Universidad Nacional de Loja

Facultad de la Energía, las Industrias y los Recursos Naturales No Renovables

Carrera de Ingeniería en Sistemas

Implementación de un Servicio Centralizado de Gestión de Identidades y Control de Acceso de usuarios en aplicaciones web para la Carrera de Ingeniería en Sistemas/Computación de la UNL: SmartLab

Implementation of a Centralized Service for Identity Management and User Access Control in web applications for the Systems/Computer Engineering Career at UNL: SmartLab.

Trabajo de Titulación, previo a la obtención del título de Ingenieros en Sistemas.

AUTORES:
Josué Andrés Macas Caraguay
Jorge Gustavo Tandazo Cueva

DIRECTOR:
Ing. Pablo F. Ordoñez-Ordoñez, Mg. Sc.

Loja - Ecuador

2024

Certificación

Loja, 23 de mayo de 2024

Ing. Pablo F. Ordoñez-Ordoñez, Mg. Sc.

DIRECTOR DEL TRABAJO DE TITULACIÓN

CERTIFICO:

Que he revisado y orientado todo el proceso de elaboración del Trabajo de Titulación denominado: **Implementación de un Servicio Centralizado de Gestión de Identidades y Control de Acceso de usuarios en aplicaciones web para la Carrera de Ingeniería en Sistemas/Computación de la UNL: SmartLab**, previo a la obtención del título de **Ingenieros en Sistemas,** de autoría de los estudiantes **Josue Andres Macas Caraguay** con **cedula de identidad** Nro. **1104123425** y **Jorge Gustavo Tandazo** con **cedula de identidad** Nro. **0705637965**, una vez que el trabajo cumple con todos los requisitos exigidos por la Universidad Nacional de Loja, para el efecto, autorizo la presentación del mismo para su respectiva sustentación pública.

Ing. Pablo Fernando Ordoñez Ordoñez, Mg. Sc.

DIRECTOR DEL TRABAJO DE TITULACIÓN

Autoría

Nosotros, **Josué Andrés Macas Caraguay** y **Jorge Gustavo Tandazo Cueva**, declaramos ser autores del presente Trabajo de Titulación y eximimos expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos, de posibles reclamos y acciones legales, por el contenido del mismo. Adicionalmente aceptamos y autorizamos a la Universidad Nacional de Loja la publicación de nuestro Trabajo de Titulación, en el Repositorio Digital Institucional - Biblioteca Virtual.

Firma: Firmado electrónicamente por: JOSUE ANDRES MACAS CARAGUAY

Cédula de identidad: 1104123425

Fecha: 23 de mayo de 2024

Correo electrónico: josue.macas@unl.edu.ec

Teléfono: 0969916597

Firma: Firmado electrónicamente por: JORGE GUSTAVO TANDAZO CUEVA

Cédula de identidad: 0705637965

Fecha: 23 de mayo de 2024

Correo electrónico: jorge.tandazo@unl.edu.ec

Teléfono: 0992420297

Carta de autorización por parte de los autores, para consulta, reproducción parcial o total y/o publicación electrónica del texto completo, del Trabajo de Titulación.

Nosotros, **Josué Andrés Macas Caraguay** y **Jorge Gustavo Tandazo Cueva**, declaramos ser los autores del trabajo de titulación denominado: **Implementación de un Servicio Centralizado de Gestión de Identidades y Control de Acceso de usuarios en aplicaciones web para la Carrera de Ingeniería en Sistemas/Computación de la UNL: SmartLab**, como requisito para optar por el título de **Ingenieros en Sistemas,** autorizamos al Sistema Bibliotecario de la Universidad Nacional de Loja para que, con fines académicos, muestre la producción intelectual de la Universidad, a través de la visibilidad de su contenido en el Repositorio Institucional.

Los usuarios pueden consultar el contenido de este trabajo en el Repositorio Institucional, en las redes de información del país y del exterior con las cuales tenga convenio la Universidad.

La Universidad Nacional de Loja, no se responsabiliza por plagio o copia del Trabajo de Titulación que realice un tercero.

Para constancia de esta autorización, suscribo, en la ciudad de Loja, a los veintitrés días del mes de mayo de dos mil veinticuatro.

Firma: Firmado electrónicamente por: JOSUE ANDRES MACAS CARAGUAY

Autor: Josué Andrés Macas Caraguay

Cédula de identidad: 1104123425

Dirección: Loja – Cdla. Ciudad Victoria

Correo electrónico: josue.macas@unl.edu.ec

Teléfono: 0969916597

Firma: Firmado electrónicamente por: JORGE GUSTAVO TANDAZO CUEVA

Autor: Jorge Gustavo Tandazo Cueva

Cédula de identidad: 0705637965

Dirección: Loja – Cdla. Tebaida Baja

Correo electrónico: jorge.tandazo@unl.edu.ec

Teléfono: 0992420297

DATOS COMPLEMENTARIOS:

Director del Trabajo de Titulación: Ing. Pablo Fernando Ordoñez Ordoñez, Mg. Sc.

Dedicatoria

Dedico este trabajo a mi familia, por ser el pilar fundamental de mi educación no solo en el ámbito académico sino también en la adquisición de buenos valores; por brindarme su amor, paciencia y apoyo constante, que me ha permitido alcanzar una meta más en mi vida; y sobre todo por ser un ejemplo de tenacidad y constancia que me ha impulsado a perseguir mis sueños. A mis amigos, quienes han compartido conmigo alegrías, tristezas, desafíos y triunfos a lo largo de este camino universitario. Su amistad y apoyo incondicional enriquecieron mi experiencia académica y me recordaron la importancia de la amistad. A mi tutor de trabajo de titulación, el Ing. Pablo F. Ordoñez-Ordoñez, que me ha guiado con su sabiduría y experiencia. Él ha sido un mentor excepcional, que me ha orientado y corregido con paciencia y rigor. A mis docentes, cuya experiencia y conocimiento me ha guiado a lo largo de este proceso. Sus consejos, críticas constructivas y dedicación a la enseñanza han sido fundamentales en mi desarrollo académico y personal. Y a todas las personas que me apoyaron y creyeron en mí, incluso cuando yo mismo dudaba de mis capacidades.

Josue Andres Macas Caraguay

A mi familia, fuente inagotable de amor y apoyo, este logro no sería posible sin ustedes. Cada esfuerzo en este trabajo de titulación está dedicado a quienes siempre creyeron en mí y me alentaron a perseguir mis sueños. A mis amigos, por su amistad, ánimo constante y risas compartidas en este arduo camino académico. A mi director de trabajo de titulación, el Ing. Pablo F. Ordoñez-Ordoñez, cuya sabiduría y orientación fueron mi brújula en este TT. Su compromiso y paciencia son invaluables. A mis profesores, por impartir una educación de calidad que sentó las bases de este logro. Cada lección y desafío contribuyó a mi crecimiento profesional. A mis compañeros de clase, quienes compartieron alegrías y desafíos, su colaboración y amistad hicieron memorable este viaje académico. A todos los que brindaron apoyo, comprensión y aliento, les dedico este trabajo como expresión de gratitud y fuente de inspiración para quienes sigan sus sueños. Este logro representa dedicación y esfuerzo, un tributo a quienes han sido parte de mi vida. Espero que sea el comienzo de un prometedor camino como ingeniero en sistemas y ser humano comprometido con el aprendizaje y el crecimiento continuo.

Jorge Gustavo Tandazo Cueva

Agradecimiento

En primer lugar, agradecemos a nuestras familias por su amor, comprensión y apoyo incondicional a lo largo de este desafiante viaje. Su confianza en nosotros ha sido el motor que nos impulsó a lograr esta meta académica.

A la Universidad Nacional de Loja, a la Facultad de la Energía, las Industrias y los Recursos Naturales No Renovables, especialmente la carrera de Sistemas/Computación y a nuestros respetados docentes, con quienes mantenemos una inmensa gratitud, por brindarnos su apoyo y concejos en el desarrollo de este trabajo.

A nuestros amigos, por compartir con nosotros las alegrías y desafíos de este camino, les agradecemos por su amistad, ánimo constante y risas compartidas, su apoyo fue fundamental en este proceso.

A nuestro director de trabajo de titulacion, Ing. Pablo F. Ordoñez-Ordoñez, quien nos guio con sabiduría y paciencia infinita, en la realización de nuestro TT.

Este trabajo de titulación no solo representa nuestra dedicación y esfuerzo individual, sino también un tributo a todos los que han formado parte de nuestra vida académica. Estamos ansiosos por aplicar los conocimientos adquiridos y seguir creciendo como profesionales en el campo de la Ingeniería en Sistemas.

Josue Andres Macas Caraguay

Jorge Gustavo Tandazo Cueva

Índice de contenidos

Índice de tablas:

Índice de figuras:

Índice de anexos:

Glosario:

- **TT:** Trabajo de titulación
- **IAM:** Identity and Access Manager
- **SSO:** Single Sign-On
- **RBAC:** Role-Based Access Control
- **MFA:** Multi-Factor Authentication
- **OIDC:** OpenId Connector
- **SAML:** Security Assertion Markup Language
- **UNL:** Universidad Nacional De Loja
- **API:** Interfaz De Programación De Aplicaciones
- **RBAC:** Control De Acceso Basado En Roles
- **MFA:** Autenticación Multifactor

1. Título

Implementación de un Servicio Centralizado de Gestión de Identidades y Control de Acceso de usuarios en aplicaciones web para la Carrera de Ingeniería en Sistemas/Computación de la UNL: SmartLab

2. Resumen

El uso de aplicaciones web ha experimentado cambios significativos en los últimos años, lo que ha generado un impacto directo en la autenticación de los usuarios. Esta evolución ha llevado a los usuarios a enfrentarse con la gestión de múltiples identificadores y contraseñas asociadas, lo que resulta incómodo y poco práctico. Ante este desafío, en la carrera de Sistemas/Computación, surgió la necesidad de implementar un servicio centralizado de gestión de identidades y control de accesos, con el fin de simplificar las tareas de administración de usuarios, mejorar las medidas de seguridad y permitir el inicio de sesión único en las diferentes aplicaciones web con las que cuenta.

Para el desarrollo del presente Trabajo de Titulación se siguió una secuencia de 3 fases, en la primera fase, se llevó a cabo una investigación para evaluar y seleccionar una herramienta Open Source para la gestión de identidades y control de accesos en aplicaciones web, obteniendo la herramienta Aerobase Server como la más adecuada debido a que sus características se adaptan a las necesidades requeridas en la carrera. Para la segunda fase, la cual fue la integración de Aerobase con las aplicaciones web de la carrera, se replicó los entornos de trabajo en producción a un entorno local y se realizó las debidas configuraciones tanto en Aerobase Server como en las demás aplicaciones replicadas; posteriormente, una vez integradas correctamente las aplicaciones de forma local, se replicó en producción las configuraciones realizadas, logrando la integración de estas. En la tercera fase se planifico y se ejecutó pruebas para evaluar diferentes aspectos de la integración y en especial el rendimiento del servicio centralizado en los servidores de la Carrera. obteniendo un rendimiento eficaz y aceptación favorable por parte de los usuarios de la carrera.

Finalmente, la implantación de un servicio centralizado de gestión de identidades y control de acceso para las aplicaciones web demostró ser una solución eficaz y necesaria para una gestión más confiable, garantizando un control preciso desde la autorización hasta la autenticación; además, al centralizar la gestión de identidades y el control de acceso, se sentaron bases sólidas para la seguridad e integridad de los usuarios, al tiempo que se impulsó la innovación en el desarrollo de aplicaciones web.

Palabras claves: *Autenticación Centralizada, Gestión de identidades, Control de acceso, IAM, Aerobase Server.*

Abstract

The use of web applications has undergone significant changes in recent years, which has had a direct impact on user authentication. This evolution has led users to be confronted with the management of multiple identifiers and associated passwords, which is cumbersome and impractical. Faced with this challenge, in the Systems/Computing career, the need arose to implement a centralized identity management and access control service, in order to simplify user administration tasks, improve security measures and allow single sign-on in the different web applications it has.

For the development of this Degree Project a sequence of 3 phases was followed, in the first phase, an investigation was carried out to evaluate and select an Open-Source tool for identity management and access control in web applications, obtaining the Aerobase Server tool as the most appropriate because its characteristics are adapted to the needs required in the career. For the second phase, which was the integration of Aerobase with the web applications of the career, the work environments in production were replicated to a local environment and the proper configurations were made both in Aerobase Server and in the other replicated applications; later, once the applications were correctly integrated locally, the configurations made were replicated in production, achieving the integration of these. In the third phase, tests were planned and executed to evaluate several aspects of the integration and especially the performance of the centralized service in the career servers, obtaining an efficient performance and favorable acceptance by the career users.

Finally, the implementation of a centralized identity management and access control service for web applications proved to be an effective and necessary solution for a more reliable management, ensuring precise control from authorization to authentication; moreover, by centralizing identity management and access control, a solid foundation was laid for the security and integrity of users, while boosting innovation in the development of web applications.

Keywords: *Centralized Authentication, Identity Management, Access Control, IAM, Aerobase Server.*

3. Introducción

En un mundo cada vez más digitalizado, donde las aplicaciones web desempeñan un papel fundamental en diversas áreas, la seguridad de la información se convierte en un aspecto primordial para el usuario. Una gestión de identidades eficaz garantiza que los usuarios sean identificados y autenticados con precisión, concediendo acceso a la información y los recursos a las personas autorizadas. Por su parte, el control de acceso mantiene que, una vez autenticado, el usuario sólo pueda ver los recursos y la información que está autorizado a ver.

Sin embargo, el problema surge cuando cada aplicación web tiene sus propios sistemas de gestión de identidades y control de acceso. Esto puede dar lugar a diferentes dificultades como: experiencias de usuario incoherentes entre aplicaciones, mayor complejidad en la gestión del acceso y los permisos de los usuarios, inconvenientes en el seguimiento y la auditoría de la actividad de los usuarios en múltiples sistemas, así como mayores riesgos de seguridad debido a la proliferación de credenciales de usuario con posibles prácticas de seguridad débiles o incoherentes.

La ausencia de una estrategia centralizada expone a las instituciones a riesgos considerables, que incluye la potencial pérdida de información confidencial, la susceptibilidad a amenazas cibernéticas y la dificultad para mantener un seguimiento preciso de las acciones realizadas por los usuarios. Esta carencia no solo implica desafíos en términos de seguridad, sino que también da lugar a complicaciones logísticas y operativas, al gestionar una variedad de datos dispersos como credenciales y permisos.

Es así que, para resolver estos problemas es esencial implantar un servicio de gestión de identidades y control de acceso, que permitan gestionar las identidades de los usuarios y controlar sus permisos de acceso, mejora las experiencias del usuario, simplifica los procesos de administración y mejora notablemente las medidas de seguridad. Además, un servicio centralizado de este tipo puede ofrecer funciones como el inicio de sesión único (SSO), que permite a los usuarios acceder cómodamente a las aplicaciones utilizando dos credenciales. Esto no sólo agiliza la experiencia del usuario, sino que también mejora los niveles generales de seguridad.

Los problemas de seguridad, almacenamiento de datos y autenticación de numerosas

aplicaciones web presentes en la carrera de Sistemas de la UNL, exigen que los usuarios demuestren que son quienes dicen ser, esto se hace mediante el uso de credenciales de acceso, lo que causa molestias a los estudiantes, ya que deben gestionar múltiples identificadores de usuario y contraseñas asociadas, lo que les resulta incómodo; motivo por el cual surge la necesidad de desarrollar el tema para el TT denominado "Implementación de un Servicio Centralizado de Gestión de Identidades y Control de Acceso de usuarios en aplicaciones web para la Carrera de Ingeniería en Sistemas/Computación de la UNL: SmartLab".

Analizar las herramientas que permiten la gestión de identidades y el control de acceso de los usuarios en las diferentes aplicaciones nos ayuda a buscar, evaluar y seleccionar la herramienta que mejor se adapte a los requerimientos de la carrera. Lo que da lugar a la instalación y configuración de la herramienta Open-Source seleccionada.

Considerando la correcta instalación y configuración de la herramienta, es importante evaluar el rendimiento de la misma y a su vez conocer el nivel de utilidad percibida por los estudiantes de la carrera; lo que permite simplificar la administración y mantenimiento de las credenciales; y fortalecer la seguridad al establecer protocolos coherentes y actualizados.

Este TT es de utilidad académica ya que se convierte en fuente de consulta para futuros trabajos afines al campo investigado; siendo su propósito lograr una supervisión más eficiente de las actividades de los usuarios, facilitando la detección temprana de posibles amenazas o anomalías en las aplicaciones controladas por la carrera, proporcionando una estructura unificada para administrar y autenticar las identidades de los usuarios, así como para regular sus derechos de acceso.

El alcance del presente trabajo es el de disponer de un servicio centralizado de gestión de identidades y control de accesos para las aplicaciones web de la carrera de Ingeniería en Sistemas/Computación, ya que se revela como una medida estratégica e indispensable para afrontar los desafíos actuales en la seguridad de las aplicaciones web, además, garantiza la experiencia del usuario, simplifica las tareas de administración, mejora las medidas de seguridad y permite funciones como el inicio de sesión único, consolidando así un marco integral que potencia el rendimiento y la seguridad en el ámbito educativo.

4. Marco teórico

4.1. Gestión de Identidades (Identity Management)

En el contexto de la seguridad de la información y las aplicaciones web, se refiere al proceso de administrar y controlar las identidades de los usuarios, sus credenciales y los permisos asociados. Según Vielberth [1], la gestión de identidades es esencial para garantizar la autenticación y autorización segura de los usuarios en sistemas digitales. Además, Autores como Shostack [2] argumentan que una sólida gestión de identidades es fundamental para proteger los datos confidenciales y mitigar los riesgos de seguridad en las aplicaciones web.

4.1.1 Autenticación

Según lo mencionado por Whitman y Mattord [3], "La autenticación es el proceso de verificar que una entidad es quien dice ser", es decir la autenticación se refiere al proceso de verificar la identidad de un usuario, esto implica el uso de contraseñas, certificados digitales, biometría o factores adicionales.

4.1.2 Autorización

La autorización, por otro lado, se relaciona con el acceso a recursos después de que un usuario ha sido autenticado y se basa en roles, privilegios y políticas de acceso. Autores como Spivey y Echeverria [4] describen la autorización como "el proceso de determinar si un usuario autenticado tiene permiso para acceder a un recurso o realizar una acción específica".

4.1.3 Manejo de perfiles de usuario

La gestión de perfiles de usuario implica la creación, actualización y eliminación de cuentas de usuario, así como la asignación de roles y privilegios. Como se menciona en [3], "el manejo de perfiles de usuario es fundamental para garantizar que los usuarios tengan el acceso adecuado a los recursos y que este acceso sea revocado cuando sea necesario".

4.2 Control de Acceso (Access Control)

El control de acceso es un componente fundamental en la seguridad de la información y las aplicaciones. En este contexto, se refiere a la gestión y regulación de quién tiene permiso para acceder a recursos o realizar acciones específicas en un sistema. Como señala [5], "El control de acceso es esencial para proteger los recursos críticos y confidenciales de una organización al

limitar el acceso solo a usuarios autorizados". El modelo de Control de Acceso Basado en Roles (RBAC), como se explica en [6], es un enfoque común que asigna permisos según roles específicos del usuario, proporcionando una estructura organizativa para la autorización.

4.3 Sistema de Gestión de Identidades y Control de Acceso

De acuerdo con [7], un Sistema de Gestión de Identidades y Accesos (IAM, por sus siglas en inglés) se define como un conjunto integrado de procesos tecnológicos, infraestructura y políticas; diseñado para administrar las identidades de los usuarios y supervisar su acceso a los recursos de una organización.

La tecnología IAM posibilita la creación, adquisición, registro y automatización de la gestión de identidades de usuarios, así como de los permisos de acceso, esto garantiza que los privilegios de acceso se otorgan en consonancia con la interpretación de las políticas establecidas, asegurando que tanto individuos como servicios estén adecuadamente autenticados, autorizados y sujetos a auditoría [8].

4.3.1. Ventajas

Según expone Castro en [8], entre los beneficios de implementar una solución de gestión de identidades y control de accesos son:

- Control de acceso basado en roles: Permite que un usuario tenga acceso sólo a los recursos que su rol permite dentro de la organización; es decir no se le conceden más privilegios que los que se le asignan en base a su función y responsabilidades.
- Automatización: Permite que todos los procesos relacionados con los usuarios sean automáticos, como la creación, eliminación y modificación de cuentas. Además, permite la aprobación instantánea de varios permisos, así como el acceso y la revocación de varios permisos, la asignación de trabajos, etc.
- Reducción de tiempo de accesos y recursos: Permite que un usuario acceda a todos los recursos que se le asignen según sus necesidades.
- Administración centralizada: Consolida los numerosos repositorios de usuarios que pueden existir dentro de una organización, en un único repositorio de gestión de identidades.

4.3.2. Desventajas

Según Castro [8], existen algunas de las desventajas que se pueden observar en la

implementación de una solución de gestión de identidades y control de acceso, de las cuales se destacan las siguientes:

- Dado que el proceso de autenticación y acceso a muchas aplicaciones se realiza en base a un único repositorio central de identidades, cualquier fallo o mal funcionamiento dentro de este repositorio, tiene consecuencias para todas las aplicaciones integradas en él.
- La facilidad de integración de las aplicaciones depende de su complejidad y de los métodos de autenticación y autorización que deban ajustarse y configurarse para el nuevo sistema.

4.3.3. Componentes

Una solución de gestión de identidades y control de acceso cuenta con los siguientes componentes según se menciona en [8]:

- Servicio de directorios: Los directorios son un tipo específico de bases de datos optimizadas para la búsqueda y lectura de datos.
- Sistema de gestión de identidades: es uno de los más importantes ya que, permite administrar las identidades de los usuarios dentro de una organización.
- Sistema de gestión de roles: es un componente que se sitúa entre la gestión de identidades y el control de acceso.
- Fuentes de autoridad: Se compone de nombres y recursos humanos.
- Sistema de gestión de autenticación y control de acceso: Este componente gestiona la configuración de las políticas de autenticación y control de acceso, utilizando la información de los usuarios y los roles almacenados en el Meta directorio.
- Meta-Directorios: es una carpeta que tiene la capacidad de almacenar información de múltiples fuentes, permitiendo que los datos fluyan entre uno o más servicios de directorio y bases de datos, mientras se mantiene la sincronización de datos, convirtiéndolo en uno de los componentes más importantes de los sistemas de gestión de identidad.

4.4. Sistemas de Autenticación

Este tema explora diversos métodos de autenticación, incluyendo contraseñas, autenticación multifactor (MFA), tokens y biometría, comparando y contrastando sus ventajas y desventajas. Según Gibson [9], "La elección del método de autenticación adecuado es crucial para equilibrar la seguridad con la comodidad del usuario", mientras que [10] menciona que la MFA y

biometría, ofrecen capas adicionales de seguridad al requerir múltiples factores de autenticación o características físicas únicas, las contraseñas y los tokens siguen siendo métodos comunes, pero más susceptibles a amenazas; cabe resaltar que es necesario comprender estas opciones, ya que resultan fundamentales para diseñar sistemas de autenticación efectivos y adecuados a las necesidades de seguridad.

4.5. Protocolos de Autenticación

Este apartado se centra en la exploración de protocolos de autenticación comunes, como OAuth, OpenID Connect y SAML, y cómo se aplican en el contexto de las aplicaciones web. [11] afirma que, "OAuth se ha convertido en un estándar ampliamente aceptado para la autorización y autenticación en aplicaciones web, permitiendo que aplicaciones de terceros accedan a recursos protegidos"; de igual manera, explica que "OpenID Connect proporciona una capa de autenticación sobre OAuth, permitiendo la autenticación de usuarios de manera segura y eficiente". En este mismo contexto [12] menciona que "SAML (Security Assertion Markup Language), facilita la autenticación y el intercambio de atributos de usuario entre diferentes sistemas de seguridad", convirtiendo en un aspecto crucial para la interoperabilidad en aplicaciones web federadas, por lo que la comprensión adecuada de estos protocolos garantiza un sólido sistema de autenticación en aplicaciones web.

