemas actuales de seguridad no utilizan ni uno ni otro de manera específica y única, sino que combinan los sistemas existentes. Estos sistemas se denominan "**Algoritmos de cifrado**" y son programas que realizan el proceso de criptografía basándose en los tipos de cifrado, ahora haremos mención de los más usados:

- **Algoritmos criptográficos simétricos**:
  - DES (Data Encryption Standard)
  - Triple-DES
  - AES (Advanced Encryption Algorithm)
  - IDEA (International Data Encryption Algorithm)

- **Algoritmos criptográficos asimétricos**:
  - RSA (Rivest - Shamir - Adleman) apellidos de los desarrolladores.
  - Diffie - Hellman
  - Algoritmos HASH
  - MD5 (Message Digest Algorithm)
  - SHA (Secure Hash Algorithm)

Un ejemplo práctico es Whatsapp, la aplicación de mensajería instantánea que utilizamos de manera diaria y que ofrece una encriptación denominada "**extremo a extremo**" ¿Qué significa?

Primero, ubiquemos en qué parte de la aplicación está dicha información. Tendremos que ingresar a **Ajustes** > **Cuenta** > **Seguridad**.



Este cifrado funciona mediante el **almacenamiento de las claves** de cifrado y descifrado en el **propio dispositivo del usuario**. El sistema hace uso de **tres claves públicas**:

1. Identifica al dispositivo.
2. Generada periódicamente y firmada digitalmente.
3. Generada con cada actualización del servicio.

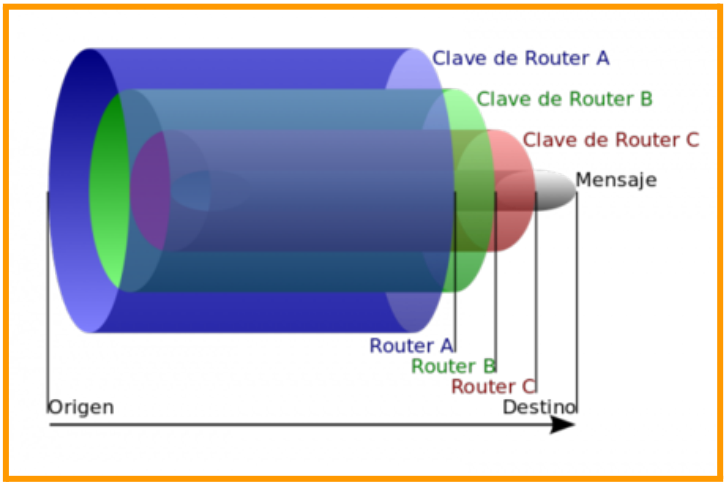
Y **tres claves de sesión** que son las siguientes:

1. Clave de administrador.
2. Clave de cadena generada a partir de la del administrador, para crear la clave de mensaje.
3. Clave de mensaje.

TOR (*The Onion Router*) es otra herramienta disponible para que los usuarios puedan navegar de forma anónima por la web. Es decir, que los mensajes intercambiados entre los usuarios no revelen su identidad que en este caso sería la dirección IP (a nivel de red), manteniendo así la integridad y el secreto de la información que viaja por ella.

➔ www.torproject.org

TOR propone, como se define en el idioma inglés, un enrutador cebolla. De esta forma los mensajes van a viajar desde el origen al destino por medio de una serie de routers especiales llamados "routers de cebolla".



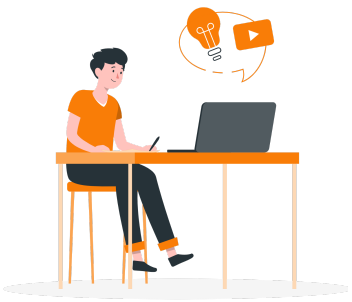
No es el objetivo de esta clase desarrollar la terminología técnica de este programa pero sí comprender que el proceso de comunicación y su vinculación con la tecnología no consiste en descargar una aplicación y empezar a interactuar como cibernautas. Sino que existen cuestiones de seguridad que pueden llegar a proteger nuestros datos o no y de esa forma darnos la privacidad que necesitamos.

