UNIVERSIDAD SIGLO 21

Licenciatura en Informática

Seminario Final de Informática

Trabajo de Investigación en Tecnologías Informáticas:

¿Como proteger la privacidad en la web?

Autor: Marcos Guillermo Lammers
Legajo: VINF09130

Docente/Tutor: Ana Carolina Ferreyra

Fecha: 13/11/2022

Tabla de contenidos

Portada....1
Título....2
Tabla de contenidos....3
Resumen....4
Palabras clave:....4
Abstract....5
Keywords:....5
Introducción....6
La privacidad....7
Los datos personales....9
¿Qué dicen las aplicaciones?....10
La criptografía....11
Protocolos seguros de navegación web o HTTPS....14
Las cookies....16
JavaScript....19
VPN y TOR....20
Objetivo general....23
Objetivos específicos....23
Métodos....24
Diseño....24
Enfoque de la Investigación....24
Muestra....25
Cuantificación para las condiciones de privacidad y seguridad de los datos:....26
Tipo de investigación....26
Resultados....27
Datos:....27
Cookies:....28
Registro de IP:....29
JavaScript desactivado:....30
Uso de VPN:....31
Uso de TOR:....32
Verificación del Protocolo HTTPS:....33
Puntaje obtenido:....34
Discusión....37
Problema de Investigación....39
Objetivos....41
Hipótesis....42
Modelo Teórico Adoptado....43
Limitaciones de la Investigación....44
Fortalezas de la Investigación....45
Conclusiones....47
Recomendaciones....48
Futuras Líneas de Investigación....51
REFERENCIAS....54

Resumen

En este trabajo buscamos dar respuesta a la pregunta que titula el mismo "¿Como proteger la privacidad en la web?". Para cumplir este objetivo, realizamos un repaso de los puntos claves en las comunicaciones a tráves de la web, como leyes que regulan el derecho a la privacidad; la criptografía: cómo, qué recolectan y qué uso hacen de nuestros datos los sitios web: las tecnologías desarrolladas para evitar la identificación y geolocalización. Realizamos pruebas y tests que nos permitieron verificar, dentro de las 5 aplicaciones web más utilizadas en el mundo y en Argentina, cómo actúan con respecto a estos puntos claves. Esto nos permitió realizar una cuantificación valorativa del nivel de privacidad. Tomando como referencia esta escala, podremos saber que aplicación usar según el nivel de privacidad que pretendemos. Para sorpresa de muchos, el sitio más empleado a nivel mundial, Google, es el que permite un mayor nivel de privacidad, con las configuraciones correctas, por supuesto. Igualmente, otra conclusión muy importante es que más allá de las promesas de otros de proteger nuestros datos, la privacidad sigue dependiendo fundamentalmente de nuestro proceder, tanto en las configuraciones al navegar como en los datos que nosotros ingresemos.

Palabras clave:

Privacidad web, VPN, TOR, cookies, protocolo HTTPS, Navegación web.

Abstract

In this work we seek to answer the question titled "How to protect privacy on the web?". To meet this objective, we review the key points in communications through the web, such as laws that regulate the right to privacy; cryptography: how and what websites collect and what use they make of our data: the technologies developed to prevent identification and geolocation. We carried out tests and tests that allowed us to verify within the 5 most used web applications in the world and in Argentina how they act with respect to these key points. This allowed us to perform an evaluative quantification of the level of privacy. Taking this scale as a reference, we will be able to know which application to use according to the level of privacy that we want. To the surprise of many, the most used site worldwide, Google, is the one that allows the highest level of privacy, with the correct settings, of course. Likewise, another very important conclusion is that beyond the promises of others to protect our data, privacy continues to depend fundamentally on our behavior, both in the configurations when browsing and in the data that we enter.

Keywords:

Web privacy, VPN, TOR, cookies, HTTPS protocol, Web navegation.

Introducción

Con el uso de internet a nivel mundial, y todo lo que abarca, se fueron abriendo muchas puertas; distintas a lo que veníamos acostumbrados. Cambios de hábitos, las formas de vivir, el acceso al conocimiento, el trabajo, la salud, cambios que todavía están por verse, seguramente.

Una película del año 1995, “La Red”, cuenta la historia de una mujer a la cual le cambian su identidad, a partir de allí pasa a “no existir”. Más allá de la historia, nos mostraba como todo era online en internet, el pedido de la comida, los registros médicos, los pasajes de avión, los “chats”, etc., la película “fantaseaba” con esto. En esa época muchos ni imaginábamos que hoy, 2022, esto iba a ser una realidad.

Figura 1: Sandra Bullock en la película "La red" en 1995 sacando pasajes de avión a través de la web.

Uno de los cambios más grandes que trajo internet es la exposición de la vida privada. Cientos, miles de aplicaciones compartiendo pensamientos, imágenes, videos, y un largo etcétera. Los blogs, fotologs, facebooks y los chats, se suman a nuevas apps que van apareciendo en el rubro ocio, por categorizarlo en algún lado. ¿Qué pasó después de esta avalancha de tecnología? Vino la pandemia. Se aceleró todo, por lo menos en Argentina. Ahora no es posible, casi, realizar ninguna cosa sin instalar una aplicación. DNI, obra social, homebanking, viajar, compras, música, cine… socializar.

Con todo esto, ¿existe la posibilidad de participar en toda esta tecnología privadamente?, ¿está garantizada?. Esta es una pregunta muy amplia y abarca muchos rubros que exceden el propósito de estudio de esta Tesis. Sin embargo, vamos a tratar de dar un pantallazo, un repaso de lo que se conoce y que requerimientos son necesarios para acercarse por lo menos un poco. Que privacidad "perdemos" al usar internet, al navegar. Cuáles no son opcionales. Medirlos y luego tratar de sacar una conclusión

La privacidad

A partir de la pandemia se renovaron muchos debates. Como ya dijimos, que es privado y que no, es algo muy amplio, donde cada uno decide lo que expone. En esta situación, lo importante es tener los elementos que nos permitan a cada uno tomar las decisiones que deseamos. "Desde la Agencia insistimos con informar a los ciudadanos cuáles son los derechos en materia de protección de datos personales vinculados con la tecnología. En ese punto, hemos publicado una serie de guías con recomendaciones para el tratamiento de datos personales de pacientes infectados con COVID-19, como también los datos que se adquieren de apps que utilizan la geolocalización de los usuarios" fue lo que dijo el director de la agencia de acceso a la información pública,

Eduardo Bertoni en la conferencia titulada “La privacidad como derecho humano”, realizada durante el mes de agosto del 2020. En Argentina tenemos legislación al respecto. La Asociación por los Derechos Civiles (ADC) y Privacy International (PI) en su Informe de las partes interesadas, Examen Periódico Universal 26º período de sesiones del 2017 dice “Si bien la Constitución Argentina no menciona la palabra ‘privacidad’, sí se refiere a ‘acciones privadas’ en su artículo 19, el cual ha sido interpretado por la Corte Suprema de Argentina como consagrando el derecho a la privacidad. El artículo dice ‘Las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios y exentas de la autoridad de los magistrados. Ningún habitante de la Nación será obligado a hacer lo que no manda la ley, ni privado de lo que ella no prohíbe.’ ”… “Además, el artículo 18 de la Constitución dice: ‘El domicilio es inviolable, como también la correspondencia epistolar y los papeles privados; y una ley determinará en qué casos y con qué justificativos podrá procederse a su allanamiento y ocupación.’ ”… “Respecto a los datos personales, el Artículo 43 dice: ‘Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos,o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos’ ”...“Argentina ha ratificado varios tratados internacionales de derechos humanos que tienen implicaciones sobre la privacidad. Ha ratificado el Pacto Internacional de Derechos Civiles y Políticos, cuyo artículo 17 dispone que ‘Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación’ ”.

Como vemos, la privacidad es algo que está establecido en las leyes y dentro del sentido común del ser humano. También podemos agregar que en países donde existen medidas restrictivas de libertad de expresión (censura), es importante saber si nuestros datos permanecen seguros.

Los datos personales

El tratamiento de los datos personales también tienen normativa en Argentina. Además de hacer referencia a la Constitución Nacional en sus artículos 19 y 43; la Ley N° 25.326 de Protección de los Datos Personales, es donde se hace mención sobre qué se entiende por datos personales, "son los datos sensibles, archivos, registros o bancos de datos, tratamiento de los datos, responsable de los datos, datos informatizados, titulares de los datos, usuarios de los datos y disociación de los datos, para luego hacer una descripción de principios y consentimientos, entre otras cuestiones. Por otra parte, como normativa principal se le agrega el Decreto 1558/2001 en donde se reglamenta la Ley de Protección de Datos Personales, del año 2001, que luego es modificado por el Decreto 1160/2010, que refiere el procedimiento de la DNPDP (Dirección Nacional de Protección de Datos Personales). De esta manera, existen leyes y decretos referidos a registro y base de datos públicos y privados, bases de datos de marketing y publicidad, información obligatoria en páginas web, sanciones e infracciones, videocámaras, registro de 'no llame', datos biométricos y de identificación personal, transferencia internacional de datos personales, etcétera" (Sumer Elías, 2017).

¿Qué dicen las aplicaciones?

Como dice el dicho "Para muestra basta un botón". Vamos a transcribir como ejemplo partes de la declaración de privacidad en su sitio web de Mercado Libre, sobre como tratan los datos personales, la privacidad y que entienden de ello:

"Información que recopilamos de manera automática, ya sea que te encuentres registrado o no:" …

"- Información de los dispositivos o computadoras desde los que accedes a la plataforma de Mercado Libre y otros datos capturados automáticamente (como el tipo o versión del navegador o del sistema operativo, configuraciones, datos de conexión, información sobre algunas de las aplicaciones descargadas y parámetros)." …

"Dirección IP de internet que utilizas al conectarte a nuestros servicios o al navegar nuestros sitios web" …

"- Cierta información sobre la actividad de los usuarios y visitantes dentro de nuestro sitio web y las apps. Como por ejemplo, la URL de la que provienen o a qué URL acceden seguidamente (estén o no en nuestro sitio web). También las páginas visitadas, las interacciones con dichas páginas, las búsquedas realizadas, las publicaciones, compras o ventas, calificaciones y réplicas ingresadas, reclamos realizados y recibidos, mensajes en los foros, entre otra información podrá ser almacenada y retenida."…

"- Información sobre tu ubicación (geolocalización)" …

"- Listas de contactos de los dispositivos móviles utilizados por los usuarios". (Mercado Libre, 2021. Recuperado de https://www.mercadolibre.com.ar/privacidad/declaracion-privacidad).

La empresa cumple con la ley al notificarnos perfectamente qué datos nuestros va a tomar y que tratamiento va a hacer de ello. Volvemos a la pregunta que nos motiva, ¿y si quiero permanecer anónimo?, que no me identifiquen individualmente por mis gustos, preferencias, ubicación, amigos. Según la declaración, parecería, que en caso de querer mantener nuestro anonimato, no nos conviene usarla.

Tomando en cuenta que además pueden existir episodios como lo que cuenta este diario el 7 de marzo del 2022: https://www.infobae.com/economia/2022/03/07/filtracion-masiva-en-mercado-libre-acceden-sin-autorizacion-a-los-datos-de-300000-usuarios/

La criptografía

Sumado a esto que venimos describiendo, lo cual sería una cuestión ética y de decisión, tenemos el problema de que nuestros datos sean vulnerados por un tercero sin nuestro conocimiento o aprobación. Para solucionarlo existe desde hace muchísimos años la criptografía. Sobre esto hay material de estudio e investigación muy vasto, con niveles superiores a lo que pretendemos demostrar en este trabajo. Sólo vamos a reflejar un breve repaso con el fin de darnos una idea de que se trata.

Vamos a citar la definición de la Universidad Internacional de Valencia:

“La definición de criptografía nos dice que es el estudio de técnicas de comunicaciones seguras que permiten que solo el remitente y el destinatario previsto de un mensaje vean su contenido. Los criptógrafos protegen los sistemas informáticos y de tecnología de la información mediante la creación de algoritmos y códigos para cifrar los datos.”

"Esta disciplina gira alrededor de la protección de cuatro pilares: físico, datos, procesos y arquitectura del sistema. Lo consigue gracias al uso de herramientas específicas."

"El token de seguridad o el token de autenticación es el que se considera herramienta de criptografía. Usando el token de seguridad, se puede autenticar al usuario. También se utiliza para proporcionar estado al protocolo HTTP. El token de seguridad debe estar cifrado para permitir el intercambio seguro de datos." (Universidadviu, 2021).