4.6. Estándares de Identidad

La gestión de identidades en informática se basa en estándares y protocolos que permiten la autenticación y autorización de usuarios en sistemas y aplicaciones. Algunos de los estándares de identidad más relevantes en informática incluyen:

4.6.1. OpenID Connect (OIDC)

El OIDC es un protocolo de autenticación y autorización ampliamente utilizado, que se basa en el estándar OAuth 2.0., además proporciona una forma estandarizada de autenticar a los usuarios y compartir información de identidad de manera segura, destacando en aplicaciones web y móviles que requieran autenticación de usuarios.

Según [13],OpenID Connect “es un protocolo que permite a las aplicaciones que hacen uso de este, verificar la identidad del usuario y obtener información de su perfil", lo que ha permitido que OIDC gane popularidad, gracias a su simplicidad y facilidad de implementación; convirtiéndolo en una opción atractiva para la gestión de identidades en aplicaciones en línea.

4.6.2. Security Assertion Markup Language (SAML)

SAML al igual que el anterior, es otro protocolo ampliamente utilizado en la gestión de identidades, especialmente en aplicaciones empresariales y servicios de federación de identidades; ya que se centra en el intercambio de declaraciones de seguridad entre entidades, lo que resulta valioso en situaciones donde se necesita la federación de identidades. De acuerdo con [14], "SAML permite la autenticación y autorización entre dos partes, generalmente un proveedor de servicios y un proveedor de identidades, esto de manera segura y basada en estándares". El protocolo SAML es esencial en escenarios donde la interoperabilidad y la seguridad son cruciales.

4.6.3. Open Authorization (OAuth 2.0)

Aunque principalmente utilizado para permitir la autorización a recursos alojados por otras aplicaciones, el OAuth 2.0 también desempeña un papel crucial en la gestión de identidades; ya que permite la autorización de aplicaciones y servicios para acceder a información del usuario de manera segura [11].

4.6.4. Open Identity (OpenID)

Según [13], OpenID es un estándar antiguo y menos común que OIDC, sin embargo, sigue siendo relevante puesto que, permite a los usuarios autenticarse en varios sitios web utilizando una única identidad en lugar de múltiples credenciales. Estos estándares desempeñan un papel fundamental en la gestión de identidades dentro del ámbito de la informática, garantizando la seguridad y la interoperabilidad en aplicaciones y servicios en línea, por lo que la elección del estándar adecuado depende de las necesidades específicas de autenticación y autorización de cada sistema o aplicación.

4.7. Administración de usuarios

La administración de usuarios en aplicaciones web es un componente decisivo para garantizar la seguridad, la eficiencia y la satisfacción del usuario. En este sentido, existen mejores y diversas prácticas que deben seguirse para llevar a cabo una gestión efectiva de usuarios. A continuación, se describen algunas de estas mejores prácticas, respaldadas por fuentes bibliográficas relevantes:

4.7.1. Proceso de registro seguro

Implementar un proceso de registro seguro que incluya la verificación de la dirección de

correo electrónico y la autenticación de la identidad del usuario. Esto ayuda a prevenir cuentas falsas o duplicada [15].

4.7.2. Política de contraseñas robustas

Según [16] se basa en establecer requisitos de contraseñas sólidas, que incluyan una combinación de letras, números y caracteres especiales; adicional a esto surge el requerimiento de cambios periódicos en las contraseñas.

4.7.3. Autenticación Multifactor (MFA)

De acuerdo con lo mencionado por [17], promover el uso de la autenticación multifactor contribuye en la protección de información ya que se añade una capa adicional de seguridad; esto implica la verificación de la identidad a través de múltiples métodos, como contraseñas, códigos SMS o aplicaciones de autenticación.

4.7.4. Gestión de permisos y roles

Según [18] es importante asignar permisos y roles de manera adecuada y granular, asegurándose de que los usuarios solo tengan acceso a las áreas y funciones que son relevantes para su trabajo.

4.7.5. Auditoría y monitorización continua

[1] Manifiesta que, es primordial establecer un sistema de auditoría y monitorización continua, esto con la finalidad de detectar actividades inusuales o sospechosas, y a la vez poder generar una respuesta rápida a posibles amenazas.

4.8. Single Sign-On (SSO)

Según expone Rivera en [19], se refiere a tener acceso a varios recursos a través de un único proceso. Gran número de las arquitecturas implementadas en diversas organizaciones fueron creadas con el objetivo de proporcionar a los usuarios acceso a varios servicios web y/o aplicaciones. En la gran mayoría de los casos, cada uno de los servicios o aplicaciones tiene su propio componente de seguridad, lo que compromete la seguridad de todo el sistema; ya que el nivel de seguridad de cada componente es igual al nivel de seguridad del componente más inseguro; es decir el SSO permite a los usuarios acceder a múltiples aplicaciones con una sola autenticación.

4.8.1. Implementación de un SSO

La implementación de un Sistema de Single Sign-On (SSO) se presenta como una estrategia esencial en la gestión de identidades y accesos en el ámbito de las aplicaciones y sistemas. El SSO ofrece una variedad de enfoques para su implementación, a continuación, se detallan algunas de las soluciones más utilizadas, por ser de código abierto (Open Source) o software libre (Free Software); y por sus características clave. Estas implementaciones son respaldadas por la investigación de Torres [20]:

- ✓ **CAS (Central Authentication Service):** CAS, con licencia Apache 2.0, es una implementación de SSO que goza de un sólido respaldo y es ampliamente conocida por su extenso soporte. Ofrece compatibilidad con una serie de protocolos, incluyendo CAS, SAML1, SAML2, OAuth2, SCIM, OpenID Connect y WS-Fed.
- ✓ **JBoss SSO:** desarrollado por Red Hat, JBoss SSO es una solución de SSO federado que se destaca por ser software libre (Free Software).
- ✓ **JOSSO:** desarrollado por la propia JOSSO, ofrece un servidor de SSO de código abierto (Free Software).
- ✓ **Keycloak:** Esta solución de SSO federado, desarrollada por Red Hat, destaca por su capacidad para soportar protocolos normalizados, como OpenID Connect, OAuth 2.0 y SAML 2.0 para la web, además de ofrecer funciones de clustering y single sign-on.
- ✓ **OpenAM:** Originaria de OpenSSO desarrollado por SUN y respaldada por la empresa ForgeRock; OpenAM se especializa en la gestión de accesos, derechos y la plataforma del servidor de federación. Su arquitectura basada en Java cuenta con soporte para una variedad de protocolos, entre ellos SAML, WS-Federation, OpenID y XACML.
- ✓ **Shibboleth:** Se trata de un proyecto de identidad federada con licencia Apache que se basa en el estándar SAML.
- ✓ **WSO2 Identity Server:** Creado por WSO2, el mismo creador del Enterprise Service Bus WSO2, este servidor de identidades ofrece soporte para una serie de protocolos, como SAML 2.0, OpenID, OpenID Connect, OAuth 2.0, SCIM, XACML y Federación pasiva.

Estas implementaciones de SSO representan opciones diversas y adaptables que pueden satisfacer las necesidades específicas de cada organización. La elección de la solución adecuada dependerá de los requisitos y objetivos particulares de cada entorno.

4.8.2. Tipos de SSO

En la actualidad, existen diversas soluciones de Single Sign-On (SSO) que se pueden clasificar en cinco paradigmas según Torres [21]. A continuación, se describen brevemente cada uno de estos enfoques:

Enterprise Single Sign-On (E-SSO): Este enfoque intercepta las solicitudes de autenticación, permitiendo a los usuarios interactuar con sistemas que eliminan la pantalla de inicio de sesión. Es especialmente útil en entornos empresariales donde se necesita un acceso fluido a múltiples aplicaciones. Los sistemas E-SSO evitan la necesidad de ingresar credenciales una y otra vez.

Web Single Sign-On (Web-SSO): Esta variante se enfoca en aplicaciones y recursos basados en la web. Funciona mediante la monitorización del acceso a través de un proxy u otro mecanismo. Los usuarios no autenticados son redirigidos a un servidor de autenticación en línea y solo pueden regresar una vez que han obtenido acceso o han adquirido un TOKEN para la aplicación de destino, mientras que, para identificar a los usuarios autenticados, se utilizan cookies, parámetros GET (menos seguros) o POST.

Kerberos: Kerberos es una solución ampliamente utilizada para externalizar la autenticación de usuarios. Los usuarios se registran en un servidor Kerberos y reciben un "ticket", que luego presentan a las aplicaciones cliente para acceder a los recursos deseados. Este enfoque proporciona una capa adicional de seguridad en la autenticación.

Identidad Federada: se basa en protocolos estándar que permiten a las aplicaciones reconocer a los usuarios sin requerir una autenticación duplicada. Facilita la colaboración entre sistemas y aplicaciones, ya que confía en la autenticación previamente establecida.

OpenID: OpenID es un método de SSO distribuido y descentralizado en el que la identidad de un individuo se almacena en una URL, la cual puede ser verificada por cualquier aplicación o servidor. Esto simplifica el proceso de inicio de sesión, ya que los usuarios pueden utilizar sus credenciales de OpenID en múltiples servicios sin necesidad de crear y recordar contraseñas separadas.

Estos paradigmas ofrecen una variedad de opciones para simplificar la autenticación y el acceso a sistemas y aplicaciones, lo que mejora significativamente la experiencia del usuario y la seguridad en diferentes contextos.

4.9. Autorización Basada en Roles

Se basa en que el rol de un usuario debe estar autorizado, esto garantiza que los usuarios puedan asumir solo roles para los que están autorizado, es decir este tipo de autorización se la puede emplear para controlar el acceso a recursos específicos en una aplicación.

4.10. Privacidad y Cumplimiento

Aborda las cuestiones de privacidad de los datos de usuario y cómo cumplir con regulaciones como el RGPD (Reglamento General de Protección de Datos).

4.11. Inicio De Sesión Único

Según lo mencionado por [22], el inicio de sesión único es un proceso de autenticación del usuario que le permite proporcionar sus credenciales una sola vez para acceder a múltiples aplicaciones, es decir cuando el usuario cambia de aplicación durante esa sesión, se eliminan las futuras solicitudes de autenticación. El inicio de sesión único en la web sólo funciona con las aplicaciones a las que se accede mediante un navegador web. La solicitud de acceso a un recurso web es interceptada por un componente del servidor web o por la propia aplicación. Los usuarios que no están autenticados son enviados a un servicio de autenticación y sólo son liberados después de una autenticación exitosa.

4.12. Trabajos Relacionados

Es de mucha importancia tener como referencia algunos de los trabajos que han sido desarrollados bajo el tema de autenticación centralizada, a fin de poder tener diferentes puntos de vista sobre cómo se realizó este proceso en otras instituciones, por lo que se ha realizado una revisión completa de algunos de estos trabajos de los cuales se hablara a continuación, resaltando los puntos más sobresalientes de cada uno y que resulten de utilidad para el presente TT.

Tabla 1. *Trabajos relacionados*

Titulo	Hallazgo	Referencia
Desarrollo de un prototipo para el servicio de autenticación central de usuarios en aplicaciones web	El presente proyecto tiene como finalidad mostrar el resultado de la implantación de un Sistema de Autenticación Única, expuesto en la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja. Este trabajo presenta el desarrollo del “SAC - Servicio de Autenticación Centralizada - UNL”	[22]

	apoyándose en tecnologías modernas como el protocolo CAS, LDAP entre otros, con el objetivo de integrar el proceso de autenticación de los servicios que maneja en la UTI. Esto beneficia a los usuarios pertenecientes a la entidad y que consumen los recursos de las distintas aplicaciones.	
Implementación de un sistema centralizado de autenticación para usuarios de las diferentes aplicaciones web de la UG	Este proyecto se enfoca en la implementación de un sistema de autenticación centralizada para usuarios de las diferentes aplicaciones web de la Universidad de Guayaquil. Esta solución se aplica con el fin de eliminar la creación de nuevos métodos de autenticación por cada aplicación que se disponga, y a la vez demostrar que se puede centralizar la autenticación de las aplicaciones web para que los usuarios puedan acceder a los diferentes sistemas protegidos con una única autenticación.	[25]
Autenticación centralizada para los sistemas de información de los Institutos Tecnológicos y DGEST	Este trabajo muestra cómo gestionar una sola cuenta para acceder a los sistemas, concentrando en un solo punto el acceso, expuesto en México en el Instituto Tecnológico de Celaya. En este trabajo se presenta los “Sistemas de administración de identidad federada”, con el objetivo de dar solución a los inconvenientes que se presentan al no contar con este servicio, ofreciendo un esquema de autenticación centralizado y gestión de datos personales.	[26]
Implementación de un servicio de autenticación centralizado y gestión de identidades en la Universidad de la República	El presente trabajo de la Universidad de la República de Uruguay trata sobre el mejoramiento de los procesos de autenticación y gestión de identidades, con el fin de tener una identidad unificada que facilite el acceso a recursos, aplicaciones, y servicios. Su enfoque se centra en un Proveedor de Identidad (Identity Provider, IdP) el cual brinda un servicio central de autenticación y además permite realizar Single Sign On (inicio único de sesión), dándole al usuario la posibilidad de acceder a varios sistemas con una sola instancia de autenticación.	[27]

Sistema centralizado de autenticación y autorización "SINGLE SIGN ON"	En este trabajo realizado en la Universidad del Valle de Colombia, se realiza la implementación de una aplicación para controlar la autenticación de los sistemas informáticos de la empresa Carvajal S.A. Esta solución brinda acceso a todas las aplicaciones con solo una instancia de verificación, que permite disminuir el número de peticiones a la mesa de ayuda, reduce los costos de administración y brinda una mayor seguridad en la empresa.	[28]
Sistema centralizado de gestión de usuarios para la Universidad del Tolima	Este proyecto presenta la construcción de un sistema de administración centralizada de usuarios basándose en el modelo Single Sing On (SSO). Esto permite el aseguramiento de credenciales de usuario y el acceso a las distintas plataformas que tiene la universidad del Tolima en Colombia, dependiendo de los roles de los usuarios y los niveles de acceso a la información de manera controlada.	[29]

5. Metodología

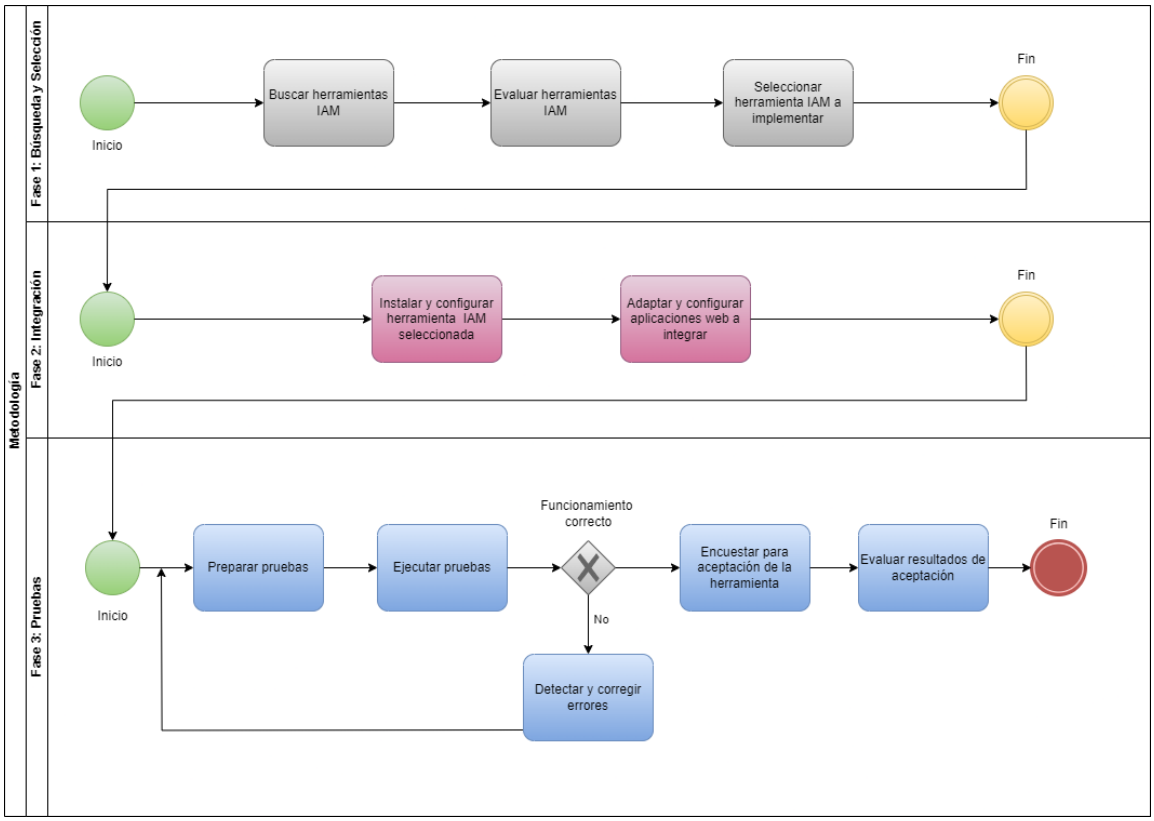


Figura 1. *Diagrama general de la metodología empleada*

Para desarrollar correctamente el TT, se empleó una secuencia de tres fases, como se muestra en la (Figura 1). En la primera fase, que abarcó la búsqueda y selección, se llevó a cabo una investigación en varios navegadores web para encontrar herramientas que se adecuaran a las necesidades expuestas en (Anexo 1, pregunta 7); Una vez recopilado un listado, se procedió a evaluar sus características, lo que permitió seleccionar aquella que ofrecía los mejores beneficios.

En la segunda fase, se procedió con la instalación y configuración de la herramienta seleccionada en la primera fase. Además, se configuraron las aplicaciones web que se mencionan en el (Anexo 1, pregunta 4), para integrarlas con la tecnología que se seleccionó.

La tercera fase culminó con el diseño y la ejecución de un plan de pruebas para verificar el correcto funcionamiento y rendimiento de los recursos integrados. Cada una de estas fases se llevó a cabo cumpliendo los objetivos establecidos para este trabajo.

5.1. Fase 1: Búsqueda y Selección

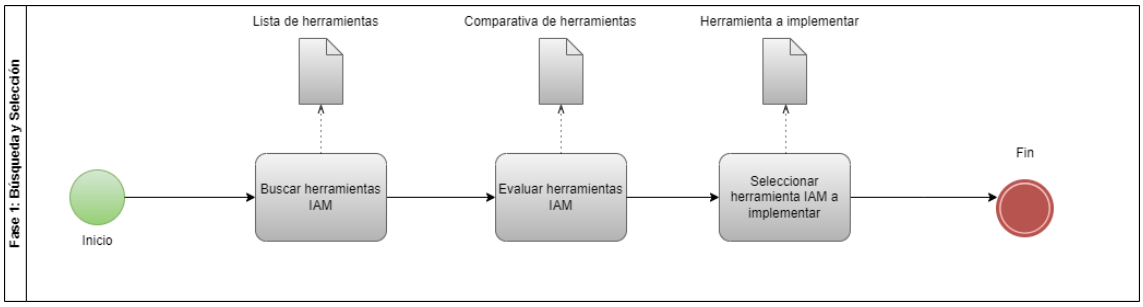


Figura 2. *Proceso de búsqueda y selección de la herramienta IAM*

Esta fase se desarrolló utilizando una metodología específica para evaluar herramientas Free/Open Source, la misma que fue propuesta en [30]. Esta metodología proporcionó una secuencia a seguir detallada para el proceso de búsqueda y selección de una herramienta que permite gestionar usuarios y controlar el acceso a diversas aplicaciones web. En la (Figura 2) se pueden observar los procesos de esta metodología a los mismos que se los describe como subfases.

5.1.1. Subfase 1: Buscar herramientas IAM

Se requirió realizar una investigación en los navegadores web con el propósito de seleccionar un subconjunto de las numerosas herramientas disponibles que se ajusten a un propósito específico. Con este fin, se recopiló y se registró la información necesaria como se muestra en la (Tabla 2):

Tabla 2. *Plantilla para listar subconjunto de herramientas*

Lista de herramientas			
N°	**Nombre**	**Descripción**	**URL**

5.1.2. Subfase 2: Evaluar herramientas IAM

En esta subfase, se completó las planillas de evaluación de acuerdo con los criterios previamente establecidos en la Subfase 1. Para ello, se recopiló información proveniente de fuentes confiables, como el sitio oficial de la herramienta o sitios reconocidos.

En la (Tabla 3) se detalló los aspectos generales de las herramientas que fueron sometidas a evaluación, entre estos están: última versión de la herramienta, año de inicio del proyecto, licencia que maneja la herramienta, plataformas de implementación, tipo de interfaz que utiliza y

lenguaje de programación que se utilizó en el proyecto. Estos datos se obtuvieron mediante visitas a los sitios web oficiales de cada herramienta, garantizando así la obtención de información pertinente y confiable, que sirvieron como base para llevar a cabo la evaluación.

Tabla 3. *Plantilla para evaluar las herramientas elegidas*

Datos generales						
Herramienta	**Versión**	**Inicio del proyecto**	**Licencia**	**Plataforma**	**Interfaz**	**Lenguaje**

En la (Tabla 4) se muestra los criterios de documentación, que nos permitieron conocer los siguientes aspectos de cada herramienta analizada:

- Guía de instalación de la herramienta
- Manual de usuario de la herramienta
- Sección de preguntas frecuentes
- Soporte de la herramienta
- Código comentado
- Información adicional que permita utilizar la herramienta

Tabla 4. *Plantilla para evaluar criterios de documentación*

Criterios de documentación								
Herramienta	**Guía de instalación**	**Manual de usuario**	**Preguntas Frecuentes**	**Soporte Online**			**Código comentado**	**Adicional**
				Foro	**Lista de email**	**Blog**		

En la (Tabla 5) se presentó las pautas que se emplearon para evaluar el nivel de madurez de cada herramienta.

Tabla 5. *Plantilla para evaluar criterios de madurez*

Criterios de madurez				
Herramienta	**Inicio del proyecto (2)**	**Grado de actualización (3)**	**Actividad en lanzamientos (4)**	**Actividad en el reporte de errores (5)**

Indicaciones:

Se completó las plantillas con las siguientes siglas donde:

M = Malo, B = Bueno, R = Regular, MB = Muy bueno

Tabla 6. *Valoración numérica para calificar la madurez de herramientas*

Valoración	**Rango**
Malo	1
Regular	2
Bueno	3
Muy bueno	4

Es importante tomar en cuenta las siguientes premisas, las cuales ayudaron a completar correctamente tabla:

- (2) Se refiere a que si es muy joven quizás no tenga una madurez suficiente
- (3) La última versión se encuentra cercana al año actual
- (4) Se refiere a la frecuencia en la publicación de versiones
- (5) Se refiere a la frecuencia con que se resuelven y reportan errores

5.1.3. Subfase 3: Seleccionar herramienta IAM a implementar

En esta subfase, se seleccionó la herramienta más apropiada para su implementación, tomando como base la información recopilada en la Fase 2. Dicha selección se fundamentó en criterios que incluyeron la calidad de la documentación, la madurez del proyecto y las características inherentes a cada herramienta. Este proceso de selección se llevó a cabo con el objetivo de garantizar una elección informada y adecuada en función de las necesidades.

5.2. Fase 2: Integración

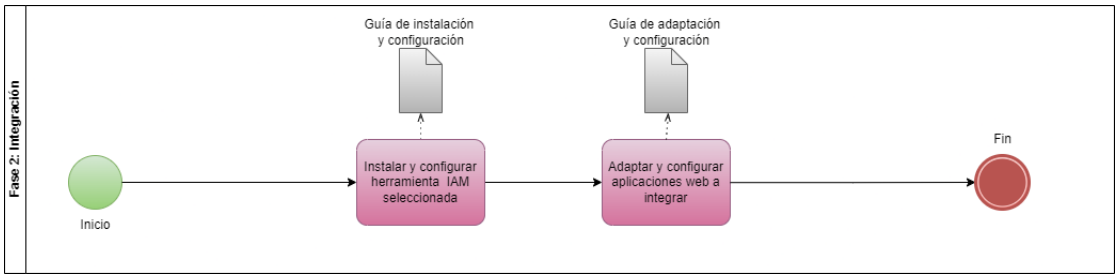


Figura 3. *Proceso para la integración de la herramienta IAM con los aplicativos webs*

El desarrollo de la fase de integración siguió un proceso secuencial tal como se ilustra en la (Figura 3). Este proceso se dividió en dos subfases claramente definidas; esta secuencia se estableció para asegurar una ejecución ordenada y efectiva de la fase de integración, permitiendo un seguimiento claro de cada etapa del proceso lo que garantizó que se cumpla el objetivo principal de esta fase del trabajo. A continuación, se describió cada una de las subfases en las que se trabajó.

