UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE GUAYAQUIL

CARRERA DE COMPUTACIÓN

ANÁLISIS SOBRE EL IMPACTO DE LOS NAVEGADORES WEB A PARTIR DE LAS CIENCIAS DEL COMPORTAMIENTO

Trabajo de titulación previo a la obtención del
Título de Ingeniero en Ciencias de la Computación

AUTOR: JACINTO ANDRES PALMA NUÑEZ

TUTOR: JOE FRAND LLERENA IZQUIERDO

Guayaquil – Ecuador

2024

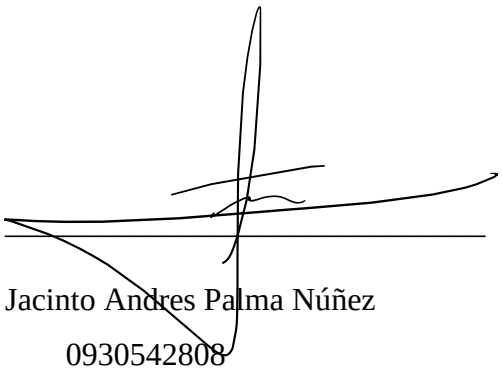
CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Yo, Jacinto Andres Palma Núñez con documento de identificación N°0930542808 manifiesto que:

Soy el autor y responsable del presente trabajo; y, autorizo a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Guayaquil, 3 de marzo del año 2024

Atentamente,



Jacinto Andres Palma Núñez
0930542808

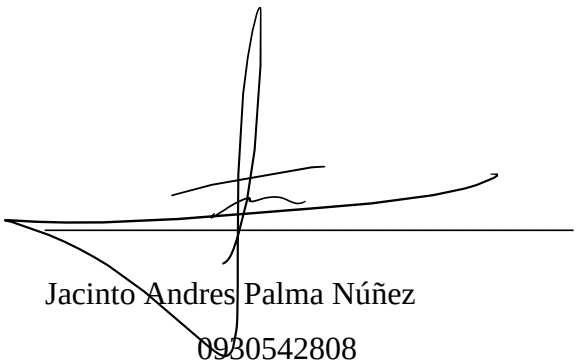
CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA

Yo, Jacinto Andres Palma Núñez con documento de identificación No. 0930542808, expreso mi voluntad y por medio del presente documento cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor(a) del Artículo Académico: "Análisis sobre el impacto de los navegadores web a partir de las ciencias del comportamiento", el cual ha sido desarrollado para optar por el título de: Ingeniero en Ciencias de la Computación, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribo este documento en el momento que hago la entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

Guayaquil, 3 de marzo del año 2024

Atentamente,



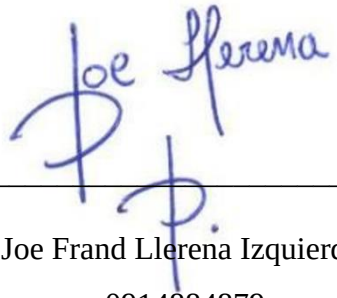
Jacinto Andres Palma Núñez
0930542808

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Joe Frand Llerena Izquierdo con documento de identificación N° 0914884879, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: Análisis sobre el impacto de los navegadores web a partir de las ciencias del comportamiento, realizado por Jacinto Andres Palma Núñez con documento de identificación N° 0930542808, obteniendo como resultado final el trabajo de titulación bajo la opción Artículo Académico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Guayaquil, 3 de marzo del año 2024

Atentamente,



Joe Frand Llerena Izquierdo
0914884879

DEDICATORIA

Dedico este trabajo a mi familia, a mis padres Lola Elizabeth Núñez Córdova y Jacinto Laurido Palma Proaño quienes siempre me han apoyado en mi trayectoria profesional con los medios para poder destacarme. Mis padres que fueron un ejemplo tanto como profesionales, como padres y como calidad de seres humanos. A mis hermanos María del Sol Palma Núñez y Michael Giuliano Palma Núñez, porque siempre me dieron buenos consejos, aportando ideas para poder mejorar mi forma de entender la ingeniería. Por último, a Natasha Palma Núñez porque fue una gran influencia para mí, me ayudó a decidirme por esta hermosa carrera en la cual me encuentro.

AGRADECIMIENTO

Agradezco a la Universidad Politécnica Salesiana por brindarme los medios para facilitar mi aprendizaje en esta carrera en la cual me encuentro, agradezco al docente Joe Llerena por ser mi tutor para esta investigación la cual su tema es muy relevante en esta época digital donde los usuarios necesitan conocer más sobre su privacidad y seguridad.

RESUMEN

Esta investigación se centra en el impacto de los navegadores web relacionado a la experiencia del usuario, de su privacidad, seguridad y el comportamiento que posee al interactuar con los navegadores web. Se abordan temas como la personalización, las funcionalidades de los navegadores web, la retención de clientes, los modelos de predicción, el uso de modelos cognitivos y los anuncios basados en modelos, se resalta además la evolución de los navegadores web y cómo han cambiado la forma en que los investigadores recopilan y analizan datos. Se discute el uso de extensiones de navegador para personalizar la experiencia del usuario, sobre cómo estas pueden afectar la privacidad y la seguridad de los usuarios, además sobre cómo los modelos cognitivos en conjunto con los anuncios basados en modelos pueden mejorar la comprensión de los usuarios sobre la información en línea e incluso llegar a controlar su estado emocional durante la navegación web. También se exploran los posibles problemas emocionales y de comportamiento que pueden surgir del uso excesivo de los navegadores web, las medidas de seguridad implementadas por los navegadores, de cómo se pueden emplear las ciencias del comportamiento para fomentar el uso responsable de los navegadores web. La metodología empleada para esta investigación es del tipo empírico-analítico de corte cuantitativo cuasiexperimental, utilizando la técnica de revisión de literatura mediante el uso del flujo de datos PRISMA. Se propone la recopilación y análisis de datos a través de encuestas para consultar a los usuarios de navegadores web sobre su experiencia, conocimientos, y la comprensión de su privacidad y seguridad.

Palabras claves: Navegadores web, experiencia de usuario, privacidad, seguridad, Modelos cognitivos.

ABSTRACT

This research focuses on the impact of web browsers related to user experience, privacy, security, and behavior when interacting with web browsers. Topics such as personalization, web browser functionalities, customer retention, prediction models, the use of cognitive models and model-based ads are addressed, and the evolution of web browsers and how they have changed the way researchers collect and analyze data. We discuss the use of browser extensions to personalize the user experience, how they can impact user privacy and security, and how cognitive models in conjunction with model-based ads can improve understanding of the users. about online information and even manage to control your emotional state during web browsing. Also explored are potential emotional and behavioral problems that may arise from excessive use of web browsers, security measures implemented by browsers, and how behavioral sciences can be used to encourage responsible use of web browsers. The methodology used for this research is of the empirical-analytical quasi-experimental quantitative type, using the literature review technique using the PRISMA data flow. Data collection and analysis through surveys is proposed to query web browser users about their experience, knowledge, and understanding of their privacy and security.

Keywords: Web browsers, user experience, privacy, security, cognitive models.

ÍNDICE DE CONTENIDO

1. INTRODUCCIÓN

Los adelantos tecnológicos conllevan muchos beneficios, sin embargo, estos poseen sus riesgos y desafíos (de la Nube Toral Sarmiento et al., 2018; López-Chila et al., 2024). Para los usuarios de los navegadores web es importante que sus experiencias sean las más óptimas, por ejemplo los navegadores poseen pequeños programas los cuales permiten personalizar las mismas agregando más funcionalidades aprendiendo de cada interacción, llamados "extensiones" las cuales según (X. Wang et al., 2022), "plantea preocupaciones de seguridad y privacidad, ya que a las extensiones se les otorgan capacidades privilegiadas e inherentemente tienen acceso a datos confidenciales del usuario" (Alvarado Zambrano, 2021; Pérez González, 2021; Vera Navas, 2021). Estos datos en manos de atacantes pueden ser usados para realizar ataques informáticos avanzados como el de secuestro de sesión, para espionaje, ataques de denegación de servicios, entre los más comunes (Recalde Monar, 2021; Toala Indio, 2021).

Los usuarios o clientes son la pieza más importante para las empresas, estas actúan como curadores al momento de presentar la información a cada usuario y retener su atención, según (X. Wu et al., 2022), "centran sus esfuerzos de marketing en la retención de clientes en lugar de en la adquisición de clientes.". Existen investigadores especializados en el entendimiento y la mejora continua de los modelos de predicción, como por ejemplo el de "abandono" en las aplicaciones de los navegadores los cuales almacenan y analizan datos para, "obtener una comprensión más completa y detallada de los patrones y, al mismo tiempo, mejorar el rendimiento del algoritmo" (X. Wu et al., 2022). También son muy usados los motores de predicción y captación previa (Joo et al., 2021) desarrolló WebPrefetcher, "un novedoso esquema de captación previa web que deduce la intención y el contexto del usuario en función de los eventos de interacción que ocurren durante la navegación web", los cuales afectan positivamente la calidad de la experiencia (Atiaja Balseca, 2023). También según (Singh & Meenu, 2017) el uso de Minería de uso web se utiliza para recuperar información de las páginas web almacenadas en el servidor de registro web, ayudando a evaluar la eficacia de un sitio web y es útil para lograr el éxito en la campaña de marketing (Cristellot Paredes et al., 2024; Cueva Estrada & Sánchez-Bayón, 2024; Lindao Palma et al., 2023).

Desde la perspectiva de las ciencias del comportamiento, (Morita et al., 2022) también utiliza modelos cognitivos, anuncios basados en modelos los cuales amplían el modelo de memoria para poder mejorar la comprensión de los usuarios sobre la información y poder regular su

estado emocional durante la navegación web donde también se busca prevenir los comportamientos negativos en línea. El interés de este trabajo de investigación es realizar un mapeo sistemático de artículos más relevantes de diversas bases de datos de referencias bibliográficas, evaluando su relevancia, y asegurando que la revisión de los artículos sea bastante amplia.

2. REVISIÓN DE LITERATURA

2.1. Evolución de los navegadores web, extensiones y herramientas

Antes de la creación de los navegadores web, el tipo de investigación que se realizaba en el área de ciencias del comportamiento se realizaba por métodos tradicionales como son: la observación directa, las entrevistas y las encuestas. Por lo que los especialistas necesitaban una interacción frente a frente y el análisis manual de los datos obtenidos por sus sujetos de estudio.

La innovación generada por la creación de los navegadores web y su uso para la navegación en internet tuvo como consecuencia un cambio drástico, ahora los investigadores especialistas pueden recopilar una mayor cantidad de datos a gran escala, se aborda también que el uso de encuestas web es muy útil porque: “Las tecnologías de Internet se utilizan activamente para realizar encuestas y estudios web en el campo de la psicología porque suelen ser más baratas, rápidas y fáciles de realizar que en otros modos” (Nikulchev et al., 2021) y según (Henninger et al., 2022),ofrece una investigación más adaptable y asequible que, a su vez, conduce a descubrimientos más robustos.

Realizar experimentos en línea puede ser un desafío debido a las barreras técnicas y los problemas potenciales con los navegadores web. Como menciona (A. L. Anwyl-Irvine et al., 2020, p.1), para asegurar la precisión y fiabilidad de las pruebas, los investigadores necesitan dominar lenguajes de programación como JavaScript. Algunos datos en consideración que pueden ser obtenidos en estas pruebas son: retrasos en el tiempo de reacción (RT), una precisión, retraso visual en fotogramas, retraso auditivo y variación de combinaciones. Existen nuevas herramientas que han surgido como el uso de lab.js el cual es un creador de estudios en línea, abierto y gratuito que permite ejecutar experimentos basados en la web de una manera flexible y personalizable con una interfaz amigable para el usuario, como, por ejemplo: centrar la atención visual y se desea medir el tiempo de reacción de los participantes para identificar un objetivo en una matriz de letras.

