UNIVERSIDAD TECNICA DE BABAHOYO
FACULTAD DE ADMINISTRACION, FINANZAS E INFORMATICA
ESCUELA DE TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACION
CARRERA DE INGENIERIA EN SISTEMAS DE INFORMACIÓN

TEMA

ESTUDIO DE INTERFAZ DE PROGRAMACIÓN DE APLICACIONES (API), PARA LA AUTENTICACIÓN A TRAVÉS DE REDES SOCIALES PARA APLICACIONES MÓVILES. CASO DE ESTUDIO "GESTIÓN DE COMUNIDADES ACADÉMICAS Y RECREATIVAS DE LA UNIVERSIDAD TÉCNICA DE BABAHOYO"

AUTOR

HERRERA BARCOS RENE ALEJANDRO

TUTOR

Msc. HARRY ADOLFO SALTOS VITERI

Babahoyo – Los Ríos – Ecuador

PERIODO

ABRIL 2024 – AGOSTO 2024

Dedicatoria

A mis padres Rene Herrera Peñafiel y Rosa Barcos Arias, cuya constante guía y apoyo incondicional han sido la base de todas mis conquistas, a quienes, les debo más de lo que las palabras pueden expresar.

A mi hermano Javier Herrera Barcos, por ser mi compañero y fuente de inspiración a lo largo de este viaje académico, su ánimo y ejemplo han sido esenciales para mí.

A mis amigos Yefer Moran, Elías Orellana, Axel Luna, Adonis Almeida y Oscar Muñoz, con quienes hemos vivido tanto en nuestro tiempo como compañeros de clases, por su paciencia, comprensión y por estar siempre presentes, brindándome su apoyo en los momentos más desafiantes, sus palabras de aliento y compañía han sido invaluables.

Agradecimiento

A la Universidad Técnica de Babahoyo, por su invaluable apoyo y auspicio en la realización de este trabajo de investigación, este proyecto no habría sido posible sin el respaldo y los conocimientos proporcionados por esta institución.

Agradezco especialmente al MSc. Harry Saltos, mi tutor y guía durante este proceso investigativo, por su orientación experta, paciencia y dedicación. Sus consejos y conocimientos han sido fundamentales para el desarrollo y éxito de este estudio.

Finalmente, a todos los docentes que han dejado una huella imborrable en mi formación académica, les expreso mi sincero agradecimiento por compartir sus conocimientos y experiencias a lo largo de mi trayectoria universitaria, cada enseñanza recibida ha contribuido significativamente a mi crecimiento profesional y personal.

Informe Anti-plagio

CERTIFICADO DE ANÁLISIS
magister

Informe Final de Trabajo de Integración Curricular

6% Textos sospechosos

5% Similitudes
< 1% similitudes entre comillas
0% entre las fuentes mencionadas
< 1% Idiomas no reconocidos
1% Textos potencialmente generados por la IA

Nombre del documento: Informe Final de Trabajo de Integración Curricular_HerreraRene.docx
ID del documento: 0e7dae2e7e714378afc99388b576d400e1e8cbdf
Tamaño del documento original: 1,6 MB
Autor: Rene Herrera Barcos

Depositante: Rene Herrera Barcos
Fecha de depósito: 7/8/2024
Tipo de carga: url_submission
fecha de fin de análisis: 7/8/2024

Número de palabras: 11.410
Número de caracteres: 74.965

Ubicación de las similitudes en el documento:

Fuentes principales detectadas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	TRABAJO FINAL ANTIPLAGIO.docx | TRABAJO FINAL ANTIPLAGIO El documento proviene de mi grupo	1%		Palabras idénticas: 1% (133 palabras)
2	Luna-Alvarado-Antiplagio.docx | Luna-Alvarado-Antiplagio El documento proviene de mi grupo	1%		Palabras idénticas: 1% (131 palabras)
3	es.godaddy.com | ¿Qué es una app? Explorando las aplicaciones móviles https://es.godaddy.com/blog/que-es-una-app-y-para-que-se-utiliza/#:~:text=Utilizan los recursos del... 4 fuentes similares	1%		Palabras idénticas: 1% (126 palabras)
4	www.lifeder.com | Redes sociales: qué son, historia, características, para qué sirv... https://www.lifeder.com/redes-sociales/ 2 fuentes similares	< 1%		Palabras idénticas: < 1% (81 palabras)
5	www.google.com.ec | Google Books https://www.google.com.ec/books/edition/Primeros_pasos_con_Flutter_Ii_iOS_Windows/XgB8EAAAQ... 1 fuente similar	< 1%		Palabras idénticas: < 1% (81 palabras)

Fuentes con similitudes fortuitas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	dspace.utb.edu.ec http://dspace.utb.edu.ec/bitstream/49000/5428/6/P-UTB-FCJSE-ARTE-SECED-000138.pdf.txt	< 1%		Palabras idénticas: < 1% (22 palabras)
2	Documento de otro usuario El documento proviene de otro grupo	< 1%		Palabras idénticas: < 1% (11 palabras)
3	newformacion.com | Métodos de autenticación en redes: principales opciones y b... https://newformacion.com/seguridad-2/metodos-autenticacion-redes-opciones-beneficios/	< 1%		Palabras idénticas: < 1% (13 palabras)
4	dspace.utb.edu.ec http://dspace.utb.edu.ec/bitstream/handle/49000/14263/TIC-UTB-FAFI-SIST.INF-000006.pdf?sequen...	< 1%		Palabras idénticas: < 1% (11 palabras)
5	auth0.com | ¿Qué es OpenID Connect y para qué se utiliza? - Auth0 https://auth0.com/es/intro-to-iam/what-is-openid-connect-oidc#!	< 1%		Palabras idénticas: < 1% (10 palabras)

Índice General

Índice de tablas

Índice de ilustraciones

Resumen

La presente investigación se centra en el estudio y análisis de las APIs de autenticación a través de redes sociales para su integración en aplicaciones móviles, con un enfoque particular en el proyecto "Plataforma Tecnológica para la Gestión de Comunidades Académicas y Recreativas de la Universidad Técnica de Babahoyo"; el objetivo principal es realizar un estudio técnico alineado con la funcionalidad de APIs para que facilite los inicio de sesión de la gestión de Comunidades Académicas y Recreativas de la Universidad Técnica de Babahoyo con redes sociales, ayudando a mejorar la funcionalidad del sistema, para esto se empleará un tipo de investigación aplicada, adicional una investigación de campo y bibliográficas con un enfoque deductivo, cuantitativo y cualitativo para evaluar las diferentes alternativas de autenticación disponibles en el mercado. Dentro de la investigación la población objetivo incluye a un profesional en el área, que participará con lista de cotejos para una evaluación técnica, como también los estudiantes de la Universidad Técnica de Babahoyo, a los que se les encuestará para medir frecuencia de uso, facilidad de uso, seguridad, conveniencia, satisfacción, preferencias, y problemas encontrados y así asegurar que la integración de estas APIs no solo promete mejorar la seguridad y la experiencia de los usuarios, sino también aumentar la tasa de adopción de la plataforma al simplificar el proceso de registro y autenticación.

Palabras claves: APIs de autenticación, Redes sociales, Plataforma tecnológica, Universidad Técnica de Babahoyo, Desarrollo de software, Prototipo funciona y Gestión de comunidades académicas.

Abstract

This research focuses on the study and analysis of authentication APIs through social networks for integration into mobile applications, with a particular focus on the project "Technological Platform for the Management of Academic and Recreational Communities of the Technical University of Babahoyo"; the main objective is to conduct a technical study aligned with the functionality of APIs to facilitate logins for the management of Academic and Recreational Communities of the Technical University of Babahoyo with social networks, helping to improve the functionality of the system, for this we will use a type of applied research, additional field and bibliographic research with a deductive, quantitative and qualitative approach to evaluate the different authentication alternatives available in the market. Within the research the target population includes the developers of the seed project and professionals in the area, who will participate in structured interviews, as well as the students of the Technical University of Babahoyo, who will be surveyed to measure frequency of use, ease of use, security, convenience, satisfaction, preferences, and problems encountered and thus ensure that the integration of these APIs not only promises to improve security and user experience, but also to increase the adoption rate of the platform by simplifying the registration and authentication process.

Keywords: Authentication APIs, social media, Technological platform, Technical University of Babahoyo, Software development, Functional prototype and Academic community management.

CAPÍTULO I. - INTRODUCCIÓN.

1.1. Contextualización de la situación problemática

1.1.1. Contexto Internacional.

Según Colmenares (Colmenares, 2022), las APIs sirven como puente entre las aplicaciones, pero solo los desarrolladores de las aplicaciones pueden verlas, por esta razón es importante para el desarrollo web, porque simplifican la vida del usuario consumidor al ver información sin tener que ir directamente a la fuente, es por esto que cuando ingresas en algún sitio con tu cuenta ya sea de Facebook o Google, se debe tener en claro la importancia que genera tener bien integradas las interfaces de programación de aplicaciones (APIs) para la autenticación a través de redes sociales en los proyectos que se estén desarrollando, ya que tal y como nos lo hace saber en su artículo la empresa de (Cloudflare, 2024), nos dice que "la autenticación verifica que las solicitudes de la API que provienen de una fuente confiable y así el servidor puede saber si el cliente solicitante está autorizado a obtener los datos solicitados mediante la autorización.".

Uno de los casos de éxitos más conocidos lo presenta una de la red social más conocida a nivel mundial, (Facebook for Developers, s. f.) en su página oficial para desarrolladores Facebook nos da a conocer la historia de éxito de la plataforma de Pinterest, en la que gracias a la implementación del SDK del inicio de sesión de Facebook "Aumentó del 20 % en el número de usuarios que inician sesión con éxito en Pinterest con el inicio de sesión de Facebook después de introducir el inicio de sesión exprés" y en este mismo sitio se encuentra una cita textual del gerente de Ingeniería de Crecimiento, Pinterest (Brian Lee) quien nos dice que "Facebook proporcionó dos opciones rápidas y fluidas que mejoraron la experiencia de nuestros usuarios con dispositivos Android. Al iniciar sesión con Express Login o Custom Tabs para Android, nuestros

usuarios pueden iniciar sesión rápidamente en Pinterest con su cuenta de Facebook, lo que les permite volver a su contenido personalizado o a los Pines y tableros guardados con facilidad”

1.1.2 Contexto Nacional.

En las aplicaciones que tenemos en nuestro móvil integrando una autenticación por medio de APIs en redes sociales tanto en los que desarrollan y de las compañías locales es algo prometedor en su avance, haciendo posible que esta práctica a los usuarios le dé la facilidad de ingresar sesión o registrarse por medio de sus apps, usando su cuenta ya sea de Facebook, Twitter, entre otras.

Gracias a esta función no solo agiliza el proceso de ingreso a los usuarios, si no que puede ser una excelente experiencia debido a que el usuario puede descartar al crear una nueva contraseña y hacer uso de una sola.

Diferentes empresas hacen uso de esta nueva estrategia móvil, sobre todo en sectores que implique los servicios, tanto de transporte y comercio electrónico, adaptándose a esta tecnología facilitando el incorporo de usuarios nuevos y en la mejora de clientes retenidos

Empresas emergentes, especialmente en sectores como el comercio electrónico, transporte y servicios, están adoptando esta tecnología para facilitar la incorporación de nuevos usuarios y manteniendo a los clientes satisfechos, por ejemplo, aplicaciones locales como las mencionadas podrían beneficiarse significativamente al implementar un sistema de autenticación eficiente a través de redes sociales, lo que les permite captar un número mayor de usuarios de manera rápida y efectiva las cuales mencionando algunas pueden ser:

Buen Plan, tiene una variada lista de diferentes eventos culturales gracias a que es una plataforma que hace su venta en línea, ya sea de eventos familiares, deportivos, talle, seminarios

y entre otros más donde facilitan al usuario reconocer los próximos eventos cercanos. (Primicias, 2024)

Ktaxi, originaria de Loja es aquella aplicación móvil muy popular a nivel nacional e internacional en América Latina ofreciendo el servicio de un transporte de taxi seguro, enviar encomiendas y transportas mascotas. (Primicias, 2024)

No obstante, esta perspectiva no está fuera de dificultades, hay diversas preocupaciones debido a la privacidad de sus datos en los usuarios, hay muchas críticas debido a la poca seguridad ofrecida que debe ser abordada correctamente, los que desarrollen deben tener una adecuada implementación de prácticas en el gestiona miento de tokens tanto de acceso y de datos sensibles.

1.1.3. Contexto Local

Dentro del contexto local de la Universidad Técnica de Babahoyo en Ecuador, se podría explorar y estudiar cómo las APIs de autenticación a través de redes sociales podrían integrarse dentro de la plataforma tecnológica diseñada para la gestión de comunidades académicas y recreativas. De esta mismo manera se detectó que aún no han llevado a cabo el desarrollo de aplicaciones móviles dentro de la Universidad Técnica de Babahoyo que hagan el uso de las APIs de autenticación para tanto dar una mayor seguridad a sus usuario, como para tener una mayor actividad dentro de dichas aplicaciones, por esta razón el enfoque se centra en cómo estas tecnologías se pueden aprovechar para optimizar el acceso y la seguridad dentro de los aplicativos móviles que se pueden llevar a cabo en un futuro.

1.2. Situación problemática

El proyecto semillero “Plataforma tecnológica para la gestión de comunidades académicas y recreativas de la Universidad Técnica de Babahoyo” enfrenta desafíos problemáticos significativos en la implementación de APIs para la autenticación a través de redes sociales; los integrantes del proyecto han encontrado dificultades específicas en la integración de la autenticación multiplataforma debido a la falta de tiempo, capacitación insuficiente, y la implementación incorrecta de SDK de login solo en el Front-End, lo cual compromete la seguridad de la gestión de sesiones y tokens, de esa misma manera, la ausencia de una investigación profunda sobre las bibliotecas de autenticación y la documentación de los proveedores afecta negativamente la calidad y seguridad de la autenticación en la aplicación.

Estas complicaciones no solo retrasan el transcurso del proyecto, si no que de tal modo involucra su seguridad y operatividad de la plataforma, importante para gestionar de manera eficiente a los usuarios del sector académico.