El 4 de octubre de 2021, hubo fallas en Whatsapp, Instagram y Facebook lo que provocó la nulidad del servicio de dichas aplicaciones. A raíz de esto muchos usuarios se pasaron de manera inmediata a Telegram o Signal ¿se pensó previamente el tipo de seguridad que nos ofrecen estas aplicaciones?. Estos temas suelen crear tensión entre los usuarios y la decisión de instalar una aplicación, más allá de la seguridad también nos cuestionamos qué tipos de ventajas o servicios nos ofrecen y en qué presenta desventajas. ¿Conocían estas aplicaciones? ¿Cuál prefieren?

➔ **Recomendaciones:**

- Beneficios de Telegram sobre Whatsapp: Por qué usar TELEGRAM y no WHATSAPP en Chica Geek
- ¿Es más seguro Whatsapp o Telegram? por Ale Alem para Filo.News
- Microaprendizaje: ¿cómo crear un perfil en una red social?

Actividad de la semana



En esta clase tienen mucha información y muchos videos para ver y analizar, así que disfruten de los contenidos y por cualquier consulta o interés los espero en el foro para los intercambios.

Referencias Bibliográficas

- Andrada, Ana María. (2017). Capítulo 8: Ciudadanía digital. En *Nuevas tecnologías de la información y la conectividad NTICx. Dispositivos, saberes y prácticas.* Maipue, pp. 259-270.
- Alonso, Agustín. (29 de julio de 2008). Tim Berners-Lee: "La web es la humanidad conectada por la tecnología". En *rtve*. https://www.rtve.es/noticias/20080729/tim-berners-lee-web-humanidad-conectada-tecnologia/124050.shtml
- Argentina.gob.ar (19 de diciembre de 2020). ¿Qué es la huella digital en Internet?. https://acortar.link/iTOFmX
- Chica Geek. (24 de septiembre de 2021). Por qué usar TELEGRAM y no WHATSAPP. Youtube. https://youtu.be/Eq0DU3RUAXE
- Educar Portal (11 de julio de 2019). Microaprendizaje: ¿Qué es la huella digital?. Youtube. https://acortar.link/4sNJbR
- Educar Portal (11 de julio de 2019). Microaprendizaje: ¿cómo crear un perfil en una red social?. Youtube. https://acortar.link/K83Pu9
- Educar Portal (11 de julio de 2019). Microaprendizaje: ¿Cómo navegar por internet de manera segura?. Youtube. https://acortar.link/7ifIEL
- Filo News (17 de diciembre de 2019). Así de fácil es robar tus datos privados del teléfono móvil | Filo.Tech. Youtube. https://acortar.link/gFw9jk
- Filonewsok (26 de julio de 2021). ¿Es más seguro Whatsapp o Telegram? por Ale Alem. Instagram. https://acortar.link/cHZVJF
- Marazzi, Axel (4 de septiembre de 2020). Internet se rompió. Los arrepentidos de la tecnología. En *Anfibia*. https://www.revistaanfibia.com/internet-se-rompio/
- Rhodes, Larissa [Productora]. El dilema de las redes sociales (*The social dilemma*). (2020). [Película]. Orlowski, Jeff [Director]. Netflix.
- Sanjuan, Leudis. (s.f.). Criptografía I. Seminario: Seguridad en desarrollo de Software. Universidad del Norte. https://acortar.link/GqqtV3
- UPT (10 de noviembre de 2010). Lección 2: Sistemas de cifra con clave secreta (intypedia). Youtube. https://youtu.be/46Pwz2V-t8Q
- UPT (15 de noviembre de 2010). Lección 3: Sistemas de cifra con clave secreta (intypedia). Youtube. https://youtu.be/On1clzor4x4
- TEDxTalks (22 de septiembre de 2015). ¿Por qué me vigilan, si no soy nadie? | Marta Peirano | TEDxMadrid. Youtube. https://www.youtube.com/watch?v=NPE7i8wuupk