5.2.1. Subfase 1: Instalar y configurar herramienta IAM seleccionada

En esta subfase, se realizó la instalación y configuración de la herramienta que fue seleccionada dentro del Objetivo 1. Esta acción fue fundamental, ya que sentó las bases para la implementación exitosa de la herramienta en el entorno deseado. La instalación y configuración adecuadas fueron esenciales para asegurar que la herramienta funcione de manera eficiente y cumpla con las necesidades previamente identificados (Anexo 1, pregunta 7).

5.2.2. Subfase 2: Adaptar y configurar aplicaciones web a integrar

Una vez que se completó la subfase 1, en la que se instaló y configuró la herramienta que permite llevar a cabo la gestión de usuarios de manera centralizada, se inició la etapa de adaptación y configuración de las aplicaciones web; Tanto estas adaptaciones como configuraciones fueron fundamentales para establecer una integración efectiva entre las aplicaciones. A través de esos ajustes, se estableció las conexiones y parámetros necesarios para que las aplicaciones puedan trabajar en conjunto.

5.3.Fase 3: Pruebas

La Fase 3 se centró en las pruebas, las cuales se centraron en dos actividades fundamentales que garantizan la calidad y un funcionamiento eficaz de cada integración. Estas actividades son:

5.3.1. Diseño de Pruebas

En este apartado se planificó las pruebas a realizar con el fin de validar que el sistema cumple con las necesidades requeridas (Anexo 1, Pregunta 7); para esto, se utilizó una secuencia de pasos la cual se muestra en la (Figura 4), y se detalla cada paso a continuación:

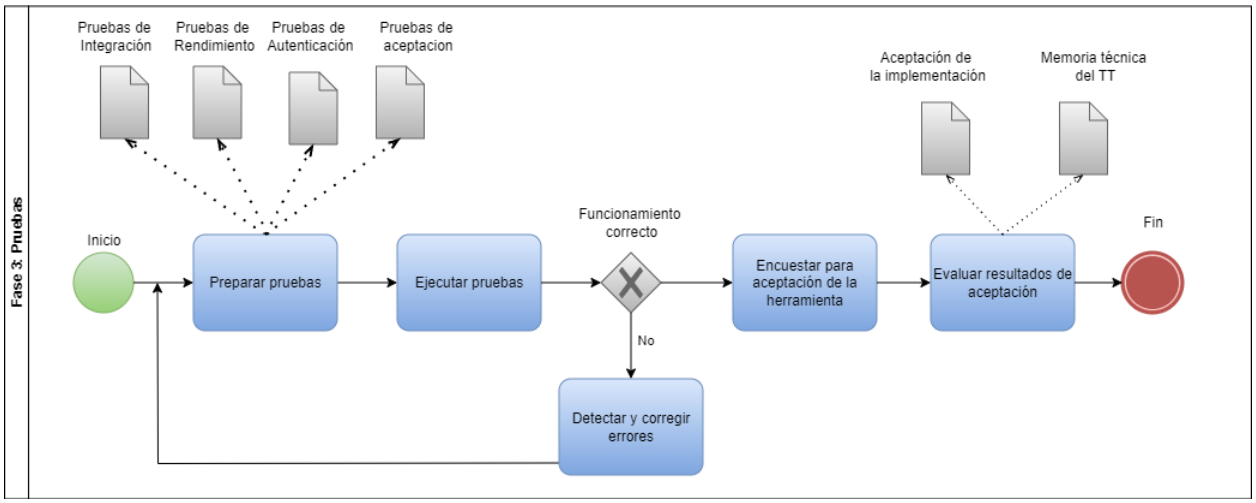


Figura 4. Secuencia de pasos para la fase de pruebas

Preparar pruebas: En esta etapa, se planificó las pruebas que se llevaron a cabo. Aquí se incluyó la identificación de los casos de prueba, una descripción y el resultado de cada prueba.

Ejecutar pruebas: Una vez que las pruebas estuvieron listas, se llevó a cabo la ejecución de las pruebas.

Detectar y corregir errores: Durante la ejecución de las pruebas, era probable que se encuentren errores o problemas. Si el sistema no funcionaba correctamente, se debía tomar medidas para corregir los problemas y asegurarse de que el sistema funcione según lo esperado.

Encuestar para aceptación de la herramienta: Después de la ejecución de las pruebas, se realizó una encuesta para determinar si el sistema pasaba o no las pruebas de aceptación por parte de los usuarios finales.

Evaluar resultados de aceptación: Finalmente, se realizó una evaluación de los resultados de las pruebas de aceptación para saber si se habia cumplido con los objetivos e identificar cualquier área que pueda necesitar mejoras.

A continuación, se describe una a una las pruebas que se realizaron:

Pruebas de integración

Culminadas las configuraciones se verifica el correcto funcionamiento de las aplicaciones, mediante pruebas de integración. Para lo cual se necesitó detallar los casos de prueba que serán verificados; y dicha información será presentada con las respuestas esperadas para definir la veracidad de las pruebas y especificadas en el formato de la (Tabla 7) [31], [32]. En este caso, las pruebas se centraron en la interacción de interfaces entre distintos sistemas.

Tabla 7. Formato de casos de pruebas de integración

Id	Objetivo	Descripción de la prueba	Resultados esperados

Los test de integración de sistemas se pueden realizar tanto después de las pruebas de sistema, como de forma paralela a ellas [33].

Pruebas de rendimiento

Para verifica el rendimiento del sistema se necesitó detallar la muestra de usuarios para cada caso de prueba, la misma que se presentó con el tiempo promedio de respuesta del sistema y tasa de error, especificadas en el formato de la (Tabla 8).

Tabla 8. *Formato de casos de pruebas de rendimiento*

Muestra	Tiempo promedio de respuesta	Tasa de error	Rendimiento del sistema

Pruebas de autenticación

Para las pruebas de autenticación se enfocó en evaluar diez aspectos clave de la autenticación web, presentando la vulnerabilidad que se analizó y los resultados que se esperaban, esto se especificó en el formato de la (Tabla 9).

Tabla 9. *Formato de casos de pruebas de autenticación*

No. de Referencia	Vulnerabilidad	Resultados de vulnerabilidad

Prueba de aceptación

Para la prueba de aceptación, se recopiló datos para evaluar la utilidad del Servicio Centralizado de Gestión de Identidades y Control de Acceso de Usuarios (IAM), esto mediante una encuesta de utilidad percibida. El diseño de la encuesta se basó en la pregunta de investigación y los objetivos específicos, posteriormente se revisó y se validó el cuestionario para asegurar la claridad y relevancia de las preguntas.

5.3.2. Ejecución de Pruebas

En esta sección, se ejecutó las pruebas previamente diseñado. Durante esta ejecución, se analizaron los resultados obtenidos a través de criterios de evaluación y aceptación establecidos para cada prueba realizada:

- Pruebas de integración: caso de prueba, descripción de lo que se probara y resultado.
- Pruebas de rendimiento: carga de usuarios, tiempo de respuesta, tasa de error, rendimiento del sistema.
- Pruebas de autenticación: número de referencia, vulnerabilidad y resultados de vulnerabilidad.

Finalmente se realizó una encuesta, la cual se aplicó a los estudiantes de 8vo y 9no ciclo de la carrera de computación, para conocer la utilidad percibida de la integración del servicio de gestión de identidades y control de acceso.

5.4.Recursos

5.4.1. Bibliográficos

Revisión de registros: Dio lugar a una revisión exhaustiva de documentación relevante, la cual permitió obtener información valiosa de las herramientas Open Source, a su vez que ayudó a identificar sus características principales.

5.4.2. Técnicos

Entrevista: Se realizó una entrevista virtual; donde se utilizó preguntas para obtener información acerca de la necesidad de implantar una herramienta para gestionar usuarios y controlar accesos en la carrera de Sistemas/Computación, además de las tecnologías con las que se contaba para realizar la integración de las mismas.

Encuesta: Se realizó una encuesta en línea, donde se estableció preguntas claves las cuales permitieron conocer el nivel de rendimiento de la implementación realizada en el presente TT.

5.4.3. Recursos de Software y Hardware

Tabla 10. *Recursos de Software*

Recurso	Descripción	Acceso
OneDrive	Sistema de almacenamiento para llevar un control de versiones del documento	https://www.microsoft.com/es-ww/microsoft-365/onedrive/online-cloud-storage
Node js	Entorno para desarrollar el backend con javascript	https://nodejs.org/es
Visual Studio Code	Editor de código fuente	https://code.visualstudio.com
GitHub	Repositorio online para almacenar y realizar el control de versiones de la DApp.	https://github.com
Selenium IDE	Es una herramienta para diversos tipos de pruebas.	https://www.selenium.dev/
JMetter	Aplicación diseñada para probar la carga del comportamiento funcional y medir el rendimiento.	https://jmeter.apache.org/
OWSTG	Recurso de pruebas de ciberseguridad para desarrolladores de aplicaciones web y profesionales de la seguridad.	https://owasp.org/www-project-web-security-testing-guide/v41/
AngularJS	Framework de JavaScript, que se utilizan para crear sitios web dinámicos.	https://angularjs.org/

Tabla 11*. Recursos de Hardware*

Recurso	Descripción
Laptop	Dispositivo tecnológico fundamental para la elaboración del Trabajo de titulación.

5.4.4. Personal

Tabla 12. *Encargados de realizar el trabajo de titulación*

Cargo	Nombres y Apellidos	Correo
Director de TT y director de carrera	Pablo F. Ordoñez-Ordoñez, Mg. Sc.	pfordonez@unl.edu.ec
Encargado de desarrollar el TT	Josué Andrés Macas Caraguay	josue.macas@unl.edu.ec
Encargado de desarrollar el TT	Jorge Gustavo Tandazo Cueva	jorge.tandazo@unl.edu.ec

6. Resultados

6.1. Analizar los servicios Open Source que permitan la gestión de identidades y control de acceso mediante una metodología para la evaluación de herramientas Free/Open Source.

R1. Servicios Open Source para la gestión de identidades y control de acceso.

Se realizó una búsqueda minuciosa en navegadores web populares como Chrome y Firefox, con el fin de identificar herramientas Open Source que cumplieran con los requisitos de gestión de usuarios y control de acceso en aplicaciones web. De un conjunto de opciones disponibles, se seleccionaron seis de estas herramientas como sujetos de estudio, lo que implicó un proceso de filtración y evaluación para determinar cuáles eran las más adecuadas para los objetivos del TT.

La (Tabla 13), que se presenta a continuación, proporciona un resumen de las herramientas seleccionadas para su posterior evaluación. Cada herramienta se acompañó de una descripción detallada, lo que permitió comprender sus características clave y su funcionalidad. Además, se incluyó la dirección electrónica de los sitios web oficiales de estas herramientas, lo que proporcionó un acceso directo a recursos adicionales que resultaron valiosos en el proceso de evaluación.

Tabla 13. *Datos generales de las herramientas a evaluar*

Lista de herramientas			
N°	**Nombre**	**Descripción**	**URL**
1	CAS	CAS es una solución empresarial multilingüe de inicio de sesión único y un proveedor de identidad para la web e intenta ser una plataforma integral para sus necesidades de autenticación y autorización. Además, es un protocolo de autenticación abierto y bien documentado. La implementación principal del protocolo es un componente de servidor Java de código abierto con el mismo nombre alojado aquí, con soporte para una gran cantidad de funciones y protocolos de autenticación adicionales.	https://www.apereo.org/projects/cas
2	IdentityServer	Es un marco OpenID Connect y OAuth 2.0 para ASP.NET Core, está rediseñado para ASP.NET Core y .NET Core, incorpora todas las implementaciones de protocolo y los puntos de extensibilidad necesarios para integrar la	https://identityserver4.readthedocs.io

		autenticación basada en token, el SSO y el control de acceso API en sus aplicaciones. Se puede usar para hacer que su aplicación sea un servidor de autenticación/inicio de sesión único. También puede emitir tokens de acceso para clientes de terceros, empresas que utilizan .NET para crear soluciones de control de acceso e identidad para aplicaciones modernas, incluido el inicio de sesión único, la gestión de identidades, la autorización y la seguridad de API. IdentityServer tiene certificación OpenID y forma parte de .NET Foundation	
3	Aerobase Server	Aerobase es una solución IAM que básicamente se deriva de Keycloak y algunos otros proyectos de código abierto, pero agregó más funciones al juego. Se forjó como un nuevo marco de IAM para admitir microservicios y ampliar las funcionalidades de control de acceso, la regulación de la privacidad. La lista de características del servidor de Aerobase incluye inicio de sesión único (SSO), inicio de sesión social, autenticación de dos factores, compatibilidad con LDAP y Active Directory, interfaz de usuario personalizable, administración de identidad/acceso y gestión de identidad. Es compatible con OpenID Connect, OAuth2.0 y SAML 2.	https://aerobase.io/
4	Open Identity Platform	Open Identity Platform es un ecosistema completo de soluciones IAM para la empresa. El proyecto se compone de varios subproyectos: **OpenAM:** gestión de acceso abierto **OpenDJ:** un directorio compatible con LDAPv3 basado en tecnologías Java **OpenIG:** puerta de enlace de identidad abierta. Un servidor proxy diseñado para la gestión de sesiones. **OpenIDM:** es una solución de administración de acceso e identidad abierta de Libre. **OpenICF;** Open Identity Connector Framework: es una solución de marco de conector que actúa como puente entre la gestión de identidades y la gestión de seguridad/auditoría. Todos los proyectos de Open Identity Platform se publican con una licencia de código abierto en GitHub.	https://www.openidentityplatform.org/

5	Apache Syncop	Es una solución multiplataforma para administrar identidades digitales para la empresa. Está construido sobre Java y, como parte de la base de Apache, se publica bajo la licencia Apache 2.0. Apache Syncop ofrece un control completo sobre el proceso de gestión de identidades que incluye el aprovisionamiento, la auditoría, la generación de informes, la administración, la gestión de políticas, la gestión de contraseñas y la gestión de políticas de contraseñas. Viene con una rica API REST.	https://syncope.apache.org/
6	Keycloak	Es una solución de gestión de acceso e identidad (IDM) patrocinada por Red Hat. Es un proyecto rico en características que lo hace listo para la empresa. Keycloak admite SSO "Single-Sign-On", varios protocolos como OpenID Connect, OAuth 2.0, SAML 2.0, inicio de sesión en redes sociales y admite LDAP y Active Directory. También admite políticas de contraseña personalizadas. Está diseñado para ser extensible para agregar nuevas funcionalidades personalizadas con la ayuda de un desarrollador experimentado.	https://www.keycloak.org/

R2. Evaluación de servicios Open Source

En esta sección se expuso la evaluación individual de cada herramienta seleccionada para su análisis dentro de este TT; para ello se tomó en cuenta los siguientes criterios generales: datos generales, criterios de documentación y criterios de maduración; en donde cada uno de estos criterios presentaron distintas pautas que permitieron evaluar de mejor manera cada herramienta.

Tabla 14. *Datos generales de las herramientas elegidas*

Datos generales						
Herramienta	**Versión**	**Inicio del proyecto**	**Licencia**	**Plataforma**	**Interfaz**	**Lenguaje**
CAS	CAS SERVER 7.0.X	2005	Apache 2.0 License	Windows, Linux	GUI	Java
IdentityServer	IdentityServer4	2020	Apache 2.0 License	Independiente	GUI	.NET
Aerobase Server	aerobase-2.17.3	2018	Apache 2.0 License	Windows, Linux, Unix	GUI	Ruby, Java

Open Identity Platform	OpenIDM-5.5.0	2019	Common Development and Distribution License 1.1	Linux	GUI	XML, Java, PHP
Apache Syncop	Apache Syncop-3.0.6	2006	Apache 2.0 License	Windows, Linux, Unix, Mac	GUI	Java
Keycloak	Keycloak-24.0.1	2014	Apache 2.0 License	Linux	GUI	C#, Java, Python

De acuerdo con los criterios del apartado de datos generales se pudo observar que las herramientas más recientes son: IdentityServer en el año 2020, Open Identity Platform en el año 2019 y Aerobase Server en el año 2018; todas estas en su versión más actualizada.

Tabla 15. *Evaluación de criterios de documentación de las herramientas elegidas*

Criterios de documentación								
Herramienta	**Guía de instalación**	**Manual de usuario**	**Preguntas Frecuentes**	**Soporte Online**			**Código comentado**	**Adicional**
				Foro	**Lista de email**	**Blog**		
CAS	SI	NO	SI	NO	NO	SI		
IdentityServer	SI	NO	NO	NO	NO	SI		
Aerobase Server	SI	SI	SI	SI	NO	SI		
Open Identity Platform	SI	NO	NO	NO	SI	SI		
Apache Syncop	SI	SI	NO	NO	NO	NO		Java docs
Keycloak	SI	SI	SI	NO	NO	SI		

Según los criterios de documentación, la herramienta que contó con mayor información de su funcionamiento fue Aerobase Server, seguida de CAS, Open Identity Platform e IdentityServer. Considerando la valoración numérica presentada en la (Tabla 6) en donde prevalecen cuatro rangos de calificación: malo (1), regular (2), bueno (3) y muy bueno (4); se realizó la puntuación individual de las herramientas analizadas dentro del ámbito Criterios de madurez.

Tabla 16. *Evaluación de criterios de madurez de las herramientas elegidas*

Criterios de madurez					
Herramienta	**Inicio del proyecto (2)**	**Grado de actualización (3)**	**Actividad en lanzamientos (4)**	**Actividad en el reporte de errores (5)**	**Promedio Total**
CAS	B	B	R	R	2.5
IdentityServer	R	B	R	R	2.25
Aerobase Server	B	MB	B	B	3.25
Open Identity Platform	B	B	R	B	2.75
Apache Syncop	B	R	R	R	2.25
Keycloak	B	R	R	R	2.25

Tomando en cuenta todos los criterios de madurez de las herramientas y la calificación otorgada a las mismas; sobresalió la aplicación Aerobase Server con una puntuación de 3.25 equivalente a Bueno.

R3. Herramienta Open Source para la integración

En base a los resultados obtenidos con anterioridad en la (Tabla 15) y (Tabla 16), sobresalió la herramienta Aerobase Server, la misma que proporcionó una documentación extensa para su instalación y configuración. Dentro de los beneficios que nos brido sobresalen algunos tales como:

- Autenticación multifactor.
- Autenticación móvil.
- Certificación de acceso.
- Gestión de contraseñas.
- Gestión de credenciales.
- Gestión de cuentas privilegiadas.
- Gestión de políticas.
- Gestión de usuarios.
- Panel de comunicaciones.
- Provisión de usuarios.
- Registro único.

En la (Figura 5), se observa de forma general como se compone esta herramienta, la misma que por medio de protocolos como Oauth2.0, OpenID Connect Y SAML permitieron gestionar la autenticación en las aplicaciones web.

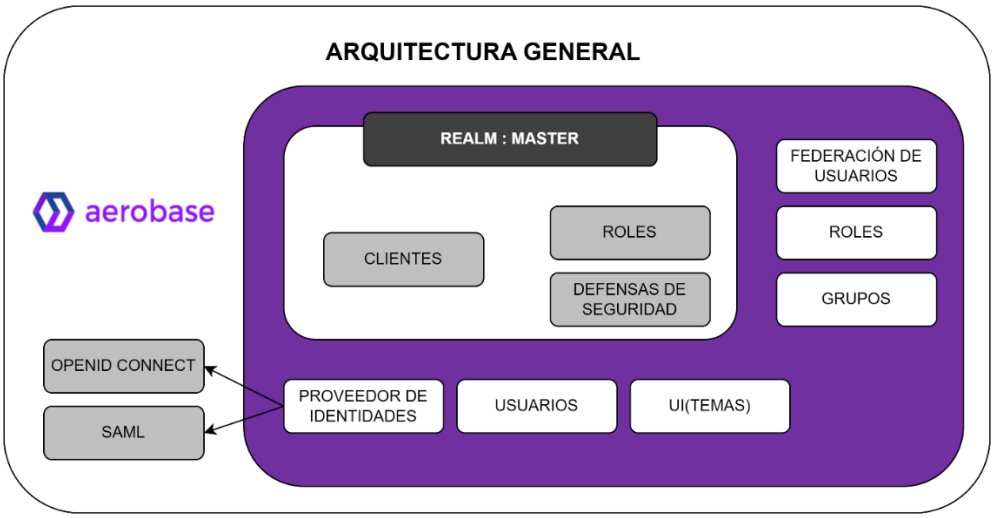


Figura 5. *Arquitectura general de Aerobase*

6.2. Integrar el servicio centralizado de gestión de identidades y control de acceso con las aplicaciones web existentes en la carrera.

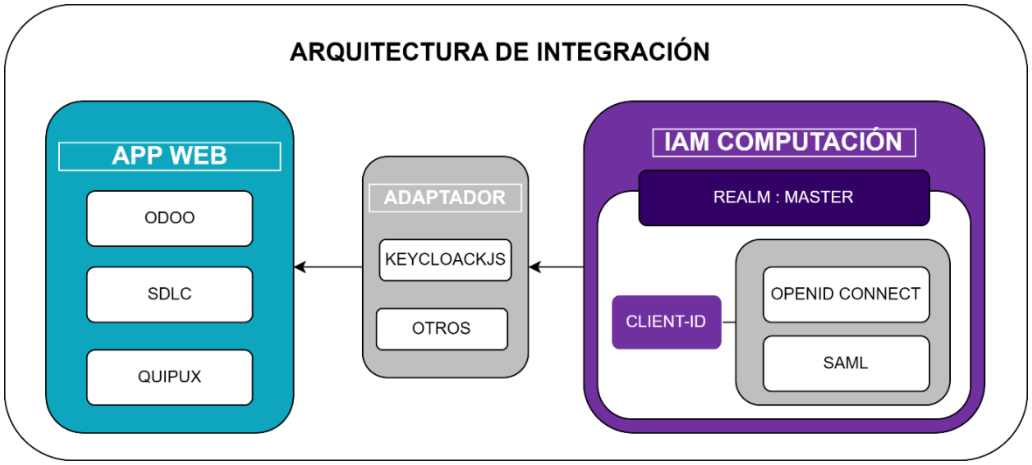


Figura 6. *Arquitectura utilizada para la integración*

En esta fase se llevó a cabo la instalación de Aerobase la misma que se empezó a denominar como IAM Computación. En la (Figura 6), se presenta de manera general como se integró los aplicativos webs con IAM Computación, para lo que se utilizó un adaptador que nos permitió entablar una conexión (Oauth, OpenID Connect, SAML), entre las dos partes.

R4. Instalación de Aerobase Server.

Para llevar a cabo este proceso de instalación fue necesario contar con los recursos básicos tales como:

- Tener al menos 512Mb de RAM
- Tener al menos 1GB de espacio en disco
- Tener instalado mínimo Java 11 JDK, o posteriores

En el entono de producción donde se procedió a realizar la instalación de la herramienta se cuenta con un almacenamiento de 30GB, 8GB de RAM, sistema operativo CentOS7, Java 11JDK. Para descargar los paquetes de instalación de Aerobase se utilizó:

- *"curl -k -O https://packages.aerobase.io/rhel/aerobase-2.17.3-1.el7.x86_64.rpm"* para descargar el primer paquete de instalación; y
- *"curl -k -O https://packages.aerobase.io/rhel/aerobase-iam-2.17.3-1.el7.x86_64.rpm"* para el segundo paquete de instalación.

Una vez descargados los paquetes se realizó la instalación de estos utilizando el comando *"rpm -vhi"* tal como se muestra en la (Figura 7).