Hay 3 tipos de criptografía: clave secreta, clave pública y función hash:

- **Criptografía de clave secreta (ver figura 2):** utilización de una única clave tanto para el cifrado como para el descifrado; también llamado cifrado simétrico, principalmente para la privacidad y la confidencialidad.
- **Criptografía de clave pública (ver figura 3)**: utiliza una clave para el cifrado y otra para el descifrado. A este método se le conoce como cifrado asimétrico. Se utiliza principalmente para autenticación e intercambio de claves.
- **Funciones hash:** emplea una transformación matemática para "cifrar" la información de forma irreversible, proporcionando una huella digital. Se utiliza principalmente para la integridad de los mensajes.

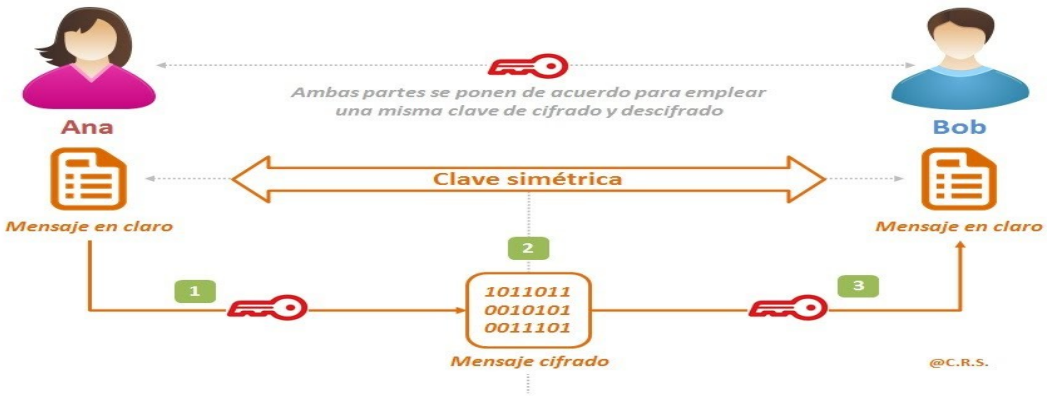

Figura 2: Funcionamiento de clave simétrica. Recuperado de https://sites.google.com/site/seguridadinformaticadavid/tema-4---criptografia/4-2--cifrado-de-la-clave-simetrica

También Lucena López nos dice "En la actualidad, la práctica totalidad de las aplicaciones criptográficas emplean computadoras en sus cálculos, y las computadoras convencionales están diseñadas para ejecutar algoritmos. … La Criptografía depende en gran medida de la Teoría de Algoritmos, ya que, por un lado, hemos de asegurar que el usuario legítimo, que posee la clave, puede cifra y descifrar la información de forma rápida y cómoda, mientras que por otro hemos de garantizar que un atacante no dispondrá de ningún algoritmo eficiente capaz de comprometer el sistema." (Manuel J. Lucena López, 2010).

Figura 3: Funcionamiento del cifrado asimétrico. Recuperado de https://academy.bit2me.com/wp-content/uploads/2019/05/como-funciona-clave-privada.jpg

Evidentemente, se podría profundizar mucho más en los distintos algoritmos. La tesis de grado de María Eugenia Ansalas de 1998 realiza un estudio recomendable sobre esto.

Por otra parte, sabemos que los algoritmos de cifrado más utilizados no son seguros en la computación cuántica, "Es importante tener en cuenta que, la aparición de las computadoras cuánticas y su posterior comercialización, deja obsoletos muchos de los algoritmos criptográficos que actualmente son seguros; tales como RSA, DSA o ECDSA" (Cordoba, Méndez-Garabetti, 2017). Esta afirmación surge del trabajo de investigación de la Universidad de Mendoza de los citados autores.

Para cumplir con el objetivo del trabajo también tenemos que tener en cuenta otras variables importantes que analizamos en el texto que sigue.

Protocolos seguros de navegación web o HTTPS

HTTPS es el protocolo utilizado en la *capa de aplicación* del conjunto de protocolos TCP/IP para la comunicación segura del navegador cliente y un servidor HTTP. Hace uso del protocolo SSL (Secure Sockets Layer) y del protocolo TLS (Transport Layer Security).

Lucena Lopez afirma: "El protocolo SSL (Secure Sockets Layer), desarrollado originalmente por la empresa Netscape, permite establecer conexiones seguras a través de Internet, de forma sencilla y transparente."… "Su fundamento consiste en interponer una fase de codificación de los mensajes antes de enviarlos a través de la red. Una vez que se ha establecido la comunicación, cuando una aplicación quiere enviar información a otra computadora, la capa SSL la recoge y la codifica, para luego enviarla a su destino

a través de la red. Análogamente, el módulo SSL del otro ordenador se encarga de decodificar los mensajes y se los pasa como texto claro a la aplicación destinataria.”(p. 226).

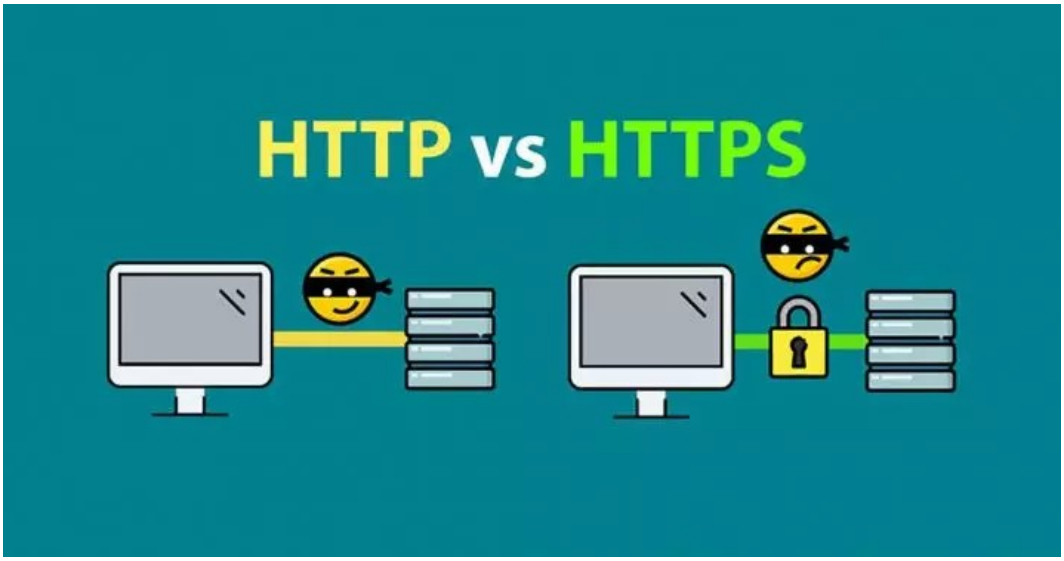

*Figura 4: Protocolo **HTTP** versus **HTTPS**. Recuperado de https://www.adslzone.net/2019/06/11/paginas-web-https-falsas-certificados/*

Sobre TLS dice “es un protocolo basado en la versión 3.0 de SSL”…“En este protocolo se emplea una serie de medidas de seguridad adicionales, encaminadas a protegerlo de distintos tipos de ataque, en especial de los de intermediario” ... “Si bien el método usado con más frecuencia para establecer conexiones seguras a través de Internet sigue siendo SSL, cabe esperar que con el tiempo sea paulatinamente reemplazado por TLS, y que este último se convierta en el estándar de seguridad para las comunicaciones cifradas en Internet.”(p. 227-228). Nosotros vamos a partir de que los métodos actuales de cifrado son seguros.

Las cookies

¿Qué son las cookies? Veamos que dice Gomez Vientes:

"Mediante 'cookies' que se almacenan en el propio navegador Web y que registran el 'identificador de sesión' asignado al usuario por el servidor. En este caso podríamos distinguir entre 'cookies persistentes' (aquellas que se almacenan en el disco duro del usuario) y 'cookies no-persistentes' (solo se guardan en memoria RAM y se destruyen al cerrar el navegador). Asimismo, las cookies seguras son aquellas que sólo pueden ser enviadas al servidor al que pertenecen mediante una conexión HTTPS (protocolo criptográfico SSL)."(p. 542).

"Gracias a las cookies, el servidor Web puede recordar algunos datos sobre el usuario que le visita: sus preferencias para la visualización de las páginas en ese servidor (personalización de servicios y contenidos), cuál es su nombre de usuario y Contraseña, etc."..."La técnica de las cookies fue desarrollada por la empresa Netscape para mejorar las capacidades de las aplicaciones cliente/servidor basadas en el Web, ya que hay que tener en cuenta que el protocolo HTTP es un protocolo sin estado, que no recuerda anteriores fases de la conexión a un servidor Web."(p. 567)

Volviendo a la citada aplicación de Mercado Libre:

"Reconocés y aceptás expresamente que Mercado Libre podrá utilizar un sistema de seguimiento de conducta mediante la utilización de 'cookies' y/u otras tecnologías similares de seguimiento.

Estas tecnologías se utilizan con el fin de conocer los intereses y el comportamiento de quienes visitan o son usuarios de nuestro sitio web" ... "También usamos la información obtenida a través de cookies para analizar las páginas navegadas por el

visitante o usuario, las búsquedas realizadas" … "también las utilizamos para que el usuario no tenga que introducir su clave tan frecuentemente durante una sesión de navegación, también para contabilizar y corroborar las inscripciones, la actividad del usuario y otros conceptos para acuerdos comerciales" … "Adicionalmente, se pueden encontrar 'cookies' u otros sistemas similares instalados por terceros en ciertas páginas de nuestros sitios web o utilizados por anunciantes ajenos a Mercado Libre." (Mercado Libre, 2021). Nuevamente, si queremos conservarnos anónimos, nos dice claramente que no nos conviene usarla.

Asimismo, las cookies seguras son aquellas que sólo pueden ser enviadas al servidor al que pertenecen mediante una conexión HTTPS (protocolo criptográfico SSL).

En este y cualquier caso, nos prometen utilizar VPN para garantizar privacidad. ¿Es así? Podemos encontrar muchos artículos periodísticos y publicitarios, pero papers científicos sobre esto, lamentablemente muy pocos.

Figura 5: Las cookies que dejan las aplicaciones y paginas web en nuestros dispositivos. Recuperado de https://www.udelistmo.edu/blogs/que-son-las-cookies-y-por-que-siento-que-me-espian

Existen diferentes tipos de cookies:

Cookies de primera parte: Las cookies de la primera parte se guardan directamente en el sitio web. Estas cookies son las que permiten a los dueños de los sitios web recolectar datos, conocer los datos de lenguaje de cada usuario y, en general, se usan para mejorar la experiencia de cada usuario.

Cookies de segunda parte: Son cookies que se venden entre empresas. Hay empresas que venden información almacenada en las cookies como patrones de comportamientos e intereses.

Cookies de sesión: Conocidas como cookies temporales, son las que el sitio debe descargar en una sesión para poder dar una mejor experiencia en ese momento. Estas cookies se borran al cerrar la página en el navegador.

Cookies permanentes: Estas con las cookies a las que más se les da permiso. Se guardan en el ordenador aunque ya no se esté en el sitio web. Son las que recuerdan los datos de entrada de los usuarios. Dichas cookies se deberían borrar cada 12 meses en algunos países y cada 2 años en otros.

Flash cookies: Son un tipo de cookies independiente a los sitios web. Se guardan directamente en el ordenador de los usuarios y se quedarán ahí aunque se borre el historial de cookies.

Cookies zombie: Son un tipo de flash cookies que se replica cuando las borras, así que deshacerse de ellas es muy complicado y detectarlas, aún más. Este tipo de cookies se usa generalmente en videojuegos online para prevenir que los usuarios hagan trampas

en los juegos. Sin embargo, hay casos en los que se usa con objetivos nefastos, usualmente para instalar software malicioso en los dispositivos de los usuarios.

Cookies necesarias: Aunque parezca que las cookies están ahí para seguir los datos y guardar información, hay algunas cookies que son esenciales para que los sitios web funcionen. Algunas de las funciones que cumplen las cookies esenciales son la habilidad de registrarse y entrar en un sitio, o que los productos del carrito se guarden y los puedas ver cada vez que entres, entre otras opciones.

Cookies de rendimiento: Estos tipos de cookies realmente no guardan ninguna información de los usuarios, simplemente están ahí para dar información sobre el estado y rendimiento del sitio web. Puede ser para ver lo rápido que carga la página, cuánto tiempo estuvo un usuario navegando o cuánto permaneció en una página específica, etc. (keepCoding, 2022. Recuperado de https://keepcoding.io/blog/tipos-de-cookies/).