Además (Krajbich & Yang, 2021) afirma en su investigación una descripción del procedimiento estándar de seguimiento ocular en el laboratorio físico puede ser relevante para entender cómo se estudia el comportamiento del usuario en relación con la interacción con la interfaz de un navegador web, además que el proceso de calibración y validación del seguimiento ocular puede proporcionar información sobre cómo se mide la atención del usuario y cómo se alinea con la ubicación de la mirada en la pantalla utilizando WebGazer, un set de herramientas que proporciona JavaScript creada para monitorear los movimientos oculares de las personas mientras están en Internet, que los sujetos entiendan que no están siendo grabados por lo tanto, no hay violaciones de privacidad ya que las imágenes y el video no salen de la computadora del sujeto.

Con el masivo uso de los navegadores web se facilitó algunas formas de personalización de experiencia con el navegador web como lo son el uso de las "extensiones" para poder brindar a los usuarios el mejor servicio y experiencia, pero la credibilidad de los programas de extensión que son maliciosos se ha convertido en uno de los nuevos retos que enfrenta la era del internet. En su estudio (K. Wang & Yu, 2021) propone un método para adquirir automáticamente el comportamiento de una extensión durante la fase de ejecución, simulaba comportamientos del usuario para activar varios módulos de procesamiento de eventos de la extensión probada, permitiendo que la extensión muestre más comportamientos y acciones. (Sam & Ancy Jenifer., 2023) propuso un marco para evaluar la seguridad de las extensiones del navegador muy completo, donde incluye aspectos como los permisos, el control de acceso, la criptografía, la calidad del código, las actualizaciones y las bibliotecas de terceros puede proporcionar una evaluación integral de la seguridad de una extensión.

Las extensiones de navegador pueden ser utilizadas para la auto-regulación de dispositivos digitales, se trata de extensiones obtenidas según (Lyngs et al., 2022) "… tiendas Google Play, Chrome Web y Apple App", las cuales pueden aportar a la investigación de interacción humano-maquina sobre patrones de diseño para auto regularización digital. Es decir, de cómo los usuarios pueden controlar o gestionar su propio uso de la tecnología digital, por ejemplo, funciones para bloquear distracciones.

Algunas extensiones se usan para estudiar el comportamiento de clientes en plataformas digitales E-Commerce, (Fuchs et al., 2022) desarrolló una extensión del navegador web Chrome para un supermercado en línea real y evaluó el efecto de la misma intervención en la etiqueta

digital de los alimentos (es decir, la visualización del Nutri-Score junto a los productos visibles) sobre la calidad nutricional de las compras semanales de los individuos con el fin de mejorar el valor nutricional de los alimentos que son preferidos por los consumidores.

Sin embargo, a pesar de que las extensiones web comunican sus prácticas de datos a los usuarios, se ha ignorado la no concordancia significativa entre las prácticas de datos verdaderas y los avisos de privacidad que publican, es decir, aunque los datos se recojan con intenciones inofensivas, si estos actos no se revelan, una extensión podría infringir su política de privacidad (Bui et al., 2023). Por ejemplo, si una extensión almacena datos de ubicación y pulsaciones de teclas para análisis y depuración, pero declara que no usa datos del usuario, entonces estaría incumpliendo su propia política de privacidad.

2.2. Seguridad y privacidad en la web, el papel de los navegadores

La configuración de los encabezados HTTP y su procesamiento por los navegadores afectan la seguridad y privacidad del usuario. Los especialistas en seguridad y desarrolladores crean mecanismos de aislamiento para mejorar la seguridad del navegador. Los navegadores comparan los encabezados HTTP con las especificaciones del protocolo, políticas de seguridad locales, configuraciones del usuario para garantizar una comunicación segura y eficiente. Según un estudio de (Siewert et al., 2022) se proporciona una herramienta para probar automáticamente el comportamiento del navegador al recibir encabezados HTTP relevantes para la seguridad, también analiza los sitios web Top 1M de Tranco en busca de configuraciones erróneas comunes y discute el impacto potencial de estas configuraciones en la seguridad del procesamiento de encabezados HTTP, además los navegadores Chrome, Safari y Firefox exhiben comportamientos distintos cuando el encabezado contiene un carácter no válido según la definición del ABNF.

Otro componente crítico para mantener la seguridad y privacidad en la web es el que (Berbecaru & Lioy, 2023) resalta, una debilidad en algunos navegadores ya que estos tienen la capacidad de evitar la verificación de revocación de certificados si los datos necesarios no están al alcance, optando por métodos alternativos si es requerido. La Infraestructura de Clave Pública, que confiere un alto grado de autoridad a diversas partes, impone limitaciones mínimas sobre los certificados. En su trabajo se implementaron salvaguardas para proteger contra ataques derivados de una incorrecta comprobación de certificados, en particular aquellos de alta seguridad. Es decir, las elecciones de diseño y las políticas de los navegadores pueden tener un

impacto en cómo los usuarios se comportan. Por ejemplo, la forma en que un navegador web administra las advertencias de seguridad o muestra los detalles del certificado puede influir en la percepción y respuesta de los usuarios ante estas situaciones.

Al navegador por la web, los usuarios deben ser cautelosos al interactuar con ciertos elementos en línea que podrían ser riesgoso, en su estudio (M.-H. Wu et al., 2022), propone un mecanismo de defensa contra la descarga de malware, lo que podría influir en las decisiones de los usuarios al navegar en línea mediante el navegador de Firefox con el uso de un complemento. Sugiere que los usuarios deben ser cautelosos al abrir archivos adjuntos de correo electrónico desconocidos, descargar software de fuentes no confiables y visitar sitios web no seguros. En su estudio (Zhang et al., 2024) afirma que, también existen incidentes de ataques de inyección en navegadores web, diseñados para robar información delicada del usuario como contraseñas y detalles de tarjetas de crédito, menciona que los desarrolladores de navegadores como Google Chrome y Mozilla Firefox son los han tomado medidas activas para combatir este tipo de amenazas.

2.3. Comportamientos del usuario en navegadores web, herramientas para su medición

Los investigadores de ciencias del comportamiento también poseen herramientas para realizar pruebas psicologías en línea (Gómez-Bayona et al., 2020; Ortega-Vivanco, 2020). Aunque tradicionalmente según (Shevchenko, 2022) : "... crear experimentos en línea requería una enorme experiencia técnica, pero se ha vuelto más fácil gracias a una variedad de recursos basados en la web diseñados específicamente para psicólogos cognitivos" (p. ej., jsPsych, PsychoPy, lab.js, (Gómez-Bayona et al., 2020)), como consecuencia se necesita que los especialistas se encuentren capacitados para realizar los experimentos usando los navegadores, vincular estas tecnologías es técnicamente difícil, requiere mucho tiempo y es costoso, hasta hace poco, quienes tenían los recursos para superar estas barreras la hacían (y analizaban) (Anwyl-Irvine et al., 2020; Cárdenas Rebelo & Orozco-Toro, 2020; Ortegón Cortázar, 2023). Además, menciona que los investigadores poseen una variedad de herramientas a su disposición para la creación de experimentos, más allá de la flexibilidad que tienen los participantes (Guiñez-Cabrera et al., 2020; París, 2020).

Estas herramientas pueden ser desde bibliotecas de programación como jsPsych hasta constructores de experimentos visuales como Gorilla Experiment Builder. Cada una de estas

opciones tiene características únicas en términos de manejo del tiempo, presentación de estímulos visuales y auditivos, además de recolección de respuestas.

Existen además herramientas automatizadas que utilizan inteligencia artificial para dar seguimiento de la salud mental de los usuarios en la web es la que propone (Liu et al., 2022), aiMSE un sistema en línea basado en IA que simplifica la autoinspección de la salud mental, únicamente empleando una cámara y un micrófono, disponible para cualquier individuo con un dispositivo digital. Para especialistas en marketing digital, la librería FingerprintJS fue diseñada ampliar el conjunto de características para recopilar atributos del navegador del usuario, mejorando la eficiencia ya que se manejaba con registros de auditoría estándar como conjunto de datos principal para un algoritmo (Iskhakov et al., 2023), así pudiendo detectar anomalías en el comportamiento de los usuarios en las plataformas web.

Entre las propuestas para medir el comportamiento (Farid, 2023) explora la idea de emplear la biometría ligera y las circunstancias laborales contextuales para detectar los estados de ánimo de los usuarios. Esta metodología podría emplearse para añadir un nivel adicional de protección siendo capaz de prevenir y reaccionar a conductas que podrían ser riesgosas antes de que sucedan eventos de ciberseguridad empleando navegadores web ya que pueden influir en cómo los usuarios responden a las notificaciones, recomendaciones y contenido personalizado (Ubaidah et al., 2023). A partir de las ciencias del comportamiento, la forma en que los usuarios interactúan con los navegadores web es influenciada por su percepción de seguridad y privacidad. Si son conscientes de que un navegador web tiene un IDS robusto que puede detectar y prevenir actividades sospechosas como afirma (Shao et al., 2021) en su estudio, es probable que se sientan más seguros y confiados al usar dicho navegador.

2.4. Educación en línea y ciberseguridad, estrategias para mejorar la enseñanza

En su estudio (Xu et al., 2023) complementa esta discusión cómo las estrategias de participación de los estudiantes pueden mejorar los resultados del aprendizaje en un entorno en línea (Ayala-Carabajo & Llerena-Izquierdo, 2023).

Por otro lado, en su estudio (Nigam et al., 2021) también menciona una nueva metodología de un sistema de monitoreo en línea que se compone de una cámara web para registrar al estudiante durante el examen y un bloqueo que impida abrir otras pestañas en los navegadores por medio del diseño de un Sistema de Supervisión basado en Inteligencia Artificial (AIPS), considerando

factores como la discreción, la compatibilidad, la privacidad y la facilidad de uso. Dicho sistema considera parámetros psicológicos y están ganando popularidad, debido a su integración con los navegadores web que facilitan el acceso a recursos de aprendizaje y servicios de supervisión.

Además (Matos et al., 2023) sugiere un marco para mejorar la calidad de los informes de errores llamada Watson, herramienta clave para optimizar la usabilidad, que ofrece a los desarrolladores una perspectiva integral de la interacción de los usuarios con su aplicación web facilitando la detección y corrección de problemas de usabilidad, mejorando considerablemente la experiencia del usuario (Isanoa-Sinche & Llerena-Izquierdo, 2023). Otro aspecto que afecta a la usabilidad es el que (Parlakkiliç, 2022) resalta, la sencillez es el aspecto más valorado en la usabilidad de un diseño adaptable, lo cual puede afectar la elección de los usuarios de seguir empleando una web o app específica. Se descubrió además que el diseño adaptable justifica el 74,7% de la variación en la eficacia entre los aspectos de usabilidad, influyendo considerablemente en las decisiones de los usuarios (Pilapaxi-Cunalata & Llerena-Izquierdo, 2023).

Los factores como usabilidad y experiencia de usuario en navegadores web pueden también ser afectados por el criptojacking ya que deterioran la experiencia del usuario al disminuir la velocidad del navegador y usar recursos del sistema sin permiso. Por lo que como menciona (Hong et al., 2022), en su estudio ofrece soluciones eficaces para identificar y evitar el criptojacking, como CIRCUIT, pueden ayudar a optimizar la usabilidad y experiencia del usuario en los navegadores web. (Fonseka et al., 2023) da a conocer en su estudio sobre cómo los ataques de tabnabbing explotan el comportamiento de los usuarios en los navegadores web, se basan en la suposición de que los usuarios no notarán el cambio en una pestaña que no están viendo activamente.