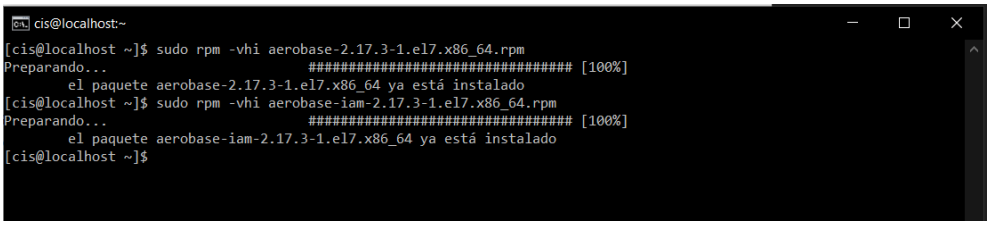


Figura 7. *Instalación de los paquetes de Aerobase Server*

Posteriormente, se ejecutó el proceso de configuración por defecto que trae Aerobase, con el fin de activar las configuraciones en sus componentes, las cuales se realizaron mediante el comando *"sudo aerobase-ctl reconfigure",* tal como se muestra en la (Figura 8).

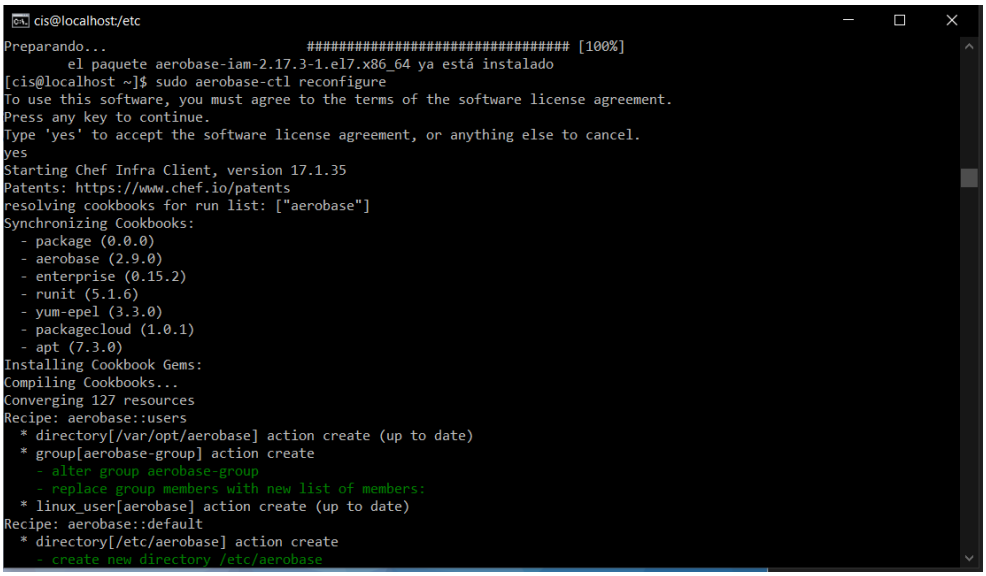


Figura 8. *Ejecución del comando aerobase-ctl reconfigure*

Una vez realizada la configuración se modificó el archivo aerobase.rb ubicado en el directorio */et/aerobase/,* en el cual se cambió la opción *external_url* tal como se muestra en la (Figura 9), ya que es la dirección desde la cual Aerobase Server será accesible.

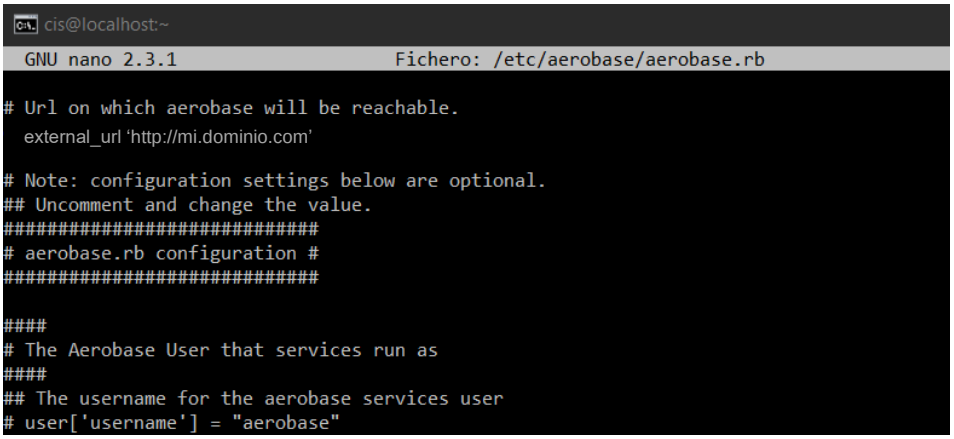


Figura 9. *Configuración del external_url*

Adicional a esto se crearon los certificados SSL para establecer la conexión segura entre el servidor de Aerobase y el Navegador, dichos certificados se establecieron en la carpeta SSL ubicada en /etc/aerobase/ssl. En el archivo aerobase.rb se habilitó el proxy inverso nginx y se agregó la dirección de los certificados SSL. Para aplicar todos los cambios realizados anteriormente se ejecutó el comando *"sudo aerobase-ctl reconfigure".*

Aplicados los cambios se ingresó al servidor de forma local, para crear el usuario de Superadministrador y poder continuar la administración mediante la interfaz de Usuario; una vez creado el usuario de Superadministrador se puedo acceder a la administración de Aerobase desde "http://mi.dominio/auth/admin", la misma que nos redirecciono hacia un formulario de inicio de sesión el cual que se puede observar en la (Figura 10).

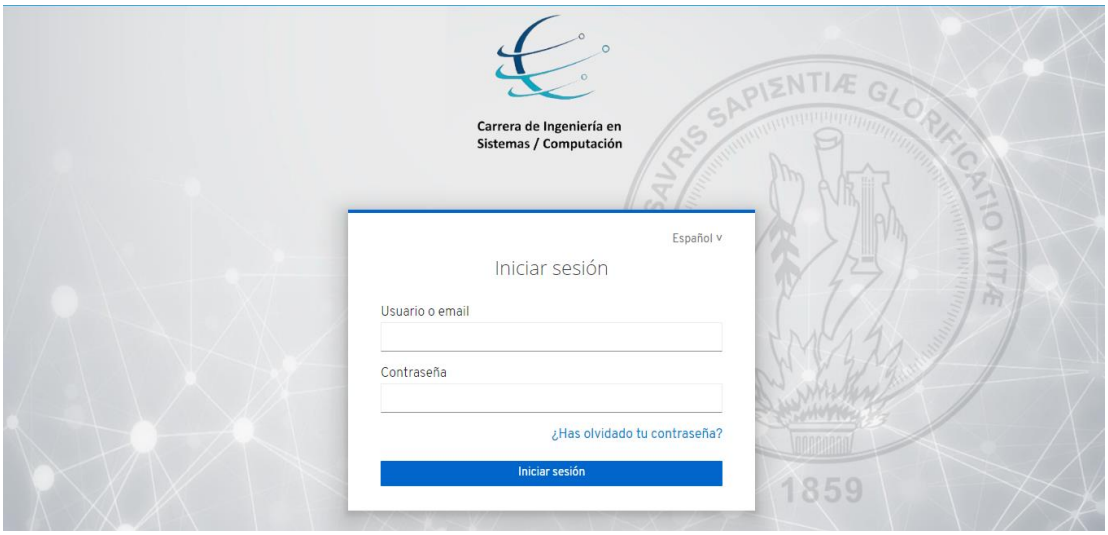


Figura 10. *Página de inicio de sesión de Aerobase*

Finalmente, se ingresó las credenciales correctamente con el fin de poder ingresar a la interfaz principal de Aerobase tal como se muestra en la (Figura 11), mediante la cual se pudo realizar configuraciones adicionales para la administración de usuarios y grupos, gestión de identidades, autenticación, entre otras características.

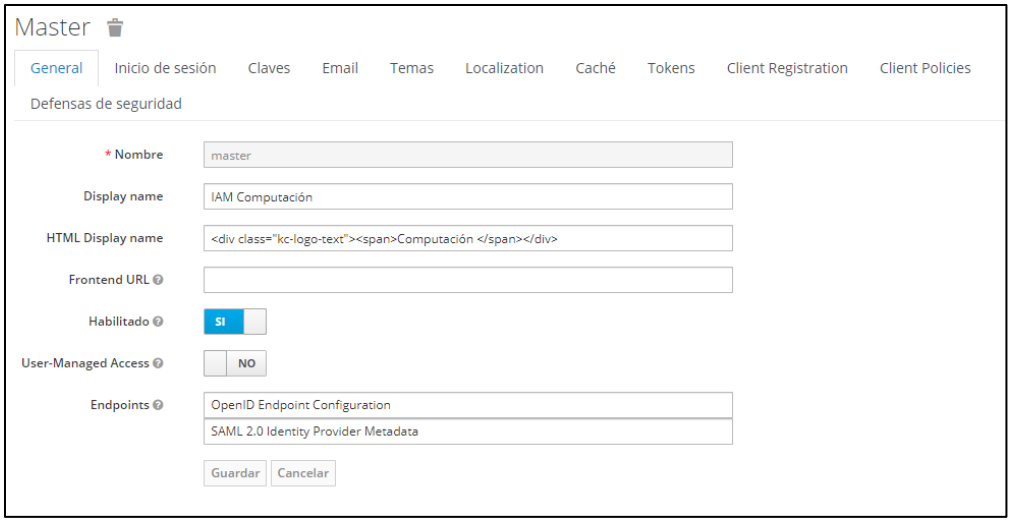


Figura 11. *Interfaz principal de Aerobase*

R5. Configuración de Aerobase

R5.1. Configuración de grupos y roles de usuarios

Para la creación de grupos, primero se seleccionó la opción "Grupos" del menú de la izquierda y se dio clic en la opción "Nuevo". Después, se asignó un nombre descriptivo al grupo y finalmente, se guardó el grupo recién creado.

Figura 12. *Creación de grupos*

Para asignar usuarios a grupos se navegó a la sección de "Usuarios" y se seleccionó el usuario al que se quería asignar al grupo. Dentro del perfil del usuario, se redirecciono a la pestaña "Grupos" y se agregó el usuario al grupo correspondiente.

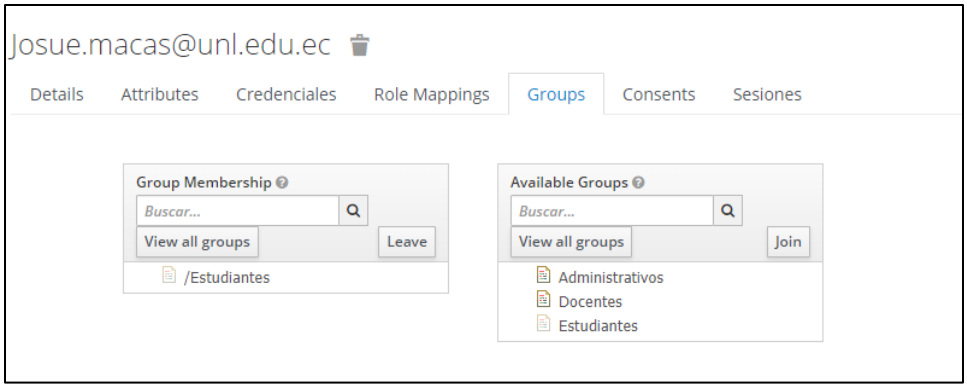


Figura 13. *Asignación de usuarios a los grupos*

Para la creación de roles se dirige a la sección "Roles" en el menú lateral izquierdo, luego, se hiso clic en "Añadir Rol" y se asignó un nombre representativo al nuevo rol.

Figura 14. *Creación de roles*

Para asignar roles a Grupos o Usuarios se navegó a la sección "Grupos", se seleccionó el grupo y se agregó los roles deseados.

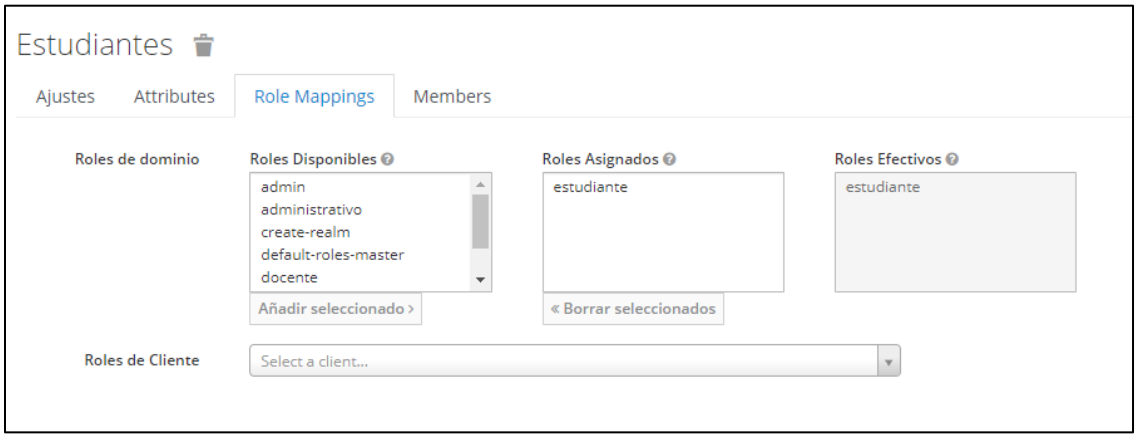


Figura 15. *Asignación de roles a los grupos*

Para asignar un rol a un usuario, se redirecciono a la sección "Usuarios", donde se elige el usuario y se le asigna los roles en la pestaña correspondiente.

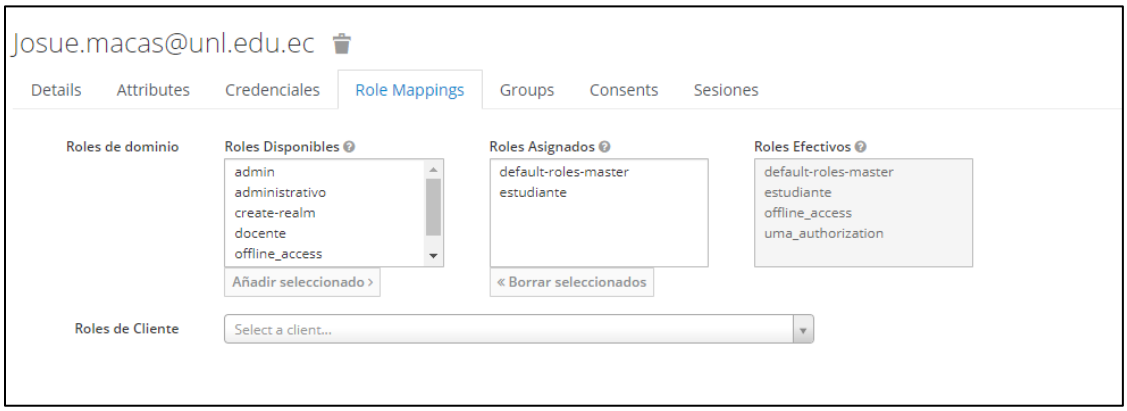


Figura 16. *Asignación de roles a usuarios*

Finalmente, para verificar la configuración se inició sesión con los usuarios asignados a diferentes roles y grupos, asegurándose de que los usuarios tengan acceso adecuado según sus roles y grupos.

Esta configuración proporcionó un enfoque escalonado y organizado para la administración de usuarios y sus permisos en Aerobase. Al asignar usuarios a grupos y roles, se simplifica la gestión y se estableció un marco flexible para la aplicación de políticas de seguridad y autorización. Fue fundamental realizar pruebas exhaustivas para garantizar que la configuración se ajustó a las necesidades específicas.

R5.2. Creación de cliente de conexión

Para realizar el proceso de creación y configuración de un nuevo cliente de conexión dentro de Aerobase se utilizó el protocolo OpenID Connect o el protocolo SAML 2.0. Para registrar un cliente se accedió al apartado de Clientes donde aparece una lista con todos los clientes ya configurados, se procedió a dar clic en el botón Crear, tal como se puede observar en la (Figura 17).

Figura 17. *Creación un cliente de conexión*

Se estableció el ID Cliente y la URL raíz (URL Base de aplicación web), en este caso, la URL fue "http://mi.dominio.com". En el apartado de Protocolo del Cliente se aseguró de que esté configurado en openid-connect y se guardó la información para registrar el nuevo cliente.

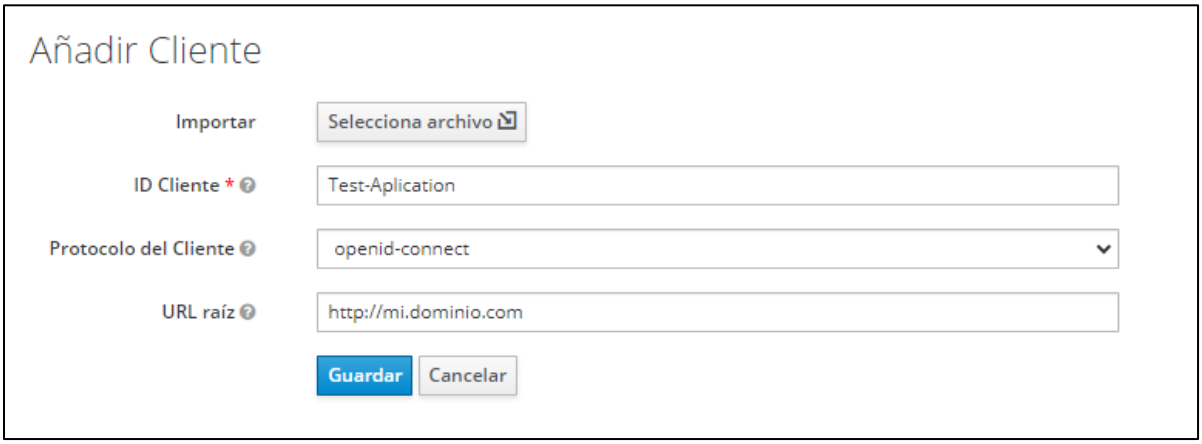


Figura 18. *Configuración para añadir un cliente*

En la (Tabla 17), se observa las URL necesarias para la configuración correcta de un cliente en Aerobase.

Tabla 17. *Valores para completar configuración del cliente en Aerobase*

Propiedad	Valor	Razón
Root URL	• http://mi.dominio.com	Se antepone a las URL redirigidas
Valid Redirect URIs	• /realms/master/account/* • http://mi.dominio.com:3334/*	Redirigir ubicación después de cerrar sesión
Base URL	• /	Url que se utiliza por defecto para usar cuando el servidor de autorización necesita redirigir al cliente
Web Origins	• http://mi.dominio.com/*	Origen permitido para CORS (Realmente importante para aplicaciones web)

En la (Figura 19), se observa la configuración que se llevó a cabo en Aerobase para poder realizar la conexión con la aplicación a proteger.

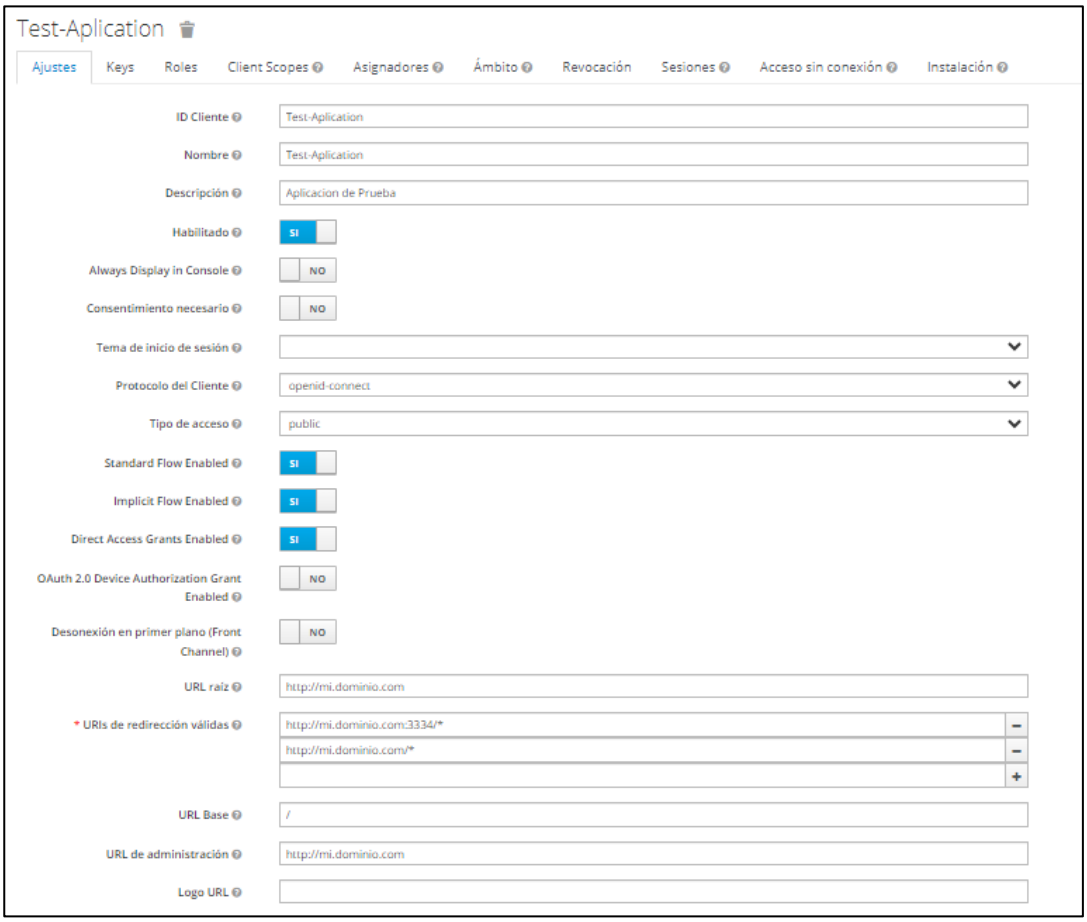


Figura 19. *Configuración completa de un cliente en Aerobase*

R6. Configuración de los aplicativos webs ODOO, SDLC Y QUIPUX.

En la (Figura 20) se muestra el proceso general que se empleó para la integración entre Aerobase y los aplicativos webs con los que cuenta la carrera.

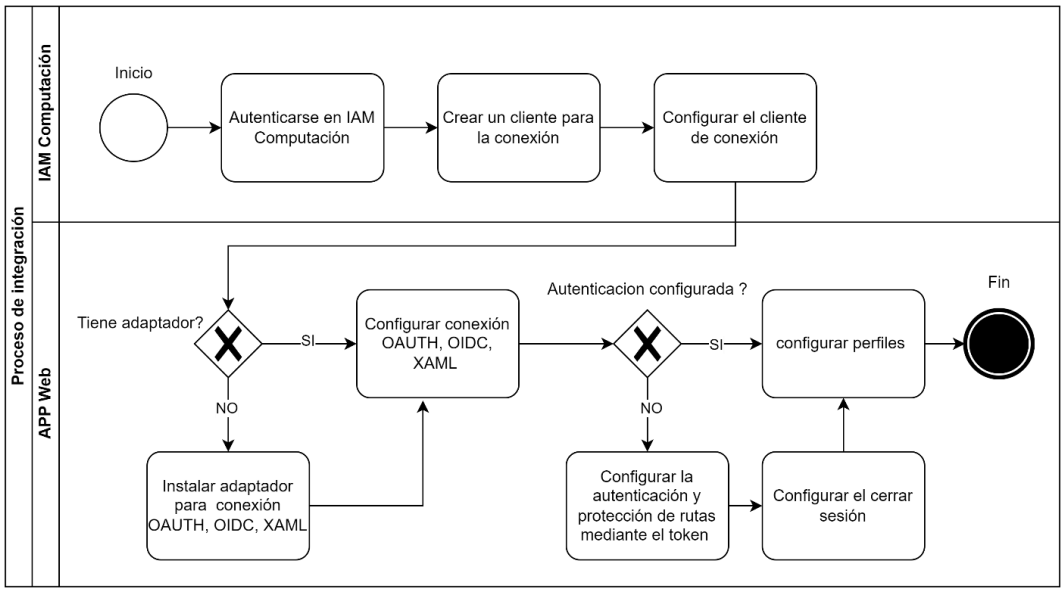


Figura 20. *Proceso seguido para la integración*

R6.1. Configuración de ODOO

OIDC (OpenID Connect), funciona como un marco de autorización, las aplicaciones pueden acceder a las cuentas de usuario en un servicio HTTP. Este protocolo opera a través de la delegación de la autenticación al servicio que aloja la cuenta del usuario, permitiendo que las aplicaciones de terceros obtengan autorización para acceder a dichas cuentas. En este contexto, Aerobase cumple un rol crucial como servicio de autenticación y autorización para las aplicaciones que optan por delegar el proceso de acceso.