JavaScript

"JavaScript es un lenguaje de programación o de secuencias de comandos que te permite implementar funciones complejas en páginas web, cada vez que una página web hace algo más que sentarse allí y mostrar información estática para que la veas, muestra oportunas actualizaciones de contenido, mapas interactivos, animación de Gráficos 2D/3D, desplazamiento de máquinas reproductoras de vídeo, etc., puedes apostar que probablemente JavaScript está involucrado." (Mozilla, 2022. Recuperado de https://developer.mozilla.org/es/docs/Learn/JavaScript/First_steps/What_is_JavaScript)

Según un informe de Tala Security, el 99% de los sitios de internet son vulnerables al ataque vía JavaScript. El Peligro reside cuando el código JavaScript (o la ubicación

donde se creó/alojó el código) se ve comprometido (es decir, se agrega código malicioso al código existente). Es un problema muy peligroso, especialmente cuando las páginas web ofrecen contenido confidencial o realizan actividades que pueden manipular datos, como pagos online. (Tala Security, 2020. Recuperado de https://go.talasecurity.io/blog/external-javascript-website-security).

Esto también va a ser tenido en cuenta en la investigación. Si un sitio permite o no poder navegar con JavaScript desactivado.

VPN y TOR

VPN

Una Red Privada Virtual, conocida como VPN (Virtual Private Network), brinda privacidad y anonimato en línea al crear una red privada desde una conexión pública a Internet. Las VPN enmascaran su dirección de protocolo de Internet (IP) para que sus acciones en línea sean difíciles de rastrear. Lo que es más importante, los servicios de VPN establecen conexiones seguras y encriptadas para dar mayor privacidad.

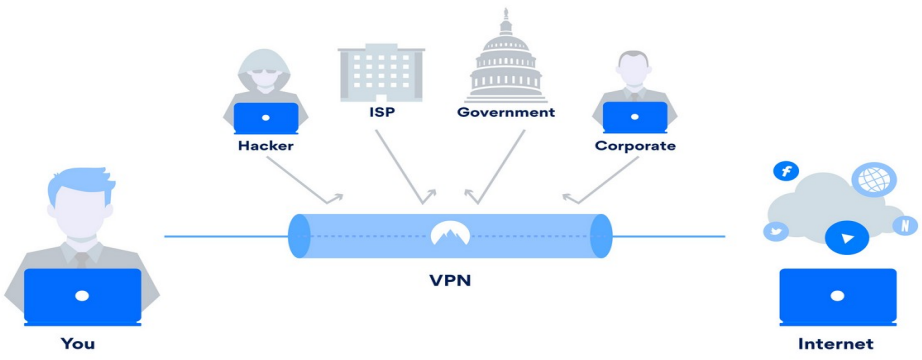

Figura 6: Tunelización de una VPN. Recuperado de https://www.themovieblog.com/2019/10/what-my-isp-sees-when-i-use-vpn-explained/

Una VPN crea un tipo de túnel, ver figura 6, que oculta la actividad en línea, incluidos los enlaces en los que hace clic o los archivos que descarga, para que posibles ciberdelincuentes, empresas o agencias gubernamentales u otros no puedan verlo.

Una VPN le permite conectarse a Internet de forma encriptada, lo que agrega seguridad y privacidad a su navegación en línea.

Una VPN puede ocultar información que puede poner en riesgo tu privacidad:

-Historial de navegación: El proveedor de servicios de Internet y su navegador web pueden rastrear casi todo lo que hace en Internet. Muchos de los sitios web que visita mantienen un historial. Los navegadores web pueden rastrear su historial de búsqueda y vincular esa información a su dirección IP.

- Dirección IP y ubicación: Cualquiera que capture su dirección IP puede acceder a lo que ha estado buscando en Internet y dónde estaba ubicado cuando realizó la búsqueda.

-Dispositivos: Los dispositivos pueden ser objetivos principales para los ciberdelincuentes cuando accede a Internet. A través de la VPN se oculta la información del mismo.

Se puede usar una VPN si está preocupado por su privacidad. Si la conexión a Internet es a través de una VPN, el proveedor de tus servicios de Internet no podrá ver lo que está haciendo.

TOR

Navegador TOR: Es una tecnología de navegador de ingeniería avanzada diseñada para enrutar su tráfico web a través de una red TOR y VPN segura. Funciona encriptando y luego redirigiendo sus datos a través de tres nodos aleatorios (servidores) para proteger sus datos y desviar a cualquier pirata informático o ciberdelincuente que lo esté rastreando.

"Tor es un programa que puede ejecutar en su computadora que lo ayuda a mantenerse seguro en Internet. Lo protege haciendo rebotar sus comunicaciones a través de una red distribuida de repetidores administrados por voluntarios de todo el mundo: evita que alguien que esté viendo su conexión a Internet sepa qué sitios visita y evita que los sitios que visita conozcan su ubicación física. Este conjunto de repetidores voluntarios se denomina **red Tor**. La forma en que la mayoría de la gente usa Tor es con **Tor Browser**, que es una versión de Firefox que soluciona muchos problemas de privacidad."(TOR Project, 2019).

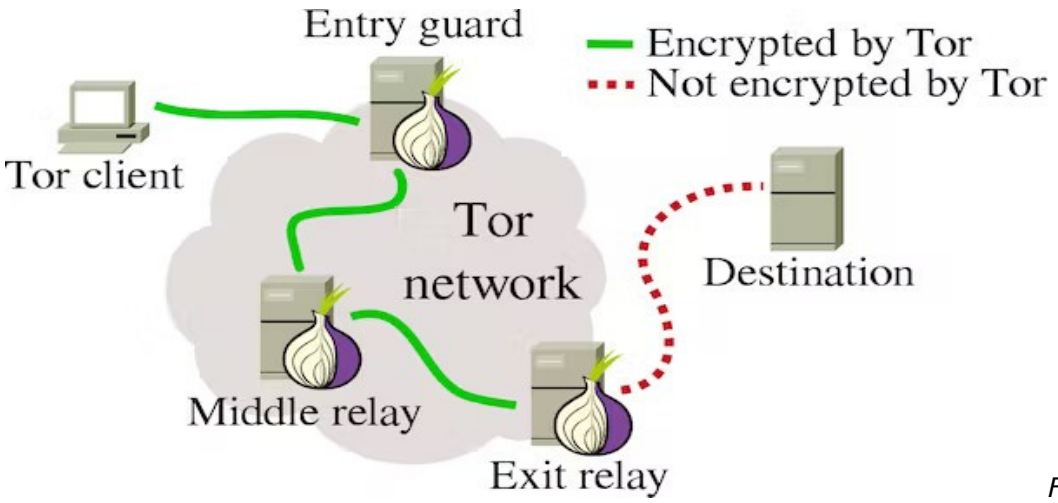

Figura 7: Funcionamiento en capas de la red TOR. Recuperado de https://theconversation.com/tor-upgrades-to-make-anonymous-publishing-safer-73641

Como se ve en la figura 7, el diseño por capas está diseñado para canalizar su tráfico web a través de la red TOR segura y anónima para garantizar que su identidad personal permanezca intacta.

Objetivo general

Verificar con una investigación hasta donde se garantiza la privacidad a la hora de navegar por la web, ver cuáles son los rastros dejados en los servidores que nos pueden llegar a identificar y cuál sería la utilización segura de la criptografía.

Objetivos específicos

- Determinar el nivel de seguridad criptográfica de nuestros datos privados que viajan a través de la red al usar sitios web.

- Puntualizar qué datos dejamos al visitar diferentes sitios de internet. Localizaciones, datos privados, etc.

- Examinar cuáles son las condiciones de navegación segura en los sitios de internet más usados.

Métodos

Diseño

En los últimos años, casi toda la vida de las personas pasaron a estar en la web. Al principio no existía ningún tipo de codificación de los datos. Hoy hay muchos métodos que dicen garantizar privacidad y protección de datos, pero la tecnología va avanzando y no sabemos hasta donde eso es cierto.

El alcance de este trabajo es descriptivo. Se pretende hacer una vista sobre el tema mencionado para cualquier usuario de internet, buscando que opciones hay y cuáles son las más se acercan a cumplir con este objetivo, si es que es posible.

Enfoque de la Investigación

El enfoque de la investigación es mixto. Lo primero es una breve investigación sobre métodos de criptografía en la navegación web, su nivel de seguridad y vulnerabilidades conocidas. A partir de ahí, establecer una escala numérica donde se cuantifique según las formas y programas utilizados el nivel de privacidad.

En relación con las variables de estudio, para poder cuantificar, vamos a identificar cuáles son las condiciones para que no nos identifiquen. Armaremos una tabla con puntaje del 0 al 10, donde 0 son las perores condiciones y 10 las mejores (ver tabla 1). En las mejores, eso implica el no reconocimiento del número IP, ligado a una PC en particular. Y las formas en las cuales podemos navegar a través de la web sin que nos dejen cookies que nos identifiquen, como se describió en la primera parte. Dentro de

esto está también la posibilidad de usar una VPN o TOR, que cada uno de estos sistemas tienen sus tácticas para evitarlo.

Muestra

El muestreo es no probabilísticos intencional. Se simulará un usuario cualquiera de internet y se utilizará software disponible para recabar datos. Analizando las cookies que dejarán diferentes sitios web en la computadora, en este caso, Google, Youtube, Facebook, Instagram y MercadoLibre, de las cuales 4 son los más visitados en el mundo (Galeano 2022) y las 5 más visitada en Argentina (BAE Negocios, 2022). Se analizará a través del número IP la geolocalización. Se harán pruebas de si es posible ocultar esta información por diferentes métodos como la utilización de una VPN (protonVPN) y un navegador TOR.

Para realizar la verificación del número IP, se va a utilizar un software llamado "open visual trace route" que chequea los pasos de las conexiones desde un servidor hasta nuestro dispositivo.

Con las cookies, se verificará que permisos de acceso tiene a nuestra pc. Utilizaremos Chrome para ver las cookies guardadas y se buscará en la base de datos CookieDatabase sus características. Ver en https://cookiedatabase.org/

Por otro lado, está la criptografía. Esta también es una variable a tener en cuenta en la cuantificación. Hay sistemas criptográficos que ya se sabe que no son seguros y otros que sí. Al navegar en la web con el protocolo HTTPS, no todos utilizan el más seguro. Se va a verificar la utilización del protocolo a través de la herramienta online:

https://geekflare.com/, que cuenta con tests para comprobar los mismos.

Cuantificación para las condiciones de privacidad y seguridad de los datos:

Condiciones	Puntaje	
	Si	No
Cookies de identificación	0	1
Cookies de Seguimiento	0	1
Otras Cookies	0	1
Registra IP	0	1
Permite JavaScript desactivado	1	0
Permite VPN	2	0
Permite uso de TOR	1	0
Usa HTTPS	2	0

Tabla 1 – Cuantificación de variables

Desde el punto de vista de la privacidad y el anonimato a la hora de usar la web, hay un primer problema que es la NO revelación del usuario de sus propios datos. Luego de esta "obviedad", los dos problemas siguientes son la geoubicación a través del número IP y el uso de captura de datos privados cuando viajan por la red, por eso la criptografía pasa a ser tan importante. Esa es la razón por la cual en esta tabla, colocamos el empleo de una VPN, que permite ocultar nuestra geolocalización verdadera y el protocolo HTTPS para la protección de los datos con un puntaje de 2, por encima del resto.

Tipo de investigación

El tipo de investigación no experimental transversal. Es no experimental porque la investigación se realiza sin la manipulación deliberada de variables y solo se observan los fenómenos tal cual son. No se llevará a cabo la manipulación deliberada de variables, solo se observan los fenómenos tal cual son para después analizarlos y es transversal porque la recolección de datos se hará una única vez.