El inconveniente se trata de que al incorporar APIs para autenticar por medio de redes sociales no se ha ejecutado en buenas prácticas, ni con fundamentos sólidos investigativos, lo que conlleva la utilidad y seguridad de la plataforma tecnológica que pertenece del proyecto semillero registrado en el periodo 2023-2024 destinado a la gestión de comunidades académicas y recreativas en la Universidad Técnica de Babahoyo.

En la presente indagación, se tratará en especial al desarrollar un prototipo de manera que al iniciar sesión en la plataforma tecnológica se utilizará APIs para autenticar mediante redes sociales. Por otra parte, optimizar la efectividad y seguridad, se analizará como se facilita integrando este modo de acceso, aumentando la selección de la plataforma por los usuarios.

1.2.1. Planteamiento del problema

¿Cómo desarrollar una interfaz de autenticación de autenticación a través de redes sociales que mejore la seguridad y la eficiencia en la gestión de comunidades académicas y recreativas en la plataforma tecnológica de la Universidad Técnica de Babahoyo?

1.2.2. Delimitación de la investigación

La investigación se llevará a cabo en la Universidad Técnica de Babahoyo, centrada en su plataforma tecnológica que está en su proceso de desarrollo y está destinada a la gestión de comunidades académicas y recreativas, de esta misma manera este estudio se enfocará en el periodo actual, para el estudio y pruebas de las APIs de autenticación, comprendido entre abril 2024 y agosto 2024.

La investigación involucrará tanto a los desarrolladores que están trabajando en la mencionada plataforma tecnológica, como a los estudiantes de la Universidad Técnica de Babahoyo, quienes serán el universo principal del estudio.

El contenido de la investigación abordará un estudio técnico alineado con la funcionalidad del inicio de sesión utilizando APIs de autenticación a través de redes sociales, por ende, se analizarán las buenas prácticas de integración y las medidas de seguridad necesarias para proteger los datos de los usuarios, con este enfoque se permitirá mejorar la experiencia de usuario y garantizar la protección de la información sensible en la plataforma de la Universidad Técnica de Babahoyo.

1.3. Justificación.

La investigación sobre la integración de APIs de autenticación mediante redes sociales en la plataforma tecnológica para la gestión de comunidades académicas y recreativas de la Universidad Técnica de Babahoyo presenta una relevancia tanto teórica como práctica, ya que desde la perspectiva teórica estudiar este problema permite avanzar en el conocimiento sobre el correcto desarrollo de tecnologías de autenticación en entornos educativos. Así mismo, es fundamental entender como aquellas APIs facilita la seguridad, ayudando a tener un proceso de rápido registro para el usuario en estas plataformas bajo el uso de apps móviles, colaborando en el desarrollo de buenas prácticas en tanto a la ciberseguridad y gestión de acceso digital.

Desde un punto de vista práctico investigativo, tratar estos retos favorecerá a los desarrolladores del proyecto semillero en la Universidad Técnica de Babahoyo, al suministrar un marco organizado para examinar y escoger las excelentes alternativas de integración de APIs, esto no solo perfeccionaría la evolución al ingresar a la plataforma, sino que además aseguraría una implementación segura.

Dentro del estudio de las APIs de autenticación a través de redes sociales resultan beneficiados varios actores, como pueden ser instituciones educativas quienes pueden hacer uso de mi investigación como material educativo que pueda utilizarse en las enseñanza de clases sobre APIs de autenticación a través de redes sociales, incluyendo el análisis de las alternativas disponibles, permitiendo mejorar la capacitación tanto de estudiantes como de personal académico en el manejo y aplicación práctica de estas tecnologías, asimismo, para universitarios de una carrera técnica como lo es una ingeniería de sistemas de información o desarrolladores que estén llevando a cabo un proyecto de desarrollo de una nueva aplicación móvil, estos podrían

podrán utilizar los resultados de este estudio para desarrollar soluciones similares en otros contextos, aprovechando las mejores prácticas identificadas y el marco comparativo desarrollado.

1.4. Objetivos de investigación.

1.4.1. Objetivo general.

Realizar un estudio técnico alineado con la funcionalidad de APIs para los inicios de sesión de la gestión de comunidades académico y recreativas de la Universidad Técnica de Babahoyo con redes sociales.

1.4.2. Objetivos específicos.

1. Analizar las APIs de autenticación de redes sociales más adecuadas para la plataforma tecnológica para la gestión de comunidades académico y recreativas de la Universidad Técnica de Babahoyo
2. Evaluar el rendimiento, seguridad y presupuesto del sistema de autenticación para la gestión de comunidades académico y recreativas de la Universidad Técnica de Babahoyo
3. Determinar la funcionalidad de aplicaciones móviles con la autenticación mediante APIs de redes sociales

1.5. Hipótesis.

La correcta estructuración de las Interfaces de Programación de Aplicaciones (APIs) para la autenticación a través de redes sociales, ayudará a mejorar la funcionalidad e integración de inicios de sesión con redes sociales en el contexto de la “gestión de comunidades académico y recreativas de la Universidad Técnica de Babahoyo”.

CAPÍTULO II. - MARCO TEÓRICO

2.1. Antecedentes.

A este trabajo de integración curricular, le antecede la tesis de grado con el tema de "Implementación de una aplicación para el Sistema de Seguimiento a Graduados basada en Moodle en la Universidad Politécnica Salesiana" hecho por el autor (Rendón Solano, 2018) se hace el uso del framework OAuth 2.0 con el que se le permitió la integración de redes sociales con la plataforma del Moodle de Universidad Politécnica Salesiana, haciendo uso de la API de Facebook y LinkedIn para llevar a cabo una autenticación a través de estas redes sociales, que según (diego.coder26, 2023) nos hace saber que "la autenticación básicamente es el proceso de verificación de una identidad. Una entidad puede ser un usuario, un servicio o un dispositivo. El objetivo principal de la autenticación es garantizar que la identidad es quien dice ser." Queriendo así cubrir parte de su problemática la cual era "la baja participación y compromiso de los graduados; y así, contar con un mayor número de interesados en el proceso, apoyándose en las Tecnologías de Información y Comunicación (TIC) para resolver una preocupación institucional." Llegando a una de sus conclusiones en la que menciona que a través de plugins, APIs y frameworks, se crea una plataforma adaptada a necesidades específicas, integrando sistemas existentes mediante estándares compatibles y aprovechando sus funcionalidades sin tener que desarrollar nuevos componentes.

Por otra parte, en la tesis de maestría registrada con el título "Desarrollo de una aplicación móvil con Flutter. Orientat" hecha por la autora (Pellicer de Juan, 2021) realiza la integración de la autenticación a través de redes sociales mediante la plataforma de firebase, esto ya que como

menciona en su documento que “se utilizó los servicios de autenticación de usuarios (Authentication), la base de datos en tiempo real para gestionar la información relativa a cada usuario (Cloud Firestore) y almacenamiento para administrar las imágenes de los usuarios (Storage) proporcionado por Firebase.” Dando como resultado no solo el inicio de sesión por medio tradicionales, sino también haciendo uso de los perfiles de otras plataformas como Google y Faceebook agilizándole el proceso de a los usuarios más reacios, y así mismo cumpliendo con los puntos de sus requisitos tantos funcionales como no funcionales, los cuales son por partes de los funcionales: permitir el registro y/o inicio de sesión de usuarios, compartir información en redes sociales. Por otro lado, los puntos de los requisitos no funcionales que la autenticación a través de redes sociales les permite son: garantizar el proceso de inicio de sesión seguro, conectar y consumir una API externa, y el más relevante según mi contexto de investigación el cual es implementar una aplicación multiplataforma.

2.2. Bases teóricas

Las interfaces de programación de aplicaciones (APIs) en los proyectos de software le permite al desarrollador que sus aplicaciones de software tengan comunicación entre estas mismas para que mediante estás le permita obtener datos, características y otras funcionalidades.(IBM, 2024), desde otra perspectiva más amplia (redhat, 2020) nos dice que “una API o interfaz de programación de aplicaciones es un conjunto de definiciones y protocolos que se usa para diseñar e integrar el software de las aplicaciones”, esto permitiendo que exista una comunicación con otros entre los productos o servicios que se ofrezcan, de esta misma manera las API son un medio agilizado para establecer una conexión en su propia infraestructura a través del desarrollo de aplicaciones en la nube.

Desde la perspectiva de (Amazon Web Services, Inc., 2024a) “las integraciones de las API son componentes de software que actualizan automáticamente los datos entre los clientes y los servidores”, esta plataforma nos habla también que la utilización de las APIs trae sus beneficios en 4 puntos a tomar en cuenta, los cuales son:

1. Integración

   Esto ya que las APIs al integrarse en nuevas aplicaciones con software ya existentes aumenta la velocidad de su desarrollo ya que, si se necesita una funcionalidad no se debe hacer desde 0, sino que se puede aprovechar el código ya existente

2. Innovación

   Como sabemos todas las empresas deben responder de manera rápida conforme avancen estás tecnologías para ofrecer nuevos servicios en sus aplicaciones, esto se ve simplificado al utilizar las APIs ya que se pueden realizar hacer cambios sin tener que reescribir todo el código.

3. Ampliación

   Conforme exista una innovación, se pueden ampliar los servicios que la empresa desea ofrecer para satisfacer nuevas necesidades, las APIs permiten que estas empresas puedan ofrecer estos nuevos servicios debido a que presentan una oportunidad única al dar un acceso a bases de datos cargadas de información

4. Facilidad de mantenimiento

   Como ya se ha hablado las APIs son un puente entre dos sistemas, con el pasar del tiempo, los sistemas siempre se ven obligados a tener cambios internos,

pero al utilizar las APIs, no importa el cambio que se haga en las partes del código, estas nunca se verás afectadas.

Teniendo muy claro tanto el concepto de lo que es una API más los beneficios que estás pueden ofrecer, estás investigación se enfocarás en aquellas APIs las cuales sirven para la autenticación a través de redes sociales.

Para (Jain et al., 2021) la perspectiva que tiene con referente a las APIs de autenticación es que son fundamentales para garantizar que solo usuarios legítimos accedan a las redes sociales y no bots, gracias a la integración de esta autenticación se pueden aplicar procedimientos como como CAPTCHA y autenticación de dos factores, esto ayuda a mitigar el riesgo de que una cuenta sea comprometida y evitan que un atacante secuestre una cuenta legítima para publicar contenido malicioso.

Desde el punto de vista de (Newberry, 2023) en su artículo nos hace saber que estas APIs de redes sociales les brinda a los desarrolladores externos acceso a ciertos tipos de datos que las herramientas relacionadas con las redes sociales requieren para funcionar, básicamente esto es un fragmento de código que permite que las redes sociales se integren con aplicaciones y herramientas de terceros, igualmente (Oracle, s. f.) nos dice que estas APIs nos ayuda con la verificación de las credenciales que utilizaría usuario y contraseña de quienes inicien sesión como método de autenticación principal.

Sin embargo, en el contexto de la autenticación a través de redes sociales las credenciales que se utilizarían para llevar a cabo el registro de los usuarios, es mediante sus cuentas de redes sociales como, por ejemplo lo son Facebook, X (Twitter), LinkedIn, TikTok o Google, que tienen

ya desarrollados sus propios SDK, con la posibilidad de acceder a sus APIs de autenticación, en el caso de Facebook, la página oficial nos informa que el inicio de sesión con Facebook es un modo rápido y cómodo de crear cuentas e iniciar sesión en tu app en diversas plataformas, esta tecnología está disponible en iOS, Android, Web, apps para computadoras, dispositivos como Smart TV y objetos de Internet de las cosas, este inicio de sesión con Facebook contempla dos escenarios posibles: la autenticación y la solicitud de permisos para acceder a los datos de los usuarios, puedes usar el inicio de sesión con Facebook solo para autenticación o para autenticación y acceso a datos. (Facebook, s. f.)

De esta misma manera Google nos da a conocer que el uso de su servicio de autenticación para acceder con a otras aplicaciones, ayuda a administrar rápidamente la autenticación de usuarios en sitios web o aplicaciones móviles, teniendo en cuenta que los usuarios que utilizan sus Cuentas de Google, dan su consentimiento y comparten la información de su perfil de forma segura con las demás plataformas.

El registro se refiere a los pasos para obtener el consentimiento del titular de una Cuenta de Google para compartir su información de perfil con tu plataforma, por lo general, se crea una cuenta nueva en tu sitio con estos datos compartidos, pero no es un requisito. (Google for Developers, s. f.).

Pero hay que entender que ambas redes sociales son proveedores de sus propios SDK que incluye la autenticación en la misma al igul que las demás redes sociales.

Un SDK desde el punto de vista de (Amazon Web Services, Inc., s. f.-a) es un kit de desarrollo de software (SDK) está es un instrumento de código para desarrolladores utilizado para la creación de nuevas plataformas, para que dicho código se integre dentro de las plataformas que

se estén desarrollando se necesitan componentes como depuradores, compiladores y bibliotecas para lograr que ese bloque de código se pueda ejecutar sin problemas en cualquier sistema operativo o lenguaje de programación específicos.

Por otra parte, en este proyecto de investigación, al realizar un marco comparativo también se tendrá en cuenta los servicios que ofrecen librerías que permiten realizar la integración de la autenticación a través de redes sociales.

Una de las alternativas de estos servicios es OAuth2.0, que en su misma plataforma nos hace saber que se trata de un protocolo de autorización y que más no de un protocolo de autenticación, el objetivo principal de este servicio es que funciona como un medio para otorgar un acceso a varios recursos.