Una vez configurado el cliente de lado de Aerobase, se realizó la configuración en Odoo, partiendo de una actualización en su módulo de proveedores de Oauth, para lo cual se instaló una librería llamada **Auth OAuth Keycloak**, el mismo que está disponible en **https://www.odoo-wiki.org/auth-oauth-keycloak.html.**

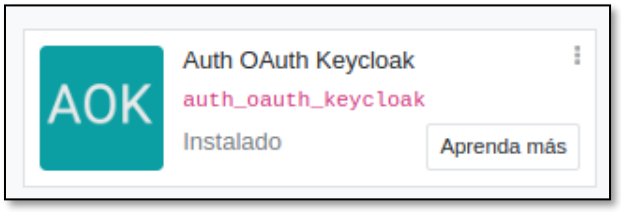


Figura 21. *Módulo para instalar en ODOO*

Este módulo realizó los siguientes cambios:

- Agregó un nuevo campo x_keycloak al modelo auth. oauth.provider.
- Actualizó la vista *auth_oauth. view_oauth_provider_form* con el campo Keycloak.
- Anuló los métodos de la clase _auth_oauth_rpc y _auth_oauth_validate res.users

Los nuevos métodos admitieron el formato de token de acceso de portador, por lo tanto, hicieron posible la autenticación con Aerobase. Seguidamente se agregó a Aerobase como proveedor de OAuth en Odoo.

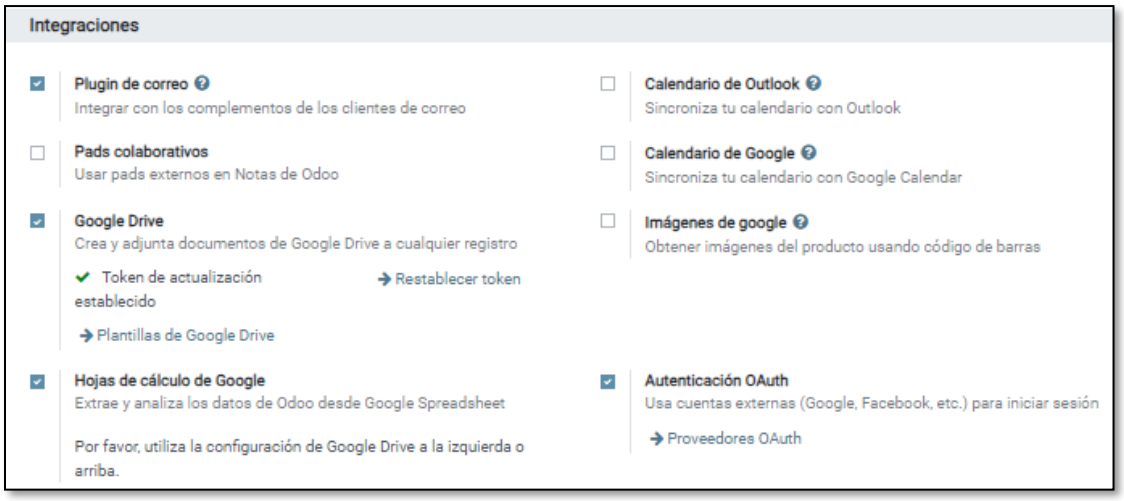


Figura 22. *Sección de integraciones en ODOO*

Para realizar la creación de un nuevo proveedor OAuth en Odoo, se abrió el panel de control de Odoo y se dirigió a ajustes, luego se bajó a la sección de Configuración general y en el apartado Integraciones se habilito la Autenticación OAuth; luego se hizo clic en Proveedores OAuth, seguido apareció la lista de los proveedores OAuth que se encontraban registrados, en caso de tenerlos. Se seleccionó la opción de Crear para agregar un nuevo proveedor, para esta integración la configuración establecida se dio tal y como se muestra en la (Figura 23).

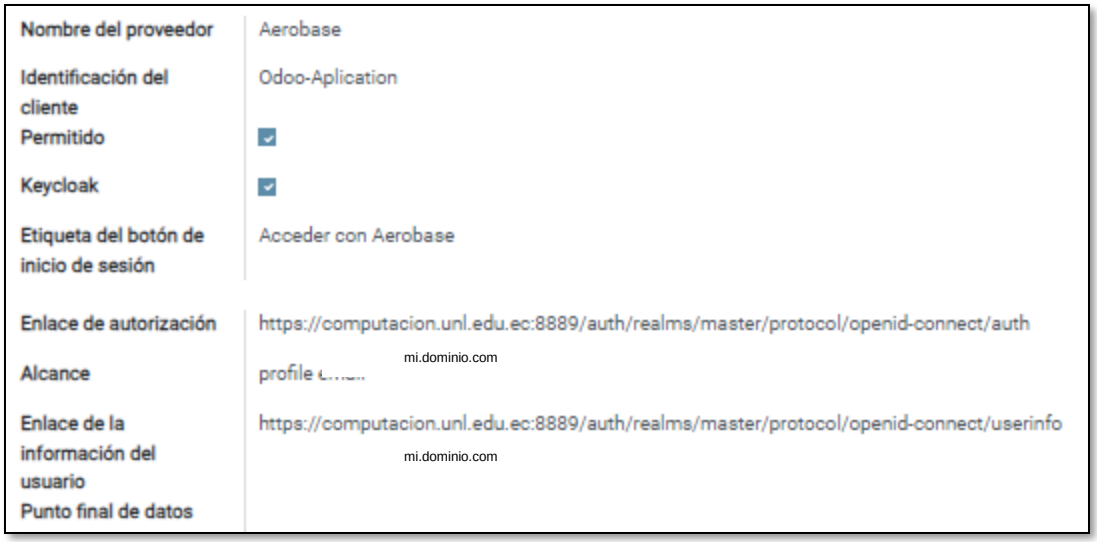


Figura 23. *Datos del proveedor OAuth de Aerobase en ODOO*

Para probar la configuración se partió desde el inicio de sesión de Odoo el mismo que se observa en la (Figura 24). En este caso apareció una opción nueva de acceder, la cual se denominó como Acceder con IAM Computación, el mismo que redirecciono a un formulario donde se ingresaron las credenciales de Aerobase.

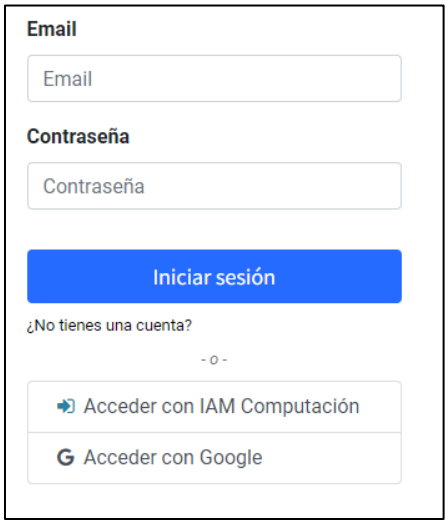


Figura 24. *Inicio de sesión de Odoo*

En caso de no estar iniciado sesión con IAM computación, se presenta el formulario de la (Figura 25), el que tiene como requisitos: correo electrónico y una contraseña, dando acceso a la aplicación.

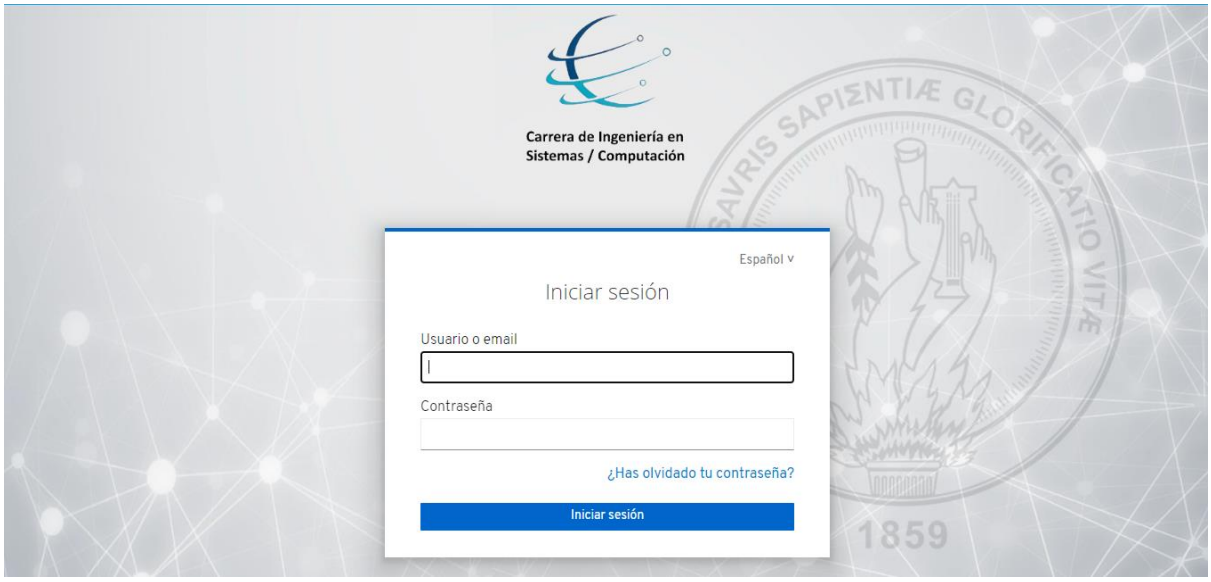


Figura 25. *Inicio de sesión con Aerobase*

De contar con los permisos de acceso correspondientes a la aplicación Odoo, Aerobase procede a redirigir a la aplicación tal y como se presenta en la (Figura 26).

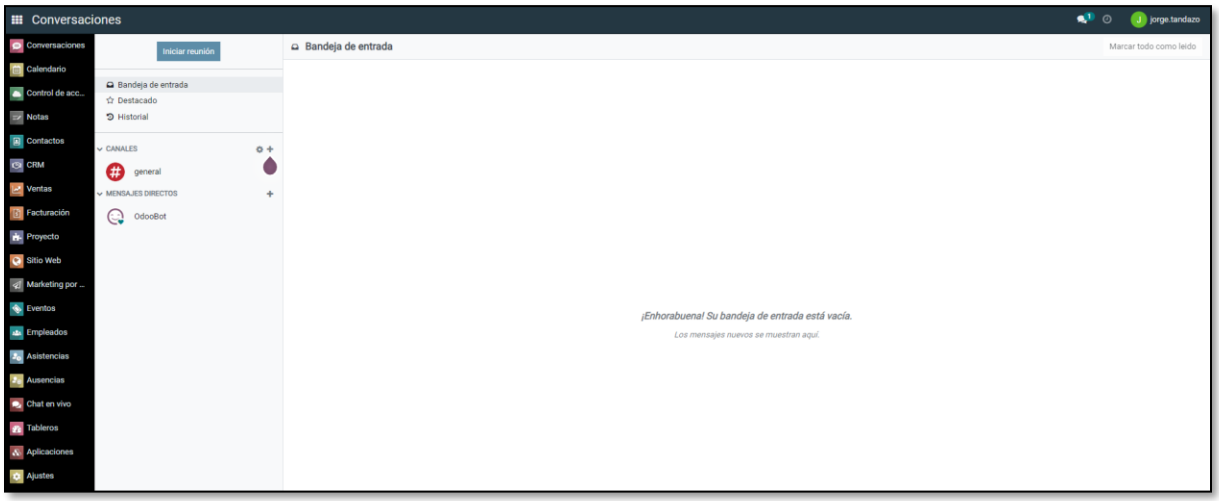


Figura 26. *Inicio de sesión a ODOO exitoso*

R6.2. Configuración SDLC

Una vez configurado el cliente de lado de Aerobase, se realizó la configuración en SDLC. Dentro del archivo App.module.ts, la conexión inicial se estableció mediante la implementación de la biblioteca Keicloack.js. A través del protocolo OpenId Connect, se logró instaurar un eficiente canal de comunicación entre Aerobase y SDLC, como se detalla en la (Tabla 18), y en la (Figura 27). Este proceso de conexión se realizó juntamente con el proyecto en el frontend

desarrollado en Angular.

Tabla 18. *Código para la configuración de conexión entre Aerobase y SDLC*

```
import {KeycloakAngularModule, KeycloakService} from 'keycloak-angular';
import {AuthenticationService} from './_services/auth.service';
function initializeKeycloak (keycloak: KeycloakService) {
 return () =>
  keycloak.init({
   config: {
    realm: 'Nombre_realms',
    url:'http://mi.dominio.com/auth',
    clientId: 'ID_cliente'
   },
   initOptions: {
    onLoad: 'login-required',
    checkLoginIframe: false
   }, enableBearerInterceptor:true
  });
}
```

Figura 27. *Inicialización de conexión entre SDLC y Aerobase*

En la (Tabla 19), se describe el proceso de obtención del token, fundamental para la emisión al backend y la ejecución de las peticiones necesarias. Este token garantizó la seguridad

de las rutas, permitiendo así un control efectivo sobre el acceso y las acciones autorizadas dentro del sistema.

Tabla 19.*Configuración para la protección de rutas*

```
isAccessAllowed (route: ActivatedRouteSnapshot, state: RouterStateSnapshot): Promise <boolean | UrlTree> {
    return new Promise(async (resolve, reject) => {
      if (!this.authenticated) {
        this.keycloakAngular.login();
        resolve(false);
        return;
      }
      var data_token = await this.keycloakAngular.loadUserProfile();
      var res = await fetch(`${environment.apiURL.v1}/user/email/${data_token.email}`, {
        method: 'GET',
        headers: {
          'Content-Type': 'application/json'
        }
      });
      res = await res.json();
      await localStorage.setItem('currentUser', JSON.stringify(res));
      const requiredRoles = route.data["roles"];
      let granted: boolean = false;
      if (!requiredRoles || requiredRoles.length === 0) {
        granted = true;
      } else {
        for (const requiredRole of requiredRoles) {
          if (this.roles.indexOf(requiredRole) > -1) {
            granted = true;
            break;
          }
        }
      }
      if (granted === false) {
        resolve(granted)
      }
      resolve(granted)
    });
  }
```

La (Tabla 20) exhibe la función encargada de cerrar sesión tanto en el entorno de desarrollo

de software (SDLC) como en Aerobase, esta función permitió una finalización segura y coherente de las sesiones, contribuyendo a la gestión eficiente de la seguridad y la integridad del sistema.

Tabla 20. *Función para el cierre de sesión en SDLC*

```
async logout() {
    await localStorage.removeItem('currentUser');
    await this.keycloakAngular.logout();
    this.currentUserSubject.next(null);
}
```

En la parte del backend, se llevó a cabo la decodificación del token con el propósito de validar su autenticidad y obtener los correspondientes permisos, además de la información del usuario. Esta información permitió la creación del perfil en caso de que no estuviera previamente configurado, esto se muestra en la (Tabla 21).

Tabla 21. *Configuración de token en el bakend de SDLC*

```
try {
    var payload = jwt_decode(token);
    if (payload.exp <= moment().unix()) {
      return res.status(401).send("Token Expirado");
    }
    var account = await User.findOne({ email: payload.email });
    if (account) {
      account = await User.findByIdAndUpdate(account._id,{ $set: data }, { new: true });
    } else {
      account = await User.create(data);
    }.
  } catch (error) {
    console.log(error);
    return res.status(401).send("Token no válido");
  }
```

R6.3. Configuración Quipux

Una vez configurado el cliente en Aerobase, se llevó a cabo la configuración en Quipux. Este proceso se inició con la creación del archivo destinado a la conexión y configuración inicial de Aerobase. Esto se logró mediante la inclusión de la biblioteca JavaScript de Keycloak en el encabezado HTML, tal como se muestra en la (Tabla 22).

Tabla 22. *Inclusión del script Keycloak.js*

```
<script src="http://mi.dominio.com/auth/js/keycloak.js"></script>
<script src="https://ajax.googleapis.com/ajax/libs/jquery/3.5.1/jquery.min.js"></script>
```

En la (Tabla 23), se muestra la configuración de la conexión especificando parámetros como: el dominio (realm), la URL del servidor de autenticación, el identificador del cliente (clientId), y otras configuraciones relevantes para asegurar la comunicación; estos parámetros fueron esenciales para que la aplicación web supiera cómo y dónde autenticar a los usuarios.

Tabla 23.*Configuración para la conexión con Aerobase*

```
const keycloak = Keycloak({
        "realm": "Nombre_realm",
        "auth-server-url": "http://mi.dominio.com/auth",
        "ssl-required": "external",
        "clientId": "ID_Cliente",
        "resource": "php_service",
        "public-client": true,
        "verify-token-audience": true,
        "use-resource-role-mappings": true,
        "confidential-port": 0
      })
```

Luego, se inicializó Keycloak con las opciones definidas (modo de respuesta y flujo de autenticación), donde se indicó que fuera necesario el inicio de sesión o login-required, para continuar, es decir que, al acceder a la página, el usuario fuera redirigido automáticamente a la página de inicio de sesión de Keycloak, si no se ha iniciado sesión previamente. Una vez que el usuario estuviera autenticado exitosamente, el código captura el correo electrónico del usuario autenticado como parte del token proporcionado por Keycloak y posteriormente, redirige al usuario a la página autenticación_aerobase.php dentro de la aplicación, pasando el correo electrónico como parte de la URL, esto se muestra en la (Tabla 24).

Tabla 24. *Inicialización de Keycloak.js*

```
const initOptions = {
        responseMode: "fragment",
        flow: "standard",
        onLoad: "login-required"
      };
```

En el archivo autenticación_aerobase.php, primero se estableció una ruta base y se incluyó archivos esenciales como: el manejador de conexiones a la base de datos, la configuración principal de la aplicación y configuraciones relacionadas con la replicación de datos, esto se muestra en la (Tabla 25).

Tabla 25. *Inclusión de archivos esenciales de configuración global*

```
1. $ruta_raiz = ".";
2. include_once("$ruta_raiz/include/db/ConnectionHandler.php");
3. include_once("$ruta_raiz/config.php");
4. include_once("$ruta_raiz/config_replicacion.php");
5. $db = new ConnectionHandler("$ruta_raiz");
6. $db->conn->SetFetchMode(ADODB_FETCH_ASSOC);
```

Luego se verificó si se proporciona un parámetro email a través de la URL, si está presente, se procede a buscar al usuario correspondiente en la base de datos y se extraen cédula y código de usuario. Si se encuentra el usuario en la base de datos, se prepara y se establece variables para la sesión, iniciando sesión mediante la inclusión de session_orfeo.php y la configuración de seguridad de sesión con securesession.class.php, (Tabla 26).

Tabla 26. *Validación y autorización del usuario mediante token*

```
 1. if (isset($_GET['email'])) {
 2.   $email = $_GET['email'];
 3.   if (isset($krd)) {
 4.     $acceso = "login";
 5.     $_GET['acceso'] = $acceso;
 6.     $_POST['krd'] = $krd;
 7.     include_once "$ruta_raiz/session_orfeo.php";
 8.     require_once "$ruta_raiz/securesession.class.php";
 9.     if (!isset($_SESSION['initiated']) && isset($_SESSION["krd"])) {
10.       $ss = new SecureSession();
11.       $ss->check_browser = true;
12.       $ss->check_ip_blocks = 2;
13.       $ss->secure_word = 'QUIPUX_COMUNIDAD_V4';
14.       $ss->regenerate_id = false;
15.       $ss->Open();
16.       $_SESSION['initiated'] = true;
17.     }
18.     if (isset($_SESSION["krd"])) {
19.       echo "<script>window.location = 'index_frames.php';</script>";
```

```
20.     }else{
21.       echo "error";
22.     }
23.   } else {
24.     echo "<script>window.location = 'perfilNoEncontrado.php';</script>";
25.   }
26. } else {
27.   echo "<script>window.location = 'perfilNoEncontrado.php';</script>";
28. }
```

Finalmente, si la sesión se inicia correctamente, el usuario es redirigido a la página principal de la aplicación, tal como se muestra en la (Figura 28); caso contrario, se redirige al usuario a una página de error.

Figura 28. *Página principal de Quipux*

6.3. Evaluar el servicio centralizado de gestión de identidades y control de acceso en escenarios de experimentación.

Preparar pruebas

Se diseñaron diversos tipos de pruebas para evaluar distintos aspectos de la herramienta implementada. Entre ellas, se prepararon tres casos de prueba específicos para verificar la integración de la herramienta con las aplicaciones web seleccionadas. Estas pruebas se centraron en comprobar la conexión, los accesos o autenticación y la finalización de sesión.

Tabla 27. *Casos de pruebas de integración*

Número del Caso de Prueba	Componente	Descripción de lo que se probará	Prerrequisitos
CP01	IAM Computación	Conexión de Aerobase con las aplicaciones Odoo, SDLC, Quipux.	Navegador web, clientes registrados en Aerobase para cada aplicación
CP02	IAM Computación	Accesos a las aplicaciones Odoo, SDLC, Quipux.	Navegador web y Cuenta con permisos a aplicaciones en Aerobase
CP03	IAM Computación	Verificar el cerrado de sesión en las aplicaciones Odoo, SDLC, Quipux.	Navegador web y Cuenta con permisos a aplicaciones en Aerobase

Para medir el rendimiento, se prepararon seis tipos de casos de prueba, los cuales fueron evaluados utilizando la herramienta JMeter. Estos casos incluyeron aquellos que se espera sean utilizados con mayor frecuencia por los usuarios, garantizando así una evaluación exhaustiva y representativa del rendimiento en condiciones de uso real.

Tabla 28. *Casos de pruebas de rendimiento*

Número del Caso de Prueba	Componente	Descripción de lo que se probará
CP01	IAM Computación	Página de inicio de sesión
CP02	IAM Computación	Acceso a la cuenta mediante el inicio de sesión
CP03	IAM Computación	Información de perfil
CP04	IAM Computación	Actualización de credenciales
CP05	IAM Computación	Autenticación de un cliente de IAM Computación
CP06	IAM Computación	Cerrado de sesión

Para realizar pruebas de autenticación, se tomó como referencia el manual OWASP, específicamente el apartado 4.4, que proporciona diez casos de prueba fundamentales para validar la seguridad de la implementación. Este enfoque asegura que las pruebas aborden los aspectos

críticos de autenticación, incluyendo la robustez de las contraseñas, la gestión de sesiones y la protección contra ataques de fuerza bruta. Al seguir estas directrices, se busca garantizar que la implementación cumpla con los estándares de seguridad más rigurosos y proteja adecuadamente los datos de los usuarios. La aplicación de estos casos de prueba es esencial para identificar y mitigar posibles vulnerabilidades en el sistema.

Tabla 29. *Casos de pruebas de autenticación*

Categoría	Numero de Referencia	Nombre de la Prueba	Vulnerabilidad
Pruebas de autenticación	OWASP-AT-001	Transporte de Credenciales sobre canal cifrado	Transporte de Credenciales sobre canal cifrado
	OWASP-AT-002	Credenciales predeterminadas	Credenciales predeterminadas
	OWASP-AT-003	Mecanismo de bloqueo débil	Mecanismo de bloqueo débil
	OWASP-AT-004	Omitir el esquema de autenticación	Omitir el esquema de autenticación
	OWASP-AT-005	Recordar contraseña vulnerable	Recordar contraseña vulnerable
	OWASP-AT-006	Debilidades de la caché del navegador	Debilidades de la caché del navegador
	OWASP-AT-007	Política de contraseñas débiles	Política de contraseñas débiles
	OWASP-AT-008	Respuesta débil a preguntas de seguridad	Respuesta débil a preguntas de seguridad
	OWASP-AT-009	Funcionalidades de cambio o restablecimiento de contraseña débil	Funcionalidades de cambio o restablecimiento de contraseña débil
	OWASP-AT-010	Autenticación más débil en un canal alternativo	Autenticación más débil en un canal alternativo

Para evaluar la aceptación de la implementación, se llevó a cabo una encuesta compuesta por 12 preguntas. Estas preguntas fueron diseñadas para medir de manera precisa y detallada la satisfacción y aceptación de los usuarios respecto a la nueva herramienta.