Resultados

Datos:

	Google	Youtube	Facebook	Instagram	MercadoLibre
Usa Cookies de identificación	1	1	0	0	1
Usa Cookies de Seguimiento	1	1	0	0	1
Usa Otras Cookies	1	0	0	0	1
Registra IP	1	1	1	1	1
Permite JavaScript desactivado	1	0	0	0	0
Permite VPN	1	1	1	1	1
Permite uso de TOR	2	2	0	0	0
Usa HTTPS	2	2	2	2	2
Resultados según cuantificación de tabla 1	**9**	**7**	**4**	**5**	**7**

Tabla 2 – Resultados de los sitios más comunes

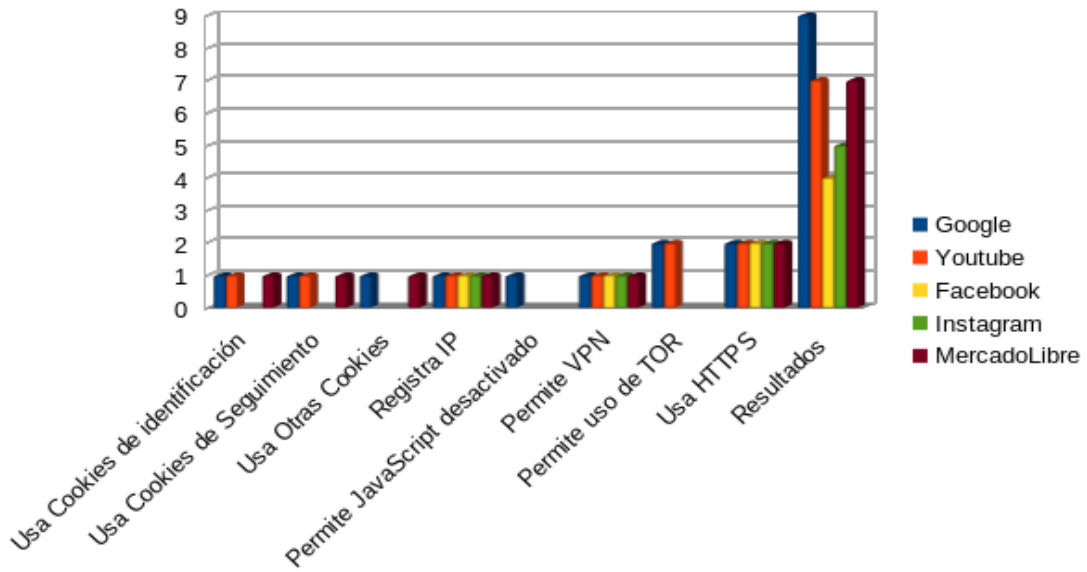

Figura 8: Grafico con los resultados de los sitios más comunes

Cookies:

Al ingresar con el navegador a los diferentes sitios las cookies tiene un nombre específico. Algunos permiten hacer uso del sitio sin habilitarlas, otros no. Cuando dejan las cookies. Acá vemos un ejemplo:

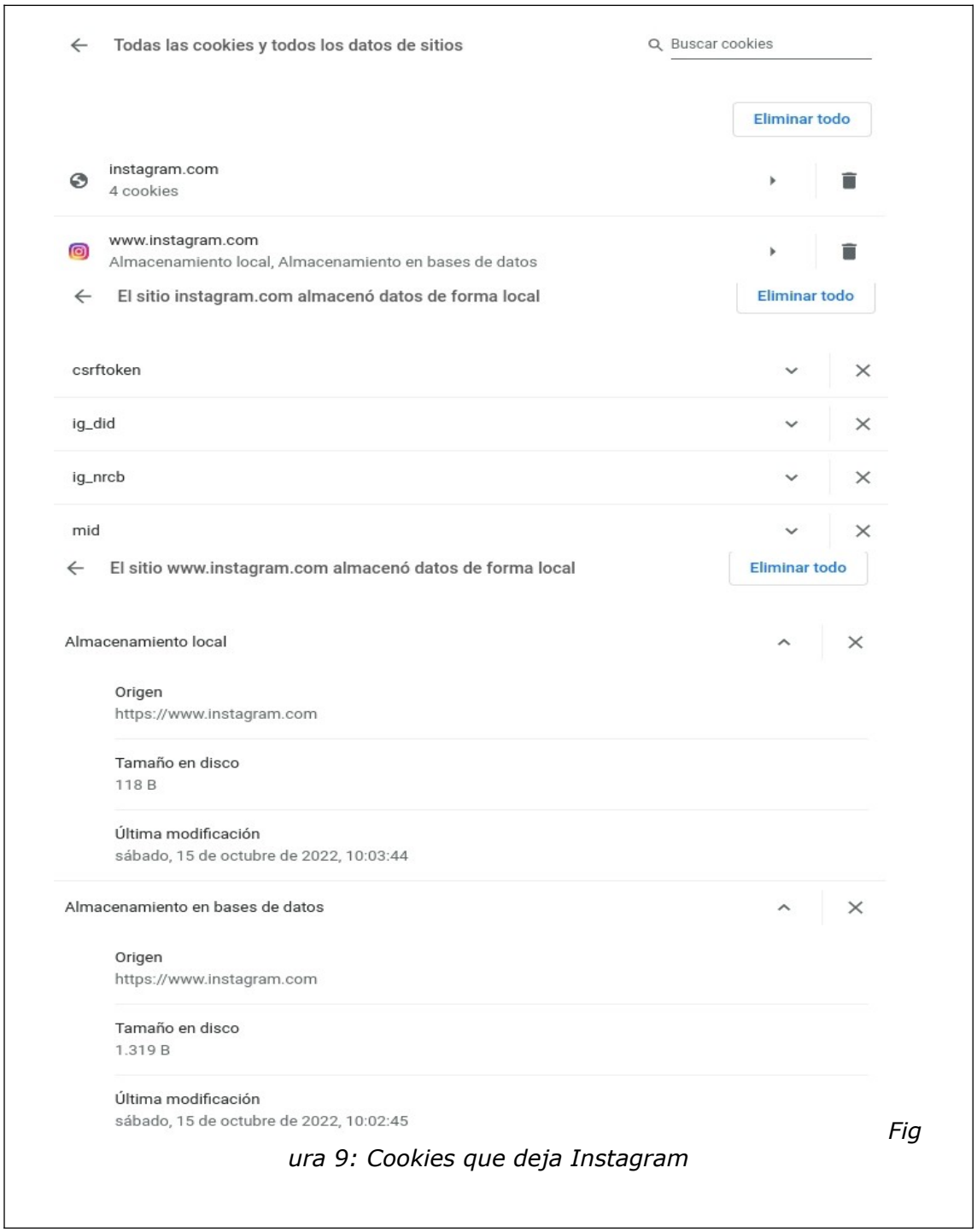

Figura 9: Cookies que deja Instagram

Registro de IP:

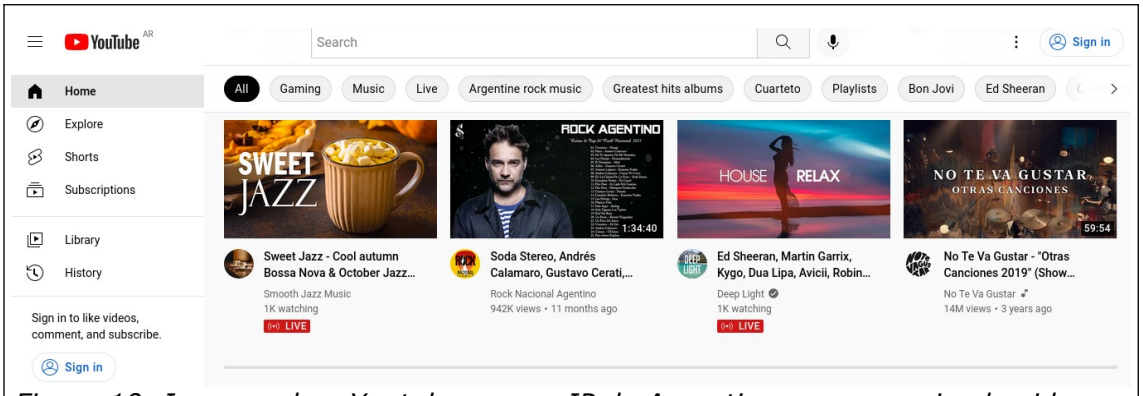

Figura 10: Ingresando a Youtube con un IP de Argentina, nos recomienda videos y música de Argentina

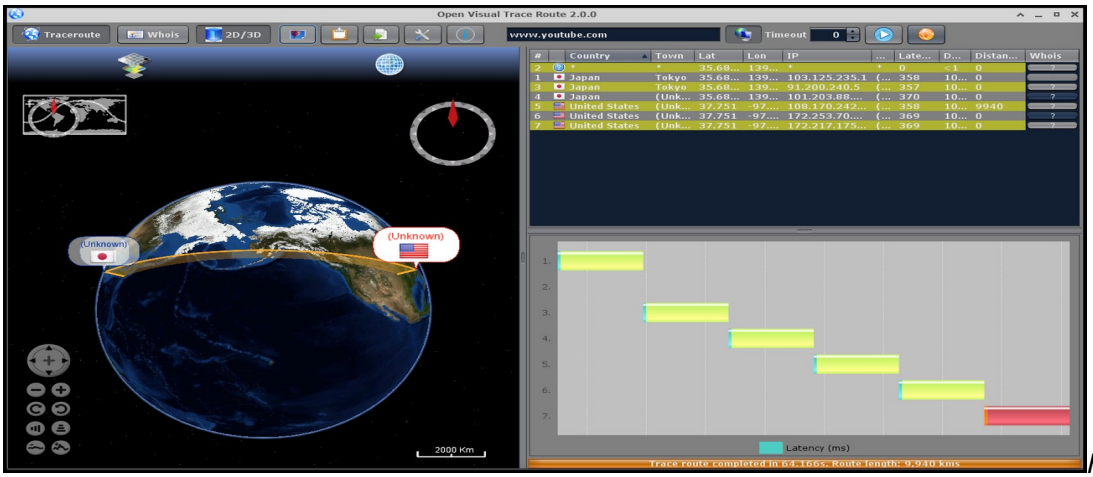

Figura 11: Ingresando a Youtube con una IP de Tokyo, Japón

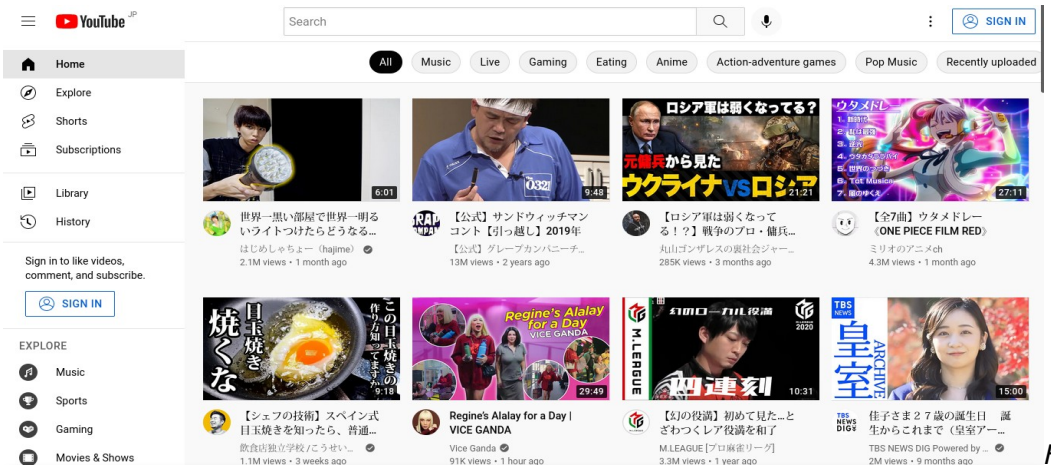

Figura 12: Ingresando a Youtube con un IP de Japón, nos recomienda videos y música Japonesa

JavaScript desactivado:

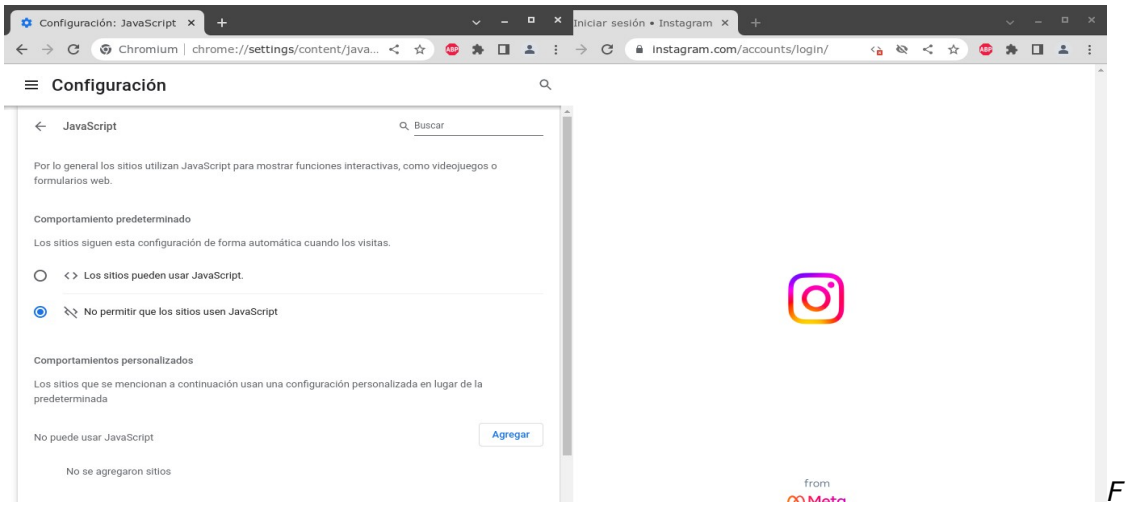

Figura 13: Con JavaScript desactivado, Instagram no carga

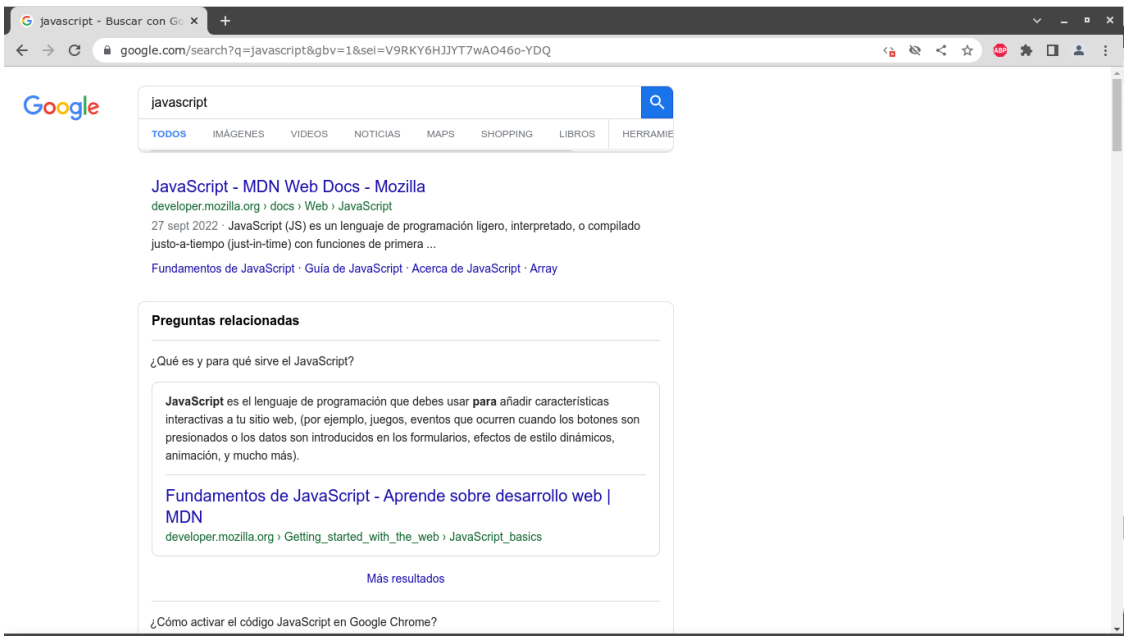

Figura 14: Google permite realizar búsquedas sin JavaScript activado

Uso de VPN:

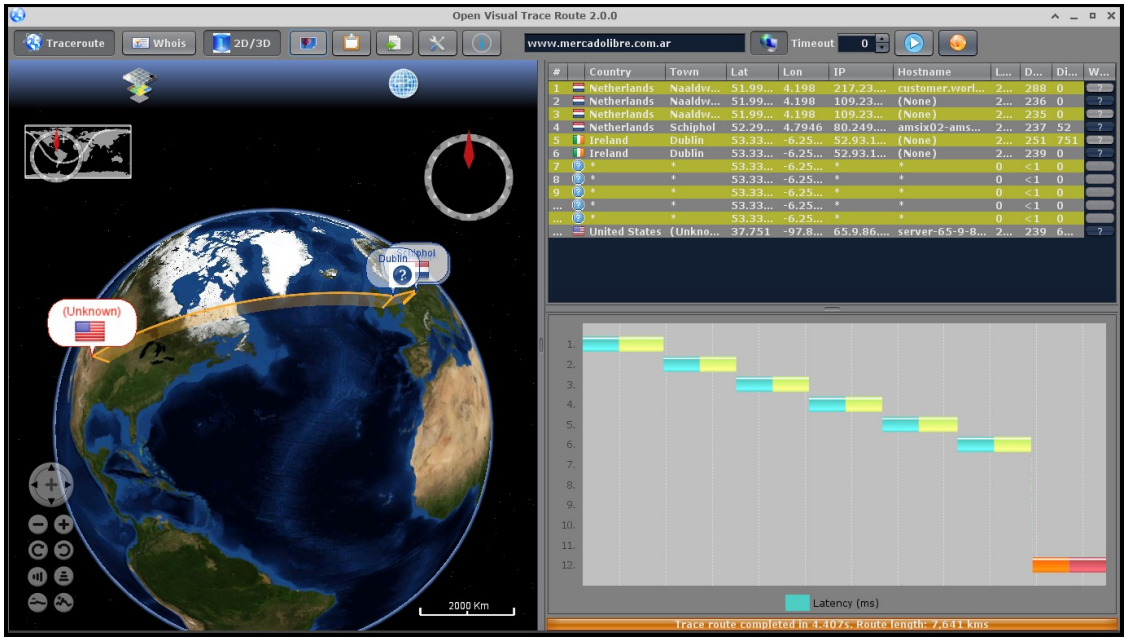

Figura 15: Ingresando al servidor de MercadoLibre desde una VPN de Holanda

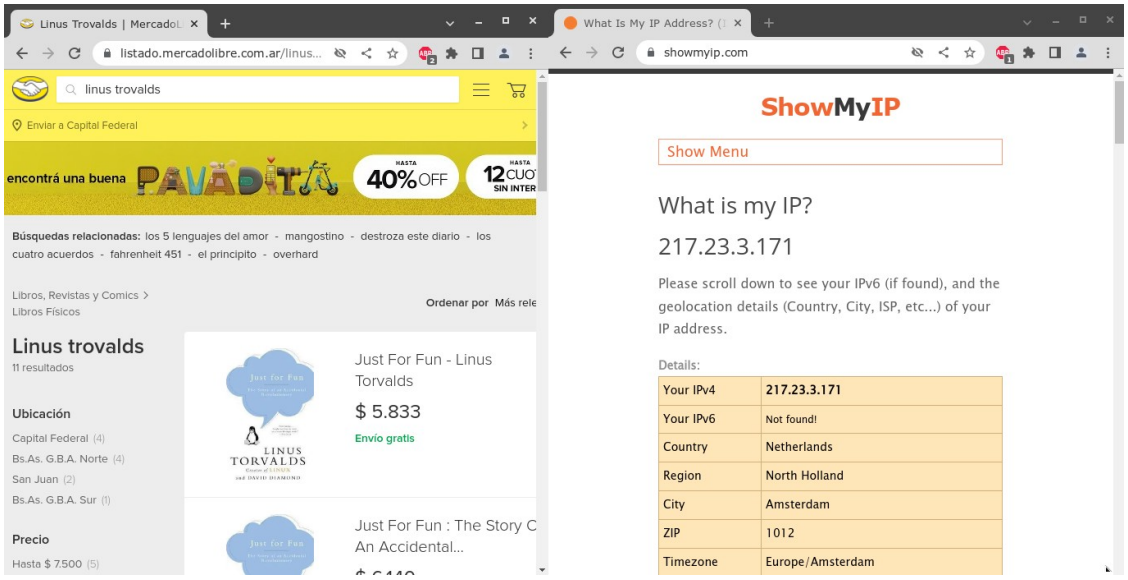

Figura 16: MercadoLibre permite su uso desde una VPN

Uso de TOR:

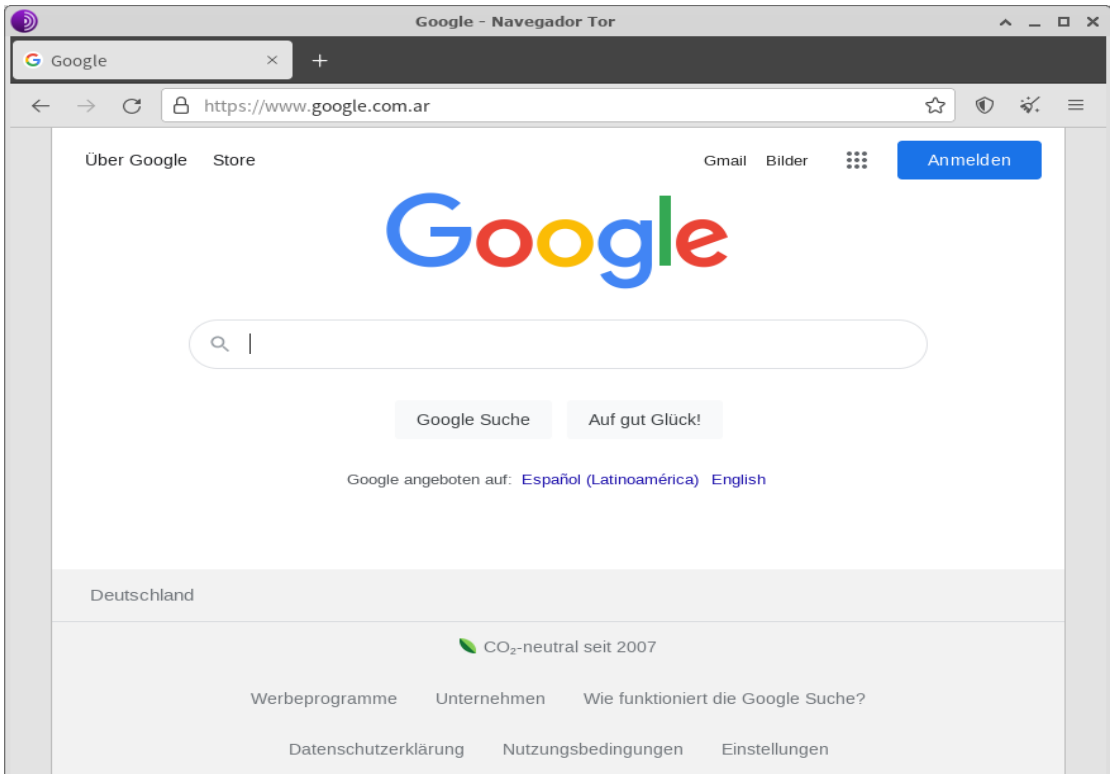

Figura 17: Google Sí esta habilitado para usar TOR

Figura 18: MercadoLibre No permite el uso de TOR

Verificación del Protocolo HTTPS:

www.google.com
IP: 142.251.163.99

Tested on October 14, 2022 6:54 PM

TLS Protocols

TLS Protocol	Finding
SSLv2	not offered (OK)
SSLv3	not offered (OK)
TLS1	offered (deprecated) (LOW)
TLS1_1	offered (deprecated) (LOW)
TLS1_2	offered (OK)
TLS1_3	offered with final (OK)

Server's cipher preferences

Has server cipher order?	Yes (OK)
Negotiated protocol	Default protocol TLS1.3
Negotiated cipher	TLS_AES_256_GCM_SHA384, 253 bit ECDH (X25519)

Figura 19: Tanto Google, Youtube, Facebook e Instagram utilizan por defecto TLS1.3, pero permiten la versión desactualizada 1 y 1.1

www.mercadolibre.com
IP: 18.67.65.99

Tested on October 14, 2022 7:02 PM

TLS Protocols

TLS Protocol	Finding
SSLv2	not offered (OK)
SSLv3	not offered (OK)
TLS1	not offered (INFO)
TLS1_1	not offered (INFO)
TLS1_2	offered (OK)
TLS1_3	offered with final (OK)

Server's cipher preferences

Has server cipher order?	Yes (OK)
Negotiated protocol	Default protocol TLS1.3
Negotiated cipher	TLS_AES_128_GCM_SHA256, 253 bit ECDH (X25519)

Figura 20: Mercado Libre por defecto utiliza TLS 1.3, y es el único protocolo que ofrece.