Auth 2.0 hace uso de los tokens de acceso, esto básicamente es un dato que plasma la autorización para que en nombre de un usuario final pueda acceder a los recursos. Un punto a resaltar es que no tiene definido un formato para los tokens de acceso. Si bien, en algunas circunstancias, se puede utilizar el formato JSON Web Token (JWT), lo que esto permite es que aquellos emisores de tokens puedan incluir datos específicos en token, por otro lado, por cuestiones de protección a los usuarios con la integración de seguridad, los tokens de acceso incluso pueden incluir una fecha de caducidad. (Auth0, s. f.-a)

Un Tokens de Acceso para (Fortinet, 2024) es un Token de autenticación con el cual los usuarios pueden acceder a sus apps o servicios sin la necesidad de tener que ingresar las credenciales de inicio de sesión por cada vez que lo visitan, por lo que, podemos decir que ese token tiene el objetivo de hacerle más fácil el acceso a páginas y recursos protegidos a los

usuarios durante un período sin tener que volver a ingresar sus credenciales (nombre de usuario y contraseña).

En cambio, para (Google Cloud, s. f.) en el contexto de la autenticación a través de Google nos dice que los tokens de acceso son tokens opacos que se ajustan al framework de OAuth 2.0. Contienen información de autorización, pero no información de identidad. Se usan para autenticar y proporcionar información de autorización a las APIs de Google.

Si se usa credenciales predeterminadas de la aplicación (ADC) y las bibliotecas cliente de Cloud o las bibliotecas cliente de las APIs de Google, no es necesario que se administren los tokens de acceso, las bibliotecas recuperan la credencial de forma automática, lo intercambian por un token de acceso y lo actualizan según sea necesario.

Otra de las alternativas que se evaluará es OpenId que según (Owen, 2024) OpenID Connect (OIDC) se lo podría tomar como una variante alternativa del protocolo de autorización OAuth 2.0 ya que este servicio trabaja bajo la misma compañía y OpenId es un proyecto que nace a raíz de este protocolo, OpenId permite habilitar un inicio de sesión único entre las aplicaciones habilitadas para OAuth mediante un token de seguridad llamado también como token de identificador, al estar construido sobre OAuth 2.0, OpenID Connect utiliza tokens que le da una capa de identidad sencilla integrada con la autorización subyacente.

Haciendo mención a una alternativa más como lo es Firebase, (Agreda, 2023) nos hablas de que Firebase es una plataforma de desarrollo de aplicaciones móviles de Google, sus ventajas incluyen un entorno de desarrollo integral, un menor tiempo de comercialización para crear aplicaciones e infraestructura ampliable, así que Firebase es una plataforma backend para crear aplicaciones web y móviles.

Las funciones principales de Firebase incluyen gestión de bases de datos, almacenamiento de archivos, código en la nube, análisis, alojamiento escalable, APIs de autenticación y aprendizaje automático; dado que los servicios están alojados en la nube, los desarrolladores pueden realizar ampliaciones a demanda casi sin codificación de backend.

También hay que tener en cuenta el con concepto de lo que es una red social, (Lifeder, 2021) en su artículo sobre las redes sociales designa a los diferentes medios de comunicación que se basan en la internet y en diversidad de dispositivos (teléfonos inteligentes, laptops, computadores de escritorio o tablets) para facilitar el intercambio de imágenes, textos, vídeo y sonido entre usuarios de todo el mundo, el objetivo principal de una red social es que las personas se conecten entre sí de manera libre e inmediata y sin otras limitaciones más allá de contratar un servicio de internet y poseer un dispositivo adecuado.

De esta misma manera hay que tener en claro lo que es una aplicación móvil, que en el artículo escrito por (Calvo, 2023) menciona que una app es una aplicación de software diseñada para funcionar en dispositivos móviles, como smartphones y tabletas. El término app proviene de la palabra inglesa aplicación, estas aplicaciones pueden servir para múltiples propósitos, ya sea para trabajo, ocio o entretenimiento, yendo desde plataformas de redes sociales hasta herramientas de productividad o juegos.

A diferencia de las webapps, que son accesos directos a páginas web y no requieren de instalación alguna, las apps se instalan en el dispositivo, su popularidad se disparó tras el lanzamiento de tiendas de aplicaciones como la App Store de Apple y el Android Market (ahora Google Play) en 2008, convirtiéndose en un término cotidiano y en un tipo de software con el que la gran mayoría de la población interactúa a diario.

Para llevar a cabo un estudio técnico alineado con la funcionalidad de APIs para el inicio de sesión utlizaré las herramientas más adecuadas conforme se estén utilizado dentro del proyecto con el tema “gestión de comunidades académicas y recreativas de la universidad técnica de babahoyo” para poder armar un entorno de desarrollo controlado de la aplicación desde el lado del front-end que para (Pérez Ibarra et al., 2021) “el FrontEnd es responsable de la interfaz visual, que permite que los usuarios interactúen con nuestro sitio o sistema. Está enfocado en el lenguaje de programación web de ejecución de marcas y clientes”, se usará tanto Visual Studio Code que según (Gamarra, 2024), Visual Studio Code, es un editor de código fuente gratuito y de código abierto desarrollado por Microsoft, siendo este uno de los más populares entre los desarrolladores debido a su capacidad para soportar múltiples lenguajes de programación y sistemas operativos, y a su amplia gama de extensiones, que permiten personalizar las experiencias de desarrollo.

De igual modo también ser hará uso de una herramienta como lo es Android Studio para llevar a cabo la emulación de la aplicación y poder ver los cambios en tiempo real, que bajo el concepto de la página oficial de esta herramienta nos hace saber que, Android Studio en si es un entorno de desarrollo integrado (IDE) que básicamente es una herramienta que sirve para el desarrollo de apps para Android creado y distribuido por Google. Un IDE contiene herramientas que permiten a los desarrolladores de software diseñar, compilar, ejecutar y probar software. En este caso, apps para la plataforma de Android. (Google Developers, 2024).

Desde el lado del Back-End, que para (Pérez Ibarra et al., 2021) el backend se encarga de la manipulación de datos, por lo que no es útil si no hay un frontend de por medio. El desarrollador del backend debe estar familiarizado con bases de datos, marcos y aspectos de seguridad. Él debe estar a cargo de almacenar los datos que llegan desde el FrontEnd en una base

de datos, basado en esa observación se usará una herramienta que es totalmente compatible con el front-end.

La herramienta de IntelliJ, la cual destaca por ser una herramienta integral y altamente personalizable que ha demostrado su eficacia en el desarrollo de aplicaciones java y otros lenguajes. Ofrece una interfaz de usuario muy intuitiva y amigable, lo que facilita la navegación y utilización de sus diversas características. (Martínez Ibáñez, 2024)

Una vez estando bien establecidas las herramientas de editor de código tanto para el back-end, como para el front-end, se establecerá igualmente los frameworks como los lenguajes de programación que se están usando dentro del contexto del proyecto al que se enfoca esta investigación.

Tal y como no los hace saber (Juan de Assembler Institute, 2022), un framework es un marco de trabajo diseñado para facilitar la solución de problemas que pueden surgir al programar. Los marcos facilitan tareas como la organización del código o el trabajo en equipo dentro de un proyecto, lo que acelera el proceso de programación.

Reforzando este conocimiento la revista (UNIR FP, s. f.) nos habla de que un framework se lo puede considerar como un marco de trabajo que ofrece una estructura con la que se puede elaborar un proyecto cuando se tiene objetivos específicos, en otras palabras, se trata como de una especie de plantilla que se la puede tomar como punto de partida para la organización y desarrollo de programas y aplicaciones, mayormente, los frameworks son usados por programadores ya que estos les permite acelerar su trabajo y además favorece que este sea colaborativo, lo que ayuda a reducir errores y obtener más calidad en su resultado.

Asimismo, (Carla et al., 2021) nos habla sobre los lenguajes de programación como herramientas esenciales para llegar a cabo la solución de problemas en las diversas áreas de la Ciencia y la Ingeniería, este concepto apunta a que la metodología que se emplea para la resolución de una variedad de problemas matemáticos consiste en plantear un algoritmo, para luego programarlo en el lenguaje de programación que se escoja y así ejecutar el programa desde un ordenador.

El framework del lado del front-end con el que se está trabajando dentro del proyecto es Flutter., para (Amazon Web Services, Inc., 2024b) Flutter es un marco open source (recursos abiertos) desarrollado por Google lo que lo hace totalmente compatible con muchos de sus servicios. Flutter se lo utiliza en su mayoría de veces para crear interfaces de usuario (IU) en varias plataformas con un único código base, es de destacar también que actualmente es compatible con el desarrollo de aplicaciones en plataformas como: iOS, Android, web, Windows, MacOS y Linux.

Agregando un opinión más empírico para (Cruz, 2022) Flutter es la herramienta del momento cuando se trata en crear aplicaciones móviles para Android e iOS; y esto, no se trata de una moda ni nada que se le aparezca; su sintaxis limpia y expresiva con Dart, su programación declarativa con los widgets y otras características como el Hot Reload, lo convierten en una interesante solución para crear aplicaciones nativas para Android e iOS y que pocas herramientas que ofrecen también soluciones para crear aplicaciones móviles, se les puede comparar.

Ahora por parte del Back-end se hará uso del famoso framework basado en java el cual es Spring Boot, para situarnos en el contexto que se basa este framework se hablará primero de Java, que Java es un lenguaje de programación popular para crear aplicaciones web. Con millones de aplicaciones Java disponibles en la actualidad, Java dentro de la comunidad de

desarrolladoras ha sido popular por más de dos décadas. Java es un lenguaje orientado a objetos, centrado en la red y multiplataforma que funciona como una plataforma. Es un lenguaje de programación confiable, rápido y seguro para codificar todo, desde software empresarial y aplicaciones móviles hasta aplicaciones de macrodatos y tecnologías de servidores.(Amazon Web Services, Inc., s. f.-b)

De aquí parte el framework que usará, por lo que podemos decir de Spring Boot bajo el concepto de (Microsoft Azure, s. f.), es que es una herramienta de código abierto que facilita la creación de microservicios y aplicaciones web utilizando un marco basado en Java. Cualquier definición de Spring Boot debería iniciar la conversación con Java, uno de los lenguajes de desarrollo y plataformas informáticas más populares y utilizados para el desarrollo de aplicaciones, desarrolladores de todo el mundo se están iniciando en el mundo de la codificación aprendiendo Java. Flexible y fácil de usar, Java es uno de los favoritos entre los desarrolladores de una variedad de aplicaciones, desde redes sociales, Internet y juegos hasta aplicaciones empresariales y web.

CAPÍTULO III. - METODOLOGÍA DE LA INVESTIGACIÓN.

3.1. Tipo y diseño de investigación.

Según el propósito:

Investigación Aplicada

La investigación aplicada se utilizará para llevar a cabo un estudio técnico sobre la funcionalidad de las Interfaces de Programación de Aplicaciones (API) para la autenticación a

través de las redes sociales en aplicaciones móviles y con esta poder realizar pruebas de integración de las APIs en un entorno de desarrollo controlado.

Según el lugar:

Investigación de campo

Se hará uso de esta investigación ya que se llevará una entrevista con los encargados del desarrollo de la plataforma para la gestión de las comunidades académicas y recreativas, permitiendo la obtención de información relevante de una manera directa y detallada de los aspectos que se deberían tener cuenta para la integración de APIs de autenticación.

Investigación bibliográfica

Debido a que el tema de este proyecto trata de un estudio de las Interfaz de Programación de Aplicaciones (API), para la autenticación a través de redes sociales para aplicaciones móviles, se realizará una exhaustiva revisión de la documentación y estudios previos relacionados con las APIs de autenticación a través de redes sociales, esto llegaría a incluir artículos académicos, informes técnicos y documentación de los proveedores, con el objetivo de identificar y comparar las alternativas que se encuentran en el mercado.

3.1.1 Método de investigación

Método deductivo

Se empleará el método deductivo para estructurar una base teórica sobre las APIs de autenticación a través de redes sociales y su aplicabilidad general, a partir de esto se validará la hipótesis que una correcta estructuración mejorará la funcionalidad de los inicios de sesión en la

plataforma de la Universidad Técnica de Babahoyo, permitiendo evaluar las diferentes alternativas de APIs que se encuentran en el mercado y determinar su impacto en este contexto de la Universidad.

Método cuantitativo

El método cuantitativo se aplicará mediante una encuesta dirigida a estudiantes de la Universidad Técnica de Babahoyo, con el objetivo de recopilar datos numéricos sobre la percepción que ellos tienen y experiencia con las APIs de autenticación en aplicaciones móviles, incluido a esto también se utilizará una lista de cotejos para que profesionales en el área hagan una evaluación objetivamente de la funcionalidad de las APIs seleccionadas en el contexto específico de la gestión de comunidades académicas y recreativas.

3.2. Operacionalización de variables.

Variable Independiente

La interfaz de programación de aplicaciones (API), para la autenticación a través de redes sociales para aplicaciones móviles.

Variable Dependiente

Proceso de autenticación en aplicaciones móviles

Tabla 1
Operacionalización de las variables

Variables	**Definición Conceptual**	**Dimensiones**	**Indicadores**	**Ítem / Instrumento**

V. Independiente: La interfaz de programación de aplicaciones (API), para la autenticación a través de redes sociales para aplicaciones móviles.	Conjunto de métodos y herramientas proporcionadas por plataformas de redes sociales para permitir a los usuarios autenticarse en aplicaciones de terceros.	-Selección de APIs -Integración de APIs -Documentación -Costo -Flexibilidad -Escalabilidad	-Cantidad de APIs disponibles -Permite acceso a documentación de las APIs -Precio de uso de la API -Posibilidad de personalización Cantidad de manejo de usuarios	-Marco comparativo -Análisis documental -Encuesta
V. Dependiente: Proceso de autenticación en aplicaciones móviles	El proceso de autenticación en aplicaciones móviles es un mecanismo mediante el cual se verifica la identidad de un usuario antes de permitirle acceso a una aplicación o a sus funcionalidades.	-Funcionalidad -Seguridad -Compatibilidad -Eficiencia	-Número de protocolos de seguridad implementados -Compatibilidad con diferentes plataformas -Tiempo de respuesta y rendimiento -Cantidad de vulnerabilidades	-Lista de cotejo, pruebas funcionales -Lista de cotejo, pruebas de seguridad -Pruebas de rendimiento

Notas. En esta tabla está establecido la Variable dependiente e independiente con sus definiciones, dimensiones, indicadores e instrumentos

3.3. Población y muestra de investigación.

3.3.1. Población.

La población objetivo de esta investigación está compuesta por los 12,221 estudiantes matriculados en la Universidad Técnica de Babahoyo en el periodo 2023-2024, este grupo representa el foco principal para evaluar la viabilidad y aceptación de las APIs de autenticación a través de redes sociales en aplicaciones móviles, dentro del contexto de la gestión de comunidades académicas y recreativas, adicional a esta población objetivo se tendrán en cuenta a los 6 miembros del equipo de desarrollo y a los profesionales en el área.