También existen los comandos ejecutados por el navegador en segundo plano llamados Service Workers un script que se mantiene en ejecución, aunque una página esté cerrada, según (Subramani et al., 2022) afirma que, a pesar de las medidas de seguridad, pueden ser explotados para fines maliciosos como ataques DDoS, minería de criptomonedas, y phishing a través de publicidad dañina, propone la introducción de nuevas políticas para los navegadores web que utilizan el código fuente de Chromium, como se señala en la investigación, Opera y Edge. Estos navegadores, incluyendo Chrome, son vulnerables a determinados ataques y los programadores están debatiendo posibles soluciones. En su estudio (Jampen et al., 2020) menciona la

importancia de capacitación antiphishing ya que puede cambiar el comportamiento de los usuarios con respecto a los correos electrónicos benignos (Rosero Tejada, 2021).

2.5. La influencia de los anunciantes en las redes sociales

Dado los avances en las formas de investigación que ahora poseen los especialistas del área de ciencias del comportamiento y el creciente uso de Internet los usuarios pueden acceder a contenidos disponibles de forma gratuita e inmediata por los editores. Lo que provoca que estos moneticen a su audiencia mediante la publicidad. Según (Alyoubi & Alotaibi, 2021, p.1), en las redes sociales más relevantes actualmente como Instagram, se suben alrededor de 50.000 fotos, mientras que en Twitter se generan 473.400 tweets. Además, YouTube atrae a 4,3 millones de espectadores para ver videos. La mayoría de estas interacciones son relevantes para la marca de cada empresa (Rigchc Mero, 2022; Vera Navas, 2021). Lo que sugiere que existen muchas oportunidades para una publicidad revelada dirigida (Gonzalez Marin et al., 2024; Sumba Nacipucha et al., 2024).

Según (Alyoubi & Alotaibi, 2021, p.1), la omnipresencia de las redes sociales ha proporcionado a los investigadores un vasto acceso a datos para análisis (Bauer et al., 2023; Veletsianos et al., 2013). Estos datos son una fuente valiosa para entender el comportamiento humano, la formación de redes y los patrones de flujo de información. El autor aplico un algoritmo de agrupación de dosel ya que pudo manejar eficientemente gran cantidad de conjuntos de datos, como los generados por la publicidad en línea y es capaz de dividir estos datos en grupos superpuestos basados en criterios concretos, permitiendo una segmentación más precisa de los usuarios, resaltando la importancia de identificar las mejores oportunidades para mostrar publicidad en línea con el objetivo de mostrar un anuncio publicitario a un consumidor que se espera que realice una acción preferida, como por ejemplo: el registrarse para recibir un boletín informativo o incluso llegar a comprar un producto.

También existen formas de fraude con la publicidad que pueden presentarse en las empresas como menciona (Gabryel et al., 2022) el fraude de tráfico es un delito en línea común que implica inflar fraudulentamente los ingresos publicitarios mediante la generación automática de vistas de página, clics o la finalización de formularios en línea (Pérez González, 2021). Esto proporciona como consecuencia ganancias financieras a los estafadores y genera pérdidas para las empresas competidoras.

La mayoría de los usuarios de los navegadores web no conoce en su totalidad es que los que pagan por el espacio o tiempo publicitario también llamados “anunciantes” pueden ser empresas que compran exposición en línea. (Gabryel et al., 2022, p.2), los editores ofrecen servicios de red a los usuarios, proporcionando recursos para el tráfico publicitario. Este tráfico se genera cuando un usuario visita sus sitios, creando la oportunidad de mostrar anuncios. Los anunciantes compran este tráfico para entregar sus anuncios a los visitantes de un sitio web. Además, el uso corporativo de los datos personales según (Kiviat, 2021) actualmente, las corporaciones tienen más acceso que nunca a datos sobre individuos, gracias al apogeo de la información digital y a los intermediarios que la hacen circular. Las empresas usan estos datos para clasificar a los consumidores y decidir de manera más rentable a quién ofrecer qué (Alcívar-Cruz & Llerena-Izquierdo, 2023; Peñafiel Espinoza & Lopez Chila, 2012).

Los “Anunciantes” poseen varias técnicas tecnológicas como el uso de cookies para poder identificar al público objetivo en los sitios web y crear un historial de navegación. De acuerdo con (Mingsheng et al., 2022) las cookies poseen una debilidad son susceptibles a ataques de programa maligno y suplantación de identidad, ya que los atacantes pueden usar cookies como tokens de autenticación o suplantar a usuarios legítimos en el servidor (Norta et al., 2018; Z. Wu & Weaver, 2007). También se pueden crear perfiles detallados de usuarios para poder personalizar todavía más los anuncios para incrementar la probabilidad de interacción. Estos perfiles según (Maliki et al., 2021) son la recopilación y organización de datos para describir a un usuario y su historial en un sistema interactivo, en su estudio describe la construcción de un perfil de seguridad de un usuario analizando datos de navegación y elementos de ciudadanía digital para clasificar utilizando SVM, concluye que el perfil de comportamiento de seguridad del usuario puede ayudar a entender la conciencia de seguridad en Internet del usuario de acuerdo con las prácticas de ciudadanía digital.

Por otro lado (Hovorushchenko et al., 2022) concluye que la identificación del usuario en Internet permite formar su retrato informativo. El reconocimiento en línea del usuario ayuda a crear su perfil informativo, una tarea crucial para la mejora de la entrega de información y permite establecer su imagen digital. La interacción en línea revela información de los usuarios, facilitando el perfilado para publicidad y seguimiento, el seguimiento puede ser activo con cookies o pasivo. Sin embargo, la eliminación de cookies por parte de usuarios preocupados por su privacidad ha llevado al desarrollo de huellas digitales.

Debido a la creciente conciencia sobre la privacidad y el manejo de las cookies, llevo a la introducción del RGPD, lo que hizo que muchos sitios web dejaran de rastrear a las personas a través de cookies. (Mudassar et al., 2023), otra herramienta para detectar las huellas digitales de los navegadores web es la que (Zhao, 2023) sugiere FProbe, dicha herramienta utiliza un método estático y consciente del contexto para examinar los flujos de datos de los atributos del navegador en JavaScript siendo capaz de identificar los atributos del navegador, analizar sus flujos de datos, calcular la unión de estos flujos y clasificarlos para detectar las huellas digitales del navegador. También (Rodriguez-Garcia et al., 2021) aborda la importancia de salvaguardar de manera anticipada la privacidad de los usuarios en relación con los motores de búsqueda. Analiza la posibilidad de que los perfiles de usuario sean empleados para la segmentación conductual o incluso compartidos con terceros, genera inquietudes en términos de privacidad y seguridad.

Es crucial interpretar correctamente la información para evitar datos imprecisos o no confiables. Los estudiantes deben aprender a buscar información en la Web de manera efectiva. Ayudando a que se puedan tomar medidas para proteger su privacidad en línea, los especialistas del área de las ciencias del comportamiento desempeñan un papel muy importante en la forma de como educar a los usuarios que interactúan con los navegadores web y recopilar esos datos para desarrollar estrategias de educación para concientizar a los mismos.

3. METODOLOGÍA

La metodología de este trabajo es empírico-analítico de corte cuantitativo cuasiexperimental. Se utiliza la técnica de revisión de literatura mediante el uso del flujo de datos PRISMA (Preferred Reporting Items for Systematic Reviews and Meta Analyses).

Se identifican y evalúan los artículos más relevantes del tema de ciencias del comportamiento y su relación con los navegadores web, empleando el estándar PRISMA el cual ayudara realizar una revisión sistemática de la literatura en diversas bases de datos de referencias bibliográficas, evaluando su relevancia, y asegurando que la revisión de los artículos fue bastante amplia.

Mediante una recopilación y análisis de datos empleando el uso de encuestas para consultar a 32 profesionales del área de TI, usuarios de navegadores web relacionando su experiencia, conocimientos, la comprensión de su privacidad y seguridad.

3.1. Métodos y técnicas de recopilación de datos empleadas

A continuación, se procede a especificar las preguntas de esta investigación ya que los objetivos planteados en este proyecto de investigación son de naturaleza exploratoria, descriptiva y evaluativa, respectivamente, hacen posible la identificación de diversos aspectos del impacto de los navegadores web que pueden ser analizados, por lo que se eligió las preguntas de investigación debido a que permiten una exploración del tema de esta investigación más amplia y flexible. Las cinco preguntas de investigación propuestas son las siguientes (ver Tabla 1):

Tabla 1. Preguntas de Investigación

Pregunta de investigación	Descripción
Q1	¿Cómo mejorar la seguridad, usabilidad y retención de clientes en navegadores web?
Q2	¿Qué problemas de la seguridad, accesibilidad y experiencia de calidad se presentan en la navegación web?
Q3	¿Cómo superar las limitaciones en ciberseguridad y usabilidad web?
Q4	¿Qué propuestas pueden mejorar la seguridad, privacidad y usabilidad en la web?
Q5	¿Qué soluciones se pueden implementar para mejorar la seguridad, privacidad y experiencia del usuario en la web?

Además de las preguntas de investigación antes descritas se elaboraron preguntas de investigación para la elaboración de una encuesta a profesionales del área de TI para evaluar la experiencia/conocimiento de cómo afecta el impacto de los navegadores web a partir de las ciencias del comportamiento, las 8 preguntas fueron las que se describen a continuación (ver Tabla 2):

Tabla 2. Preguntas estructuradas para la aplicación de la técnica de la encuesta

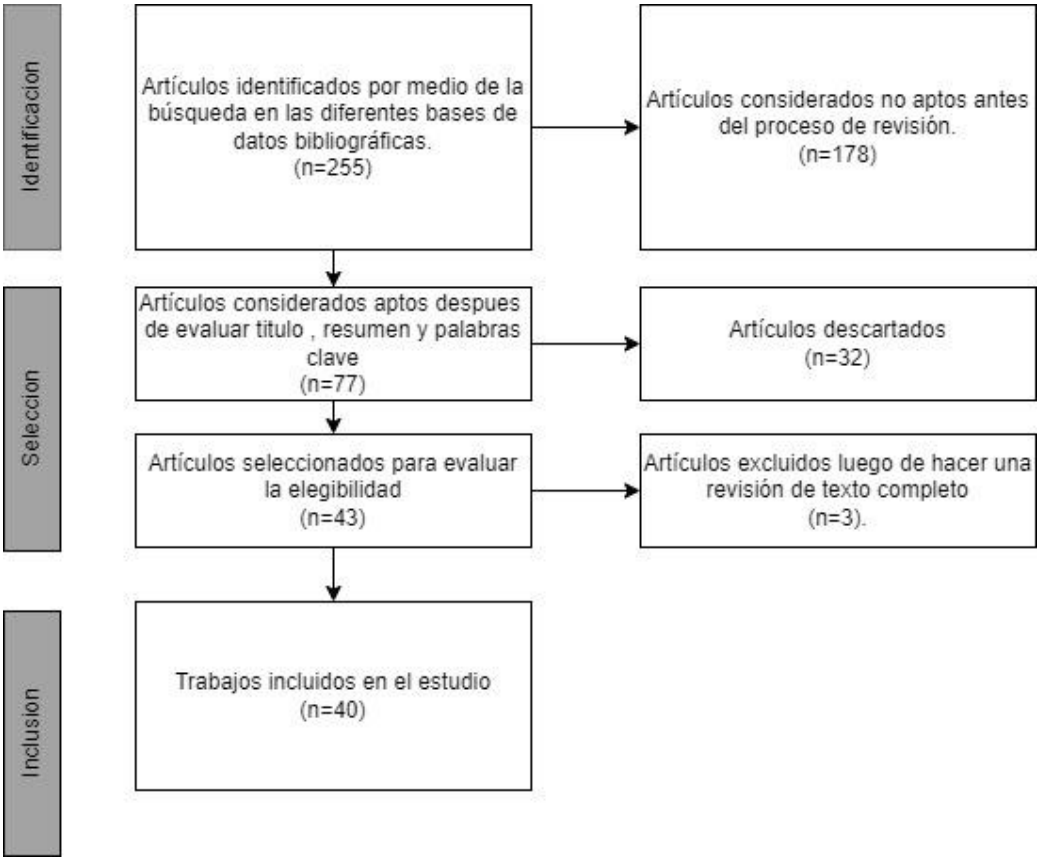
Pregunta de la encuesta	Descripción
Pregunta 1	¿Cómo calificaría su experiencia general con el navegador web que utiliza con más frecuencia?
Pregunta 2	¿Cuánto conocimiento tiene sobre las configuraciones de privacidad y seguridad de su navegador web? ¿Ha cambiado alguna vez estas configuraciones?
Pregunta 3	¿Utiliza extensiones de navegador para personalizar su experiencia? Si es así, ¿Cómo cree que estas extensiones afectan su privacidad y seguridad en línea?
Pregunta 4	¿Ha notado que los anuncios que ve en línea están personalizados según su comportamiento de navegación? ¿Cómo se siente al respecto?
Pregunta 5	5. ¿Cree que la información que ve en línea está diseñada para influir en su estado emocional o comportamiento?
Pregunta 6	¿Alguna vez ha sentido que pasa demasiado tiempo navegando en la web? ¿Cómo maneja este problema?
Pregunta 7	¿Está familiarizado con las medidas de seguridad implementadas por su navegador? ¿Confía en ellas?
Pregunta 8	¿Cree que las ciencias del comportamiento podrían ayudar a fomentar un uso más responsable de los navegadores web? ¿Por qué o por qué no?