Puntaje obtenido:

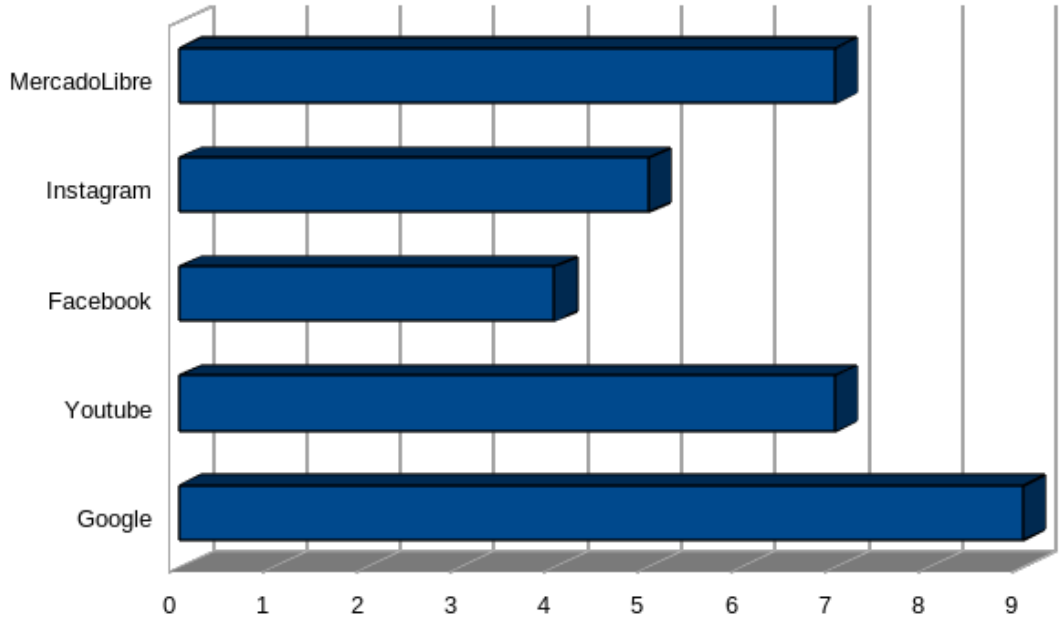

Figura 21: Puntaje según tabla 2 - Comparación entre sitios según nivel de privacidad posible

Considerando detenidamente los resultados de las pruebas y el análisis minucioso que hemos llevado a cabo, se puede afirmar con confianza que Google emerge como un destacado defensor de la privacidad de sus usuarios. Su estrategia de permitir el funcionamiento de su plataforma sin la necesidad de activar JavaScript ofrece una doble ventaja. En primer lugar, esta decisión mejora la experiencia del usuario al agilizar la navegación y proporcionar un entorno más eficiente. En segundo lugar, y quizás más importante, esta práctica reduce significativamente la exposición del usuario a posibles amenazas de malware, lo que garantiza un entorno más seguro para explorar la web. Además, Google se destaca al brindar una mayor flexibilidad en cuanto al control de la privacidad, lo que permite a los usuarios adaptar su experiencia según sus preferencias.

YouTube merece un reconocimiento especial por permitir el uso de la red anónima TOR. Esta característica fundamental contribuye de manera significativa a mantener la

privacidad del usuario en línea. Al habilitar el uso de TOR, YouTube permite a los usuarios navegar sin ser rastreados y evita la geolocalización, lo que es valioso para aquellos que buscan mantener el anonimato en internet. Este enfoque demuestra el compromiso de YouTube con la privacidad de sus usuarios y su voluntad de proporcionar opciones seguras para la navegación.

MercadoLibre también se distingue en términos de privacidad al permitir a los usuarios realizar búsquedas en su plataforma sin requerir la activación de cookies. Esta característica agrega un nivel adicional de privacidad al navegar por su plataforma, ya que la información relacionada con la actividad del usuario no se almacena mediante cookies. Esto contribuye a obtener un puntaje positivo en nuestra evaluación de privacidad y demuestra la consideración de MercadoLibre hacia la seguridad y la privacidad de sus usuarios.

Por otro lado, Instagram y Facebook, si bien son plataformas ampliamente utilizadas, no se destacan en términos de privacidad. Ambos sitios no permiten que los usuarios hagan uso de la plataforma con las cookies deshabilitadas, lo que significa que estos sitios pueden rastrear a los usuarios con mayor facilidad y recopilar datos relacionados con su actividad en línea. Esto puede plantear preocupaciones en términos de privacidad para aquellos que desean un mayor control sobre su información personal.

Un aspecto positivo que debemos destacar es que todos los sitios web analizados ofrecen el protocolo HTTPS, específicamente el protocolo TLS, lo que garantiza que los datos viajen de manera segura por la red. Este es un estándar esencial para proteger la privacidad del usuario en línea y evitar la exposición no deseada de información personal.

Nuestras pruebas y análisis han proporcionado una base para evaluar el nivel de privacidad posible en estos sitios web populares. Esta evaluación es fundamental para que los usuarios tomen decisiones informadas sobre su privacidad en línea y comprendan los diferentes enfoques adoptados por las plataformas en términos de seguridad y privacidad. La privacidad en línea es un aspecto crucial en la era digital, y esta investigación ofrece una visión clara de cómo algunas de las plataformas más utilizadas abordan esta cuestión.

Discusión

La discusión sobre los resultados obtenidos en nuestra investigación arroja luz sobre la compleja cuestión de la privacidad en línea y las diversas formas en que los usuarios pueden gestionarla. Nuestro objetivo principal era verificar el grado de privacidad garantizado al navegar por la web, identificar los rastros que los servidores pueden utilizar para identificarnos y explorar cómo se puede utilizar la criptografía de manera segura en este contexto.

En primer lugar, es fundamental reconocer que la privacidad y seguridad de nuestros datos en línea recae en gran medida en nuestras manos como usuarios. Esta noción es especialmente relevante en un mundo donde la mayoría de nuestras actividades cotidianas transcurren en la web. Sin embargo, a menudo esta búsqueda de privacidad se contradice al ingresar información personal, como nombres de usuario y contraseñas, en los sitios web que visitamos. En este sentido, debemos ser conscientes de la paradoja de querer mantener la privacidad mientras compartimos datos personales con las plataformas en línea.

Un aspecto valioso que se reveló es el papel de las cookies en la navegación web. Estas pequeñas porciones de datos son esenciales para el funcionamiento de la internet moderna, ya que permiten la personalización de la experiencia del usuario en los sitios web. Sin embargo, al mismo tiempo, las cookies representan un desafío para la privacidad, ya que pueden acumular información personal y ser utilizadas para rastrear la actividad en línea de los usuarios. Es importante destacar que no todos los sitios web ofrecen la posibilidad de deshabilitar las cookies, lo que resalta la importancia de la elección de plataformas que respeten la privacidad del usuario.

Otro aspecto esencial es el de la dirección IP, que es como una especie de huella digital en línea. Cada dispositivo en una red debe tener su propia dirección IP, lo que significa que al ingresar a un sitio web, automáticamente proporcionamos una identificación única. En este contexto, las VPN desempeñan un papel crucial al ocultar nuestra verdadera IP al sitio al que accedemos, protegiendo así nuestra privacidad. Sin embargo, debemos confiar en que el proveedor de VPN mantendrá nuestros datos seguros. Es alentador observar que todos los sitios web analizados permitieron la conexión a través de una VPN, lo que otorga a los usuarios una mayor flexibilidad para proteger su privacidad.

No obstante, la red TOR representa un enfoque diferente y más privado para la navegación en línea. Basada en una comunidad open source y un sistema de capas de cebolla, TOR ofrece una mayor privacidad al ocultar la identificación del usuario. Sin embargo, es importante destacar que la mayoría de las direcciones IP en la red TOR son públicas, lo que plantea preocupaciones de seguridad para los sitios web que desean evitar el acceso desde allí. Plataformas como Mercado Libre, Instagram y Facebook no permitieron el acceso desde la red TOR, lo que refleja una preferencia por mantener un mayor control sobre la privacidad de los usuarios.

Otro aspecto crucial en la evaluación de la privacidad es el uso del protocolo HTTPS, especialmente el protocolo TLS 1.3, que garantiza la seguridad de la transferencia de datos en línea. Identificamos que la mayoría de los sitios web analizados ofrecen este protocolo, lo que es una práctica esencial para proteger la privacidad del usuario. Sin embargo, algunos sitios ofrecen versiones desactualizadas de TLS, lo que puede representar un riesgo potencial para la seguridad de los datos. En este

contexto, es relevante destacar que el buscador Google permite el uso sin problemas de su plataforma sin JavaScript habilitado, lo que puede contribuir a una experiencia de navegación más segura.

En última instancia, se resalta que la privacidad absoluta en línea es una meta difícil de alcanzar. En cambio, la medida de la privacidad se relaciona en gran parte con la configuración de las preferencias y la disposición del usuario para utilizar determinados sitios web. Cada plataforma adopta un enfoque único en términos de privacidad y seguridad, y los usuarios deben ser conscientes de estas diferencias para tomar decisiones informadas y adaptar sus prácticas de navegación en consecuencia. La privacidad en línea es un tema crucial en la era digital, y esta investigación proporciona una visión profunda de cómo las plataformas populares abordan esta cuestión y cómo los usuarios pueden proteger su privacidad en un mundo cada vez más conectado.

Problema de Investigación

El problema de investigación que abordamos en este estudio se enmarca en la creciente preocupación por la privacidad en un mundo cada vez más digitalizado. En la era actual, donde la mayoría de las actividades cotidianas se realizan en línea, es fundamental indagar en hasta qué punto se garantiza la privacidad de los usuarios al navegar por la web en sitios de amplia popularidad. La protección de la privacidad se ha erigido como un aspecto crítico en la era digital, y nos propusimos arrojar luz sobre esta cuestión apremiante.

La creciente digitalización ha dado lugar a una explosión en la generación y el flujo de datos personales en línea. A medida que más usuarios comparten información personal, efectúan compras, se comunican y participan en actividades diversas en la web, surge la necesidad de comprender cómo se manejan sus datos y qué riesgos o vulnerabilidades pueden surgir en el proceso. El avance tecnológico ha proporcionado innumerables beneficios, pero al mismo tiempo, ha planteado desafíos significativos en términos de privacidad y seguridad en línea.

La pregunta fundamental que guió nuestro estudio fue la siguiente: ¿Hasta dónde llega la garantía de privacidad de los usuarios en su experiencia de navegación por la web? Exploramos este interrogante en el contexto de los sitios web populares que millones de personas utilizan a diario. Teníamos como objetivo arrojar luz sobre las prácticas adoptadas por estas plataformas en línea y cómo influyen en la privacidad de los usuarios.

Este problema de investigación no solo es relevante en la actualidad, sino que también plantea cuestiones éticas y legales cruciales. La recopilación de datos, el seguimiento de la actividad en línea y la gestión de la privacidad se han convertido en temas candentes en debates públicos y en foros legislativos. Por lo tanto, abordar estas preocupaciones es fundamental para informar a los usuarios y permitirles tomar decisiones más informadas sobre su privacidad en línea.

La investigación se erige como un intento de comprender las prácticas y políticas que afectan directamente la privacidad de los usuarios en un entorno digital en constante evolución. Al hacerlo, aspiramos a proporcionar un conocimiento más profundo de la protección de la privacidad en línea y, a su vez, capacitar a los usuarios para que puedan

tomar decisiones informadas y salvaguardar su privacidad en el vasto y complejo mundo de la web.

Objetivos

Fijamos una serie de metas que consideramos fundamentales para comprender y abordar este desafío complejo y en constante evolución.

Nuestro objetivo primordial fue llevar a cabo una evaluación de la privacidad ofrecida por sitios web de gran renombre, entre ellos, Google, YouTube, MercadoLibre, Instagram y Facebook. Deseábamos proporcionar a los usuarios una base sólida y confiable para tomar decisiones informadas acerca de su privacidad mientras exploran el vasto panorama de la web. Reconocimos que la privacidad es un activo preciado en la era digital y que la toma de decisiones fundamentadas es esencial. Por lo tanto, nos sumergimos en el análisis de las políticas, configuraciones y prácticas de privacidad de estos sitios populares, con el propósito de arrojar luz sobre cómo protegen (o no) la información de los usuarios.

También nos orientamos hacia la exploración de herramientas y enfoques que permitieran mejorar la privacidad en línea. Aquí, nuestras miras se dirigieron hacia las VPN y la red TOR, que se han convertido en recursos esenciales para aquellos que buscan salvaguardar su anonimato y proteger sus datos en el vasto mundo digital. El objetivo era proporcionar a los usuarios no solo una comprensión de estas tecnologías, sino también recomendaciones prácticas sobre cómo pueden implementarlas de manera efectiva en su navegación por la web. La seguridad en línea es una prioridad constante,

y nuestro trabajo tenía como objetivo ofrecer a los usuarios pautas concretas para proteger su privacidad y datos personales.