3.3.2. Muestra.

Muestreo Aleatorio Simple para realizar la encuesta a los estudiantes de la Universidad Técnica de Babahoyo.

Fórmula para el muestreo de poblaciones finitas.

$$n = \frac{Z^2 * N * p * q}{e^2 * (N-1) + Z^2 * p * q}$$

Donde:

Z= Nivel de confianza, corresponde a la tabla de valores de Z

p= % de la población que tiene la particularidad deseada.

q= % de la población que no tiene la particularidad deseada. (1-p). cuando no especifican la población que posee, se asume 50% para p y 50% para q.

N= Tamaña del universo, es conocido debido a que es finito.

e= Error de estimación máximo aceptado.

n= Tamaño de la muestra.

Aplicado quedaría:

Z= Se optará por un nivel de confianza 1,96

N= El universo en este caso es de 12221

e= Margen de error del 5%

p= % de la población que tiene la particularidad deseada .92%

q= % de la población que no tiene la particularidad deseada. 8%

Cálculo:

$$n = \frac{3{,}84 * 12221 * 92\% * 8\%}{0{,}003\% * (12221 - 1) + (3{,}84 * \ 92\% \ * \ \ 8\%)}$$

$$n = 112,\ 07$$

3.4. Técnicas e instrumentos de medición.

3.4.1. Técnicas

Encuesta

Se realizará una encuesta utilizando la escala de Likert para recopilar información de los estudiantes de la Universidad Técnica de Babahoyo, con el objetivo de tener una comprensión detallada sobre la percepción y experiencia de los estudiantes en relación con las APIs de autenticación en las aplicaciones móviles.

3.4.2. Instrumentos

Cuestionario de encuesta

Se realizará un cuestionario de preguntas que permita obtener la información pertinente que se desea obtener de los estudiantes.

Cuadro comparativo

Se realizará un marco comparativo para así determinar cuáles de las alternativas para la autenticación a través de redes sociales existen en el mercado son las más apropiadas para la plataforma tecnológica para la gestión de comunidades académicas y recreativas de la Universidad Técnica de Babahoyo.

Lista de Cotejo

Este instrumento tendrá sus indicadores para que los profesionales en el área puedan hacer una correcta evaluación de cómo están integradas las APIs dentro del proyecto y así tener una opinión objetiva de las carencias del inicio de sesión de la aplicación.

3.5. Procesamiento de datos.

Como herramienta principal se hará el uso de SPSS para el procesamiento de los datos recopilados durante esta investigación, se utilizará el software estadístico SPSS (Statistical Package for the Social Sciences), esta herramienta permitirá realizar un análisis exhaustivo de los datos obtenidos a través de las encuestas aplicadas a los estudiantes de la Universidad Técnica de Babahoyo, así como de las entrevistas a los integrantes del proyecto y las evaluaciones realizadas por los profesionales en el área.

3.6. Aspectos éticos.

El presente proyecto de integración curricular se basa en la consideración de los aspectos éticos fundamentales, buscando la seguridad a la identidad de cada uno de los estudiantes que muestren interés en usar la aplicación móvil, ofreciendo la protección de sus datos personales mediante prácticas de privacidad y confidencialidad adecuadas, por otra parte, el proyecto está diseñado para promover un uso responsable de las tecnologías de autenticación a través de redes sociales, para que así el resultado final no comprometa la seguridad ni la integridad de los usuarios finales.

CAPÍTULO IV.- RESULTADOS Y DISCUSIÓN.

4.1. Resultados

4.1.1 Marco comparativo.

Tabla 2
Marco comparativo entre las opciones de autenticación

Indicador	**Facebook SDK**	**Google SDK**	**OAuth2.0**	**OpenID Connect**	**Firebase**
Facilidad de Implementación	Provee SDKs bien documentados para múltiples plataformas y lenguajes. La integración es rápida y sencilla gracias a las guías	Similar a Facebook, Google proporciona documentación extensa y ejemplos prácticos. La	Requiere una comprensión más profunda de los flujos de autorización y manejo de tokens. Aunque es	Más sencillo que OAuth2.0, ya que está diseñado específicamente para autenticación. Sin	Firebase proporciona una amplia documentación, ejemplos claros y herramientas de integración

	paso a paso y ejemplos disponibles. Además, la comunidad de desarrolladores es grande, lo que facilita la resolución de problemas (Kong Inc.) (Rafael Neto).	integración es fluida, especialmente si ya se utilizan otros servicios de Google. La documentación y soporte de la comunidad son excelentes (Kong Inc.) (Rafael Neto).	muy flexible, puede ser complejo de implementar correctamente si no se tiene experiencia previa con el protocolo OAuth (Rafael Neto).	embargo, aún requiere conocimientos sobre flujos de autenticación y configuración de servidores (Rafael Neto).	que facilitan el uso de múltiples proveedores de autenticación. Además, cuenta con un fuerte soporte de la comunidad y recursos educativos (Kong Inc.).
Indicador	Facebook SDK	Google SDK	OAuth2.0	OpenID Connect	Firebase
Compatibilidad y Multiplataforma	Compatible con aplicaciones web, Android, iOS y más. Los SDKs están diseñados para funcionar en diversas plataformas, lo que facilita el desarrollo	Soporte amplio para aplicaciones web, Android, iOS y otros dispositivos. La integración con otros	Implementaciones disponibles para casi cualquier plataforma, pero puede requerir más trabajo para integrarse	Basado en OAuth2.0, lo que garantiza una amplia compatibilidad con diversas plataformas y servicios.	Extensa compatibilidad con plataformas móviles y web. Firebase también facilita la integración

	multiplataforma (Kong Inc.) (Rafael Neto).	servicios de Google, como Google Cloud, es sencilla y efectiva (Kong Inc.) (Rafael Neto).	perfectamente con sistemas existentes (Rafael Neto).	Es una opción estándar en la industria para autenticación segura (Rafael Neto).	con otros servicios de Google y proveedores externos, permitiendo una solución robusta y completa (Kong Inc.)

.

Indicador	Facebook SDK	Google SDK	OAuth2.0	OpenID Connect	Firebase
Seguridad y Privacidad	Facebook implementa altas medidas de seguridad y privacidad, incluyendo la autenticación de dos factores y monitoreo de amenazas, pero la centralización de datos en Facebook puede ser una preocupación para algunos usuarios. (Kong Inc.) (Rafael Neto).	Google ofrece altos estándares de seguridad y privacidad, incluyendo protección contra amenazas y la gestión de datos está sujeta a las políticas de privacidad de Google (Kong Inc.) (Rafael Neto).	La seguridad es configurable, pero requiere una implementación cuidadosa para evitar vulnerabilidades, lo que deja una brecha de peligro en la autenticación, aunque OAuth ofrece flujos seguros como Authorization Code Flow para protección contra ataques no deseados. (Rafael Neto).	Añade una capa de autenticación a OAuth2.0, proporcionando una seguridad adicional mediante sus tokens de identificación y autenticación de usuario, esto es ideal para aplicaciones que necesitan una autenticación fuerte y segura (Rafael Neto).	Integra medidas de seguridad modernas y estándares como OAuth2.0 y OpenID Connect, esta herramienta proporciona opciones como verificación por email y número de teléfono para la autenticación en caso de un intento de robo de identidad, y monitorización de amenazas en tiempo real. (Kong Inc.).

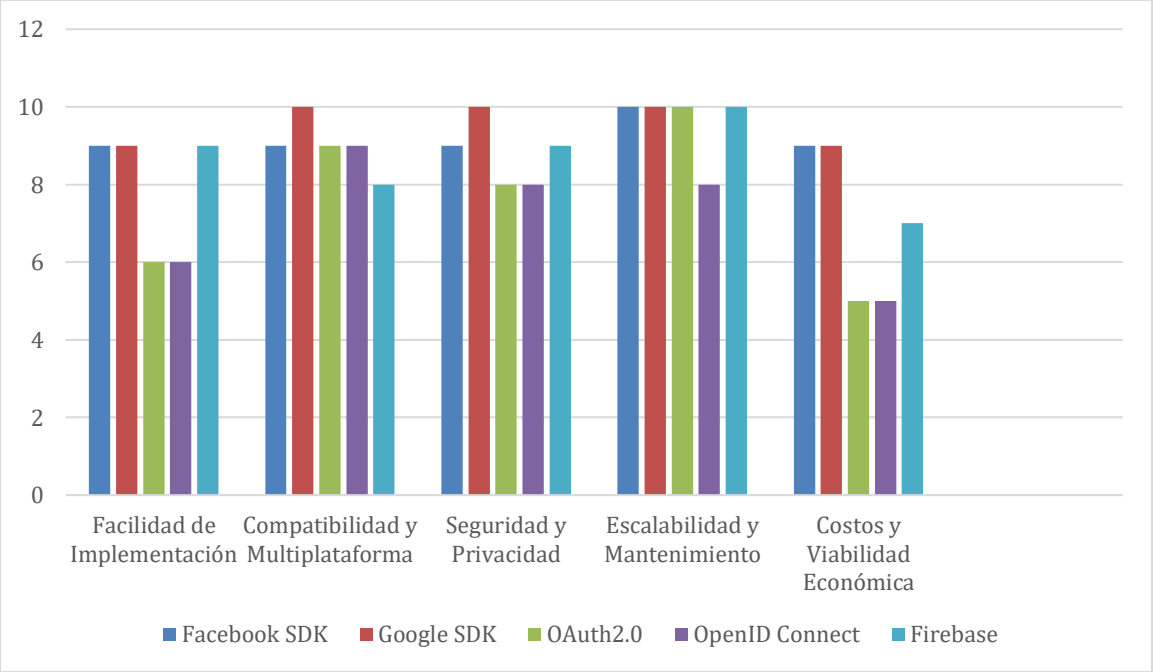
Indicador	Facebook SDK	Google SDK	OAuth2.0	OpenID Connect	Firebase
Escalabilidad y Mantenimiento	Infraestructura robusta y soporte continuo de Facebook. Permite manejar grandes volúmenes de usuarios y solicitudes sin problemas, aunque puede ser dependiente de cambios en la API de Facebook (Kong Inc.) (Rafael Neto).	Infraestructura global y soporte de Google. Escalable a nivel mundial, ideal para aplicaciones con una gran base de usuarios. El mantenimiento es sencillo gracias a las actualizaciones y soporte de Google (Kong Inc.) (Rafael Neto).	Muy escalable, pero requiere mantenimiento constante para asegurar su correcto funcionamiento y seguridad. Ideal para aplicaciones que necesitan control detallado sobre la autenticación (Rafael Neto).	Extensión de OAuth2.0, con beneficios similares en escalabilidad. Requiere un mantenimiento similar al de OAuth2.0, pero con una configuración inicial más sencilla (Rafael Neto).	Respaldado por la infraestructura de Google, con escalabilidad integrada. Permite manejar un gran número de usuarios sin problemas y facilita el mantenimiento a través de actualizaciones regulares (Kong Inc.).

Indicador	Facebook SDK	Google SDK	OAuth2.0	OpenID Connect	Firebase
Costos y Viabilidad Económica	Gratuito con limitaciones, y opciones de pago para funciones avanzadas. Los costos pueden aumentar si se utilizan características adicionales o servicios de análisis de datos (Kong Inc.) (Rafael Neto).	Similar a Facebook, con una estructura de costos que depende del uso y las características avanzadas. Los servicios básicos suelen ser gratuitos, pero las funcionalidades avanzadas tienen un costo (Kong Inc.) (Rafael Neto).	Generalmente gratuito, pero puede tener costos asociados a la infraestructura necesaria para su implementación y mantenimiento. Es una opción económica si se tiene el conocimiento técnico necesario (Rafael Neto).	Similar a OAuth2.0, con costos mínimos asociados a la implementación inicial. La infraestructura adicional puede incrementar los costos, pero sigue siendo una opción económica para muchas aplicaciones (Rafael Neto).	Ofrece un nivel gratuito generoso, pero puede tener costos adicionales para características avanzadas y uso intensivo. Es una opción viable económicamente para aplicaciones de cualquier tamaño (Kong Inc.).

Nota: Este es un marco comparativo entre las opciones de autenticación tanto de las APIs dadas directamente por los proveedores, como otras opciones en el mercado que ofrecen estas APIs como servicios.

Ilustración 1

Gráfico comparativo



Los SDKs de proveedores como Facebook y Google, así como Firebase, presentan una alta facilidad de implementación, compatibilidad y soporte multiplataforma, respaldados por una robusta infraestructura de seguridad y escalabilidad, estos SDKs son normalmente los más adecuados para desarrolladores que buscan una solución rápida, eficiente y segura para implementar autenticación en sus aplicaciones, la documentación extensa, el soporte de la comunidad y que son de código abierto, son ventajas significativas que facilitan la resolución de problemas y la implementación de características avanzadas.

OAuth2.0 y OpenID Connect, siendo estándares abiertos, permiten una mayor flexibilidad y personalización, estos protocolos son ideales para desarrolladores que buscan controlar detalladamente los flujos de autenticación y autorización y que pueden gestionar la infraestructura necesaria para soportarlos, aunque requieren una mayor comprensión y

configuración, ofrecen un alto nivel de seguridad y compatibilidad con diversas plataformas, pero de no configurarse bien deja una gran vulnerabilidad dentro de las aplicaciones que usen estas alternativas, por otro lado, estos servicios si bien ofrecen una mejor gestión de las autenticaciones por parte de los usuarios, hay que tener en consideración cuales son los precios que hay que pagar para obtener esos beneficios.