Tabla 30. *Encuesta para aceptación*

Nro.	Pregunta
*	Edad
*	Genero
1	¿Con qué frecuencia utiliza la aplicación de gestión de identidad y acceso centralizado?

2	¿Cuál es el propósito principal de utilizar esta aplicación?
3	¿Cómo calificaría la actualización de credenciales proporcionado por IAM Computación?
4	Respecto a la recuperación de contraseña, ¿Considera que IAM Computación ofrece un proceso claro y eficiente para recuperar contraseñas olvidadas o perdidas?
5	¿Qué tan efectiva considera usted la implementación de la autenticación de doble factor en IAM Computación para garantizar la seguridad de las cuentas de usuario?
6	En general, ¿Cómo calificaría la utilidad del servicio proporcionado por IAM Computación en relación con la gestión de credenciales y accesos a los aplicativos webs?
7	¿Cómo evalúa la experiencia de acceso a las aplicaciones web mediante el Servicio IAM incorporado en la Carrera de Ingeniería en Sistemas/Computación de la UNL?
8	¿Qué características de la aplicación encuentras más útiles?
9	¿Qué características de la aplicación cree que podrían mejorarse para que sea más útil?
10	¿Confía en la seguridad de la aplicación para proteger sus datos personales y contraseñas?
11	¿Siente que sus datos personales están adecuadamente protegidos mientras utiliza esta aplicación?
12	¿Ha experimentado algún problema significativo al utilizar IAM Computación en cualquiera de los aspectos mencionados?

R7. Resultados de las pruebas de Integración

Tabla 31. *Resultados de las pruebas de Integración*

Nro. Caso de Prueba	Elemento	Descripción de lo que se probará	¿OK?	Observación
CP01	IAM, Odoo, SDLC, Quipux.	Conexión de Aerobase con las aplicaciones Odoo, SDLC, Quipux.	✓	N/A
CP02		Accesos a las aplicaciones Odoo, SDLC, Quipux.	✓	N/A
CP03		Verificar el cerrado de sesión en las aplicaciones Odoo, SDLC, Quipux	✓	N/A

En este apartado se muestra el resultado de las pruebas de integración realizadas en el (Anexo 5), las cuales se complementan con las pruebas unitarias del (Anexo 4). Además, se muestra los casos de pruebas planificados y ejecutados bajo el framework de testing denominado Selenium IDE, como se muestra en la (Figura 29).

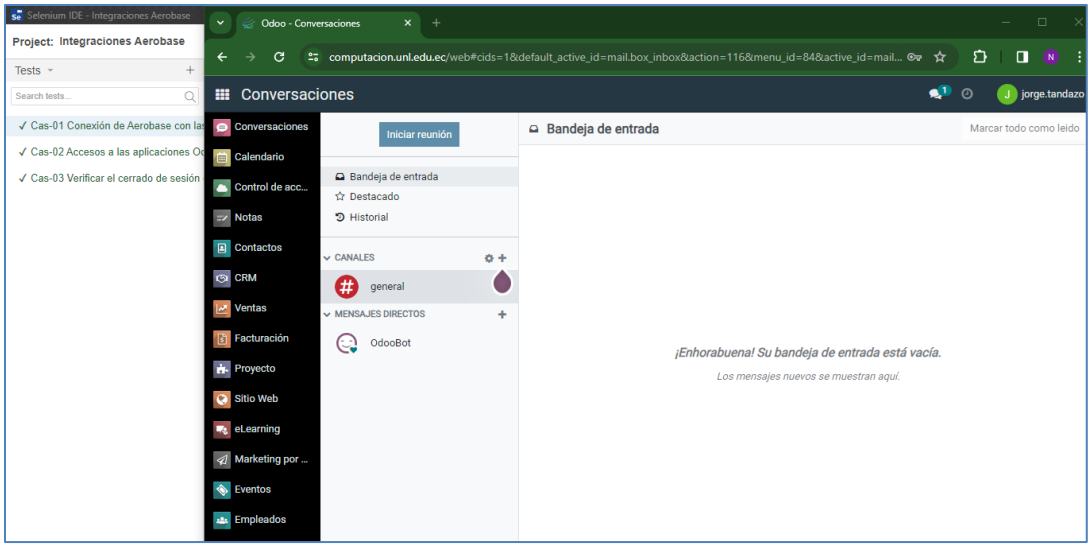


Figura 29. *Resultado de las Pruebas de Integración*

R8. Resultados de las pruebas de Rendimiento

Durante la evaluación de IAM Computación, se llevaron a cabo pruebas de rendimiento (Anexo 7) en: página de inicio de sesión, acceso a la cuenta mediante el inicio de sesión, información de perfil, actualización de credenciales, autenticación de clientes y cierre de sesión. Estas pruebas se realizaron utilizando muestras 100, 200, 800, 1600 y 5000 usuarios interactuando simultáneamente.

Tabla 32. *Resultados de las pruebas de rendimiento*

Muestra	Tiempo promedio de respuesta	Tasa de error	Rendimiento del sistema
100 usuarios	1878 milisegundos	0%	32.3 transacciones por segundo
200 usuarios	1156 milisegundos	0%	105.4 transacciones por segundo
800 usuarios	6409 milisegundos	0%	91.3 transacciones por segundo
1600 usuarios	9025 milisegundos	0%	75,1 transacciones por segundo
5000 usuarios	32101 milisegundos	16,65%	75,5 transacciones por segundo

En la presente tabla se puede visualizar que cada muestra se aplicó a los 6 casos de prueba, mencionados en el (Anexo 7), en donde una carga de 100 usuarios por caso da como resultado un

tiempo de respuesta de 1878 ms y una tasa de error del 0%; mientras que, al establecer una carga de 5000 usuarios el tiempo de respuesta aumenta a 32101 ms, al igual que su tasa de error con el 16,65%, es decir que su aumento es considerable en la tasa de error, sin embargo esta no tiene una mayor afección en el rendimiento del sistema, esto se puede evidenciar en la (Figura 30).

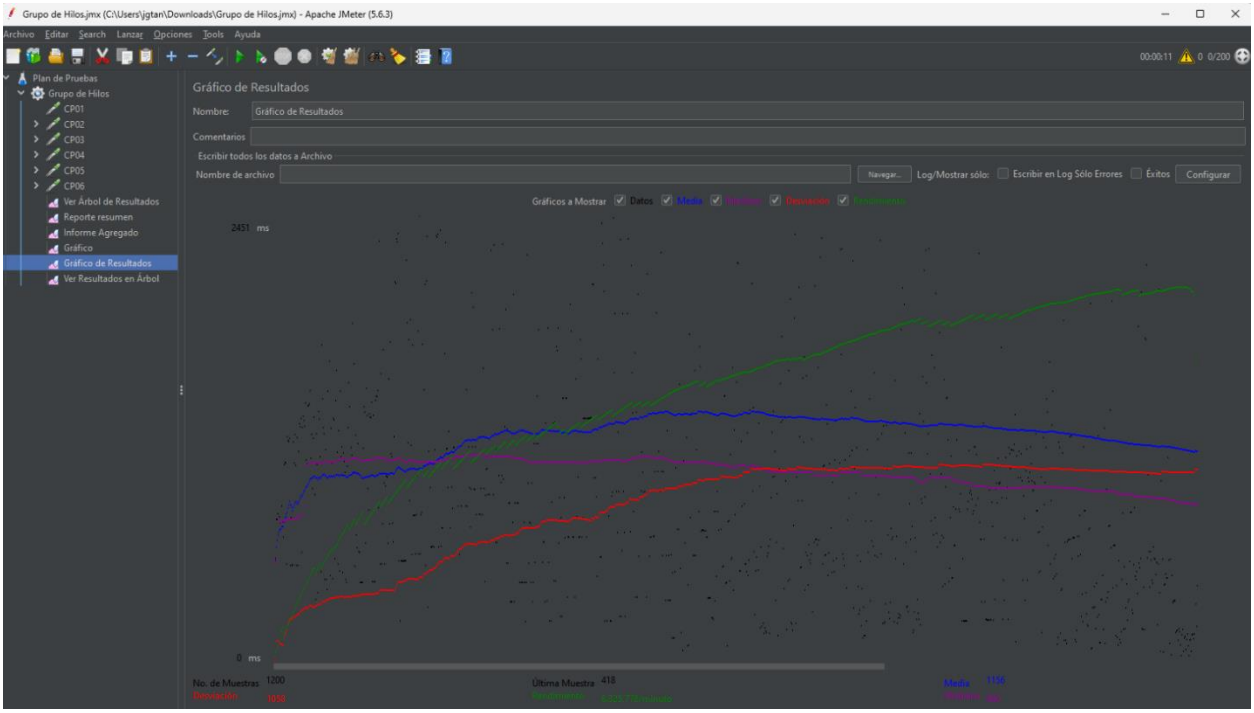


Figura 30.*Rendimiento del sistema durante la ejecución de pruebas*

R9. Resultados de las pruebas de Autenticación

Tabla 33. *Resultados de las pruebas de Autenticación*

No. de Referencia	Vulnerabilidad	Resultados de vulnerabilidad
OWASP-AT-001	Transporte de Credenciales sobre canal cifrado	• En el inicio de sesión, las credenciales se cifran gracias a la URL de solicitud HTTPS. • El servidor devuelve información de cookie para un token de sesión
OWASP-AT-002	Credenciales predeterminadas	• IAM Computación no acepta credenciales predeterminadas; para obtener acceso, es necesario registrarse por parte del administrador del sistema.

OWASP-AT-003	Mecanismo de bloqueo débil	• IAM Computación no bloquea la cuenta después de algún número de intentos de sesión fallidos.
OWASP-AT-004	Omitir el esquema de autenticación	• Al intentar acceder a la cuenta de usuario sin una sesión activa, se redirigió automáticamente al inicio de sesión
OWASP-AT-005	Recordar contraseña vulnerable	• IAM Computación no mantiene habilitado el mecanismo de "recordar contraseña" para evitar posibles vulnerabilidades
OWASP-AT-006	Debilidades de la caché del navegador	• N/A
OWASP-AT-007	Política de contraseñas débiles	• Se implementa una política de contraseñas robusta en IAM Computación
OWASP-AT-008	Respuesta débil a preguntas de seguridad	• No se implementa preguntas de seguridad para una protección de la cuenta del usuario.
OWASP-AT-009	Funcionalidades de cambio o restablecimiento de contraseña débil	• Este proceso pasa por un filtro de un correo verificado por el sistema • El correo que llega al usuario tiene un conjunto de instrucciones y un tiempo de caducidad • Para realizar el nuevo cambio de clave se solicita la confirmación del usuario.
OWASP-AT-010	Autenticación más débil en un canal alternativo	• Los canales alternativos de seguridad tienen un nivel complejo de acceso

Los datos obtenidos en la (Tabla 33) se pueden resumir en que IAM Computación implementa una autenticación robusta y medidas de seguridad adecuadas para proteger las cuentas de usuario y los datos sensibles. Sin embargo, se identificaron algunas áreas de mejora potencial, como el bloqueo de cuentas después de intentos fallidos de inicio de sesión y la implementación de preguntas de seguridad adicionales. Los detalles de esta prueba se encuentran en el (Anexo 8).

R10. Resultados de la prueba de aceptación

En este apartado se presenta la tabulación de la encuesta que se aplicó a los estudiantes de octavo y noveno ciclo de la carrera de Computación de la UNL (Anexo 9); esta constó de 5 partes, la primera mostro datos generales que permitieron conocer el perfil del encuestado; la segunda parte expuso ítems referentes al funcionamiento y utilidad de la aplicación; la tercera parte permitió

conocer la experiencia del usuario; la cuarta parte hizo referencia a la seguridad y privacidad de los datos del usuario; finalmente la quinta parte correspondió a sugerencias de los usuarios sobre la aplicación.

- **Datos demográficos**

Edad

Tabla 34. *Edad*

Respuesta	Frecuencia	Porcentaje
Menor de 18 años	0	0%
18-20 años	0	0%
21-23 años	34	61,8%
24-26 años	17	30,9%
27 años o mas	4	7,3%

Género

Tabla 35. *Género*

Respuesta	Frecuencia	Porcentaje
Femenino	5	9.1%
Masculino	50	90.9%
Prefiero no decirlo	0	0%
Otro	0	0%

Interpretación: De acuerdo con los datos mostrados, el 61,8% corresponde a la edad de 21-23 años, sobresaliendo el género masculino con el 90,9%.

- **Sobre la aplicación de gestión de identidades y acceso**

Tabla 36. *Frecuencia de utilidad*

Pregunta 1: ¿Con qué frecuencia utiliza la aplicación de gestión de identidad y acceso centralizado?		
Respuesta	**Frecuencia**	**Porcentaje**
Diariamente	33	60%
Semanalmente	9	16.4%
Mensualmente	2	3.6%
Ocasionalmente	10	18.2%
Nunca la he utilizado	1	1.8%

Interpretación: La mayoría de los encuestados utilizan la aplicación diariamente lo que corresponde al 60% seguido por aquellos que lo hacen de manera ocasional con el 18,2% y finaliza con aquellos que nunca han utilizado la aplicación con el 1,8%.

Tabla 37. *Propósito de utilización*

Pregunta 2: ¿Cuál es el propósito principal de utilizar esta aplicación?		
Respuesta	**Frecuencia**	**Porcentaje**
Iniciar sesión en múltiples servicios con una sola cuenta	27	49.1%
Gestionar y proteger contraseñas	8	14.5%
Simplificar el proceso de autenticación	20	36.4%

Interpretación: Iniciar sesión en múltiples servicios con una sola cuenta fue el propósito más elegido para utilizar la aplicación con el 49.1%, seguido por simplificar el proceso de autenticación con 36.4% y el 14.5%. corresponde a la gestión y protección de contraseñas.

Tabla 38. *Actualización de credenciales*

Pregunta 3:¿Cómo calificaría la actualización de credenciales proporcionado por IAM Computación?					
	Porcentaje				
Frecuencia	1 (muy difícil e ineficaz)	2	3	4	5 (muy fácil y eficiente)
0	0%	0%			
14			19.4%		
30				55.3%	
11					25.3%

Interpretación: la calificación para la actualización de credenciales proporcionada por IAM Computación fue de 4 con el 55.3%, lo que corresponde a una calificación buena para este tipo de proceso.

Tabla 39. *Recuperación de contraseñas*

Pregunta 4: Con respecto a la recuperación de contraseña ¿Considera que IAM Computación ofrece un proceso claro y eficiente para recuperar contraseñas olvidadas o perdidas?					
Frecuencia	**Porcentaje**				
	1 (muy difícil e ineficaz)	2	3	4	5 (muy fácil y eficiente)

0	0%	0%			
14			19.6%		
33				61.7%	
8					18.7%

Interpretación: los encuestados consideraron que IAM Computación ofrece un proceso claro y eficiente para recuperar contraseñas olvidadas o perdidas, dando una puntuación de 4 que corresponde al 61.7%.

Tabla 40. *Autenticación de doble factor*

Pregunta 5:¿ Qué tan efectiva considera usted la implementación de la autenticación de doble factor en IAM Computación para garantizar la seguridad de las cuentas de usuario?					
	Porcentaje				
Frecuencia	1 (muy difícil e ineficaz)	2	3	4	5 (muy fácil y eficiente)
0	0%	0%			
13			17%		
19				33%	
23					50%

Interpretación: La implementación de la autenticación de doble factor en IAM Computación fue percibida como muy eficiente dándole una puntuación de 5 con el 50%.

Tabla 41. *Utilidad general percibida*

Pregunta 6: En general, ¿Cómo calificaría la utilidad del servicio proporcionado por IAM Computación en relación con la gestión de credenciales y accesos a los aplicativos webs?					
	Porcentaje				
Frecuencia	1 (muy difícil e ineficaz)	2	3	4	5 (muy fácil y eficiente)
0	0%	0%			
1			1.3%		
38				34.7%	
16					34%

Interpretación: los encuestados dan a este ámbito una puntuación de 4 que corresponde al 34.7%, percibiendo una utilidad favorable del servicio proporcionado por IAM Computación.

- **Experiencia del usuario**

Tabla 42. *Experiencia de acceso*

Pregunta 7: ¿Cómo evalúa la experiencia de acceso a las aplicaciones web mediante el Servicio IAM incorporado en la Carrera de Ingeniería en Sistemas/Computación de la UNL?					
	Porcentaje				
Frecuencia	1 (muy difícil e ineficaz)	2	3	4	5 (muy fácil y eficiente)
0	0%	0%			
9			11.9%		
31				54.9%	
15					33.2%

Interpretación: La mayoría de los encuestados calificaron positivamente este apartado, dándole un puntaje de 4 con el 54,9%, es decir que la experiencia de acceso a aplicaciones web mediante el Servicio IAM incorporado en la Carrera de Ingeniería en Sistemas/Computación de la UNL es buena.

Tabla 43. *Características más útiles*

Pregunta 8: ¿ Qué características de la aplicación encuentras más útiles?		
Respuesta	**Frecuencia**	**Porcentaje**
Verificación de correo electrónico	33	32%
Autenticación de doble factor	25	24.3%
Recuperación de contraseña	22	21.4%
Iniciar sesión en múltiples aplicaciones	19	18.4%
Otras	4	3.9%

Interpretación: los resultados muestran que, la característica más útil para los usuarios es la verificación de correo electrónico correspondiente al 32% y la menos seleccionada es el inicio de sesión en múltiples aplicaciones con el 18.4%. Es importante recalcar que dentro de esta pregunta los encuestados tuvieron la opción de elegir más de una respuesta.

Tabla 44. *Áreas de mejora*

Pregunta 9: ¿Qué características de la aplicación cree que podrían mejorarse para que sea más útil?		
Respuesta	**Frecuencia**	**Porcentaje**
Verificación de correo electrónico	19	27.1%
Autenticación de doble factor	19	27.1%
Recuperación de contraseña	16	22.9%
Iniciar sesión en múltiples aplicaciones	2	2.9%
Ninguna	14	20%

Interpretación: se puede observar que las características de verificación de correo electrónico y autenticación de doble factor son las que los encuestados consideran se podrían mejorar ya que cuenta con el 27.1%, siendo la característica iniciar sesión en múltiples aplicaciones la de menor requerimiento de mejoras con el 2.9%. Al igual que la pregunta anterior, en esta interrogante los encuestados tuvieron la opción de elegir más de una respuesta.

- **Seguridad y Privacidad**

Tabla 45. *Confianza en la seguridad de los datos*

Pregunta 10: ¿Confía en la seguridad de la aplicación para proteger sus datos personales y contraseñas?		
Respuesta	**Frecuencia**	**Porcentaje**
SI	31	56.4%
NO	3	5.5%
TALVEZ	21	38.2%

Tabla 46. *Confianza en la protección de datos*

Pregunta 11: ¿Siente que sus datos personales están adecuadamente protegidos mientras utiliza esta aplicación?		
Respuesta	**Frecuencia**	**Porcentaje**
SI	31	56.4%
NO	3	5.5%
TALVEZ	21	38.2%

Interpretación: La mayoría de los encuestados expresaron que confían en la seguridad de la aplicación, como en la protección de sus datos personales y contraseñas otorgándole el 56.4% a la respuesta positiva, en ambos casos.

- **Sugerencias y Comentarios Adicionales:**

Tabla 47. *Problemas experimentados*

Pregunta 12:¿Ha experimentado algún problema significativo al utilizar IAM Computación en cualquiera de los aspectos mencionados?		
Respuesta	**Frecuencia**	**Porcentaje**
SI	0	0%
NO	55	100%

Interpretación: todos los encuestados concuerdan en no haber experimentado problemas al utilizar IAM Computación.

Estos resultados reflejan una percepción general positiva del servicio IAM implementado en la Carrera de Sistemas/Computación de la UNL, con un rendimiento óptimo para una carga de usuarios considerable y una percepción de la utilidad muy buena.

7. Discusión

El presente TT partió de la selección de una herramienta Open Source para la gestión de identidades y control de accesos para las aplicaciones web de la carrera de sistemas/computación; dando como resultado la elección de la herramienta Aerobase Server (R3), la cual cumplió con los requerimientos mencionados anteriormente; esto tuvo relación con lo mencionado por Vielberth [1] y Shostack [2], los cuales mencionan que la gestión de identidades es fundamental para proteger los datos de los usuarios en las diferentes aplicaciones. Así mismo lo mencionado por Krehnke [5] y Ferraiolo et al.[6], quienes resaltan que el control de acceso permite asignar roles específicos a los usuarios lo que le brinda a la aplicación mayor seguridad y control sobre los datos que manejan las aplicaciones.

Por otro lado, la herramienta seleccionada contó con aspectos específicos necesarios para su adecuada implementación, entre ellas: la autenticación, autorización y administración de usuarios; esto coincidió con lo mencionado por Spivey y Echeverria [4], Whitman y Mattord [3], los mismos que definen estos 3 aspectos como parte fundamental para llevar una adecuada administración de los usuarios.

La metodología aplicada al TT fue beneficiosa, ya que al contar con tres fases: Búsqueda y selección; integración y pruebas; permitió obtener información detallada para el proceso de selección y evaluación de la herramienta Open Source (R2,R3), de entre todas las analizadas. Adicional a esto se empleó criterios específicos para las diferentes pruebas de integración (R7), lo que ayudo a comprobar su correcto funcionamiento.

La sección de búsqueda y selección (R1,R2 yR3) conto con tres partes: listado y datos generales de todas las herramientas que se analizaron, la segunda correspondió a los criterios de documentación, mientras que la tercera parte, la conformaron los criterios de madurez; el cumplimiento de los criterios presentados en esas tres etapas permitió la selección de la herramienta Aerobase Server.

La integración de la herramienta seleccionada se desarrolló en dos fases ; la primera correspondió a la instalación y configuración de Aerobase en los servidores de la carrera (R4 y R5), dando como resultado el registro de clientes para cada aplicación (R5.2), la segunda fase

correspondió a la integración y configuración de las aplicaciones web ODOO, SDLC y Quipux con Aerobase (R6), a través de la utilización de protocolos como OpenID Connect que contribuyó a la interoperabilidad y seguridad en la autenticación, dio lugar a una conexión eficiente, además proporcionó una visión clara de cómo se incorporó las aplicaciones en el entorno de trabajo, en donde se pudo evaluar la coherencia del proceso de integración.

Para la evaluación del servicio se estableció un proceso dividido en tres pruebas: integración (R7), rendimiento (R8) y de autenticación (R9), cada una de ellas con criterios específicos sobresaliendo los siguientes: resultados de la integración, rendimiento del sistema y resultados de vulnerabilidad; lo que ayudo a conocer los errores presentes, para su posterior solución, lo que añade una capa adicional de validación sobre las integraciones de software. Los resultados mostraron un rendimiento satisfactorio en todas estas áreas, lo que indicó que el sistema era capaz de manejar cargas de trabajo intensivas de manera eficiente y presentó un nivel adecuado de seguridad. Adicional a esto, los resultados de la encuesta realizada para percibir la utilidad de la integración del servicio IAM (R10), reflejaron una percepción general positiva del servicio, ya que los usuarios afirmaronn que su utilidad es buena, así como su funcionalidad y su seguridad para proteger datos personales.

Para dar respuesta a la pregunta de investigación planteada al inicio del estudio, misma que manifestaba lo siguiente: ¿Cuál es el rendimiento del servicio centralizado de gestión de identidades y control de acceso de usuarios en la Carrera de Ingeniería en Sistemas/Computación de la UNL?, a través de los resultados del TT, podemos decir que efectivamente el rendimiento de la implementación de este servicio aportó positivamente para la carrera, esto se demostró a través de las pruebas de rendimiento (R8) y autenticación (R9), ya que estas incluyeron casos para evaluar el rendimiento y seguridad de la página de inicio de sesión, el acceso a la cuenta, la presentación de la información de perfil, entre otros aspectos relevantes, cuyos resultados mostraron un rendimiento satisfactorio en todas estas áreas.