Estos objetivos abordaron dos dimensiones cruciales: la evaluación de la privacidad en sitios web populares y la promoción de herramientas y prácticas que mejoren la privacidad en línea. Reconocimos que estos objetivos son fundamentales en la era digital actual y buscamos cumplirlos de manera rigurosa y completa para el beneficio de los usuarios y su seguridad en línea.

Hipótesis

En este estudio, decidimos no formular hipótesis específicas, ya que nuestro enfoque se inclinó más hacia la exploración que hacia la confirmación de suposiciones preconcebidas. Nuestra principal intención radicaba en investigar y evaluar la privacidad en línea a partir de las prácticas observadas en sitios web ampliamente utilizados. No obstante, a raíz de los resultados y conclusiones obtenidos, se abren oportunidades para plantear hipótesis adicionales que podrían servir como base para futuros estudios.

Una posible hipótesis que podría derivarse de nuestro trabajo es la siguiente: "Los sitios web que permiten a los usuarios desactivar las cookies proporcionan un nivel de privacidad superior en comparación con aquellos que no brindan esta opción". Esta hipótesis se basaría en la observación de que la desactivación de cookies puede reducir la recopilación de datos personales y, en consecuencia, mejorar la privacidad en línea.

Su exploración y validación serían un paso importante para comprender mejor las prácticas que influyen en la privacidad de los usuarios en la web.

Aunque no formulamos hipótesis específicas en este estudio, reconocemos que nuestras investigaciones abren nuevas perspectivas para futuras investigaciones, lo que podría contribuir a la formulación de hipótesis adicionales y a una comprensión más profunda de la privacidad en línea.

Modelo Teórico Adoptado

El modelo teórico adoptado se fundamentó en la delicada balanza entre la recopilación de datos para mejorar la experiencia del usuario y la salvaguardia de la privacidad personal en el entorno en línea. Reconocimos que las cookies desempeñan un papel fundamental en el funcionamiento moderno de la web al permitir la personalización y la comodidad, pero también entendimos que su uso excesivo o indebido podría conllevar riesgos para la privacidad. Además, valoramos la importancia de herramientas como las VPN y la red TOR, que actúan como salvaguardias al ocultar la dirección IP del usuario y mantener su anonimato. Asimismo, dentro de nuestro modelo teórico, se consideró crucial el empleo de protocolos de seguridad, como HTTPS/TLS, para garantizar la integridad y confidencialidad de los datos transmitidos en línea.

Nos embarcamos en una exploración y una comparativa de la problemática de la privacidad en línea. Los resultados de este estudio proporcionan a los usuarios una base sólida para comprender y evaluar la privacidad en sitios web populares. Nuestra

discusión enmarca estos resultados en el contexto de los objetivos de la investigación y el modelo teórico adoptado. La protección de la privacidad en línea es un tema de creciente importancia en la sociedad digital actual, y esta investigación contribuye significativamente a la comprensión de cómo se están abordando estas cuestiones en la actualidad y cómo podrían desarrollarse en el futuro.

Limitaciones de la Investigación

Ninguna investigación está exenta de limitaciones, y este estudio no es una excepción. Algunas de las limitaciones clave de nuestra investigación incluyen:

1. **Tamaño de la Muestra**: Nuestra muestra se centró en un conjunto específico de sitios web populares y, por lo tanto, no puede considerarse representativa de todas las plataformas en línea. Las prácticas de privacidad pueden variar ampliamente entre diferentes tipos de sitios web, y la inclusión de un conjunto más amplio de sitios podría haber proporcionado una imagen más completa.

2. **Cambios en las Políticas**: Las políticas de privacidad y seguridad en línea pueden cambiar con el tiempo. Aquí nos basamos en un análisis en un momento específico, y no abordamos posibles cambios posteriores en las políticas de privacidad de los sitios web analizados.

3. **Naturaleza Dinámica de la Web**: La web es un entorno dinámico, y la privacidad en línea es un tema en constante evolución. Si bien proporcionamos

una instantánea en el tiempo, no examinamos cómo las prácticas de privacidad pueden cambiar en respuesta a amenazas emergentes o cambios regulatorios.

4. **Variables No Consideradas**: En nuestro análisis, nos centramos en la capacidad de los sitios para permitir o deshabilitar cookies, el uso de JavaScript y el acceso a través de VPN y TOR. Sin embargo, existen otras variables importantes que pueden afectar la privacidad, como las políticas de retención de datos o el uso de métodos de cifrado adicionales.

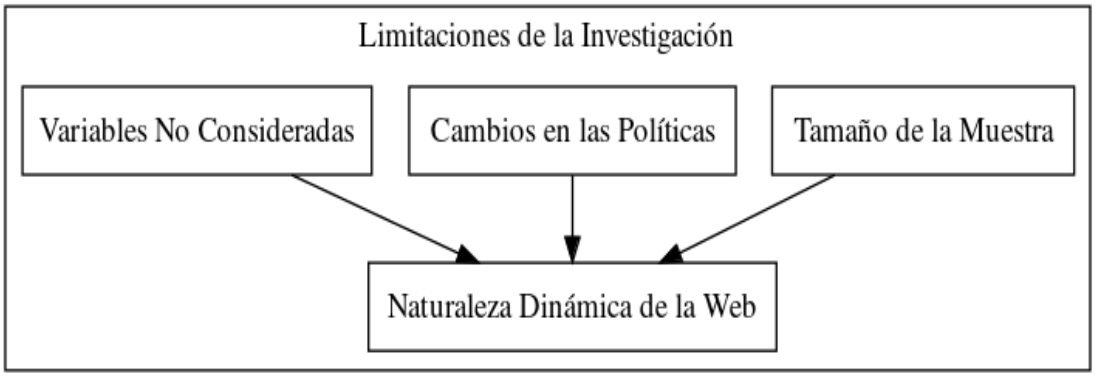

Figura 22: Limitaciones de la Investigación

Fortalezas de la Investigación

A pesar de las limitaciones, la investigación presenta varias fortalezas significativas:

1. **Enfoque Comparativo**: Nuestro enfoque comparativo permitió a los usuarios ver claramente cómo se desempeñan diferentes sitios web populares en términos de privacidad. Este enfoque ofrece una base sólida para tomar decisiones informadas sobre la elección de las plataformas en línea.

2. **Relevancia Práctica**: Al analizar sitios web ampliamente utilizados, abordamos una preocupación relevante para un amplio público. Los resultados y recomendaciones tienen aplicaciones prácticas para los usuarios que buscan proteger su privacidad en línea.

3. **Uso de Herramientas de Privacidad**: Exploramos cómo las VPN y la red TOR pueden mejorar la privacidad en línea, lo que proporciona a los usuarios alternativas prácticas para proteger su anonimato en línea.

4. **Modelo Teórico Sólido**: Adoptamos un modelo teórico sólido que consideró las complejas interacciones entre la recopilación de datos y la protección de la privacidad. Esto permitió una interpretación más profunda de nuestros hallazgos.

Figura 23: Fortalezas de la Investigación

Aunque esta investigación tiene limitaciones inherentes, las fortalezas del estudio incluyen su enfoque comparativo, su relevancia práctica y la consideración de herramientas de privacidad. Nuestros resultados ofrecen una valiosa visión de la privacidad en línea en el contexto de sitios web populares y proporcionan una base para futuras investigaciones y decisiones informadas por parte de los usuarios.

Conclusiones

Las conclusiones extraídas destacan varias cuestiones clave relacionadas con la privacidad en línea en los sitios web populares analizados:

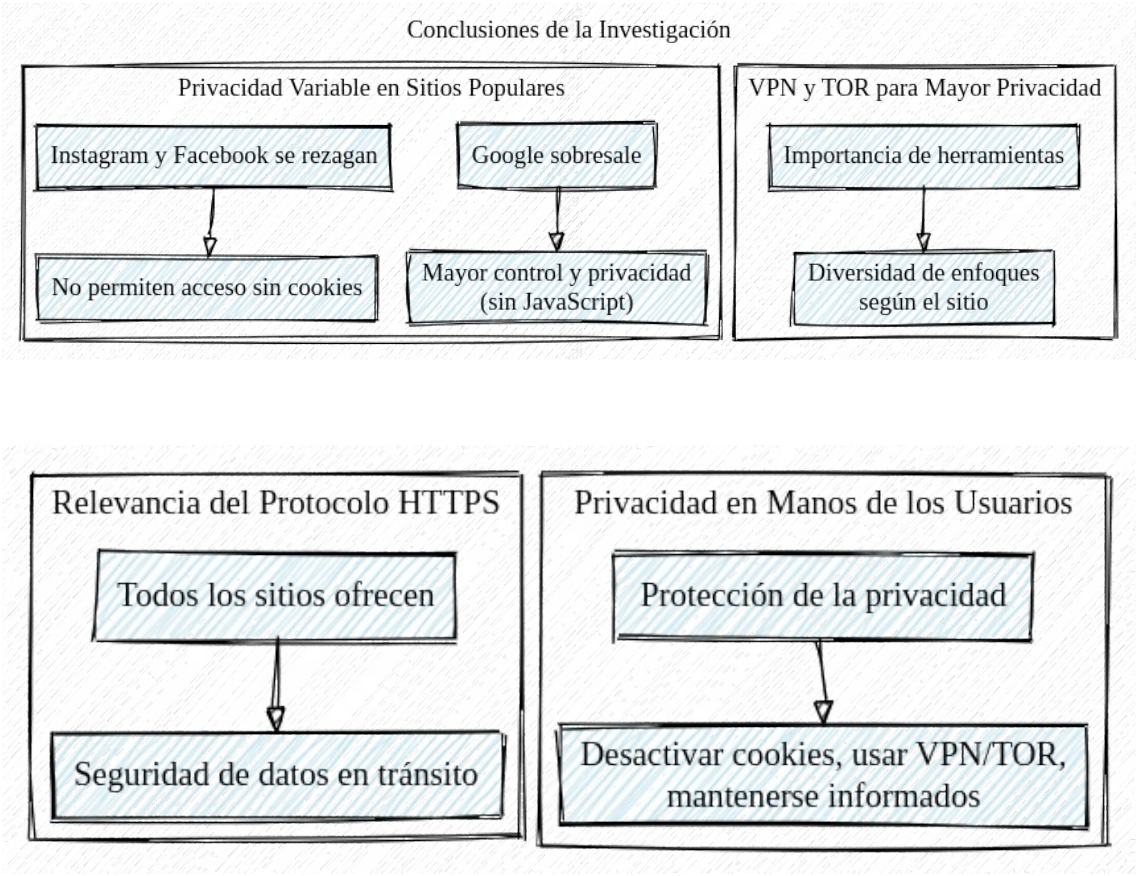

Figura 24: Conclusiones de la Investigación

1. **Privacidad Variable en Sitios Populares:** Nuestro análisis pone de manifiesto que la privacidad en línea no es un concepto homogéneo, sino que varía significativamente según el sitio web. Google sobresale al permitir un mayor control y privacidad al funcionar sin JavaScript, lo que reduce la exposición a amenazas de malware y mejora la experiencia del usuario. En contraste, Instagram y Facebook se rezagan al no permitir el acceso a sus plataformas sin cookies, lo que facilita el seguimiento de los usuarios.

2. **VPN y TOR para Mayor Privacidad:** La investigación resalta la importancia de herramientas como las VPN y la red TOR para aumentar la privacidad en línea. La posibilidad de utilizar estas herramientas varía según el sitio web, ya que algunos permiten su acceso, mientras que otros los bloquean, lo que subraya la diversidad de enfoques adoptados por diferentes plataformas.

3. **Relevancia del Protocolo HTTPS:** Todos los sitios web analizados ofrecen el protocolo HTTPS, lo que garantiza la seguridad de los datos en tránsito. Este hallazgo es reconfortante y demuestra que los sitios populares están comprometidos con la protección de la privacidad de los usuarios.

4. **Privacidad en Manos de los Usuarios:** Aquí se subraya que la protección de la privacidad en línea recae en última instancia en manos de los propios usuarios. Desactivar cookies, usar VPN o TOR y mantenerse informados sobre las políticas de privacidad son pasos fundamentales para disfrutar de una experiencia más segura en línea.