Para la mayoría de los proyectos, los SDKs de proveedores específicos como Facebook, Google, entre otras alternativas como Mircrosoft, son la mejor opción, principalmente debido a su facilidad de uso, las potentes herramientas y soporte que ofrecen, esto los hace especialmente adecuados para desarrolladores que buscan una solución rápida, eficiente y segura para implementar autenticación en sus aplicaciones o programas y aunque OAuth2.0 y OpenID Connect requieren un control más detallado y personalizado, siguen siendo opciones muy potentes y flexibles, pero siempre hay que tener en consideración el plan de pago que se elija según las necesidades del proyecto.

4.1.2 Resultados de la encuesta a los Estudiantes de la Universidad Técnica de Babahoyo

1. ¿Con qué frecuencia utiliza la autenticación a través de redes sociales para acceder a aplicaciones?

Tabla 3

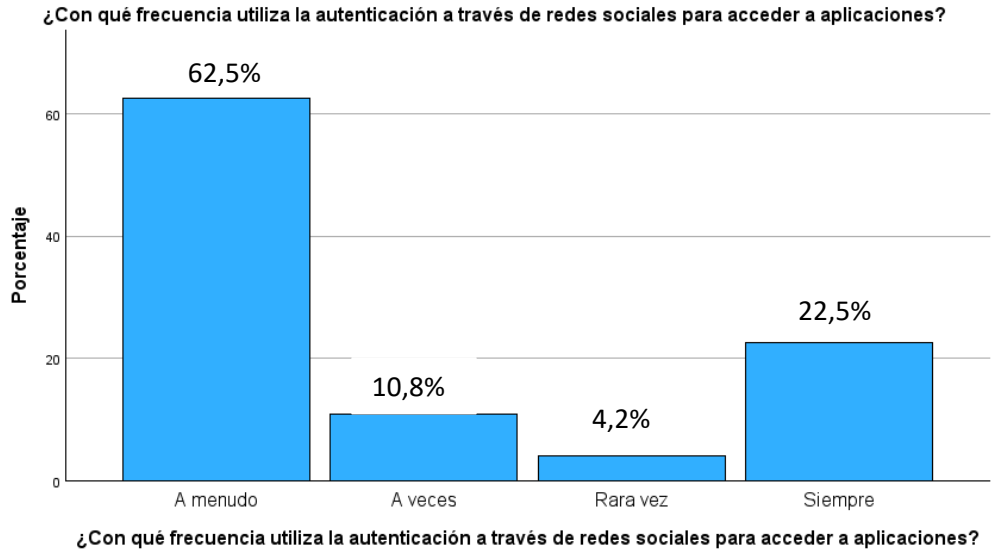
Tabla estadística de la primera pregunta realizada en la encuesta

		Frecuencia	Porcentaje
Válido	A menudo	75	62,5
	A veces	13	10,8
	Rara vez	5	4,2

	Siempre	27	22,5
	Total	120	100,0

Ilustración 2

Gráfica de los resultados de la primera pregunta de la encuesta



Los datos muestran la frecuencia con la que los usuarios utilizan la autenticación a través de redes sociales para acceder a aplicaciones. La mayoría de los usuarios, el 62,5%, utilizan esta forma de autenticación a menudo, un 22,5% de los usuarios siempre optan por esta opción. Un 10,8% de los usuarios la utilizan a veces, mientras que un 4,2% rara vez recurre a ella, por lo que se evidencia una clara mayoría (85% combinando "a menudo" y "siempre") prefiere la autenticación a través de redes sociales para acceder a aplicaciones, indicando una tendencia significativa hacia el uso de esta modalidad.

Esta tendencia puede deberse a la conveniencia y la rapidez que ofrece la autenticación a través de redes sociales, eliminando la necesidad de recordar múltiples contraseñas y simplificando el proceso de inicio de sesión, esto destaca cómo la integración de la autenticación

social no solo facilita la experiencia del usuario, sino que también puede ser un factor clave para aumentar la adopción y el uso continuo de aplicaciones.

2. ¿Le resulta más fácil utilizar la autenticación a través de sus cuentas de redes sociales como Facebook o Google para acceder a sus aplicaciones?

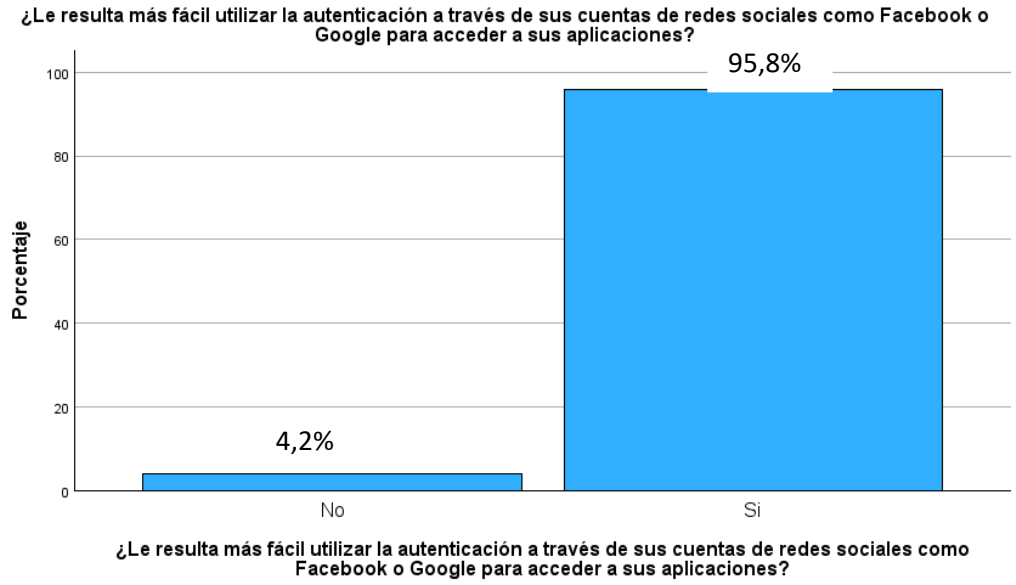
Tabla 4

Tabla estadística de la segunda pregunta realizada en la encuesta

		Frecuencia	Porcentaje
Válido	No	5	4,2
	Si	115	95,8
	Total	120	100,0

Ilustración 3

Gráfica de los resultados de la segunda pregunta de la encuesta



Los datos indican que la gran mayoría de los usuarios encuentran más fácil utilizar la autenticación a través de sus cuentas de redes sociales, como Facebook o Google, para acceder a sus aplicaciones. El 95,8% de los usuarios prefieren esta opción, mientras que solo el 4,2% no la considera más fácil, así que existe una preferencia abrumadora por la autenticación mediante redes sociales debido a su facilidad de uso.

Estos hallazgos sugieren que la integración de la autenticación mediante redes sociales no solo facilita el proceso de inicio de sesión para los usuarios, sino que también puede mejorar significativamente la experiencia del usuario al reducir las barreras de entrada y simplificar la gestión de credenciales, esta facilidad de uso puede ser un factor decisivo en la adopción y retención de usuarios, ya que elimina la necesidad de recordar múltiples contraseñas y reduce la fricción durante el acceso a las aplicaciones.

3. ¿Por qué le parece conveniente iniciar sesión en aplicaciones utilizando sus cuentas de redes sociales para acceder más rápido a sus aplicaciones?

Tabla 5

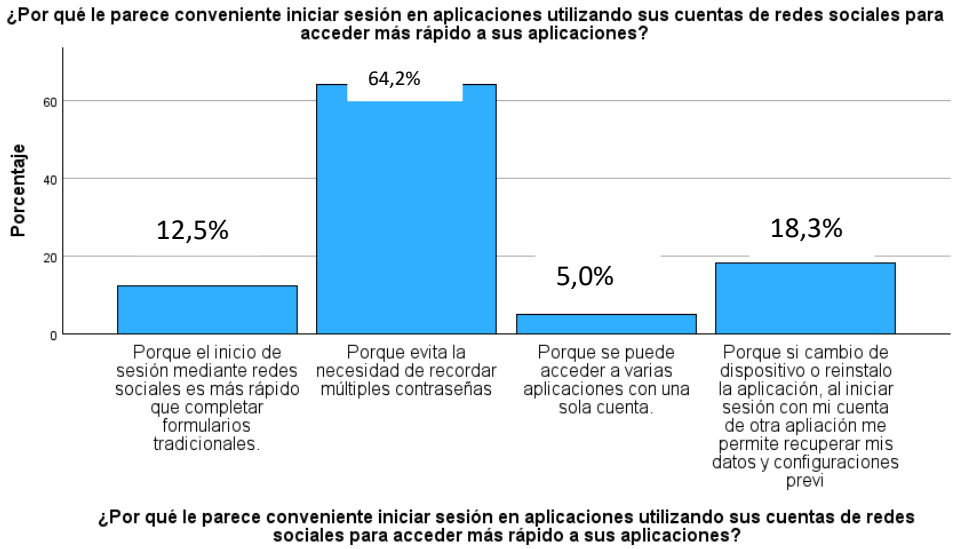
Tabla estadística de la tercera pregunta realizada en la encuesta

		Frecuencia	Porcentaje
Válido	Porque el inicio de sesión mediante redes sociales es más rápido que completar formularios tradicionales.	15	12,5
	Porque evita la necesidad de recordar múltiples contraseñas	77	64,2
	Porque se puede acceder a varias aplicaciones con una sola cuenta.	6	5,0
	Porque si cambio de dispositivo o reinstalo la aplicación, al iniciar sesión con mi cuenta de otra aplicación me permite recuperar mis datos y configuraciones previas	22	18,3

Total	120	100,0

Ilustración 4

Gráfica de los resultados de la tercera pregunta de la encuesta



La razón principal, mencionada por el 64,2% de los usuarios, es que evita la necesidad de recordar múltiples contraseñas, un 18,3% de los usuarios lo encuentra conveniente porque permite recuperar datos y configuraciones previas al cambiar de dispositivo o reinstalar la aplicación, el 12,5% considera que es más rápido que completar formularios tradicionales, y el 5% aprecia poder acceder a varias aplicaciones con una sola cuenta.

Estos datos subrayan cómo la autenticación a través de redes sociales aborda varios puntos críticos en la experiencia del usuario: simplificación de la gestión de contraseñas, facilidad de recuperación de datos, eficiencia en el proceso de acceso y conveniencia en el uso de múltiples aplicaciones, pero también reflejan una clara tendencia hacia soluciones que ofrecen simplicidad y eficiencia en la gestión de credenciales, indicando una preferencia por métodos que reduzcan la complejidad y mejoren la comodidad en el uso de aplicaciones.

4. ¿Qué tan seguro se siente utilizando la autenticación a través de redes sociales en sus aplicaciones?

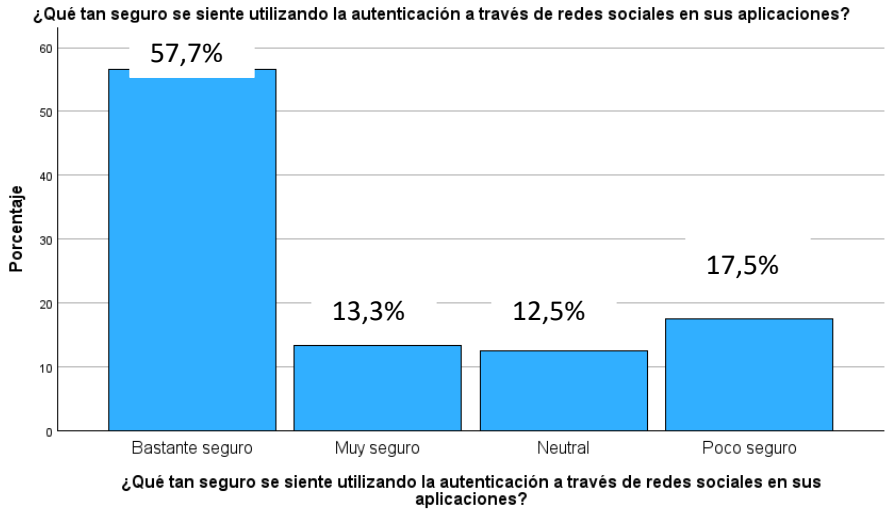
Tabla 6

Tabla estadística de la cuarta pregunta realizada en la encuesta

		Frecuencia	Porcentaje
Válido	Bastante seguro	68	56,7
	Muy seguro	16	13,3
	Neutral	15	12,5
	Poco seguro	21	17,5
	Total	120	100,0

Ilustración 5

Gráfica de los resultados de la cuarta pregunta de la encuesta



Los datos indican cómo se sienten los usuarios respecto a la seguridad al utilizar la autenticación a través de redes sociales en sus aplicaciones, el 56,7% de los usuarios se siente bastante seguro, mientras que el 13,3% se siente muy seguro, un 12,5% de los usuarios tiene una opinión neutral sobre la seguridad de esta forma de autenticación, y el 17,5% se siente poco seguro, por lo que, la mayoría de los usuarios (70% combinando "bastante seguro" y "muy

seguro") se sienten seguros utilizando la autenticación a través de redes sociales, aunque existe una minoría significativa (17,5%) que tiene preocupaciones sobre su seguridad.

Estos datos sugieren que mientras la mayoría de los usuarios confía en la autenticación a través de redes sociales, existe una necesidad de abordar y mitigar las preocupaciones de seguridad de una parte considerable de los usuarios, subrayan la importancia de mantener y reforzar la seguridad y la privacidad en la gestión de credenciales y datos personales.

5. ¿Qué tan satisfecho se siente con el uso de la autenticación (registrarse en una nueva aplicación) a través de sus cuentas de redes sociales en otras aplicaciones?