4. RESULTADOS

A continuación, se detalla tanto la implementación como los resultados que arroja la búsqueda en las distintas bases de datos académicas bibliográficas, además de los filtros para las consultas para poder discriminar hacia resultados mucho más precisos sobre la relación de los navegadores web y las ciencias del comportamiento, ya que contribuye a que la investigación sea mucho más sólida y completa, teniendo en cuenta que algunas de estas bases poseen el riesgo de no poseer todos los artículos de una revista en específico o no tener la indexación de todas las revistas de un área en particular, se reduce este riesgo al buscar en diversas bases de conocimiento para que no se pierda literatura que es relevante para esta investigación.

Para la primera etapa, los artículos que fueron considerados con criterios de inclusión y de exclusión, ver Fig.1.

Figura 1.
Estudios identificados bajo el modelo Prisma



Conforme al esquema PRISMA, se escogen los resultados que fueron más relevantes para este estudio. A partir de las búsquedas realizadas en las bases de datos establecidas como lo son Web of Science, Springer, IEEEXplore y Google Scholar se identificaron 255 artículos en total,seguidamente para poder establecer y determinar su aceptación o descarte, se examinaron tanto los títulos, los resúmenes y las palabras claves resultando de la depuración 77 artículos según los criterios de inclusión y de exclusión, (ver Tabla 3).

Tabla 3 Cadenas de búsqueda de la segunda fase.

Base de datos	**Cadena Aplicada**	**Resultados**
Web of Science	science behavior (Topic) AND web browser (Topic)	18
Springer	'behavioral AND sciences AND web AND browser' within English Computer Science Information Systems Applications (incl.Internet) Article 2020 - 2024	28
IEEE Xplore	"All Metadata":behavioral) AND ("All Metadata":sciences) AND ("All Metadata":web browser)	27

Google Scholar	science behavior online OR psychology OR usability comparison "web browser"	4
		77

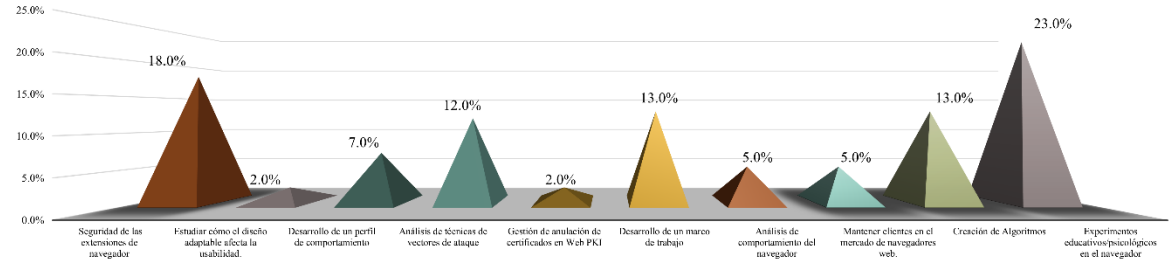
Los artículos seleccionados para evaluar la elegibilidad, depurando los estudios no aptos habiendo revisado los resúmenes, títulos y palabras clave de 43 artículos. Resultando que 40 artículos son los que satisfacen los criterios de elegibilidad una vez de realizada una revisión de texto completo, estos artículos forman parte de las áreas de neurociencias, ciencias computacionales, telecomunicaciones, psicología, ciencias cognitivas, ciencias del comportamiento, ciencias sociales, sistemas de información, educación y tecnologías de la información y más afines.

Los 40 artículos que se incluyeron tratan los temas de Seguridad y Usabilidad en el Desarrollo Web, los objetivos más relevantes están relacionados con Seguridad de las extensiones de los navegadores, experimentos educativos/psicológicos en el navegador y análisis de técnicas de vectores de ataque. Los problemas más significativos fueron relacionados con el aprendizaje automático y análisis predictivo, la seguridad de extensiones del navegador y sobre la Accesibilidad. La limitación más relevante identificada fue la de defensa por detección de amenazas, la propuesta/metodología más mencionada fue la de predicción de los comportamientos de los usuarios y la solución realizar mejoras de los modelos de aprendizaje automático.

La información que es recopilada responde a la razón de las preguntas de investigación propuestas después de aplicados los filtros respectivos para poder seleccionar los artículos más relevantes para la investigación se obtuvo un total de: 12 artículos de Web of Science, 4 artículos de Springer, 21 artículos de IEEEXplore, 3 artículos de Google Scholar.

Para responder a la pregunta de investigación Q1, ¿Cómo mejorar la seguridad, usabilidad y retención de clientes en navegadores web?, se presentan los datos obtenidos, visualizados en la figura a continuación, (ver Fig. 2).

Figura 2.
Resultados a la pregunta Q1

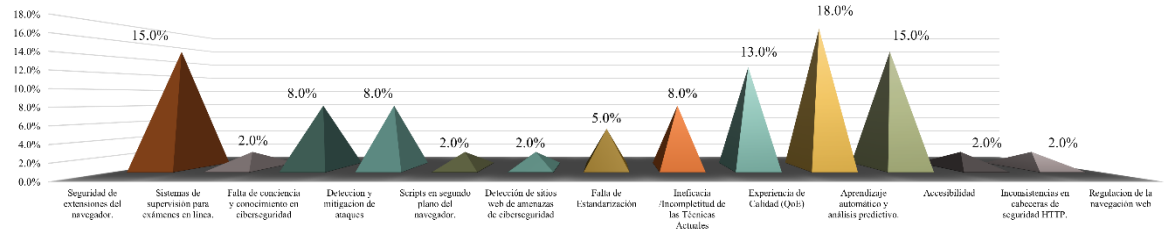


Se puede visualizar la gráfica la tendencia de artículos relacionados a experimentos educativos y psicológicos en los navegadores web relacionados al comportamiento de los usuarios es la más alta con una incidencia del 23%, seguido de la seguridad de las extensiones de los navegadores con una incidencia del 18%, el desarrollo de nuevos marcos de trabajo 13%, una incidencia del 13% también para la creación de algoritmos, Análisis de vectores de ataque con 12% de incidencia, 7% para Desarrollo de un perfil de comportamiento , 5% para Análisis de comportamiento del navegador , lo mismo para Mantener clientes en el mercado de navegadores web con 5% y por ultimo solo un 2% en el estudio de cómo el diseño adaptable afecta la usabilidad y en Gestión de anulación de certificados en Web PKI de 2%.

La investigación en el campo de la psicología y la tecnología ha avanzado enormemente en años recientes, abriendo nuevas posibilidades y desafíos. Los estudios recientes han explorado diversas áreas, desde la comprensión de los estados psicológicos como evitar la rumiación, estado psicológico relacionado con el estado de ánimo depresivo (Morita et al., 2022) , además una arquitectura de entorno aislado que permite ejecutar experimentos psicológicos cognitivos (Nikulchev et al., 2021) , facilitar la investigación basada en el navegador (Henninger et al., 2022) bastante relacionado con el estudio de (Shevchenko, 2022) con la implementación de Open Lab aplicación web para alojar y compartir experimentos en línea creados con lab.js. También las herramientas basadas en Inteligencia artificial como menciona (Liu et al., 2022) en su estudio un sistema que permite realizar un examen de estado mental en línea, usando solo una cámara y un micrófono.

Para responder a la pregunta de la investigación Q2, ¿Qué problemas de la seguridad, accesibilidad y experiencia de calidad se presentan en la navegación web?, se presenta los datos obtenidos, visualizados en la figura a continuación, (ver Fig. 3).

Figura 3.
Resultados a la pregunta Q2



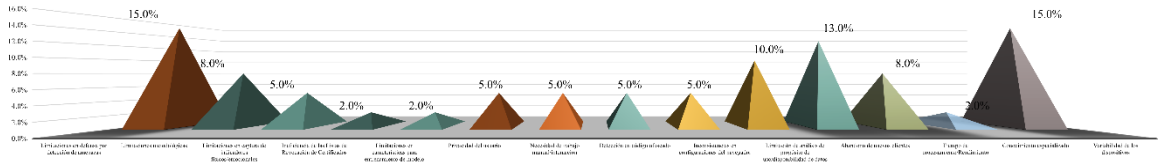
Se puede observar que se presentan con mayor incidencia los problemas relacionados con aprendizaje automático y análisis predictivo con una incidencia del 18%, seguido de un gran problema de seguridad y de privacidad inherentes en las extensiones de los navegadores con un 15% de incidencia, problemas en la accesibilidad con un 15% de incidencia y en la calidad de experiencia en la navegación web con un 13% de incidencia , se presentan también los problemas de Falta de conciencia y conocimiento en ciberseguridad con 8% , Detección y mitigación de ataques 8% , Ineficacia /Incompletitud de las Técnicas Actuales con 8% de incidencias. Además, un 5% de incidencia en Falta de Estandarización, con respecto a los problemas de Inconsistencias en cabeceras de seguridad HTTP 2%, Regulación de la navegación web 2%, Detección de sitios web de amenazas de ciberseguridad 2%, Scripts en segundo plano del navegador 2% y Sistemas de supervisión para exámenes en línea con 2% de incidencias en esta investigación.

Los entre los trabajos más relevantes identificados se encuentran: resolver el problema de predicción de abandono de clientes para los navegadores web, el autor (X. Wu et al., 2022) desarrollo el modelo Multivariate Behavior Sequence Transformer, para comprender la dinámica del comportamiento humano y de los grupos (Alyoubi & Alotaibi, 2021) utilizo el algoritmo de Canopy. Para la predicción de comportamiento (Singh & Meenu, 2017) empleo Web Log Expert Lite 9.3 para analizar los datos de registro del servidor web de una institución educativa académica y extraer información, muy útil para la minería web y en su investigación (Mingsheng et al., 2022) menciona la implementación de un método basado en aprendizaje automático para poder predecir el núcleo óptimo para renderizar el contenido web.

Para responder a la pregunta de la investigación Q3, ¿Cómo superar las limitaciones en ciberseguridad y usabilidad web?, se presenta los datos obtenidos, visualizados en la figura a continuación, (ver Fig. 4).

Figura 4.