Recomendaciones

Basándonos en los resultados, hemos desarrollado una serie de recomendaciones que apuntan a mejorar la privacidad en línea y brindar a los usuarios un mayor control sobre sus datos personales. Estas recomendaciones abarcan diversas áreas y aspectos de la seguridad en línea, y están diseñadas para promover una experiencia más segura y protegida en un entorno digital en constante evolución:

1. **Educación en Privacidad**: La educación en privacidad se presenta como una de las recomendaciones más fundamentales. Los usuarios deben dedicar tiempo a familiarizarse con las prácticas de privacidad de los sitios web que utilizan. Esto implica entender cómo funcionan las cookies, aprender a desactivarlas si es necesario y habilitar protocolos de seguridad, como HTTPS/TLS. La educación en privacidad es esencial para fortalecer a los usuarios y ayudarles a tomar decisiones más informadas sobre su seguridad en línea.

2. **Uso de VPN y TOR**: Recomendamos que los usuarios consideren el uso de una VPN (Red Privada Virtual) o la red TOR para aumentar su privacidad al navegar por la web, especialmente en situaciones donde deseen mantener su anonimato. Estas herramientas permiten ocultar la dirección IP del usuario y enmascarar su ubicación, lo que es valioso para preservar la privacidad. Sin embargo, es importante tener en cuenta que no todos los sitios permiten el acceso a través de VPN o TOR, por lo que se debe verificar la compatibilidad de cada plataforma.

3. **Políticas de Privacidad Transparentes**: Exhortamos a los sitios web a proporcionar políticas de privacidad transparentes y fácilmente accesibles para los usuarios. Estas políticas deben ser comprensibles y detalladas, explicando cómo se recopilan, utilizan y protegen los datos del usuario. La transparencia en las políticas de privacidad permite a los usuarios tomar decisiones más informadas sobre cómo desean gestionar su información personal en línea.

4. **Configuración de Privacidad Personalizada**: Los sitios web deben brindar a los usuarios la posibilidad de personalizar su configuración de privacidad. Esto incluye permitir a los usuarios desactivar cookies o ajustar sus preferencias de privacidad de acuerdo con sus necesidades y preferencias individuales. Cuanto más control tengan los usuarios sobre su privacidad, mejor podrán protegerse en línea.

5. **Actualización Continua de la Seguridad**: Los sitios web deben comprometerse con la seguridad en línea de manera continua. Esto implica mantenerse al día con las últimas prácticas y tecnologías de seguridad para garantizar la protección de los datos del usuario. Además, deben proporcionar actualizaciones regulares sobre su política de privacidad y seguridad.

6. **Colaboración entre Usuarios y Plataformas**: Fomentamos una colaboración activa entre los usuarios y las plataformas en línea. Los usuarios deben informar sobre posibles problemas de seguridad o privacidad que encuentren, y las plataformas deben responder de manera efectiva y resolver los problemas identificados. Esta colaboración puede contribuir a un entorno en línea más seguro para todos.

Estas recomendaciones se derivan directamente de los resultados de la investigación y se centran en facultar a los usuarios para que tomen un papel activo en la protección de su privacidad en línea. Además, instan a las plataformas en línea a adoptar políticas de privacidad más transparentes y a mantener un compromiso constante con la seguridad y la privacidad de los usuarios. En un mundo cada vez más digital, estas recomendaciones son esenciales para garantizar que la privacidad en línea sea una

prioridad y que los usuarios estén mejor preparados para enfrentar los desafíos de seguridad en la web.

Futuras Líneas de Investigación

En esto no solo se arroja luz sobre la situación actual de la privacidad en línea, sino que también plantea preguntas adicionales y abre nuevas oportunidades para futuras investigaciones en el campo de la seguridad en línea. Estas futuras líneas de investigación son esenciales para mantenerse al día con los desarrollos en constante evolución en el mundo digital y abordar las necesidades cambiantes de los usuarios:

1. **Evolución de las Prácticas de Privacidad**: La privacidad en línea es un campo en constante evolución. Dado que las políticas de privacidad y las prácticas de seguridad cambian con el tiempo, se necesita una investigación continua para comprender cómo evolucionan estas políticas y cómo afectan a los usuarios. Futuros estudios pueden analizar las tendencias en las políticas de privacidad y su impacto en la percepción y seguridad de la privacidad del usuario.

2. **Impacto de las Herramientas de Privacidad**: Aunque exploramos el uso de VPN y TOR para mejorar la privacidad en línea, existen áreas adicionales que requieren un estudio más profundo. Se pueden llevar a cabo investigaciones específicas para medir el impacto de estas herramientas en la protección de la privacidad de los usuarios. Esto incluiría evaluaciones de cuánto mejoran la

seguridad y la privacidad cuando se utilizan VPN y TOR en comparación con la navegación estándar.

3. **Políticas de Retención de Datos**: Un aspecto importante de la privacidad en línea es cómo se manejan y retienen los datos personales por parte de los sitios web y las plataformas en línea. Investigaciones futuras pueden enfocarse en explorar en profundidad las políticas de retención de datos de estos sitios y cómo impactan la privacidad del usuario. Esto incluye analizar qué datos se almacenan, durante cuánto tiempo y con qué fines.

4. **Seguridad de JavaScript**: Se ha revelado que JavaScript es una parte fundamental pero potencialmente vulnerable de la experiencia en línea. Futuras investigaciones pueden profundizar en cómo JavaScript puede representar una vulnerabilidad potencial y cómo los sitios web pueden adaptarse para permitir su desactivación sin comprometer la funcionalidad. Esto es especialmente relevante dada la importancia de JavaScript en la mayoría de los sitios web modernos y la necesidad de equilibrar la funcionalidad con la privacidad y seguridad del usuario.

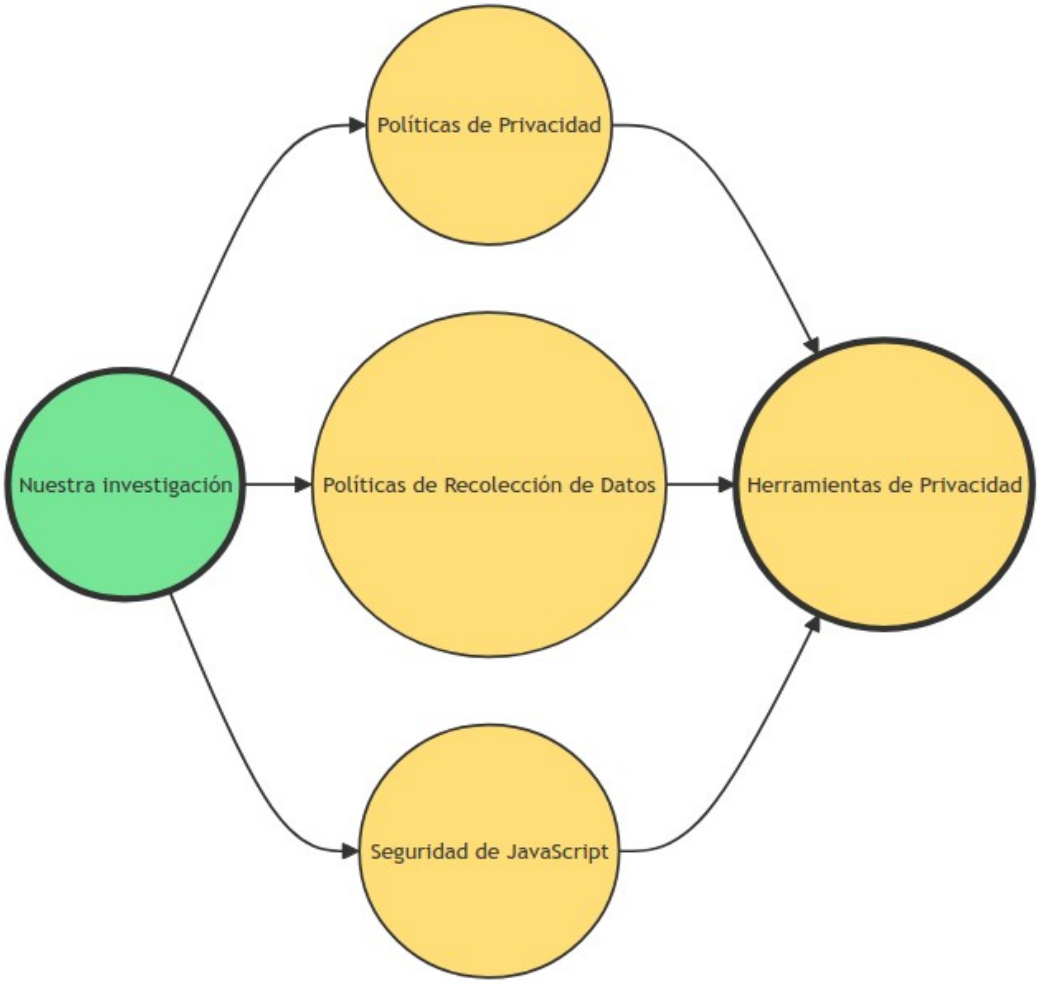

Figura 25: Posibles futuras líneas de investigación

Estas futuras líneas de investigación son cruciales para abordar los desafíos en constante cambio en el ámbito de la privacidad en línea y para mantener a los usuarios protegidos en un entorno digital en evolución. Además, contribuyen a la comprensión de las tendencias y prácticas emergentes en seguridad en línea y a la búsqueda de soluciones efectivas para la protección de la privacidad de los usuarios.

REFERENCIAS

La privacidad como derecho humano. (2020). Agencia de acceso a la información pública. Recuperado de https://www.argentina.gob.ar/noticias/la-privacidad-como-derecho-humano

El derecho a la privacidad en Argentina. (2017). Asociación por los Derechos Civiles (ADC) y Privacy International (PI). Recuperado de https://adc.org.ar/wp-content/uploads/2019/06/026-el-derecho-a-la-privacidad-en-argentina-03-2017.pdf

Ley Nro 24.430. (1994). Constitución de la Nación Argentina. Honorable Congreso de la Nación Argentina. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/804/norma.htm

Ley Nro 25.326. Ley de Protección de Datos Personales de la Constitución Argentina, 15 de abril de 2000. https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790/texto

Decreto 1160. (2010). Protección de datos personales [Modifícase el Anexo I del Decreto Nº 1558/01.]. Poder Ejecutivo Nacional. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/170000-174999/170508/norma.htm

Decreto 1558. (2001). Protección de datos personales [Apruébase la reglamentación de la Ley Nº 25.326. Principios generales relativos a la protección de datos. Derechos de los titulares de los datos. Usuarios y responsables de archivos, registros y bancos de datos. Control. Sanciones.]. Poder Ejecutivo Nacional. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70368/norma.htm

Sumer Elías, M. (2017). *Datos Personales y Privacidad.* Recuperado de http://www informaticalegal.com.ar/legislacion-informatica/datos-personales/

Declaración de privacidad y confidencialidad de la información de Mercado Libre.(2019) Mercado Libre. Recuperado de https://www.mercadolibre.com.ar/privacidad/declaracion-privacidad

Qué es la criptografía y cuáles son sus usos. (2021). Universidad Internacional de Valencia. Recuperado de https://www.universidadviu.com/es/actualidad/nuestros-expertos/que-es-la-criptografia-y-cuales-son-sus-usos

Lucena López, Manuel J. (2010)**.** *Criptografía y Seguridad en Computadores.* Universidad de Jaén.

Ansalas, Maria Eugenia. (1998) *Módulos para la transferencia segura y secreta de información*. Universidad Nacional de La Plata. Recuperado de https://repositoriosdigitales.mincyt.gob.ar/vufind/Record/SEDICI_92c798da4cfe36575ba809f42463a773

Diego Cordoba, Miguel Méndez-Garabetti (2017) *Criptografía Post Cuántica*. Universidad de Mendoza. Recuperado de http://sedici.unlp.edu.ar/handle/10915/62685

Gomez Vieites, Alvaro. (2014)**.** *Enciclopedia de la seguridad informática. 2da Edición***.** Editorial Alfaomega Ra-Ma

9 tipos de cookies que puedes encontrar. (2022). *KeepCoding.io* . Recuperado de https://keepcoding.io/blog/tipos-de-cookies/

Galeano Susana. (2022) *Cuales son las webs más visitadas del mundo*. Recuperado de https://marketing4ecommerce.net/cuales-son-las-webs-mas-visitadas-del-mundo-top/

La lista de las 15 páginas más visitadas en Argentina. (2022) BAE Negocios. Recuperado de https://www.baenegocios.com/sociedad/La-lista-de-las-15-paginas-mas-visitadas-en-Argentina-Anses-esta-en-el-top-10-20220510-0049.html

WhatIsTor. (2019) TOR Project. Recuperado de https://2019.www.torproject.org/docs/faq.html.en#WhatIsTor