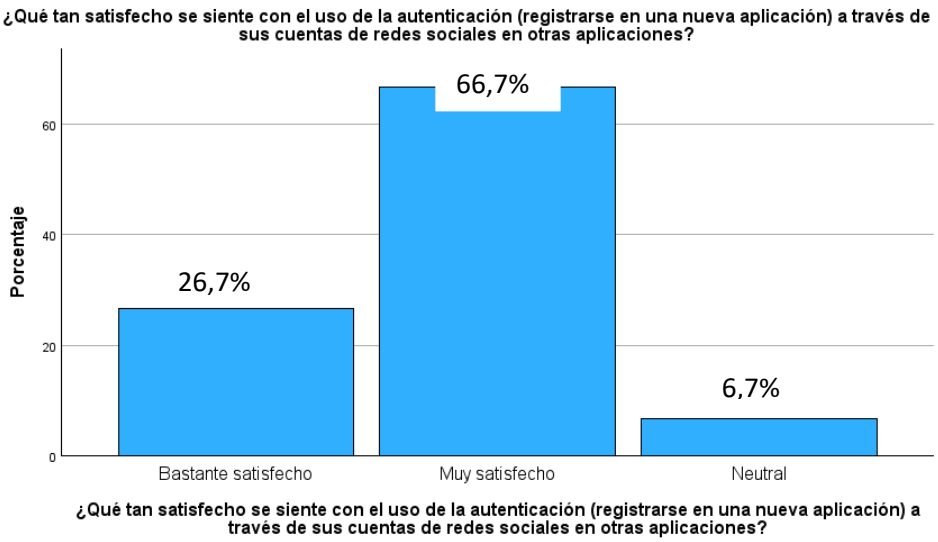
Tabla 7

Tabla estadística de la segunda pregunta realizada en la encuesta

		Frecuencia	Porcentaje
Válido	Bastante satisfecho	32	26,7
	Muy satisfecho	80	66,7
	Neutral	8	6,7
	Total	120	100,0

Ilustración 6

Gráfica de los resultados de la quinta pregunta de la encuesta



Los datos proporcionados indican el nivel de satisfacción de los usuarios con el uso de la autenticación a través de sus cuentas de redes sociales al registrarse en nuevas aplicaciones, el 66,7% de los usuarios se siente muy satisfecho con esta modalidad de autenticación, mientras que el 26,7% se siente bastante satisfecho, solo el 6,7% de los usuarios tiene una opinión neutral, así que una abrumadora mayoría (93,4% combinando "muy satisfecho" y "bastante satisfecho") está satisfecha con el uso de la autenticación a través de redes sociales para registrarse en nuevas aplicaciones.

Estos resultados destacan cómo la autenticación a través de redes sociales puede simplificar el proceso de registro y hacer que la experiencia de usuario sea más fluida y agradable, la alta satisfacción reflejada por la mayoría de los usuarios sugiere que este método es valorado no solo por su conveniencia, sino también por su capacidad para mejorar la experiencia general al interactuar con nuevas aplicaciones.

6. ¿Encuentra problemas al utilizar la autenticación a través de redes sociales para acceder a aplicaciones?

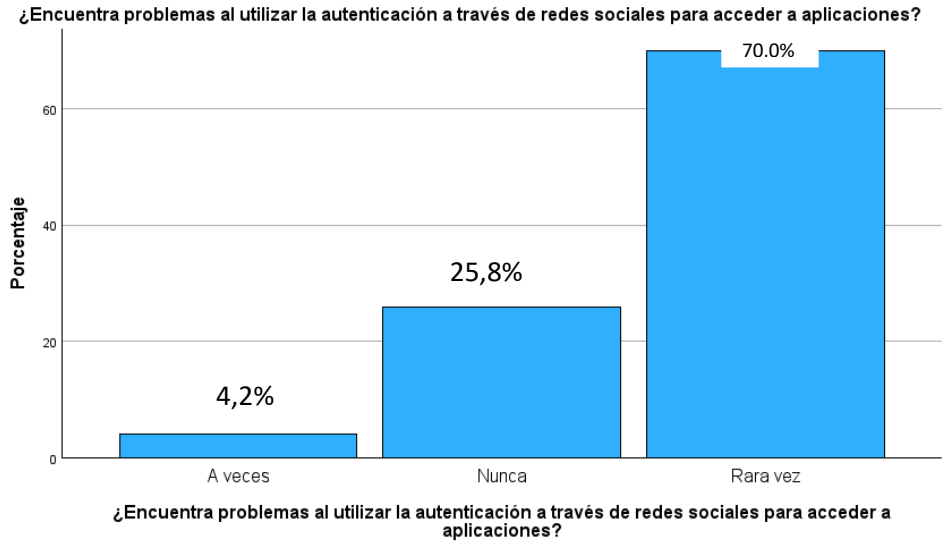
Tabla 8

Tabla estadística de la sexta pregunta realizada en la encuesta

		Frecuencia	Porcentaje
Válido	A veces	5	4,2
	Nunca	31	25,8
	Rara vez	84	70,0
	Total	120	100,0

Ilustración 7

Gráfica de los resultados de la sexta pregunta de la encuesta



Los datos indican la frecuencia con la que los usuarios encuentran problemas al utilizar la autenticación a través de redes sociales para acceder a aplicaciones, el 70% de los usuarios rara vez encuentra problemas, mientras que el 25,8% nunca ha tenido problemas, solo el 4,2% de los usuarios ha encontrado problemas a veces, por lo que se llega a la conclusión que la mayoría de

los usuarios (95,8% combinando "rara vez" y "nunca") experimenta pocos o ningún problema al utilizar la autenticación a través de redes sociales para acceder a aplicaciones.

Estos resultados son muy favorables para la autenticación a través de redes sociales, la baja incidencia de problemas reportados sugiere que este método es robusto y confiable, lo cual es crucial para mantener la satisfacción del usuario y fomentar la adopción continua, lo que nos indica que los usuarios pueden confiar en la autenticación a través de redes sociales como un método sin complicaciones para acceder a sus aplicaciones favoritas.

7. ¿Prefiere la autenticación a través de sus cuentas de redes sociales (Facebook o Google) en comparación con otros métodos tradicionales como llenando formularios con sus datos (correo electrónico, número de teléfono, etc.)?

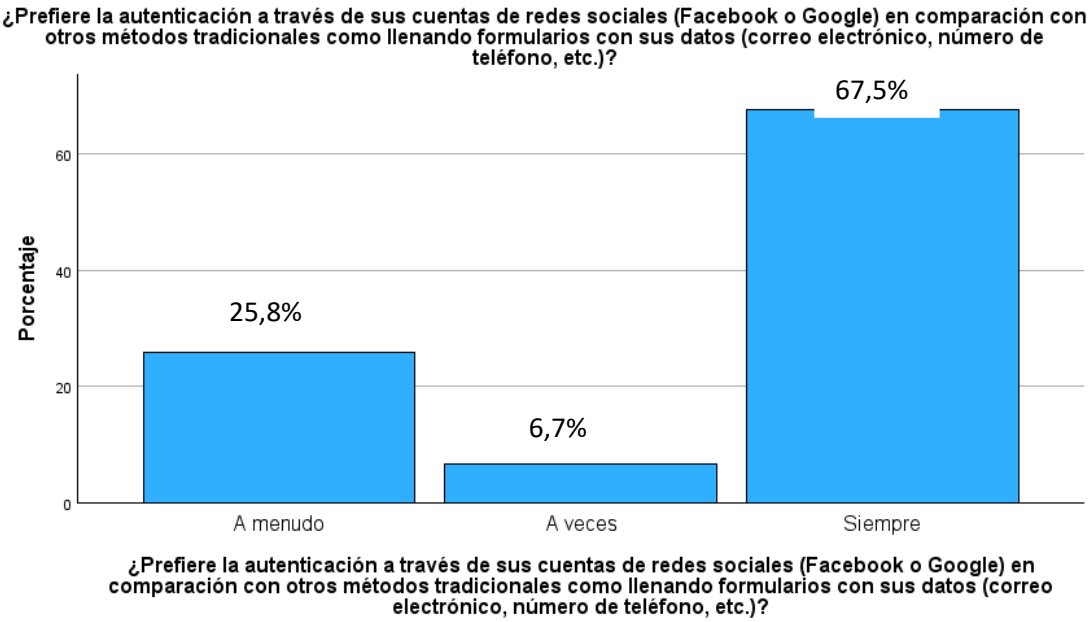
Tabla 9

Tabla estadística de la séptima pregunta realizada en la encuesta

		Frecuencia	Porcentaje
Válido	A menudo	31	25,8
	A veces	8	6,7
	Siempre	81	67,5
	Total	120	100,0

Ilustración 8

Gráfica de los resultados de la séptima pregunta de la encuesta



Los datos indican la preferencia de los usuarios por la autenticación a través de sus cuentas de redes sociales (Facebook o Google) en comparación con métodos tradicionales como llenar formularios con datos personales (correo electrónico, número de teléfono, etc.), el 67,5% de los usuarios siempre prefiere la autenticación a través de redes sociales, mientras que el 25,8% prefiere este método a tradicional, solo el 6,7% de los usuarios a veces opta por la autenticación mediante redes sociales.

La importancia de ofrecer la opción de autenticación a través de redes sociales en las aplicaciones refleja una tendencia general hacia la búsqueda de comodidad en los procesos de registro, la amplia preferencia por la autenticación a través de redes sociales sugiere que los usuarios están dispuestos a adoptar métodos que simplifiquen su experiencia digital y reduzcan el tiempo y esfuerzo requeridos para acceder a nuevas aplicaciones.

8. ¿Cuáles de estas redes sociales usted utiliza con más frecuencia para registrarse en sus nuevas aplicaciones?

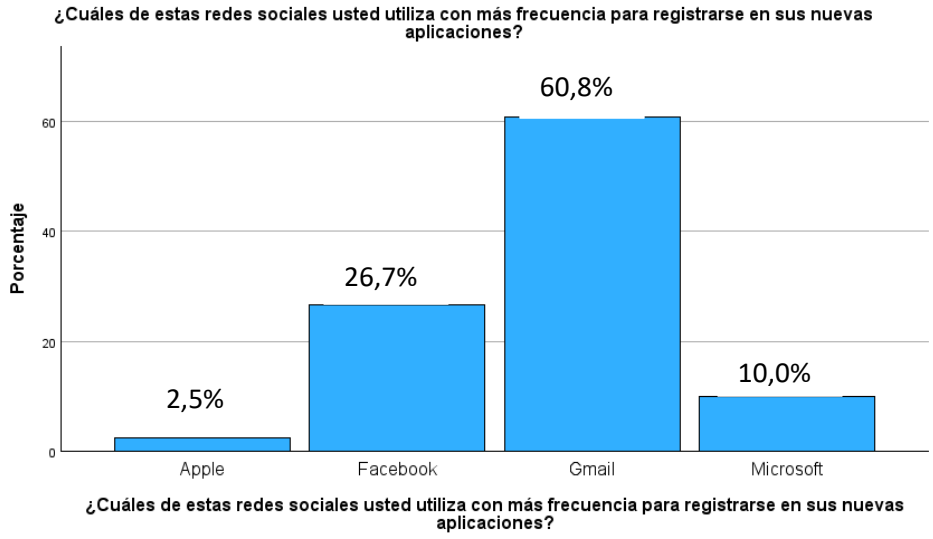
Tabla 10

Tabla estadística de la octava pregunta realizada en la encuesta

		Frecuencia	Porcentaje
Válido	Apple	3	2,5
	Facebook	32	26,7
	Gmail	73	60,8
	Microsoft	12	10,0
	Total	120	100,0

Ilustración 9

Gráfica de los resultados de la octava pregunta de la encuesta



Los datos indican que las redes sociales que los usuarios utilizan con más frecuencia para registrarse en sus nuevas aplicaciones, la mayoría de los usuarios, el 60,8%, prefieren usar Gmail para este propósito, Facebook es utilizado por el 26,7% de los usuarios, mientras que el 10% opta por Microsoft. Solo el 2,5% de los usuarios utiliza Apple, así que se puede decir que Gmail es la

red social más frecuentemente utilizada para el registro en nuevas aplicaciones, seguida por Facebook, con Microsoft y Apple siendo opciones menos comunes.

Los datos reflejan una clara preferencia por plataformas que ofrecen una experiencia de usuario sencilla y una integración amplia y siendo Gmail la opción más popular, probablemente se beneficia de su facilidad de uso y la confianza que los usuarios tienen en los servicios de Google, la menor preferencia por Microsoft y Apple podría indicar una menor adopción general o una integración menos conocida o conveniente en comparación con Gmail y Facebook.

4.1.3 Lista de Cotejos

Ilustración 10

Lista de cotejo realizada por el MSc. Carlos Julio Soto Valle

Lista de Cotejo para evaluar APIs de autenticación a través de redes sociales en aplicación móvil destinada a la "Gestión de Comunidades Académicas y Recreativas de la Universidad Técnica de Babahoyo":

Nombre: MSc. Carlos Julio Soto Valle		Fecha: 22 / 07 / 2024
Indicadores	**SI**	**NO**
Vulnerabilidades identificadas		✓
Funcionamiento correcto en diferentes dispositivos	✓	
Impacto en el rendimiento de la plataforma		✓
Tiempo de respuesta aceptable	✓	
Experiencia intuitiva y fluida para el usuario	✓	
Cumplimiento con normativas de protección de datos	✓	
Buenas prácticas de seguridad recomendadas	✓	

FIRMA

C.I: 1204358016

Análisis por cada indicador.

Vulnerabilidades Identificadas:

Resultado: NO

Análisis: La ausencia de vulnerabilidades identificadas es un indicativo de una plataforma bien diseñada y segura, esto sugiere que las prácticas de desarrollo adoptadas son efectivas en prevenir problemas de seguridad, lo que es crucial para mantener la confianza de los usuarios y proteger datos sensibles.

Funcionamiento Correcto en Diferentes Dispositivos:

Resultado: SÍ

Análisis: La capacidad de la plataforma para funcionar correctamente en diversos dispositivos asegura una experiencia de usuario consistente y accesible, esta compatibilidad es esencial para atraer y retener una base de usuarios diversa, garantizando que todos tengan una experiencia satisfactoria sin importar el dispositivo que utilicen.

Impacto en el Rendimiento de la Plataforma:

Resultado: NO

Análisis: La ausencia de impacto negativo en el rendimiento de la plataforma destaca una implementación eficiente, esto significa que las funcionalidades añadidas no comprometen la velocidad ni la eficiencia operativa, lo cual es crucial para mantener la satisfacción del usuario y la eficiencia de los recursos.