Resultados a la pregunta Q3



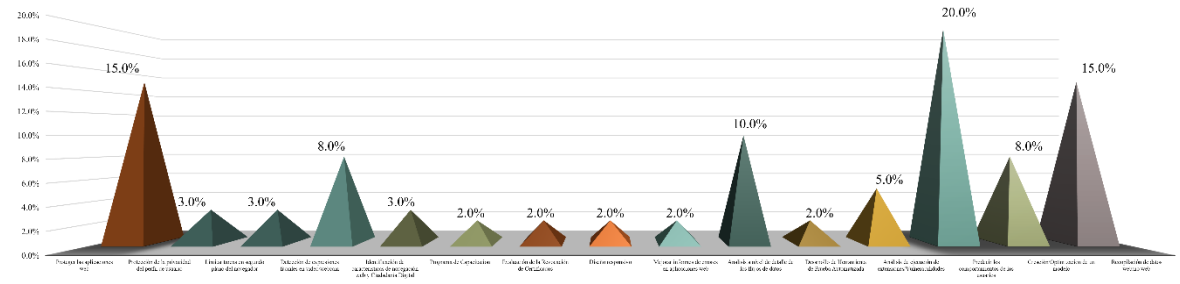
Se identificó el impacto como afecta las limitaciones de las defensas existentes para detectar amenazas con una incidencia del 15%, seguido de una variabilidad en los dispositivos con una incidencia del 15%, el posible abandono de nuevos clientes con una incidencia del 13%, y limitación de análisis de propósito de uso/disponibilidad de los datos del 10%. También se encontraron Limitaciones metodológicas con 8%, Tiempo de procesamiento/Rendimiento 8%, Limitaciones en captura de indicadores físicos/emocionales 5%, Privacidad del usuario 5%, Necesidad de trabajo manual/interacción 5%, Detección en código ofuscado 5%, Inconsistencias en configuraciones del navegador 5%. Con respecto a las limitaciones en Ineficiencia de las Listas de Revocación de Certificados 2%, Limitaciones en características para entrenamiento de modelo 2% y Conocimiento especializado de 2% de incidencia.

Los estudios más relevantes incluyen: El problema planteado de proteger a los usuarios de las extensiones maliciosas del navegador es el que (X. Wang et al., 2022) propone un marco de trabajo web que permite a los desarrolladores web aislar las partes sensibles de sus aplicaciones, también la implementación de una herramienta para identificar los comportamientos no confiables de los programas de extensión de Chrome. Por otro lado, la implementación de modelo de red neuronal artificial es la que el autor (Gabryel et al., 2022) propuso para permitir detectar anomalías en el tráfico web en tiempo real. Además (K. Wang & Yu, 2021) propone un método relacionado a la forma de expresar el comportamiento de los programas de extensión de navegador mediante un modelo de grafo, para poder identificar las características de programas que no confiables o maliciosos, mediante la comparación de sus subgrafos diferenciales con los de los programas normales, también (Sam & Ancy Jenifer., 2023) sostiene

la importancia de la creación de un marco para evaluar la seguridad de las extensiones de navegador, que son una fuente potencial de vulnerabilidades y ataques.

Para responder a la pregunta de la investigación Q4, ¿Qué propuestas pueden mejorar la seguridad, privacidad y usabilidad en la web?, se presenta los datos obtenidos, visualizados en la figura a continuación, (ver Fig. 5).

Figura 5.
Resultados a la pregunta Q4



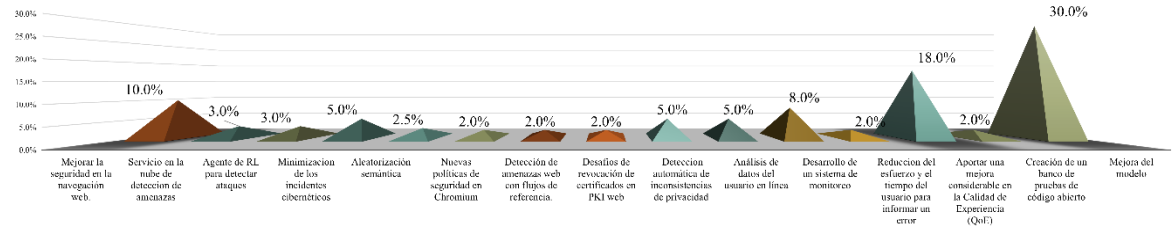
Se identificó el impacto de la importancia de predecir los comportamientos de los usuarios con una incidencia del 20%, seguido de 15% de protección a las aplicaciones web (desde el lado del servidor y del cliente), y 15% de recopilación de datos web y no web, además artículos relacionados con el análisis a nivel de detalle de los flujos de datos con el 10% de incidencia. Además de propuestas relacionadas a Detección de expresiones faciales en video/webcam con 8% , Creación/Optimización de un modelo 8% , 5% en Análisis de ejecución de extensiones/Vulnerabilidades , Protección de la privacidad del perfil de usuario 3% , Limitar tareas en segundo plano del navegador 3% , Identificación de características de navegación web y Ciudadanía Digital con 3% , Programas de Capacitación con 2% de incidencia , Evaluación de la Revocación de Certificados 2% , Diseño responsivo 2% , Mejorar informes de errores en aplicaciones web con 2% y Desarrollo de Herramienta de Prueba Automatizada con 2% de incidencia.

Para la predicción se realizó mediante algunas técnicas como el modelo Multivariate Behavior Sequence Transformer que utiliza dos mecanismos de atención complementarios para explorar la información temporal y conductual de los clientes, incluyendo un clasificador basado en árboles (X. Wu et al., 2022), además (Morita et al., 2022) empleó un modelo que utiliza la arquitectura cognitiva ACT-R para simular la memoria y la emoción humanas, y modula los parámetros del modelo según el ritmo cardíaco del usuario, que se mide con un sensor.En su

estudio (Alyoubi & Alotaibi, 2021) empleo el algoritmo Canopy a un conjunto de datos de una campaña publicitaria de Facebook, que contiene atributos como la identidad del anuncio, la edad, el género, los intereses, las impresiones, los clics, el gasto, las conversiones totales y las conversiones aprobadas , además (Lyngs et al., 2022) señala que las herramientas de autocontrol digital pueden tener un impacto en el comportamiento y las percepciones de los usuarios.

Para responder a la pregunta de la investigación Q5, ¿Cómo solucionar los problemas de la seguridad, accesibilidad y experiencia de calidad en la navegación web?, se presenta los datos obtenidos, visualizados en la figura a continuación, (ver Fig. 6).

Figura 6.
Resultados a la pregunta Q5



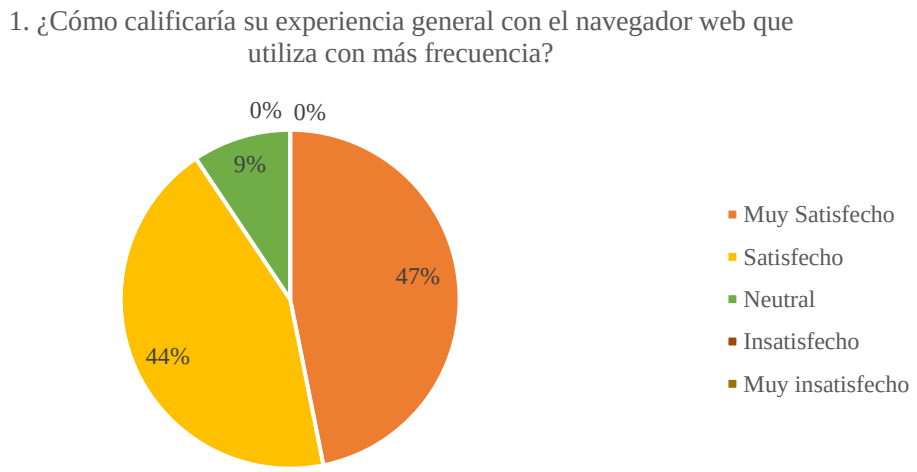
Se identificó el impacto de la implementación y mejora de modelos de aprendizaje con una incidencia del 30%, seguido de la aportación de una mejor experiencia al usuario con una incidencia del 18% y una mejora en la seguridad de la navegación web del 10% de incidencia y desarrollo de un sistema de monitoreo con una incidencia de 8%. Además de soluciones relacionadas a Minimización de los incidentes cibernéticos 5%, Detección automática de inconsistencias de privacidad con 5%, Análisis de datos del usuario en línea con 5%. Por último, soluciones de Servicio en la nube de detección de amenazas 3%, usos de Agentes de RL para detectar ataques 3%, Aleatorización semántica con 2,5% de incidencia, Nuevas políticas de seguridad en Chromium 2%, Detección de amenazas web con flujos de referencia con 2% , Desafíos de revocación de certificados en PKI web con 2% de incidencias, Reducción del esfuerzo y el tiempo del usuario para informar un error con 2% y Creación de un banco de pruebas de código abierto con 2% de incidencia.

Entre los resultados relacionados a mejoras en los modelos de aprendizaje más relevantes está el que (X. Wu et al., 2022) menciona, que el MBST es mejor que otros métodos para predecir el abandono ya que tiene una precisión del 82.72% y un AUC del 93.75%, además se encuentra el estudio de (Morita et al., 2022) donde sus resultados del estudio muestran que el modelo

contrabalanceado fue más efectivo que el sincronizado para suprimir la rumiación durante la navegación web. Además del estudio de (Gabryel et al., 2022) en su estudio se propone una solución para mejorar el modelo de aprendizaje basado en el autoencoder variacional (VAE).

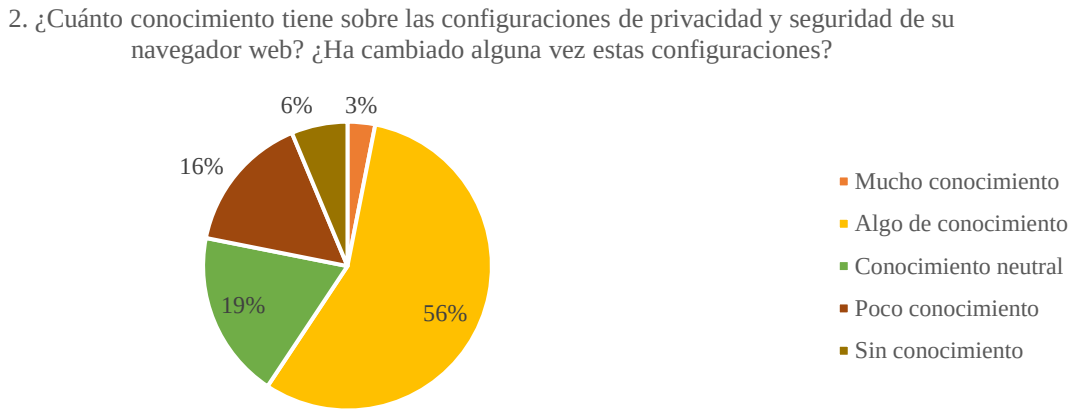
Su solución se basa en calcular los centroides y los umbrales para cada clase de datos, y luego usarlos para clasificar los datos como normales o anómalos. Además, en su investigación propone el uso de tanto IsolationForest como EllipticEnvelope como clasificadores principales, en particular este último que tiene una mayor precisión media en conjuntos de datos grandes de actividad del usuario (Iskhakov et al., 2023).

Figura 7.
Datos obtenidos en la pregunta número 1 de la encuesta



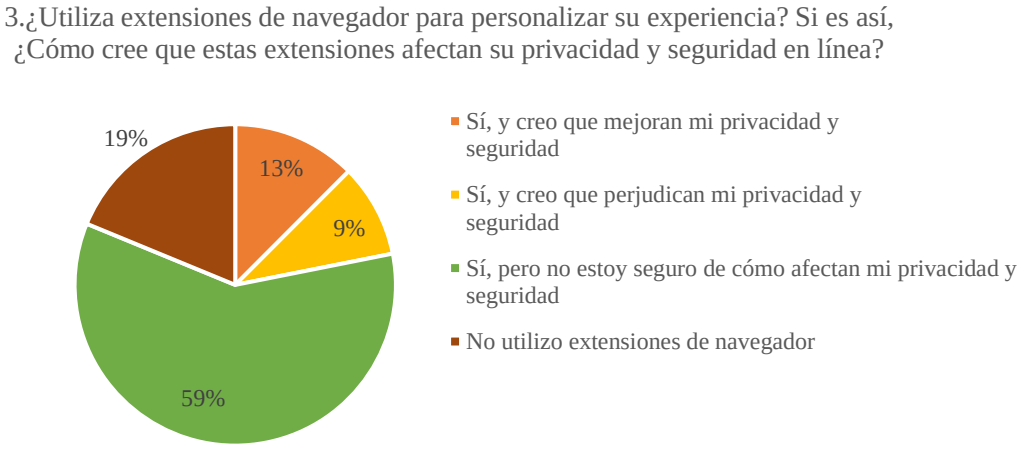
Como se puede observar en la figura 7, un 47% de los encuestados se encontró satisfecho con su experiencia en el navegador que mas utiliza, seguido de 44% que solo se encuentran satisfechos, un 9% se mantuvo neutral, ninguno se encontró Muy insatisfecho 0% ni Insatisfecho 0%.