8. Conclusiones

Una vez terminado el trabajo de titulación, se concluye que:

- La implantación de un servicio centralizado de gestión de identidades y control de acceso para las aplicaciones web ha demostrado ser una solución eficaz y necesaria para una gestión más confiable, garantizando un control preciso desde la autorización hasta la autenticación.

- Al centralizar la gestión de identidades y el control de acceso, se sientan unas bases sólidas para la seguridad y la integridad de los usuarios, además facilita la integración y escalabilidad, al tiempo que impulsa la innovación en el desarrollo de aplicaciones web.

- Después de evaluar criterios de madurez, documentación y características específicas, se concluyó que Aerobase Server es la herramienta más adecuada debido a su versatilidad, fácil instalación, y soporte para múltiples sistemas operativos, la hacen una elección optima.

- Aerobase Server permitió reducir el uso de múltiples credenciales de acceso a un único identificador de usuario y contraseña asociada, así mismo la optimización en la gestión de información en un único directorio centralizado.

- OpenID Connect utiliza estándares de autenticación modernos y robustos, como OAuth 2.0 y JSON Web Tokens (JWT), lo que garantiza un alto nivel de seguridad en la autenticación y autorización de usuarios. Esto ayuda a proteger los datos confidenciales y los recursos de la aplicación contra accesos no autorizados.

- OpenID Connect proporciona un marco estándar para la integración de servicios de identidad, lo que simplifica la interoperabilidad entre diferentes aplicaciones y proveedores de identidad. Esto facilita la integración de nuevas aplicaciones en el ecosistema existente de SmartLab, permitiendo un crecimiento escalable y sostenible del sistema.

9. Recomendaciones

Una vez terminado el trabajo de titulación, se recomienda:

- Organizar sesiones de capacitación periódicas para el personal encargado de administrar y mantener el servicio centralizado de gestión de identidades y control de acceso. Esto garantizará que estén al tanto de las últimas prácticas de seguridad y puedan aprovechar al máximo las funcionalidades ofrecidas por la herramienta seleccionada.

- Utilizar versiones estables y actuales de las aplicaciones Web para que no existan problemas de implementación e incompatibilidad durante la conexión con la herramienta Aerobase Server.

- Tomar en cuenta la adaptación de certificados de seguridad mediante una Autoridad de Certificación (CA) de jerarquía superior que garantice la confidencialidad, integridad y autenticación segura de los usuarios. Realizar evaluaciones periódicas de la herramienta y su integración con las aplicaciones para asegurarse de que siga cumpliendo con los requisitos y expectativas. Esto permitirá realizar ajustes proactivos en lugar de reactivos a medida que evolucionen las necesidades de la carrera y la seguridad de la información.

- Fomentar una cultura de seguridad de la información entre los usuarios y el personal, destacando la importancia de proteger la información confidencial y adoptar prácticas de seguridad sólidas en el uso de las aplicaciones web.

- Hacer uso de API’s para las aplicaciones o sistemas Web que no cuenten con soporte directo con la herramienta Aerobase Server.

Se recomienda para trabajos a futuros:

- Desarrollar un plan de respuesta a incidentes detallado que defina los pasos a seguir en caso de una brecha de seguridad o un incidente relacionado con la gestión de identidades y el control de acceso; esto ayudará a minimizar el impacto de los incidentes y a restablecer rápidamente la seguridad y la integridad del sistema.

- Las aplicaciones o sistemas Web que se integren a la herramienta Aerobase Server deben incorporar la multi-identificación para garantizar el acceso a los recursos de las distintas aplicaciones web en caso de existir inconvenientes en la interfaz principal de acceso.

- Para manejar la seguridad en el inicio de sesión único en diferentes aplicaciones o sistemas web, tomar en cuenta la verificación mediante hardware, verificación en dos pasos, mensaje de alerta al iniciar sesión o gestión de notificaciones de acceso.

10. Bibliografía

[1] M. Vielberth, ‘Security Information and Event Management (SIEM)’, in Encyclopedia of Cryptography, Security and Privacy, Springer Berlin Heidelberg, 2021, pp. 1–3. doi: 10.1007/978-3-642-27739-9_1681-1.

[2] Adam Shostack, Threat Modeling Designing for Security, t. 53, n. 9. 2013.

[3] M. Whitman et H. Mattord, ‘Principles of Information Security Fourth Edition’, Learning, 2011.

[4] B. Spivey et J. Echeverria, Hadoop Security: Protecting Your Big Data Platform.

[5] M. Krehnke et D. Krehnke, Information security management handbook, fifth edition, t. 3. 2006.

[6] D. Ferraiolo, R. Sandhu, S. Gavrila, D. Kuhn, et R. Chandramouli, ‘Proposed NIST Standard for Role-Based Access Control’, ACM Transactions on Information and System Security, t. 4, n. 3, 2001, doi: 10.1145/501978.501980.

[7] J. Scheidel, Designing an IAM framework with Oracle Identity and Access Management Suite. 2010.

[8] F. Castro, ‘Gestión de identidades y accesos unificados’, 2020.

[9] D. Gibson, ‘Hacking Point of Sale: Payment Application Secrets, Threats, and Solutions’, ohn Wiley & Sons, 2015.

[10] A. Jain, S. Dass, et K. Nandakumar, ‘Soft biometric traits for personal recognition systems’, t. 3072, pp. 812–821, 2004, doi: 10.1007/978-3-540-25948-0_99.

[11] D. Hardt, ‘The OAuth 2.0 Authorization Framework [RFC 6749]’, RFC 6749, 2012.

[12] L. Welling et L. Thomson, ‘Desarrollo Web con PHP y MySQL’, ANAYA, t. 25, n. 1, 2018.

[13] N. Sakimura et al., ‘OpenID Connect Core 1.0 incorporating errata set 1’, OpenID Foundation, 2014.

[14] OASIS, ‘Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0 OASIS Standard, 15 March 2005’, saml-bindings-2.0-os.

[15] E. Vega Briceño, Seguridad de la información. 2021. doi: 10.17993/tics.2021.4.

[16] P. Grassi et al., ‘Digital identity guidelines: authentication and lifecycle management’, Gaithersburg, MD, iun. 2017. doi: 10.6028/NIST.SP.800-63b.

[17] FFIEC, ‘Authentication in an Internet Banking Environment’, Federal Financial Institutions Examination Council, t. 1, 2011.

[18] D. Ferraiolo et D. Kuhn, ‘Role-Based Access Controls’, 2009.

[19] N. Rivera, ‘Modelo de Single Sign-On para Herramientas del Grupo QualDev Introducción’, 2019.

[20] J. Mart, A. Gonzalez, C. Ancert, et A. Notarial, ‘Implantación de un SSO (Single Sign On)’, pp. 1–72, 2018.

[21] J. I. Mart, A. Gonzalez, C. Ancert, et A. Notarial, ‘Implantación de un SSO (Single Sign On)’, pp. 1–72, 2018.

[22] W. Aguilar et M. Armijos, Desarrollo de un prototipo para el servicio de autenticación central de usuarios en aplicaciones web. 2019.

[23] A. Ghaffar, ‘Introducción a LDAP sobre Linux ¿Qué es LDAP? Directorio Base o Root (raíz)’, 2019.

[24] M. Jose, M. Gonzáles, et Á. España, ‘User Management with LDAP (Lightweight Directory Access Protocol) for access to technology and Information Services in Companies ´’, Journal of Science and Research: Revista Ciencia E Investigaci ´ on, E-Issn: 2528-8083, Vol. 1, Citt, Pp. 10-15, t. 1, pp. 10–15, 2016.

[25] C. Leonardo, P. Valencia, D. Mishell, V. Villafuerte, I. N. G. Marlon, et A. Di, ‘Implementación de un sistema centralizado de

autenticación para usuarios de las diferentes aplicaciones web de la UG', 2017.

[26] J. Jesús et al., 'Autenticación centralizada para los sistemas de información de los Institutos Tecnológicos', n. 106, pp. 73–85, 2013.

[27] E. Penna, M. De León, et others, 'Implementación de un servicio de autenticación centralizado y gestión de identidades en la Universidad de la República', 2016.

[28] U. Valle, "Sistema centralizado de autenticación y autorización 'Single Sign On' ", 2013.

[29] H. Mendieta et F. Andrade Navarro, 'Sistema centralizado de gestión de usuarios para la Universidad del Tolima', reponame: Repositorio Institucional de la Universidad Nacional Abierta y a Distancia, 2015.

[30] F. Díaz, C. Banchoff, A. Rodríguez, et V. Soria, 'Metodologías para la evaluación de herramientas Free / Open Source para pruebas de software proyectos Free / Open Source', Laboratorio de Investigación de Nuevas Tecnologías Informáticas, Facultad de Informática, Universidad de La Plata, Buenos Aires, Argentina, pp. 1–5, 2011, [In linea]. Praestatus ad: http://www.linti.unlp.edu.ar/uploads/docs/evaluacion_de_herramientas_open_source_para_pruebas_de_software.pdf

[31] F. Chambó, P. Bazán, et Juan Cortabitarte, 'Automatización de Pruebas de Integración en Arquitecturas Orientadas a Servicios', Universidad Nacional de la Plata, 2015.

[32] N. Gómez Rodríguez, 'Las Pruebas de Integración como Proceso de la Calidad del Software en el Ámbito de las Telecomunicaciones', 2015.

[33] AEC, 'UNE 66177 Guía para la integración de los sistemas de gestión', Iso, 2016.

11. Anexos

Anexo 1: Entrevista al Gestor de la Carrera de Ingeniería en Sistemas y Computación de la Universidad Nacional de Loja

Entrevista a Gestor de la Carrera de Ingeniería en Sistemas/Computación

Proyecto: Implementación de un Servicio Centralizado de Gestión de Identidades y Control de Acceso de usuarios en aplicaciones web para la Carrera de Ingeniería en Sistemas/Computación de la UNL: SmartLab

Versión: 1.0

Fecha: 25/12/2023

1. **¿Con cuántos aplicativos webs cuenta la carrera actualmente?**

Cuenta con 4 aplicativos webs que son:

- **Odoo:** Sistema de trabajo abierto y modular, en el cual contiene varios submódulos para: Gestionar el plan de mejoras de evaluación al docente, Crear y diseñar sílabos y Consulta de matrículas
- **BonitaSoft:** Aplicativo basado en procesos sobre el cual existen sub-aplicativos que sirven para: Solicitar una certificación, Gestionar el proceso de trabajo de Titulación y Dar seguimiento al Plan de mejoras.
- **Quipux Comunitario:** Sistema de gestión documental
- **SDLC:** Sistema para la Gestión del Ciclo de Vida de Desarrollo de Software

2. **¿Entre los aplicativos webs existe algún tipo de relación?**

Si, ciertas aplicaciones se relacionan por hecho de compartir una misma arquitectura y cierta información en cuanto a sub-aplicaciones, pero otras no mucho debido a la segmentación de tecnologías.

3. **¿Existen aplicativos webs en desarrollo actualmente?**

Sí, actualmente existen algunas aplicaciones que están en desarrollo y son alrededor de unos cuatro o cinco. Entre ellos se encuentra el de comunidades de estudiantes, el de prácticas preprofesionales, el de becas y otros dos aplicativos webs más; pero en conclusión sí hay aplicativos webs que están en desarrollo.

4. **¿Qué tecnologías utilizan estos aplicativos webs?**

Las aplicaciones que están en producción son las cuatro mencionadas anteriormente, y la tecnología que utilizan son:

- **Odoo:** Es un sistema de distribución con ERP de arquitectura modular y de software libre con licencia comunitaria, utiliza una combinación de Python, PostgreSQL y tecnologías web estándar para proporcionar una plataforma empresarial completa. La elección de estas tecnologías contribuye a la flexibilidad, escalabilidad y rendimiento de Odoo.
- **BonitaSoft:** Es un software para la gestión de procesos de negocio (BPM) y el desarrollo

de aplicaciones de negocio. Es de software libre con licencia comunitaria y está basada en tecnologías como Java, servidores de aplicaciones como Tomcat o WildFly, Hibernate para el acceso a la base de datos, JavaScript para la interfaz de usuario, y sigue los estándares BPMN para el modelado de procesos de negocio. Estas tecnologías permiten a BonitaSoft ofrecer una plataforma flexible y potente para la gestión de procesos de negocio.

- **Quipux Comunitario:** Es un sistema de gestión documental basado en tecnologías específicas utilizadas para gestionar identidades y servicios, además involucra una combinación de tecnologías de base de datos, seguridad, y desarrollo de software.
- **SDLC:** Es un sistema para la Gestión del Ciclo de Vida de Desarrollo de Software y está basado en tecnologías como AngularJs para la interfaz y ejecución del entorno del sistema, NodeJs para el acceso a los datos y MongoDB para la base de datos del sistema.

5. **¿Cuántos usuarios utilizan estos aplicativos webs?**

Los docentes son alrededor de veinte usuarios y los estudiantes que hasta ahora han consumido estas aplicaciones son alrededor de cien. En general existe un aproximado de ciento cincuenta usuarios, los mismo que no son concurrentes, sino que dependen del proceso. Por ejemplo, si vamos a iniciar el proceso de seguimiento a sílabo estaríamos hablando de alrededor de cien usuarios que van a comenzar a interactuar con esa aplicación en ese momento, pero más o menos unos cien a ciento cincuenta usuarios están interactuando con las aplicaciones.

6. **¿Se manejan perfiles de acceso para los aplicativos webs?**

No, tanto Odoo como BonitaSoft tienen gestión de usuarios, pero el que mejor gestiona los usuarios es Odoo, ahí tú puedes controlar las reglas de negocio o los permisos a las propiedades del módulo mediante los roles. Así yo puedo definir si es estudiante, si es decano, si es director, etc. Entonces dependiendo del rol se le otorga permisos a las distintas funcionalidades de los módulos. En BonitaSoft no supone roles, todas las actividades van ancladas a un rol que está sujeto a que el conjunto de actividades que hagas en el proceso pertenezca a un rol determinado nada más, como un flujo de un proceso de negocios, en otras palabras, solo se limitan a peticiones de software.

7. **¿Se ha presentado algún problema, al autenticarse de manera independiente en cada aplicativo web?**

Sí, porque obviamente se tiene un usuario para las soluciones que hay en Odoo, otro para las soluciones que está en Bonita y hay otro tercer usuario para las aplicaciones que están en otras tecnologías, por lo tanto, si se tiene acceso a estas tres arquitecturas entonces debemos tener tres perfiles o tres identificadores de usuarios, lo cual se complica bastante. Lo mejor sería una sola identificación para todas las aplicaciones, dependiendo del perfil de usuario, si es estudiante deberíamos tener un control de aplicaciones para dar el acceso a ese usuario, pero actualmente no se realiza eso. Actualmente se tiene tres usuarios o más para acceder a las aplicaciones que están en arquitecturas distintas.

Anexo 2: Listado de herramientas Open Source

Listado de herramientas Open Source a evaluar

Proyecto: Implementación de un Servicio Centralizado de Gestión de Identidades y Control de Acceso de usuarios en aplicaciones web para la Carrera de Ingeniería en Sistemas/Computación de la UNL: SmartLab

Versión: 1.0

Fecha: 25/12/2023

Tabla 1: Listado de herramientas Open Source

Herramienta	Ventajas	Desventajas
CAS	Admite múltiples protocolos como OAuth, OpenID, OpenID Connect, WsFederation, REST y SAML. Documentación proporcionada. Gestión de contraseñas. Autenticación multifactor. Plurilingüe. Integraciones proporcionadas para terceros. Interfaz de usuario para administrar. registros, monitoreo y estadísticas. Autenticación a las redes sociales.	Los datos pueden ser robados al redirigir a sitios maliciosos. Puede proporcionar acceso a aplicaciones no asignadas a terceros. La implementación y configuración pueden ser percibidas como complejas, especialmente si se requieren características avanzadas o integraciones específicas. La documentación puede ser extensa, algunos usuarios pueden encontrarla detallada, pero a la vez compleja. Menor Conocimiento en el Mercado.
IdentityServer	Opción de inicio y cierre de sesión únicos. Control de acceso para la API. Interfaz de usuario personalizada. Autorización de la API. Proveedor basado en reclamaciones. Soporte para todos los flujos de OAuth 2.0. Proporciona autorización para sitios web, aplicaciones móviles, dispositivos IoT, etc. La configuración del servidor se proporciona a través del código. Integración con .NET Core. Función de recordatorio de contraseña basada en la	La configuración y administración pueden tener una curva de aprendizaje, en especial para aquellos que no están familiarizados con los estándares de autenticación y autorización. Configuración compleja. La integración con tecnologías no .NET puede requerir más esfuerzo y ajustes. Dificultad para implementaciones pequeñas

	funcionalidad XYZ.	
Aerobase Server	Autenticación multifactor. Autenticación móvil. Certificación de acceso. Gestión de contraseñas. Gestión de credenciales. Gestión de cuentas privilegiadas. Gestión de políticas. Gestión de usuarios. Panel de comunicaciones. Provisión de usuarios. Registro único.	Posible complejidad de configuración. El soporte puede depender en gran medida de la contribución de la comunidad. Personalización limitada. Documentación detallada pero compleja a la vez. Problemas de integración con algunas tecnologías específicas.
Open Identity Platform	Admite múltiples protocolos, como SAML, OAuth 2.0, OpenID Connect, y otros protocolos de soporte. Viabilidad de la federación de usuarios. Soporte de integración en la nube de terceros. Garantiza la seguridad de los servicios web. Amigable con el desarrollador y extensible.	Menos fácil de usar. La posibilidad de personalizar las políticas puede ser una sobrecarga.
Apache Syncop	Sistema de código abierto. Administrar identidades digitales. Gestiona desde el ciclo de vida de la identidad y su almacenamiento. Sincroniza usuarios, grupos y otros objetos.	En ambientes adversos es posible que generen falsas alarmas. Puede requerir una cantidad significativa de tiempo y recursos para aprender e implementar correctamente. Es posible que no se integre tan perfectamente con determinados

		sistemas o aplicaciones. Puede requerir más configuración manual y personalización que otras soluciones
Keycloak	Inicio de sesión único. Soporte para protocolos estándar. Cuenta aplicaciones seguras y servicio simplificado. LDAP compatible como repositorio de usuarios externo. Delegación de autenticación (inicio de sesión social).	Complejidad de configuración. Dependiendo de la cantidad de usuarios y la complejidad de la implementación, se puede requerir recursos significativos de hardware. Personalización Limitada. Documentación Compleja. Problemas de integración con algunas tecnologías específicas.

Anexo 3: Descarga e instalación de Aerobase Server en forma local

Descarga e instalación de Aerobase Server

Proyecto: Implementación de un Servicio Centralizado de Gestión de Identidades y Control de Acceso de usuarios en aplicaciones web para la Carrera de Ingeniería en Sistemas/Computación de la UNL: SmartLab

Versión: 1.0

Fecha: 25/12/2023

Para instalar Aerobase Server se necesita cumplir con requisitos previos los cuales son:

- Instalar o tener instalado mínimo Java 11 JDK o superior.
- Tener un mínimo de al menos 512Mb de RAM.
- Tener al menos 1G de espacio en disco.

A continuación, se detallan los pasos a seguir para descargar e iniciar la instalación y configuración de Aerobase Server, teniendo en cuenta que esta guía está desarrollada en un servidor con el sistema Centos7:

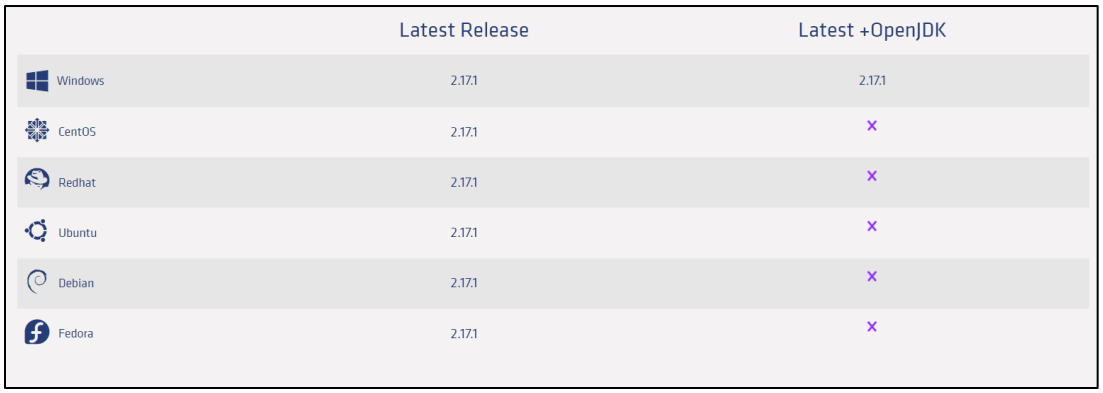
Paso 1:

Se debe actualizar la lista de paquetes disponibles y sus versiones, ingresando el siguiente comando en la terminal:

sudo yum -y update

Paso 2:

Se descarga los paquetes aerobae.deb y aerobase-iam.deb, desde el sitio oficial de Aerobase Server (https://www.aerobase.io/downloads):



	Latest Release	Latest +OpenJDK
Windows	2.17.1	2.17.1
CentOS	2.17.1	×
Redhat	2.17.1	×
Ubuntu	2.17.1	×
Debian	2.17.1	×
Fedora	2.17.1	×

Figura 1: Sistemas operativos con soporte

En la Figura 1: Sistemas operativos con soporte, se presenta la disponibilidad de soporte para ciertos sistemas operativos, en el caso de esta guía se optó por usar Centos7. Mediante el comando curl se realiza la descargar de los paquetes a instalar tal y como se muestra a continuación:

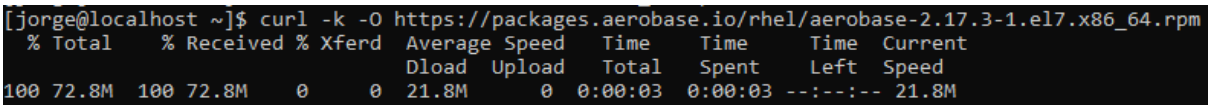


Figura 2: Uso del comando "curl -k -O https://packages.aerobase.io/rhel/aerobase-2.17.3-1.el7.x86_64.rpm"

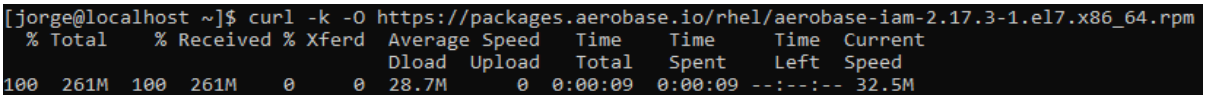


Figura 3: Uso del comando "curl -k -O https://packages.aerobase.io/rhel/aerobase-iam-2.17.3-1.el7.x86_64.rpm"

Como se puede observar en Figura 4. Resultado de descarga de paquetes mediante el comando curl, los archivos de instalación se encuentran previamente en el directorio donde se procedió a la descarga, en el caso de esta guía se encuentran en el directorio raíz "/".