Tiempo de Respuesta Aceptable:

Resultado: SÍ

Análisis: Un tiempo de respuesta rápido es fundamental para la que los usuarios puedan acceder más rápido a la plataforma, este resultado indica que los usuarios experimentan tiempos de carga rápidos y una interacción ágil con la autenticación, lo cual mejora significativamente la experiencia del usuario y la eficiencia operativa.

Experiencia Intuitiva y Fluida para el Usuario:

Resultado: SÍ

Análisis: Una experiencia de usuario intuitiva y fluida es vital para la adopción y retención de usuarios, esto sugiere que la plataforma está diseñada con un enfoque centrado en el usuario, facilitando la navegación y el uso de las funcionalidades disponibles sin complicaciones.

Cumplimiento con Normativas de Protección de Datos:

Resultado: SÍ

Análisis: El cumplimiento con las normativas de protección de datos es esencial para la legalidad y la confianza del usuario, este resultado asegura que la plataforma maneja datos personales de manera responsable y en conformidad con las leyes y regulaciones aplicables, lo que es fundamental para evitar sanciones y mantener la confianza del usuario.

Buenas Prácticas de Seguridad Recomendadas:

Resultado: SÍ

Análisis: La implementación de buenas prácticas de seguridad recomendadas es crucial para proteger la plataforma contra amenazas y ataques, este resultado refleja un enfoque

proactivo en la seguridad, adoptando medidas preventivas que aseguran la integridad y confidencialidad de los datos manejados.

Los resultados proporcionados por el MSc. Carlos Soto Valle indican una integración de las APIs de autenticación bien diseñada y administrada que cumple con estándares en términos de seguridad, rendimiento y usabilidad.

La ausencia de vulnerabilidades y el cumplimiento con normativas de protección de datos son especialmente destacables, demostrando un compromiso con la seguridad y la legalidad, sumado a esto, el enfoque en una experiencia de usuario intuitiva y tiempos de respuesta rápidos asegura que los usuarios tengan una interacción positiva con la plataforma, lo cual es crucial para el éxito a largo plazo.

Resultados finales:

Ilustración 11

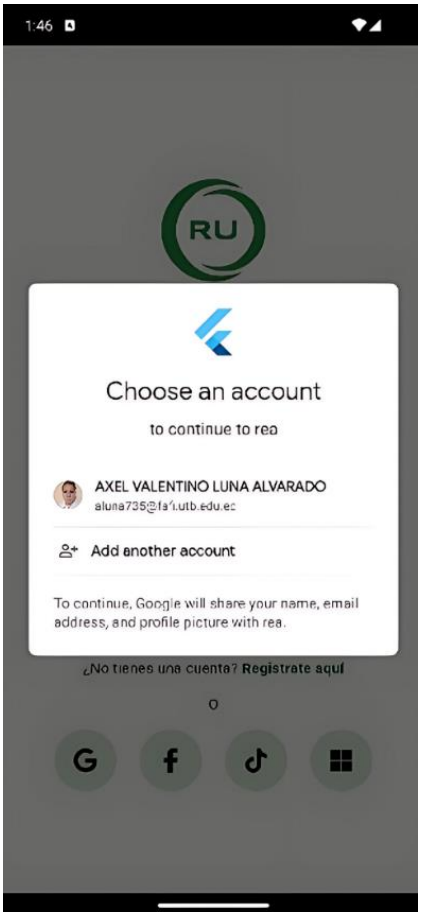
Inicio de sesión de la aplicación móvil destinada a la Gestión de Comunidades Académicas y Recreativas de la Universidad Técnica de Babahoyo.

Si bien el inicio de sesión o login de la aplicación contaba con los iconos para utilizar las redes sociales como método de autenticación, no estaban totalmente definidos con cuales se quedarían, es por eso que la pregunta número 8 dentro de la encuesta dirigida a los estudiantes de la Universidad Técnica de Babahoyo está establecida de manera que se pueda determinar con cuales redes sociales se deberían integrar dentro de la aplicación.

Resultados de la integración de las APIs de autenticación correctamente:

Ilustración 12

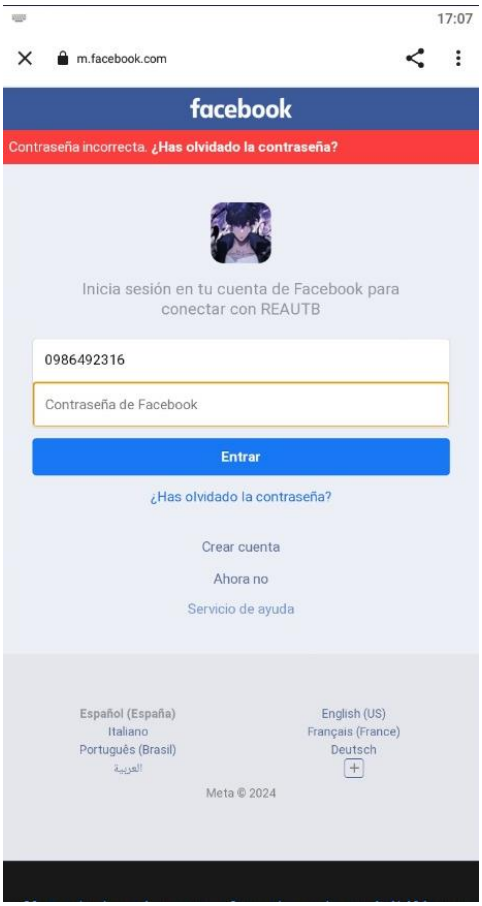
API de autenticación mediante correos Gmail



En está captura de pantalla se puede apreciar la autenticación a través de Gmail ya integrada dentro de la aplicación, en la que los estudiantes mediante sus correos tantos personales, como institucionales puedes registrarse o iniciar sesión dentro de la aplicación.

Ilustración 13

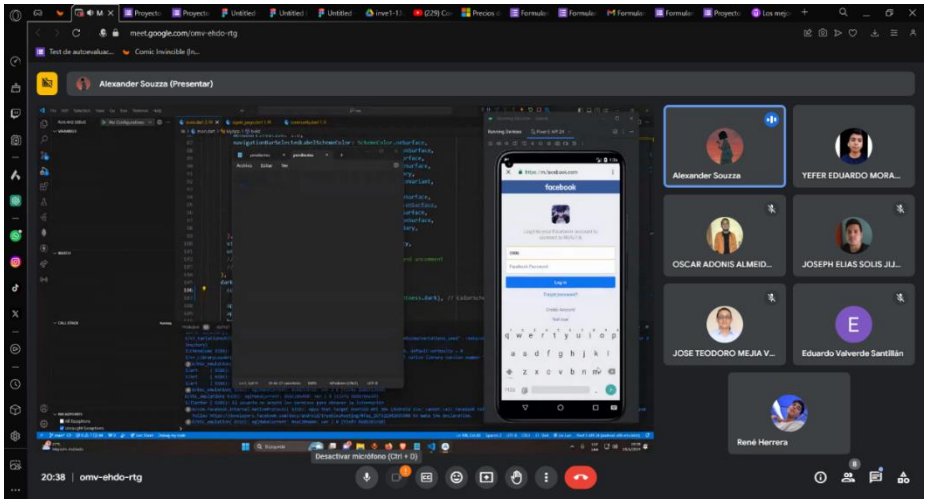
API de autenticación a través de Facebook



En la imagen se muestra la funcionalidad de inicio de sesión integrado a través de la API de Facebook dentro de la aplicación, la integración del inicio de sesión mediante la API de Facebook proporciona diversos beneficios, entre los que se incluyen un acceso más ágil al aplicativo al eliminar la necesidad de recordar una contraseña, así como la capacidad de cambiar de dispositivo sin perder datos y al iniciar sesión con la cuenta de Facebook, la aplicación puede recuperar automáticamente la configuración y preferencias previamente guardadas, mejorando la experiencia del usuario.

Ilustración 14

Presentación de API de autenticación a través de Facebook



En la ilustración presentada, se está realizando una reunión que involucra tanto a los miembros del proyecto semillero como al tutor responsable del proyecto, teniendo como objetivo principal de esta reunión presentar la API de autenticación integrada mediante la red social Facebook, teniendo en cuenta que durante la sesión, se expone en detalle el proceso de integración de la API y se demuestra su funcionamiento en un entorno práctico, este encuentro busca proporcionar una comprensión completa del sistema de autenticación y resolver cualquier duda que pueda surgir sobre su implementación y operativa.

Ilustración 15

Inicio de sesión actualizado con las plataformas para iniciar sesión escogidas

Debido a las respuestas de la pregunta 8 de la encuesta realizada a los estudiantes de la Universidad Técnica de Babahoyo (Tabla 12), se llegó a la conclusión de dejar tanto Gmail, como Facebook para los métodos de autenticación a través de redes sociales, pero sin descartar una tercera opción que según los datos obtenidos Microsoft (outlook) podría ser.

4.2 Discusión

La discusión de los resultados obtenidos en esta investigación se centra en la interpretación de estos a la luz de la pregunta de investigación y la hipótesis planteada. La hipótesis sugería que la correcta estructuración de las Interfaces de Programación de Aplicaciones (APIs) para la autenticación a través de redes sociales mejoraría la funcionalidad e integración de inicios de sesión con redes sociales en el contexto de la "gestión de comunidades académicas y recreativas de la Universidad Técnica de Babahoyo".

Los resultados de las encuestas realizadas a los estudiantes de la Universidad Técnica de Babahoyo fueron mayormente positivos, dejando en evidencia una muy buena perspectiva y aceptación sobre la autenticación a través de redes sociales, la mayoría de los encuestados respondió afirmativamente a las preguntas, demostrando que este método de autenticación es ampliamente utilizado y valorado por ellos, este hallazgo es consistente con la hipótesis, ya que sugiere una predisposición positiva hacia la integración de este tipo de tecnologías en el ámbito universitario.

Adicionalmente, el marco comparativo realizado sobre las diferentes alternativas de autenticación disponibles en el mercado permitió identificar que la opción elegida para el proyecto eran la más adecuada, se llegó a esta conclusión con base en que las opciones seleccionada cumplía con los requerimientos del proyecto semillero, que sugeriría potencialmente hacer uso de tecnología open source, proporcionando la flexibilidad y funcionalidad necesaria, con este resultado se subraya la importancia de realizar un análisis exhaustivo de las opciones tecnológicas antes de su implementación, asegurando que las soluciones elegidas se alineen con las necesidades específicas del proyecto.

Por otro lado, la lista de cotejos aplicada a un profesional en el área también corroboró los resultados obtenidos de las encuestas, la evaluación realizada mediante este instrumento destacó la exitosa integración de las APIs, así como una experiencia de usuario intuitiva y fluida que específicamente, junto al indicador 5 de la lista de cotejos, que evaluaba la experiencia del usuario, confirmó que la aplicación que se encuentra en desarrollado cumplía con las expectativas y necesidades de los usuarios finales.

Al juntar todos estos resultados nos podemos dar cuenta que validan la hipótesis de la investigación, demostrando que una correcta estructuración e implementación de APIs de autenticación a través de redes sociales puede mejorar significativamente la funcionalidad y la experiencia del usuario en plataformas tecnológicas como la desarrollada para la gestión de comunidades académicas y recreativas de la Universidad Técnica de Babahoyo, asimismo, la aceptación y uso frecuente de estas tecnologías por parte de los estudiantes, junto con la evaluación positiva de un profesional en el área, refuerzan la viabilidad y efectividad de la solución propuesta.

CAPÍTULO V.- CONCLUSIONES Y RECOMENDACIONES.

5.1. Conclusiones

Se ha logrado realizar un estudio técnico alineado con la funcionalidad de APIs para los inicios de sesión de la gestión de comunidades académicas y recreativas de la Universidad Técnica de Babahoyo con redes sociales. La investigación demostró que la implementación de estas APIs no solo es viable sino también beneficiosa, mejorando la seguridad y eficiencia del

sistema de autenticación. La aceptación positiva por parte de los estudiantes y la evaluación favorable de profesionales en el área confirman la efectividad de la solución propuesta.

Al analizar las APIs de autenticación de redes sociales más adecuadas para la plataforma tecnológica de la Universidad Técnica de Babahoyo, se identificó que las alternativas open source seleccionadas cumplen con los requisitos del proyecto semillero. Estas APIs proporcionan la flexibilidad y funcionalidad necesarias para la integración exitosa en la plataforma, garantizando una experiencia de usuario intuitiva y fluida.

La evaluación del rendimiento, seguridad y presupuesto del sistema de autenticación reveló que la solución seleccionada es no solo segura y eficiente, sino también económicamente viable. Los resultados del marco comparativo y las evaluaciones realizadas indicaron que la opción elegida se ajusta adecuadamente al presupuesto disponible y cumple con los estándares de seguridad necesarios para proteger la información de los usuarios.

La determinación de la funcionalidad de aplicaciones móviles con la autenticación mediante APIs de redes sociales mostró que esta integración mejora significativamente la experiencia del usuario. Los estudiantes respondieron positivamente a la autenticación a través de redes sociales, indicando una alta tasa de adopción y satisfacción. La evaluación profesional corroboró estos hallazgos, destacando la eficacia de las APIs en proporcionar una experiencia de inicio de sesión rápida y segura en las aplicaciones móviles.

5.2. Recomendaciones

Es recomendable seguir mejorando y actualizando continuamente las APIs implementadas para mantener altos estándares de seguridad y funcionalidad en la gestión de comunidades académicas y recreativas de la Universidad Técnica de Babahoyo, además, se sugiere realizar

pruebas periódicas y obtener retroalimentación constante de los usuarios para adaptar la plataforma a sus necesidades y preferencias cambiantes.

Se recomienda seguir explorando y comparando nuevas APIs de autenticación que surjan en el mercado para asegurarse de que la plataforma se mantenga actualizada con las mejores tecnologías disponibles, también es aconsejable establecer un protocolo de evaluación y selección de APIs que incluya criterios claros y específicos para garantizar que las futuras integraciones continúen cumpliendo con los requisitos del proyecto.