Figura 8.
Datos obtenidos en la pregunta número 2 de la encuesta



Esta pregunta relacionada con el conocimiento sobre Privacidad y Seguridad, como se puede visualizar en la figura 8, existe una variedad de conocimiento sobre las configuraciones. Se puede visualizar en la figura 8, un 56% de los encuestados poseen algo de conocimiento, seguido de 19% con un conocimiento neutral, un 16% con poco conocimiento, 6% de los encuestados, finalmente un 3% sí poseían mucho conocimiento de las configuraciones de privacidad y seguridad de su navegador web.

Figura 9.
Datos obtenidos en la pregunta nímero 3 de la encuesta

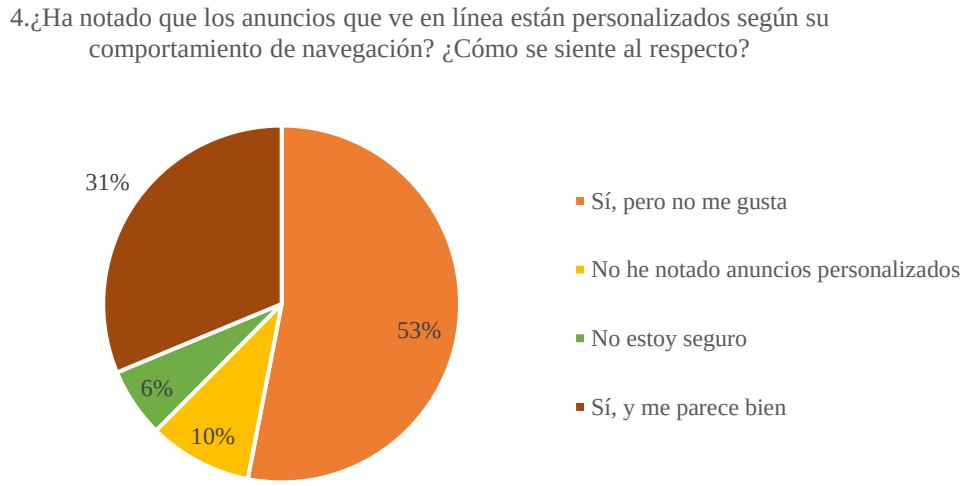


Sobre las extensiones de navegador, se visualiza en la figura 9 que un 59% sí utiliza extensiones del navegador, pero no está seguro de cómo afectan a su privacidad y seguridad, seguido de 19% que no utiliza extensiones de navegador, un 13% que sí las utiliza y creen que mejoran su

privacidad y seguridad, por un 9% respondieron que sí utilizan extensiones de navegador y creen que perjudica su privacidad y seguridad.

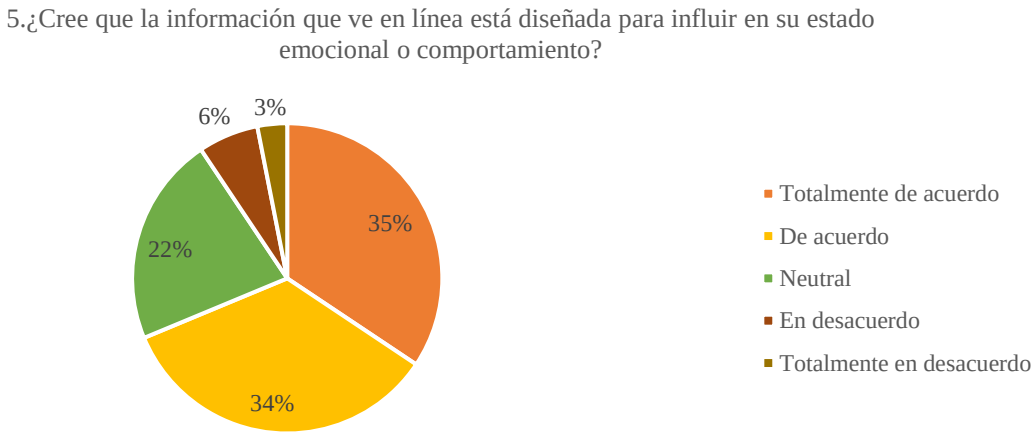
la mayoría de los encuestados las utiliza. Como se puedo observar en la figura 9, algunos sostienen que éstas mejoran la privacidad y seguridad un 68%, mientras que otros piensan lo contrario 32%. La elección de extensiones puede depender de la percepción individual de riesgo y beneficio.

Figura 10.
Datos obtenidos en la pregunta número 4 de la encuesta



Como se puede visualizar en la figura 10, los usuarios que sí notan los anuncios personalizados, pero no les gusta con un 53%, seguido de un 31% que los notaron y les pareció bien esa práctica. Por otro lado, en 10% de los encuestados no los ha notado y un 6% no está seguro. La aceptación o rechazo de los anuncios personalizados puede estar relacionada con preferencias personales y preocupaciones de privacidad.

Figura 11.
Datos obtenidos en la pregunta número 5 de la encuesta



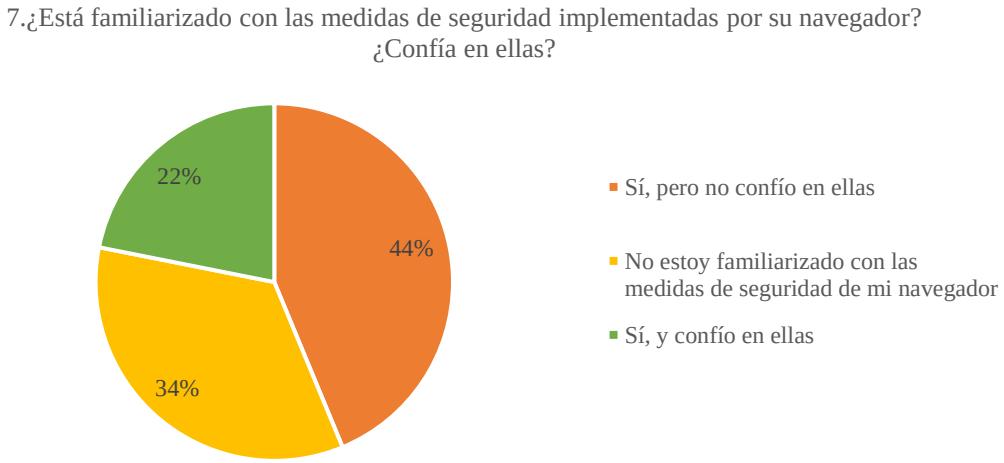
Como se puede observar en la figura 11, el 35% se encuentra totalmente de acuerdo con la idea que la información en línea está diseñada para influir en su estado emocional o comportamiento, seguido de un 34% que está de acuerdo, además un 22% se mostró neutral, por otro lado, un 6% se mostro en desacuerdo y un 3% totalmente en desacuerdo.

Figura 12.
Datos obtenidos en la pregunta número 6 de la encuesta

Como se puede visualizar en la figura 12, el 47% de los encuestados ha sentido que sí pasa demasiado tiempo navegando en la web, pero no tiene estrategias para manejarlo, la falta de estrategias para manejar esto podría indicar una necesidad de conciencia y autogestión. Seguido

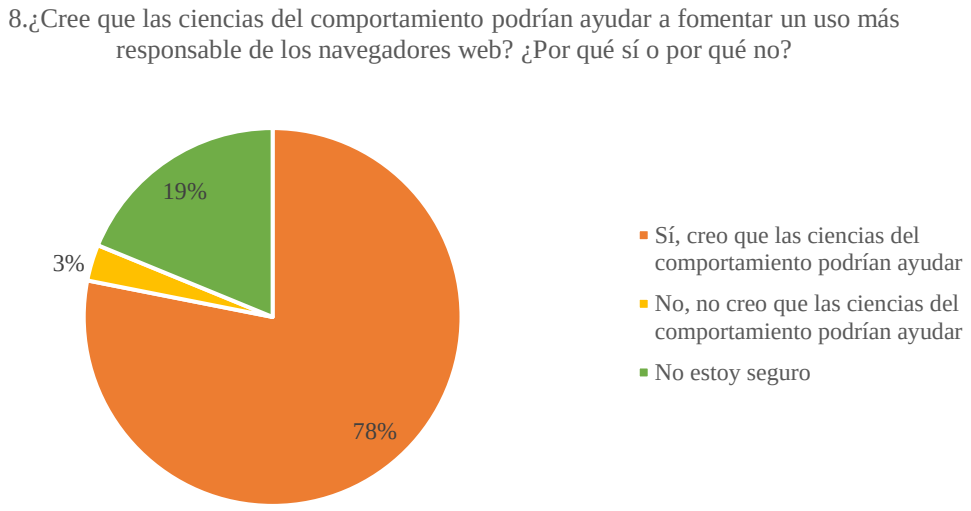
de un 28% que no cree pasar demasiado tiempo navegando en la web, por último, un 25% respondió que sí, pero poseen estrategias para manejarlo.

Figura 13.
Datos obtenidos en la pregunta número 7 de la encuesta



Como se puede visualizar en la figura 13, un 44% de los encuestados respondió que sí está familiarizado con las medidas de seguridad implementadas en su navegador pero que no confía en ellas, seguido de un 34% que no está familiarizado con medidas de seguridad de sus navegadores y por último un 22% que sí esta familiarizado con las medidas de seguridad implementadas y que confía en ellas. La confianza puede depender de la percepción de riesgo y la comprensión técnica.

Figura 14.
Datos obtenidos en la pregunta número 8 de la encuesta



Como se puede visualizar en la figura 14, un 78% de los encuestados cree que las ciencias del comportamiento podrían ayudar a fomentar un uso más responsable de los navegadores web, esto sugiere que la comprensión del comportamiento humano puede ser clave para diseñar interfaces, seguido de un 19% que piensan lo contrario, por último, un 3% que no estaba seguro. y políticas más efectivas.

5. DISCUSIÓN

El mapeo sistemático de la literatura realizado reveló las principales tendencias, problemas y propuestas relacionadas con la seguridad, usabilidad y retención de clientes en los navegadores web. Los resultados mostraron que la mayoría de los artículos se enfocan en temas como: experimentos educativos y psicológicos, problemas de aprendizaje automático, en análisis predictivo, además de propuestas de mejora de modelos de aprendizaje y experiencias de usuario. Los resultados denotan que existe un gran interés y potencial en aplicar las ciencias del comportamiento para entender y mejorar el uso de los navegadores web.

Se discute que la experiencia del usuario es prioritaria ya que es evidente en trabajos relacionas y en este estudio que se percibe inconformidad con los anuncios personalizados, la recolección de la información en línea y su administración, la limitación de análisis de propósito de uso/disponibilidad de datos es lo que se necesita informar a los usuarios, por lo que los navegadores deberían esforzarse por ser más transparentes en cuanto a la recolección de estos.

Además, resultados indican la necesidad de un enfoque al diseño de los navegadores, la accesibilidad es un área que necesita más atención.

Las ciencias del comportamiento desempeñan un papel muy importante en la mejora tanto de la seguridad, la privacidad y la usabilidad en la web, los usuarios se muestran muy interesados en que las ciencias del comportamiento puedan ayudar a fomentar un uso más responsable de los navegadores, aportando una mejora considerable en la calidad de experiencia, para ello podrían realizarse programas de capacitación en instituciones educativas, a nivel de empresa para que usuarios estén al tanto de las últimas actualizaciones en conjunto con prácticas recomendadas en la configuración de sus navegadores.

6. CONCLUSIÓN

Se puede concluir que los usuarios necesitan estar más informados además de educarse sobre las configuraciones de privacidad y seguridad de sus navegadores del día a día, que algunas mejoras a la seguridad que se ha implementado en los artículos son innovadoras y eficientes al momento de salvaguardar la integridad de los usuarios en línea, pero la percepción de los usuarios de los navegadores web tiene que mejorarse porque es muy baja.

Se puede observar que hay una convergencia entre las áreas de investigación y las necesidades de los usuarios, como la seguridad, privacidad, usabilidad y la experiencia de calidad. Por otro lado, los resultados revelan que hay una brecha entre el conocimiento y la confianza de los usuarios sobre las medidas de seguridad implementadas por los navegadores web, además que hay una diversidad de opiniones con respecto a preferencias sobre las extensiones de navegador y los anuncios personalizados, como estos pueden afectar la retención de clientes. Estos contrastes apoyan la idea que existe un desafío para los diseñadores de los navegadores web de comunicar, adaptar sus propuestas a las expectativas y comportamientos de los usuarios.

El mapeo sistemático realizado pudo identificar que el 23% de los estudios analizados sobre el impacto de los experimentos educativos y psicológicos en los navegadores web relacionados al comportamiento de los usuarios esto complementa a los resultados de la encuesta ya que reveló que la mayoría de los usuarios cree que las ciencias del comportamiento pueden ayudar a fomentar un uso más responsable de los navegadores web. Además, que el 18% de los estudios que se enfocaron en la seguridad de las extensiones de los navegadores, 13% en un marco de trabajo inherentes en las extensiones y un 13% a la creación de algoritmos para una mejora en

la experiencia, como valores altos. La encuesta en cambio mostró que algunos usuarios tienen un buen entendimiento sobre las configuraciones de privacidad y seguridad, mientras que otros simplemente carecen de información. Además, algunos piensan que las extensiones mejoran la privacidad y seguridad, pero otros no están contentos con los anuncios personalizados.

Sobre las propuestas para mejorar la seguridad, privacidad y usabilidad el mapeo sistemático señaló que el 20% de los estudios propusieron predecir los comportamientos de los usuarios, el 15% proteger las aplicaciones web en su accesibilidad y el 15% seguridad de las extensiones del navegador al recopilar datos (web y no web). La encuesta indicó que algunos usuarios confían plenamente en las medidas de seguridad implementadas por su navegador, mientras que otros no están familiarizados o no confían en ellas.

Por último, el mapeo sistemático destacó que el 30% de los estudios implementaron y mejoraron modelos de aprendizaje, el 18% aportaron una mejor experiencia al usuario y el 10% mejoraron la seguridad de la navegación web. La encuesta evidenció que muchos usuarios reconocen pasar demasiado tiempo navegando en la web, pero la falta de estrategias para manejar esto podría indicar una necesidad de conciencia sobre su seguridad en la web.

Los resultados de la investigación en síntesis sugieren la necesidad de considerar la diversidad de los usuarios y ofrecer opciones que permitan un mayor control de su navegación web. Los usuarios no están conformes con los anuncios personalizados y la recolección de información en línea, por lo que se necesita mayor transparencia.

El campo de las ciencias del comportamiento tiene un gran potencial para especialistas en diversas áreas, como la informática, el marketing y la ciberseguridad. Se necesita explorar más estas áreas para mejorar la experiencia del usuario y promover un uso seguro de la web.

REFERENCIAS

Alcívar-Cruz, B., & Llerena-Izquierdo, J. (2023). After-Sales and Customer Loyalty Strategies for Fixed Internet Through the Implementation of Virtual Assistance in the Ecuadorian Context. In V. Robles-Bykbaev, J. Mula, & G. Reynoso-Meza (Eds.), *Intelligent Technologies: Design and Applications for Society* (pp. 139–149). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-24327-1_12

Alvarado Zambrano, J. B. (2021). *Medios de comunicación virtual en la educación durante la pandemia: un mapeo sistemático*. http://dspace.ups.edu.ec/handle/123456789/20736

Alyoubi, K. H., & Alotaibi, F. S. (2021). Evaluating Conversion Rate from Advertising in Social Media using Big Data Clustering. *INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND NETWORK SECURITY*, *21*(7), 305–316. https://doi.org/10.22937/IJCSNS.2021.21.7.35

Anwyl-Irvine, A. L., Massonnié, J., Flitton, A., Kirkham, N., & Evershed, J. K. (2020). Gorilla in our midst: An online behavioral experiment builder. *Behavior Research Methods*, *52*(1), 388–407. https://doi.org/10.3758/s13428-019-01237-x

Atiaja Balseca, L. E. (2023). *Uso de la analítica del aprendizaje de los estudiantes para minimizar la pérdida escolar en las diferentes modalidades de estudio* [{B.S.} thesis]. http://dspace.ups.edu.ec/handle/123456789/25199

Ayala-Carabajo, R., & Llerena-Izquierdo, J. (2023). Modelo preventivo para minimizar estudiantes en riesgo académico para las asignaturas del primer año universitario. *Congreso de Docencia En Educación Superior CODES*, *5*.

Bauer, J. C., Murray, M. A., & Ngondo, P. S. (2023). Who's missing out? The impact of digital networking behavior \& social identity on PR job search outcomes. *PUBLIC RELATIONS REVIEW*, *49*(4). https://doi.org/10.1016/j.pubrev.2023.102367

Berbecaru, D. G., & Lioy, A. (2023). An Evaluation of X.509 Certificate Revocation and Related Privacy Issues in the Web PKI Ecosystem. *IEEE Access*, *11*, 79156–79175. https://doi.org/10.1109/ACCESS.2023.3299357

Bui, D., Tang, B., & Shin, K. G. (2023). Detection of Inconsistencies in Privacy Practices of Browser Extensions. *2023 IEEE Symposium on Security and Privacy (SP)*, 2780–2798. https://doi.org/10.1109/SP46215.2023.10179338

Cárdenas Rebelo, A., & Orozco-Toro, J. A. (2020). Publicidad social y su influencia en la percepción de las campañas sociales de prevención de accidentes de tránsito en Ecuador. *Retos*, *10*(20), 219–231. https://doi.org/10.17163/ret.n20.2020.02

Cristellot Paredes, A. M., Cueva Estrada, J., & Sumba Nacipucha, N. (2024). Análisis del Marketing experiencial en la satisfacción del cliente en el sector gastronómico de Guayaquil. *Ad-Gnosis*, *13*(13), 1–19. https://doi.org/10.21803/adgnosis.13.13.664

Cueva Estrada, J. M., & Sánchez-Bayón, A. (2024). Estudio bibliométrico de Economía Digital y sus tendencias. *Revista de Estudios Empresariales. Segunda Época*, 195–209. https://doi.org/10.17561/ree.n1.2024.8229

de la Nube Toral Sarmiento, A., Loaiza Martínez, M. de L., Llerena Izquierdo, J., Ayala Carabajo, R., Torres Toukoumidis, A., Romero-Rodríguez, L. M., Aguaded, I., Vega Ureta, N. T., Fuentes Espinoza, P. G., Peñafiel Caicedo, J. A., & others. (2018). *4to. Congreso Internacional de Ciencia, Tecnología e Innovación para la Sociedad. Memoria académica*. https://dspace.ups.edu.ec/handle/123456789/16318

Farid, F. (2023). BioEnvsense: A Usable Cybersecurity Framework for Critical Infrastructure. *2023 International Conference on Smart Applications, Communications and Networking (SmartNets)*, 1–5. https://doi.org/10.1109/SmartNets58706.2023.10215755

Fonseka, A., Pashenna, P., & Ariyadasa, S. N. (2023). Detecting Tabnabbing Attacks Via An RL-Based Agent. *2023 8th International Conference on Information Technology Research (ICITR)*, 1–6. https://doi.org/10.1109/ICITR61062.2023.10382917

Fuchs, K. L., Lian, J., Michels, L., Mayer, S., Toniato, E., & Tiefenbeck, V. (2022). Effects of Digital Food Labels on Healthy Food Choices in Online Grocery Shopping. *Nutrients*, *14*(10). https://doi.org/10.3390/nu14102044

Gabryel, M., Lada, D., Filutowicz, Z., Patora-Wysocka, Z., Kisiel-Dorohinicki, M., & Chen, G. Y. (2022). Detecting Anomalies in Advertising Web Traffic with the Use of the Variational Autoencoder. *Journal of Artificial Intelligence and Soft Computing Research*, *12*(4), 255–256. https://doi.org/doi:10.2478/jaiscr-2022-0017

Gómez-Bayona, L., Arrubla-Zapata, J. P., Aristizábal Valencia, J., & Restrepo-Rojas, M. J. (2020). Análisis de las estrategias de marketing relacional en instituciones de educación superior de Colombia y España. *Retos*, *10*(20), 343–359. https://doi.org/10.17163/ret.n20.2020.09

Gonzalez Marin, N. C., Guiracocha Arriciaga, R. V., Cueva Estrada, J., & Sumba, N. (2024). El marketing de influencias y su efecto en la decisión de compra de los clientes en el sector de la moda y la belleza en el Ecuador. *Doxa Comunicación. Revista Interdisciplinar de Estudios de Comunicación y Ciencias Sociales*. https://doi.org/10.31921/doxacom.n38a1993

Guiñez-Cabrera, N., Mansilla-Obando, K., & Jeldes-Delgado, F. (2020). La transparencia publicitaria en los influencers de las redes sociales. *Retos*, *10*(20), 265–281. https://doi.org/10.17163/ret.n20.2020.05

Henninger, F., Shevchenko, Y., Mertens, U. K., Kieslich, P. J., & Hilbig, B. E. (2022). lab.js: A free, open, online study builder. *Behavior Research Methods*, *54*(2), 556–573. https://doi.org/10.3758/s13428-019-01283-5

Hong, H., Woo, S., Park, S., Lee, J., & Lee, H. (2022). Circuit: A JavaScript Memory Heap-Based Approach for Precisely Detecting Cryptojacking Websites. *IEEE Access*, *10*, 95356–95368. https://doi.org/10.1109/ACCESS.2022.3204814

Hovorushchenko, T., Medzatyi, D., Kvanitskyi, D., & Kravchuk, S. (2022). Characteristics and Method of Forming the User Information Portrait. *2022 12th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, 1–6. https://doi.org/10.1109/DESSERT58054.2022.10018619

Isanoa-Sinche, M., & Llerena-Izquierdo, J. (2023). Towards a Meaningful Experience on the Use of Digital Educational Resources and Media created at Ardora. *2023 IEEE Seventh Ecuador Technical Chapters Meeting (ECTM)*, 1–5. https://doi.org/10.1109/ETCM58927.2023.10308988

Iskhakov, A. Yu., Mamchenko, M. V, & Khripunov, S. P. (2023). Enhanced User Authentication Algorithm Based on Behavioral Analytics in Web-Based Cyberphysical Systems. *2023 International Russian Smart Industry Conference (SmartIndustryCon)*, 253–258. https://doi.org/10.1109/SmartIndustryCon57312.2023.10110791

Jampen, D., Gür, G., Sutter, T., & Tellenbach, B. (2020). Don't click: towards an effective anti-phishing training. A comparative literature review. *Human-Centric Computing and Information Sciences*, *10*(1), 33. https://doi.org/10.1186/s13673-020-00237-7

Joo, M., An, Y., Roh, H., & Lee, W. (2021). Predictive Prefetching Based on User Interaction for Web Applications. *IEEE Communications Letters*, *25*(3), 821–824. https://doi.org/10.1109/LCOMM.2020.3038255