Es importante mantener un monitoreo constante del rendimiento y seguridad del sistema de autenticación implementado. Se recomienda establecer un sistema de alertas y auditorías regulares para identificar y corregir posibles vulnerabilidades.

Para mejorar la funcionalidad de las aplicaciones móviles con la autenticación mediante APIs de redes sociales, se recomienda realizar estudios de usabilidad adicionales para identificar áreas de mejora en la experiencia del usuario, como también se sugiere implementar programas de capacitación para los desarrolladores del proyecto, enfocados en las mejores prácticas de integración y seguridad de APIs y finalmente, es importante fomentar la colaboración con otras instituciones educativas y tecnológicas para compartir conocimientos, y experiencias que puedan enriquecer el desarrollo como la mejora continua de la plataforma.

Referencias Bibliográficas

Agreda, V. (2023, junio 27). *¿Qué es Firebase?* https://developer.oracle.com/es/learn/technical-articles/what-is-firebase

Amazon Web Services, Inc. (s. f.-a). *¿Qué es el SDK? - Explicación del SDK - AWS*. Amazon Web Services, Inc. Recuperado 16 de junio de 2024, de https://aws.amazon.com/es/what-is/sdk/

Amazon Web Services, Inc. (s. f.-b). *¿Qué es Java? - Explicación del lenguaje de programación Java - AWS*. Amazon Web Services, Inc. Recuperado 17 de junio de 2024, de https://aws.amazon.com/es/what-is/java/

Amazon Web Services, Inc. (2024a). *¿Qué es una API? - Explicación de interfaz de programación de aplicaciones - AWS*. Amazon Web Services, Inc. https://aws.amazon.com/es/what-is/api/

Amazon Web Services, Inc. (2024b, junio 15). *¿Qué es Flutter? - Explicación de la aplicación Flutter - AWS*. Amazon Web Services, Inc. https://aws.amazon.com/es/what-is/flutter/

Auth0. (s. f.-a). *¿Qué es OAuth 2.0 y para qué sirve?* Auth0. Recuperado 16 de junio de 2024, de https://auth0.com/es/intro-to-iam/what-is-oauth-2

Auth0. (s. f.-b). *¿Qué es OpenID Connect y para qué se utiliza?* Auth0. Recuperado 18 de junio de 2024, de https://auth0.com/es/intro-to-iam/what-is-openid-connect-oidc

Calvo, L. (2023, diciembre 27). *¿Qué es una app? Guía completa sobre aplicaciones móviles*. GoDaddy Resources - Spain. https://www.godaddy.com/resources/es/crearweb/que-es-una-app-y-para-que-se-utiliza

Carla, M. V., Alfonso, U. M., & Ángel, R. G. M. (2021). *Lenguajes de programación*. Editorial UNED.

Cloudflare. (2024, junio 9). *¿Qué es la seguridad de la API? | Seguridad de las API web*. https://www.cloudflare.com/es-es/learning/security/api/what-is-api-security/

Colmenares, J. (2022, agosto 9). *Las APIs y su importancia: ¿Qué son, cómo funcionan?* Asilo Digital. https://www.asilodigital.com/las-apis-y-su-importancia/

Cruz, A. (2022). *Primeros pasos con Flutter 3 - iOS - Windows - MacOS: Aquí comienza tu camino en el desarrollo de aplicaciones multiplataformas móviles, escritorio y web en Flutter con Dart*. Andres Cruz.

diego.coder26. (2023, julio 27). Métodos y estrategias de autenticación en aplicaciones con HTTP. *Medium*. https://medium.com/@diego.coder/tipos-de-autenticaci%C3%B3n-en-http-d773dc63a392

Facebook. (s. f.). *Información general—Inicio de sesión con Facebook—Documentación*. Meta for Developers. Recuperado 16 de junio de 2024, de https://developers.facebook.com/docs/facebook-login/overview/

Facebook for Developers. (s. f.). *Pinterest Success Story | Facebook for Developers*. Meta for Developers. Recuperado 16 de junio de 2024, de https://developers.facebook.com/success-stories/pinterest/

Fortinet. (2024, junio 15). *¿Qué es un token de autenticación?* Fortinet. https://www.fortinet.com/lat/resources/cyberglossary/authentication-token.html

Gamarra, F. (2024). *Visual Studio Code*. Ediciones de la U.

Google Cloud. (s. f.). *Tipos de tokens | Authentication*. Google Cloud. Recuperado 18 de junio de 2024, de https://cloud.google.com/docs/authentication/token-types?hl=es-419

Google Developers. (2024, enero 12). *Descarga e instala Android Studio*. Android Developers. https://developer.android.com/codelabs/basic-android-kotlin-compose-install-android-studio?hl=es-419

Google for Developers. (s. f.). *Descripción general | Authentication*. Google for Developers. Recuperado 16 de junio de 2024, de https://developers.google.com/identity/gsi/web/guides/overview?hl=es-419

IBM. (2024, mayo 29). *¿Qué es una API (interfaz de programación de aplicaciones)? | IBM*. https://www.ibm.com/mx-es/topics/api

Jain, A. K., Sahoo, S. R., & Kaubiyal, J. (2021). Online social networks security and privacy: Comprehensive review and analysis. *Complex & Intelligent Systems, 7*(5), 2157-2177. https://doi.org/10.1007/s40747-021-00409-7

Juan de Assembler Institute. (2022, marzo 31). *Que es un Framework en programación y sus principales usos*. Assembler Institute. https://assemblerinstitute.com/blog/framework-programacion/

Lifeder. (2021, diciembre 6). *Redes sociales: Qué son, historia, características, para qué sirven, tipos*. Lifeder. https://www.lifeder.com/redes-sociales/

Martínez Ibáñez, A. (2024). *Análisis, evaluación y construcción de una idea de negocio electrónico*. http://rua.ua.es/dspace/handle/10045/139972

Microsoft Azure. (s. f.). *¿Qué es Java Spring Boot? Introducción a Spring Boot | Microsoft Azure*. Recuperado 17 de junio de 2024, de https://azure.microsoft.com/es-es/resources/cloud-computing-dictionary/what-is-java-spring-boot

Microsoft Learn. (2024, marzo 22). *¿Qué es Power BI? - Power BI*. https://learn.microsoft.com/es-es/power-bi/fundamentals/power-bi-overview

Moreno, H. M. (2023). Sistema de videovigilancia en tiempo real a través de un dron programable. *Jóvenes en la Ciencia: Veranos de la Ciencia XXVIII Vol. 21 (2023)*. http://repositorio.ugto.mx/handle/20.500.12059/9579

Oracle. (s. f.). *Uso de la API de autenticación para desarrollar una página de conexión personalizada*. Recuperado 18 de junio de 2024, de https://docs.oracle.com/es-ww/iaas/Content/Identity/api-getstarted/usingauthenticateapis.htm

Owen, R. (2024, abril 8). *OpenID Connect (OIDC) en la plataforma de identidad de Microsoft—Microsoft identity platform*. https://learn.microsoft.com/es-es/entra/identity-platform/v2-protocols-oidc

Pellicer de Juan, E. (2021). *Desarrollo de una aplicación móvil con Flutter. Orientat*. https://openaccess.uoc.edu/handle/10609/138287

Pérez Ibarra, S. G., Quispe, J. R., Mullicundo, F. F., & Lamas, D. A. (2021). *Herramientas y tecnologías para el desarrollo web desde el FrontEnd al BackEnd*. XXIII Workshop de Investigadores en Ciencias de la Computación (WICC 2021, Chilecito, La Rioja). http://sedici.unlp.edu.ar/handle/10915/120476

Primicias. (2024, junio 15). Las aplicaciones hechas en Ecuador ofrecen juegos de azar, taxis y mensajería. *Primicias*. https://www.primicias.ec/noticias/tecnologia/apps-ecuatorianas-entretenimiento-mensajeria-transporte/

redhat. (2020, enero 23). *¿Qué es una API y cómo funciona?* https://www.redhat.com/es/topics/api/what-are-application-programming-interfaces

Rendón Solano, G. A. (2018). *Implementación de una aplicación para el Sistema de Seguimiento a Graduados basada en Moodle en la Universidad Politécnica Salesiana* [bachelorThesis]. http://dspace.ups.edu.ec/handle/123456789/16163

UNIR FP. (s. f.). *Framework: Qué es, para qué sirve y algunos ejemplos*. UNIR FP. Recuperado 18 de junio de 2024, de https://unirfp.unir.net/revista/ingenieria-y-tecnologia/framework/

Anexos

- Encuesta sobre la Autenticación a través de Redes Sociales dirigida a los estudiantes de la universidad realizada en Google forms:

  Medir frecuencia de uso:

  ¿Con qué frecuencia utiliza la autenticación a través de redes sociales para acceder a aplicaciones?

  a) Nunca

  b) Rara vez

  c) A veces

  d) A menudo

  e) Siempre

  Para medir facilidad de uso:

  ¿Le resulta más fácil utilizar la autenticación a través de sus cuentas de redes sociales como Facebook o Google para acceder a sus aplicaciones?

  a) Si

  b) No

  Para medir la seguridad percibida:

¿Qué tan seguro se siente utilizando la autenticación a través de redes sociales en sus aplicaciones?

a) Muy seguro

b) Bastante seguro

c) Neutral

d) Poco seguro

e) Nada seguro

Para medir la conveniencia de uso:

¿Por qué le parece conveniente iniciar sesión en aplicaciones utilizando sus cuentas de redes sociales para acceder más rápido a sus aplicaciones?

a) Porque evita la necesidad de recordar múltiples contraseñas

b) Porque el inicio de sesión mediante redes sociales es más rápido que completar formularios tradicionales.

c) Porque se puede acceder a varias aplicaciones con una sola cuenta.

d) Porque si cambio de dispositivo o reinstalo la aplicación, al iniciar sesión con mi cuenta de otra aplicación me permite recuperar mis datos y configuraciones previas.

Para medir la satisfacción general:

¿Qué tan satisfecho se siente con el uso de la autenticación (registrarse en una nueva aplicación) a través de sus cuentas de redes sociales en otras aplicaciones?

a) Muy satisfecho

b) Bastante satisfecho

c) Neutral

d) Poco satisfecho

e) Nada satisfecho

Para medir problemas encontrados:

¿Encuentra problemas al utilizar la autenticación a través de redes sociales para acceder a aplicaciones?

a) Siempre

b) A menudo

c) A veces

d) Rara vez

e) Nunca

Para medir la preferencia de métodos de autenticación:

¿Prefiere la autenticación a través de sus cuentas de redes sociales (Facebook o Google) en comparación con otros métodos tradicionales como llenando formularios con sus datos (correo electrónico, número de teléfono, etc.)?

a) Nunca

b) Rara vez

c) A veces

d) A menudo

e) Siempre

¿Cuáles de estas redes sociales usted utiliza con más frecuencia para registrarse en sus nuevas aplicaciones?

a) Facebook

b) Google

c) Github

d) X (Twitter)

e) Apple

f) Microsoft (Outlook)

-Aspectos que se tomarán en cuenta para hacer el marco comparativo:

Tabla 11
Estructura para llevar a cabo el marco comparativo

Indicador	Descripción	Alternativas Evaluadas
Facilidad de Implementación	Complejidad técnica para integrar la API de autenticación. Disponibilidad de documentación y soporte técnico.	Facebook Login, Google Sign-In, OAuth/OpenID, Firebase
Compatibilidad y Multiplataforma	Soporte para múltiples plataformas (Android, iOS, web, etc.). Experiencia de usuario consistente en diferentes dispositivos.	Facebook Login, Google Sign-In, OAuth/OpenID Connect, Firebase
Seguridad y Privacidad	Métodos de autenticación ofrecidos. Medidas adicionales de seguridad (verificación en	Facebook Login, Google Sign-In, OAuth/OpenID Connect, Firebase

	dos pasos, gestión de tokens). Cumplimiento con regulaciones de privacidad.	
Escalabilidad y Mantenimiento	Capacidad para manejar un crecimiento en el número de usuarios. Facilidad de mantenimiento y actualizaciones.	Facebook Login, Google Sign-In, OAuth/OpenID Connect, Firebase
Costos y Viabilidad Económica	Modelo de precios (gratuito, por uso, por suscripción, etc.). Costos adicionales y limitaciones.	Facebook Login, Google Sign-In, OAuth/OpenID Connect, Firebase

Evaluación técnica con un profesional en el área:

Carta de autorización del lugar donde va a realizar la investigación

UNIVERSIDAD TÉCNICA DE BABAHOYO
Instituto de Investigación y Desarrollo

Babahoyo 7 de agosto de 2024

El Instituto de Investigación y Desarrollo autoriza al Sr. RENE ALEJANDRO HERRERA BARCOS con cédula de identidad No. 1208395085, estudiante de la carrera Sistemas de Información matriculado en el proceso de titulación en el período ABRIL – AGOSTO 2024, realizar su investigación del proyecto titulado "ESTUDIO DE LAS APIs (INTERFAZ DE PROGRAMACIÓN DE APLICACIONES), PARA LA AUTENTIFICACIÓN A TRAVES DE REDES SOCIALES EN APLICACIONES MÓVILES, CASO DE ESTUDIO GESTIÓN ACADÉMICAS Y RECREATIVAS DE LA UNIVERSIDAD TÉCNICA DE BABAHOYO", como parte del proyecto semillero.

Detalles del proyecto semillero:

Título del proyecto: "PLATAFORMA TECNOLÓGICA PARA LA GESTIÓN DE COMUNIDADES ACADÉMICAS Y RECREATIVAS DE LA UNIVERSIDAD TECNICA DE BABAHOYO"

Fecha de inicio: 20-septiembre-2023

Fecha de finalización: 20-septiembre-2024

Tutor del Proyecto: MSc. JOSÉ TEODORO MEJIA VITERI

Este proceso permite la articulación de los procesos sustantivos de investigación y academia por lo que es pertinente su desarrollo.

Atentamente,

Lcda. Karina De Mora Litardo, MSc
Directora del Instituto de Investigación y Desarrollo – UTB

Cc. Archivo.