Kiviat, B. (2021). Which Data Fairly Differentiate? American Views on the Use of Personal Data in Two Market Settings. *Sociological Science*, *8*(2), 26–47. https://doi.org/10.15195/v8.a2

Krajbich, I., & Yang, X. (2021). Webcam-based online eye-tracking for behavioral research. *Judgment and Decision Making*, *16*(6), 1485–1505. https://doi.org/DOI: 10.1017/S1930297500008512

Lindao Palma, T. L., Carrera Jiménez, J., Cueva Estrada, J., & Sumba Nacipucha, N. (2023). Estrategias de Marketing Digital aplicadas en las empresas de Transporte Interprovincial ecuatorianas. *Revista Minerva*, *6*(1), 57–72. https://doi.org/10.5377/revminerva.v6i1.16417

Liu, Y., Xia, S., Nie, J., Wei, P., Shu, Z., Chang, J. A., & Jiang, X. (2022). aiMSE: Toward an AI-Based Online Mental Status Examination. *IEEE Pervasive Computing*, *21*(4), 46–54. https://doi.org/10.1109/MPRV.2022.3172419

López-Chila, R., Llerena-Izquierdo, J., Sumba-Nacipucha, N., & Cueva-Estrada, J. (2024). Artificial Intelligence in Higher Education: An Analysis of Existing Bibliometrics. *Education Sciences*, *14*(1). https://doi.org/10.3390/educsci14010047

Lyngs, U., Lukoff, K., Csuka, L., Slovák, P., Van Kleek, M., & Shadbolt, N. (2022). The Goldilocks level of support: Using user reviews, ratings, and installation numbers to investigate digital self-control tools. *International Journal of Human-Computer Studies*, *166*, 102869. https://doi.org/https://doi.org/10.1016/j.ijhcs.2022.102869

Maliki, N. A., Zainal, A., Abdoh Ghaleb, F. A., & Kassim, M. N. (2021). User Security Behavioral Profiling using Historical Browsing Website. *2021 International Conference on Data Science and Its Applications (ICoDSA)*, 163–168. https://doi.org/10.1109/ICoDSA53588.2021.9617493

Matos, G., Costa, D., Lins, A., Bezerra, E., Barroso, L., Aguiar, C., Ferraz, T., & Teixeira, I. (2023). Watson: Web Application Interface Data Collector for Feedback Reporting. *2023 IEEE 30th Annual Software Technology Conference (STC)*, 3–6. https://doi.org/10.1109/STC58598.2023.00007

Mingsheng, X., Chunxia, L., & Wenhui, D. (2022). Research and Development of Dual-Core Browser-Based Compatibility and Security. *2022 IEEE 8th International Conference on Computer and Communications (ICCC)*, 1697–1701. https://doi.org/10.1109/ICCC56324.2022.10065688

Morita, J., Pitakchokchai, T., Raj, G. B., Yamamoto, Y., Yuhashi, H., & Koguchi, T. (2022). Regulating Ruminative Web Browsing Based on the Counterbalance Modeling Approach. *Frontiers in Artificial Intelligence*, *5*. https://doi.org/10.3389/frai.2022.741610

Mudassar, M., Ali, M., Ali, A., Farid, Z., Asif, R., Mehmood, M. H., & Salam Mohammed, A. (2023). An Analysis of Browser and Machine Fingerprinting Techniques. *2023 International Conference on Business Analytics for Technology and Security (ICBATS)*, 1–8. https://doi.org/10.1109/ICBATS57792.2023.10111174

Nigam, A., Pasricha, R., Singh, T., & Churi, P. (2021). A Systematic Review on AI-based Proctoring Systems: Past, Present and Future. *Education and Information Technologies*, *26*(5), 6421–6445. https://doi.org/10.1007/s10639-021-10597-x

Nikulchev, E., Ilin, D., Kolyasnikov, P., Magomedov, S., Alexeenko, A., Kosenkov, A. N., Sokolov, A., Malykh, A., Ismatullina, V., & Malykh, S. (2021). Isolated Sandbox Environment Architecture for Running Cognitive Psychological Experiments in Web Platforms. *FUTURE INTERNET*, *13*(10). https://doi.org/10.3390/fi13100245

Norta, A., Fernandez, C., & Hickmott, S. (2018). Commercial Property Tokenizing with Smart Contracts. *Proceedings of the International Joint Conference on Neural Networks*, *2018-July*. https://doi.org/10.1109/IJCNN.2018.8489534

Ortega-Vivanco, M. (2020). Efectos del Covid-19 en el comportamiento del consumidor: Caso Ecuador. *Retos*, *10*(20), 233–247. https://doi.org/10.17163/ret.n20.2020.03

Ortegón Cortázar, L. (2023). ¿Por qué visitar lifestyle centers? Variables alternativas de atracción a través de un modelo de ecuaciones estructurales. *Retos*, *13*(25), 87–103. https://doi.org/10.17163/ret.n25.2023.06

París, J. A. (2020). La adaptación versus la estandarización visto desde el paradigma de marketing esencial. *Retos*, *10*(20), 195–217. https://doi.org/10.17163/ret.n20.2020.01

Parlakkiliç, A. (2022). Evaluating the effects of responsive design on the usability of academic websites in the pandemic. *Education and Information Technologies*, *27*(1), 1307–1322. https://doi.org/10.1007/s10639-021-10650-9

Peñafiel Espinoza, M. M., & Lopez Chila, R. D. (2012). *Estudio sobre la utilización y efctividad del Comercio Electronico (E-comerce) y propuesta para su Implementacion en las Pymes del Sector Comercial de Guayaquil*.

Pérez González, R. F. (2021). *Softwares de penetración utilizados por los piratas informáticos: Una revisión sistemática (2015-2020)*.

Pilapaxi-Cunalata, N., & Llerena-Izquierdo, J. (2023). Experience of the Disruption of Educational Technologies Based on the UTAUT Model. *2023 IEEE Seventh Ecuador Technical Chapters Meeting (ECTM)*, 1–5. https://doi.org/10.1109/ETCM58927.2023.10308981

Recalde Monar, J. A. (2021). *El ciberacoso por redes sociales en el Ecuador*. http://dspace.ups.edu.ec/handle/123456789/20945

Rigchc Mero, A. (2022). *Determinación de los peligros en las redes sociales en entorno a niños y adolescentes para uso y prevención*. http://dspace.ups.edu.ec/handle/123456789/22843

Rodriguez-Garcia, M., Batet, M., Sánchez, D., & Viejo, A. (2021). Privacy protection of user profiles in online search via semantic randomization. *Knowledge and Information Systems*, *63*(9), 2455–2477. https://doi.org/10.1007/s10115-021-01597-x

Rosero Tejada, L. F. (2021). *El Phishing como riesgo informático, técnicas y prevención en los canales electrónicos: Un mapeo sistemático* [{B.S.} thesis].

Sam, J., & Ancy Jenifer., J. (2023). Mitigating the Security Risks of Browser Extensions. *2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS)*, 1460–1465. https://doi.org/10.1109/ICSCSS57650.2023.10169483

Shao, S., Satam, P., Satam, S., Al-Awady, K., Ditzler, G., Hariri, S., & Tunc, C. (2021). Multi-Layer Mapping of Cyberspace for Intrusion Detection. *2021 IEEE/ACS 18th International Conference on Computer Systems and Applications (AICCSA)*, 1–8. https://doi.org/10.1109/AICCSA53542.2021.9686823

Shevchenko, Y. (2022). Open Lab: A web application for running and sharing online experiments. *Behavior Research Methods*, *54*(6), 3118–3125. https://doi.org/10.3758/s13428-021-01776-2

Siewert, H., Kretschmer, M., Niemietz, M., & Somorovsky, J. (2022). On the Security of Parsing Security-Relevant HTTP Headers in Modern Browsers. *2022 IEEE Security and Privacy Workshops (SPW)*, 342–352. https://doi.org/10.1109/SPW54247.2022.9833880

Singh, S. P., & Meenu. (2017). Analysis of web site using web log expert tool based on web data mining. *2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*, 1–5. https://doi.org/10.1109/ICIIECS.2017.8275961

Subramani, K., Jueckstock, J., Kapravelos, A., & Perdisci, R. (2022). SoK: Workerounds - Categorizing Service Worker Attacks and Mitigations. *2022 IEEE 7th European Symposium on Security and Privacy (EuroS&P)*, 555–571. https://doi.org/10.1109/EuroSP53844.2022.00041

Sumba Nacipucha, N., Sánchez-Bayón, A., Cueva Estrada, J., & Valencia-Arias, A. (2024). Social networks as a strategy to improve the visibility of scientific journals. *Cogent Social Sciences*, *10*(1). https://doi.org/10.1080/23311886.2024.2306715

Toala Indio, Y. I. (2021). *Delitos informáticos frecuentes en el Ecuador: casos de estudio* [{B.S.} thesis].

Ubaidah, S., Faqiani, N., Afiq, M. I., & Abd Aziz, N. E. (2023). Emerging Trends in Cybersecurity: Issues in Cybersecurity During Covid-19 Pandemic. *Proceedings of 1st Glocal Symposium on Information and Social Sciences (GSISS) 2023*, 102.

Veletsianos, G., Kimmons, R., & French, K. D. (2013). Instructor experiences with a social networking site in a higher education setting: Expectations, frustrations, appropriation, and

compartmentalization. *Educational Technology Research and Development*, *61*(2), 255 – 278. https://doi.org/10.1007/s11423-012-9284-z

Vera Navas, N. A. (2021). *Modelo de seguridad informática para riesgos de robo de información por el uso de las redes sociales*. http://dspace.ups.edu.ec/handle/123456789/20949

Wang, K., & Yu, X. (2021). Credibility of Browser Extension Program Based on Behavioral Statement. *2021 IEEE Asia-Pacific Conference on Image Processing, Electronics and Computers (IPEC)*, 333–336. https://doi.org/10.1109/IPEC51340.2021.9421124

Wang, X., Du, Y., Wang, C., Wang, Q., & Fang, L. (2022). WebEnclave: Protect Web Secrets From Browser Extensions With Software Enclave. *IEEE Transactions on Dependable and Secure Computing*, *19*(5), 3055–3070. https://doi.org/10.1109/TDSC.2021.3081867

Wu, M.-H., Yi, L., Chang, T.-C., Chen, Y., Dai, C., & Chen, S. (2022). Detection of Android Malware Behavior in Browser Downloads. *2022 IEEE 4th Eurasia Conference on Biomedical Engineering, Healthcare and Sustainability (ECBIOS)*, 163–166. https://doi.org/10.1109/ECBIOS54627.2022.9944991

Wu, X., Li, P., Zhao, M., Liu, Y., Crespo, R. G., & Herrera-Viedma, E. (2022). Customer churn prediction for web browsers. *Expert Systems with Applications*, *209*, 118177. https://doi.org/https://doi.org/10.1016/j.eswa.2022.118177

Wu, Z., & Weaver, A. C. (2007). Using web services to exchange security tokens for federated trust management. *Proceedings - 2007 IEEE International Conference on Web Services, ICWS 2007*, 1176–1178. https://doi.org/10.1109/ICWS.2007.185

Xu, Z., Zhou, X., Watts, J., & Kogut, A. (2023). The effect of student engagement strategies in online instruction for data management skills. *Education and Information Technologies*, *28*(8), 10267–10284. https://doi.org/10.1007/s10639-022-11572-w

Zhang, Y., Liu, W., Kuok, K., & Cheong, N. (2024). Anteater: Advanced Persistent Threat Detection With Program Network Traffic Behavior. *IEEE Access*, *12*, 8536–8551. https://doi.org/10.1109/ACCESS.2024.3349943

Zhao, R. (2023). FProbe: The Flow-Centric Detection and a Large-Scale Measurement of Browser Fingerprinting. *2023 32nd International Conference on Computer Communications and Networks (ICCCN)*, 1–10. https://doi.org/10.1109/ICCCN58024.2023.10230168