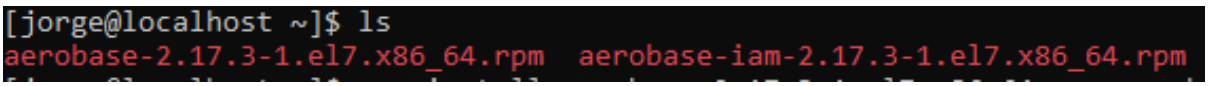


Figura 4. Resultado de descarga de paquetes mediante el comando curl

Paso 3:

Realizar la instalación de Java 8 JDK, mediante el uso del comando:

sudo yum install -y java-1.8.0-openjdk

Paso 4:

Como se muestra en la Figura 5: Instalación de paquetes de Aerobase, Se realiza la instalación desde la carpeta donde descargamos los paquetes a través del siguiente comando:

sudo yum install aerobase-2.17.3-1.el7.x86_64.rpm aerobase-iam-2.17.3-1.el7.x86_64.rpm

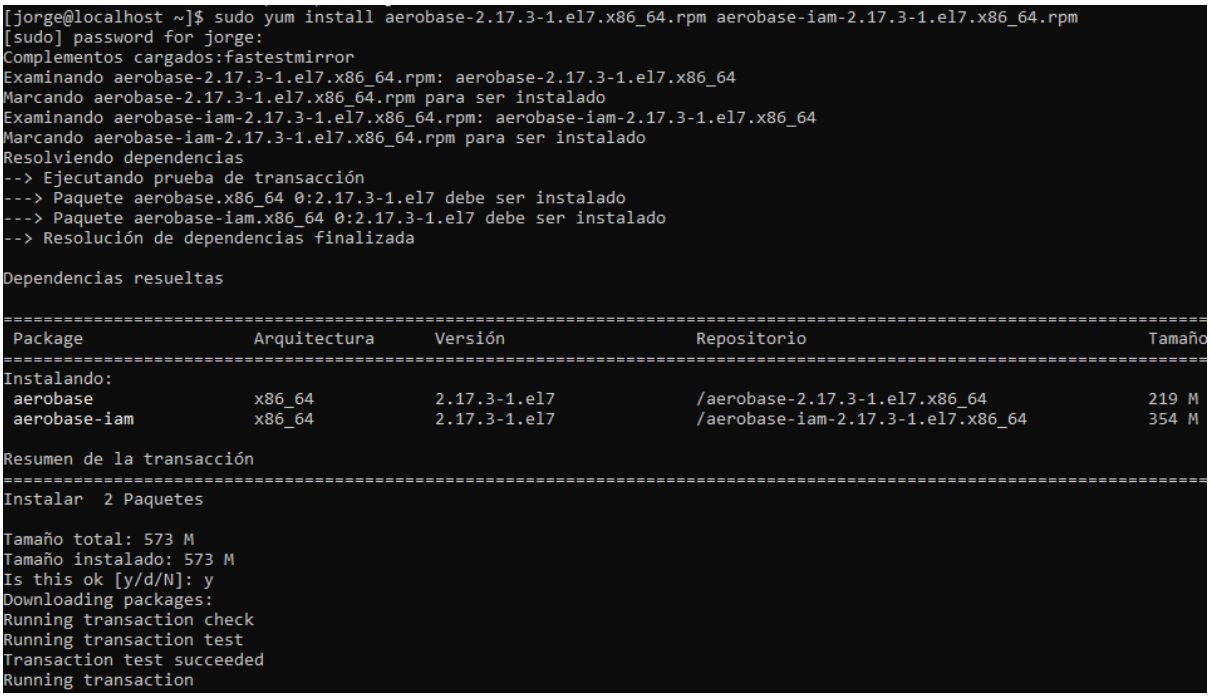


Figura 5: Instalación de paquetes de Aerobase

En la Figura 6: Resultado de instalación de paquetes, se puede observar el resultado que se debe obtener, después de una correcta instalación.

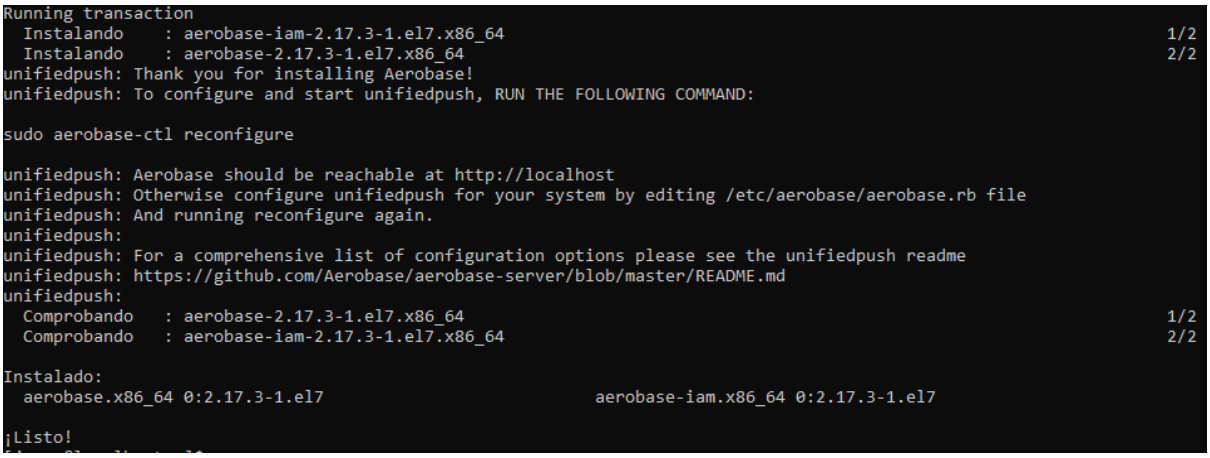


Figura 6: Resultado de instalación de paquetes.

Paso 5:

Para continuar con su correcta instalación se procede a ejecutar el proceso de configuración por defecto que trae Aerobase con el fin de activar las configuraciones en sus componentes esto

mediante el siguiente comando:

sudo aerobase-ctl reconfigure

```
[jorge@localhost ~]$ sudo aerobase-ctl reconfigure
To use this software, you must agree to the terms of the software license agreement.
Press any key to continue.
Type 'yes' to accept the software license agreement, or anything else to cancel.
Type 'yes' to accept the software license agreement, or anything else to cancel.
yes
Starting Chef Infra Client, version 17.1.35
Patents: https://www.chef.io/patents
resolving cookbooks for run list: ["aerobase"]
Synchronizing Cookbooks:
  - aerobase (2.9.0)
  - package (0.0.0)
  - enterprise (0.15.2)
  - runit (5.1.6)
  - apt (7.3.0)
  - packagecloud (1.0.1)
  - yum-epel (3.3.0)
Installing Cookbook Gems:
Compiling Cookbooks...
Converging 127 resources
Recipe: aerobase::users
  * directory[/var/opt/aerobase] action create (up to date)
  * group[aerobase-group] action create
    - create group aerobase-group
  * linux_user[aerobase] action create
    - create user aerobase
Recipe: aerobase::default
```

Figura 7: Ejecución de configuraciones.

En caso de que se esté ejecutando de manera local se puede hacer un levantamiento manual mediante el siguiente comando:

sudo aerobase-ctl start

Una vez inicializado el servidor se puede continuar con las configuraciones extras para lo cual se puede acceder a su administración desde “http://localhost/auth/admin/aerobase/console” en caso de que se ejecute localmente, la misma ruta que redireccionará hacia un formulario de inicio de sesión el mismo que se puede observar en Figura 8: Página de inicio de sesión de Aerobase.

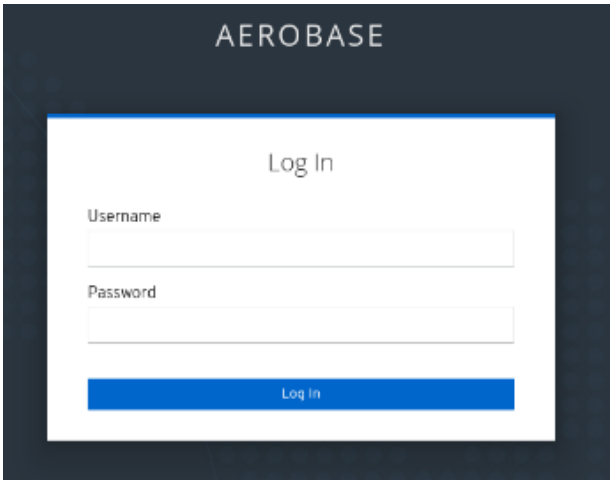


Figura 8: Página de inicio de sesión de Aerobase

En la página de inicio se debe ingresar el nombre de usuario y la contraseña por defecto (admin/123). A continuación, Aerobase pedirá actualizar nuestra contraseña para activar nuestra cuenta.

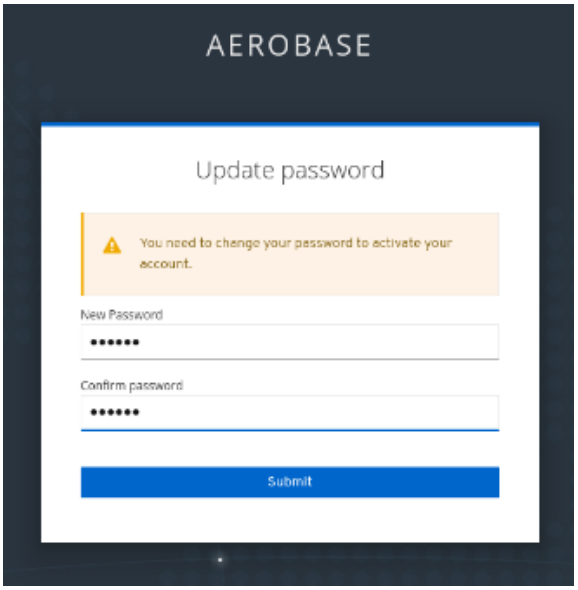


Figura 9: Actualización de contraseña para activación de cuenta

Finalmente, una vez actualizada la contraseña se presentará la interfaz principal mediante la cual se puede realizar configuraciones adicionales para la administración de usuarios y grupos, gestión de identidades, autenticación, entre otras características.

Anexo 4: Pruebas Unitarias

Proyecto: Implementación de un Servicio Centralizado de Gestión de Identidades y Control de Acceso de usuarios en aplicaciones web para la Carrera de Ingeniería en Sistemas/Computación de la UNL: SmartLab

Versión: 1.0

Fecha: 25/12/2023

Hoja de control

Organismo	Universidad Nacional de Loja		
Proyecto	Implementación de un Servicio Centralizado de Gestión de Identidades y Control de Acceso de usuarios en aplicaciones web para la Carrera de Ingeniería en Sistemas/Computación de la UNL: SmartLab		
Entregable	Pruebas Unitarias del subsistema de Aplicaciones		
Autores	Josue Macas, Jorge Tandazo		
Versión/Edición	1.0	**Fecha Versión**	25/12/2023
Aprobado por	Ing. Pablo F. Ordoñez Ordoñez, Mg. Sc	**Fecha Aprobación**	26/12/2023
		N.º Total de Páginas	3

Introducción

Objeto

El objetivo de este documento es confirmar la operatividad adecuada del subsistema de aplicaciones, analizando el código en sus elementos constituyentes y asegurando el correcto funcionamiento de cada uno, según lo previsto.

Propósito

Verificar y demostrar que el software está funcionando correctamente. La implementación de una herramienta IAM, permitirá la autenticación y autorización a los diferentes aplicativos de la carrera de Computación, y lo hará de una manera que aborde cada función principal individualmente.

Definición de los casos de pruebas

En esta sección, se presentará una explicación minuciosa de cada uno de los casos de prueba que se han previamente identificado. Se detallará el propósito de cada caso de prueba, se describirán los pasos necesarios para su ejecución, se especificarán los datos de entrada requeridos, y se establecerán los resultados esperados. La descripción pormenorizada de los casos de prueba resulta crucial para asegurar la cobertura de todas las posibles situaciones y verificar el correcto funcionamiento del sistema en cada escenario. Además, proporciona a evaluadores y desarrolladores una comprensión más profunda del comportamiento del sistema, garantizando la conformidad con los requisitos y especificaciones establecidos.

Número del Caso de Prueba	Componente	Descripción de lo que se probará	Prerrequisitos
CP01	IAM Computación	Conexión de Aerobase con las aplicaciones Odoo, SDLC, Quipux.	Navegador web, clientes de conexión de cada aplicación
CP02	IAM Computación	Accesos a las aplicaciones Odoo, SDLC, Quipux.	Navegador web y Cuenta con permisos a aplicaciones en Aerobase

CP03	IAM Computación	Cerrado de sesión en las aplicaciones Odoo, SDLC, Quipux.	Navegador web y Cuenta con permisos a aplicaciones en Aerobase

CP01

Nº	**Descripción**	**Método**	**Datos Entrada**	**¿OK?**	**Observaciones**
1	Conexión de Aerobase con las aplicaciones Odoo, SDLC, Quipux.	test ('Renderizar <App /> al dar clic en iniciar sesión')	N/A	ü	N/A
2	Mostrar adecuadamente el formulario de inicio de sesión de Aerobase	test ('Mostrar formulario para iniciar sesión con Aerobase ‘)	N/A	ü	N/A

CP02

N.º	**Descripción**	**Método**	**Datos Entrada**	**¿OK?**	**Observaciones**
1	Accesos a las aplicaciones Odoo, SDLC, Quipux.	test ('Solicitar autenticación a Aerobase)	Usuario, contraseña	ü	N/A
2	Verificar el permiso para acceder a las aplicaciones Odoo, SDLC, Quipux.	test (‘Verificar permiso para acceder a las aplicaciones’)	S/N	ü	N/A

CP03

Nº	**Descripción**	**Método**	**Datos Entrada**	**¿OK?**	**Observaciones**

1	Verificar el cerrado de sesión en las aplicaciones Odoo, SDLC, Quipux.	test ('Cerrar sesión en las aplicaciones web ‘)	N/A	ü	N/A

Glosario

En esta sección, se detallan y explican los términos técnicos, acrónimos o jerga utilizados en el documento con el fin de facilitar su comprensión. Esto es especialmente importante para aquellas personas que no tienen experiencia en el área o que no están familiarizadas con el lenguaje técnico.

Término	**Descripción**
IAM	Identity and Access Management - Gestión de Identidad y Acceso

Anexo 5: Pruebas de Integración

Proyecto: Implementación de un Servicio Centralizado de Gestión de Identidades y Control de Acceso de usuarios en aplicaciones web para la Carrera de Ingeniería en Sistemas/Computación de la UNL: SmartLab

Versión: 1.0

Fecha: 25/12/2023

Hoja de control

Organismo	Universidad Nacional de Loja		
Proyecto	Implementación de un Servicio Centralizado de Gestión de Identidades y Control de Acceso de usuarios en aplicaciones web para la Carrera de Ingeniería en Sistemas/Computación de la UNL: SmartLab		
Entregable	Pruebas de Integración		
Autores	Josue Macas, Jorge Tandazo		
Versión/Edición	1.0	**Fecha Versión**	25/12/2023
Aprobado por	Ing. Pablo F. Ordoñez Ordoñez, Mg. Sc	**Fecha Aprobación**	26/12/2023
		Nº Total de Páginas	3

Introducción

Objeto

El objetivo de este documento es ejecutar los casos de prueba que confirman que la integración de Aerobase con los diferentes aplicativos webs está funcionando correctamente. Una vez que las pruebas unitarias se han completado con éxito, se crean pruebas de integración para garantizar que se mantenga la naturaleza unitaria del software cuando se combinan elementos unitarios

Alcance

Los diferentes casos de prueba son validados por el profesor Ing. Pablo Ordoñez (director del TT), quien enseña ingeniería de sistemas y computación en la Universidad Nacional de Loja. Po otro lado Josue Macas y Jorge Tandazo, estudiantes, son quienes crean y graban los múltiples escenarios de prueba.

Definición de los casos de pruebas

Este apartado se enfoca en proporcionar una descripción detallada de cada uno de los escenarios de prueba que han sido identificados para la integración en cuestión. Aquí, se proporciona información completa sobre los casos de prueba, incluyendo los datos de entrada, la acción que se espera que se realice, la salida esperada y cualquier mensaje que pueda aparecer durante el proceso. Al proporcionar una descripción exhaustiva de cada escenario de prueba, se asegura de que se cubran todos los aspectos de la integración y se verifique su correcto funcionamiento en diferentes situaciones. Esto permitirá identificar cualquier problema o error en la integración antes de su implementación.

Número del Caso de Prueba	Componente	Descripción de lo que se probará	Prerrequisitos
CP01	IAM Computación	Conexión de Aerobase con las aplicaciones Odoo, SDLC, Quipux.	Navegador web, clientes registrados en Aerobase para cada aplicación

CP02	IAM Computación	Accesos a las aplicaciones Odoo, SDLC, Quipux.	Navegador web y Cuenta con permisos a aplicaciones en Aerobase
CP03	IAM Computación	Verificar el cerrado de sesión en las aplicaciones Odoo, SDLC, Quipux.	Navegador web y Cuenta con permisos a aplicaciones en Aerobase

CP01

Paso	**Descripción**	**Datos Entrada**	**Resultado esperado**	**¿OK?**	**Observaciones**
1	Ingresar a la página de (Odoo, SDLC, Quipux)	Clic	Ventana de la aplicación (Odoo, SDLC, Quipux)		N/A
2	Hacer clic en el botón iniciar sesión con Aerobase	Clic	Ventana de inicio de sesión de Aerobase		N/A

CP02

Paso	**Descripción**	**Datos Entrada**	**Resultado esperado**	**¿OK?**	**Observaciones**
1	Ingresar a la página de (Odoo, SDLC, Quipux)	Clic	Ventana de la aplicación (Odoo, SDLC, Quipux)		N/A

2	Hacer clic en el botón iniciar sesión con Aerobase	Clic	Ventana de inicio de sesión de Aerobase	□	N/A
3	Completar los campos de email y contraseña	String	No presentar errores de validación de campos requeridos		
4	Hacer clic en el botón Iniciar sesión	Clic	Ventana de inicio de la aplicación (Odoo, SDLC, Quipux)		

CP03

Paso	Descripción	Datos Entrada	Resultado esperado	¿OK?	Observaciones
1	Hacer clic en el botón Cerrar sesión (Odoo, SDLC, Quipux)	Clic	Ventana raíz de la aplicación (Odoo, SDLC, Quipux)	□	N/A
2	Hacer clic en el botón iniciar sesión con Aerobase	Clic	Ventana de inicio de sesión de Aerobase	□	N/A

Anexo 6: Pruebas Funcionales

Proyecto: Implementación de un Servicio Centralizado de Gestión de Identidades y Control de Acceso de usuarios en aplicaciones web para la Carrera de Ingeniería en Sistemas/Computación de la UNL: SmartLab

Versión: 1.0

Fecha: 25/12/2023

Hoja de control

Organismo	Universidad Nacional de Loja		
Proyecto	Implementación de un Servicio Centralizado de Gestión de Identidades y Control de Acceso de usuarios en aplicaciones web para la Carrera de Ingeniería en Sistemas/Computación de la UNL: SmartLab		
Entregable	Pruebas Funcionales		
Autor	Josue Macas, Jorge Tandazo		
Versión/Edición	1.0	**Fecha Versión**	25/12/2023
Aprobado por	Ing. Pablo F. Ordoñez Ordoñez, Mg. Sc	**Fecha Aprobación**	26/12/2023
		Nº Total de Páginas	9

Introducción

Objetivo

Este documento tiene como objetivo crear casos de prueba que evidencien la conformidad del software con los requisitos establecidos. Se buscó proporcionar una descripción detallada de los casos de prueba, una matriz que ilustre la correspondencia entre estos y los requisitos, así como un plan detallado para llevar a cabo la ejecución de las pruebas.

Alcance

El profesor Ing. Pablo F. Ordoñez Ordoñez, Mg. Sc (director de la TT) es el encargado de validar cada uno de los casos de prueba identificados. Él es un docente que imparte sus conocimientos en la carrera de ingeniería de sistemas y computación en la Universidad Nacional de Loja. Por otro lado, los escenarios de prueba son creados y grabados por Josue Macas y Jorge Tandazo, estudiantes del TT.

Definición de los casos de pruebas

Cada caso de prueba que se identificó para confirmar la funcionalidad del sistema se describe en profundidad en esta sección. Además de enumerar las que se deben hacer para garantizar que la herramienta IAM se implemente correctamente.

Establecer conexión con Aerobase	**CAS-01**	
	¿Prueba de despliegue?	**Sí**
Descripción: Se probará la conexión de Aerobase con Odoo, SDLC, Quipux.		
Prerrequisitos • Clientes en Aerobase Odoo, SDLC, Quipux. • Acceder a la página.		
Pasos: 1. Acceder al dominio de Odoo, SDLC, Quipux. 2. Dar clic en el botón Iniciar Sesión con Aerobase (En el caso del SDLC se redirecciona directo a Aerobase)		

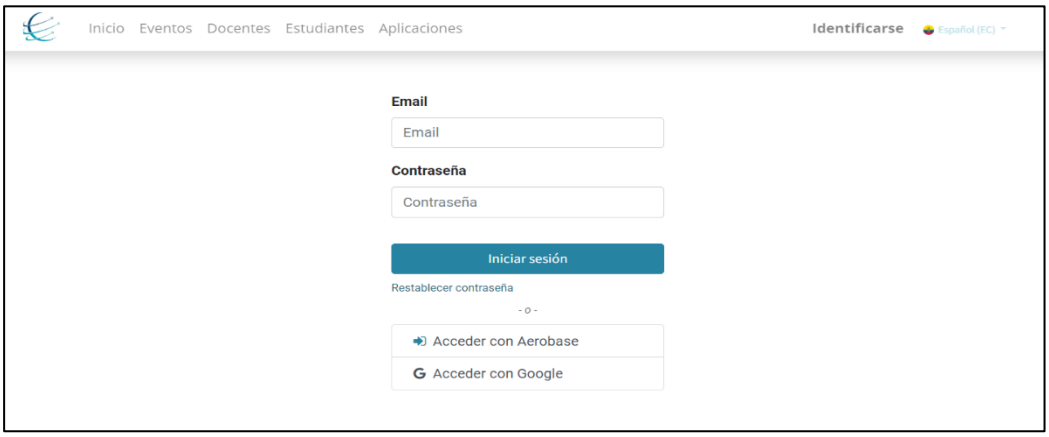
3. Esperar visualizar la página de inicio de sesión

Resultado esperado:

- Petición de acceso desde Odoo, SDLC, Quipux.
- Formulario de inicio de sesión de Aerobase

Resultado obtenido:

- Petición de acceso desde Odoo.

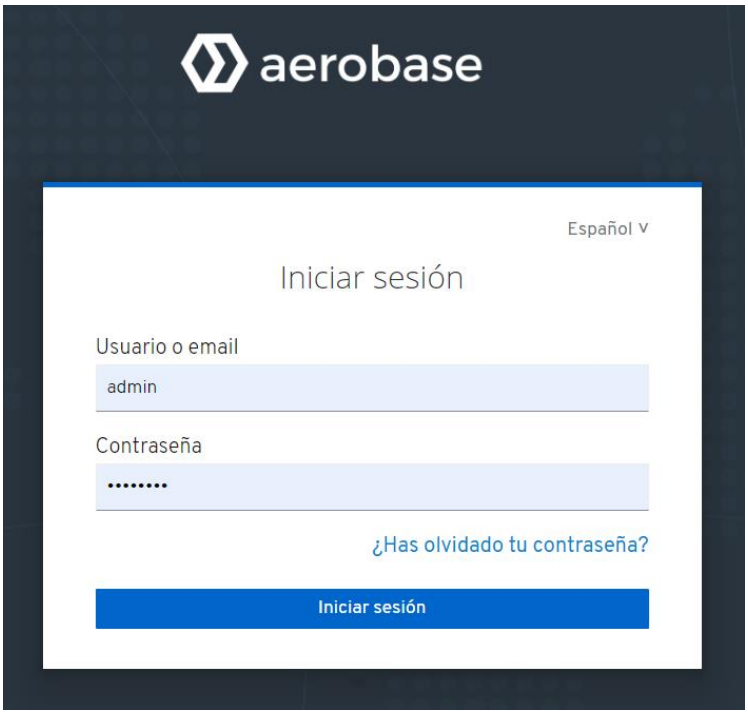


- Petición de acceso desde SDLC.

  Esta aplicación al no contar con una interfaz inicial procede a redireccionar directamente a la vista de inicio de sesión de Aerobase.

- Petición de acceso desde Quipux.

- Formulario de inicio de sesión de Aerobase



Validar accesos a Odoo, SDLC, Quipux.	CAS-02	
	¿Prueba de despliegue?	Sí

Descripción:
Se verificará los accesos a Odoo, SDLC y Quipux, mediante Aerobase

Prerrequisitos

- Establecer conexión con Aerobase (CP01)
- Credenciales con permisos para acceder a Odoo, SDLC y Quipux

Pasos:

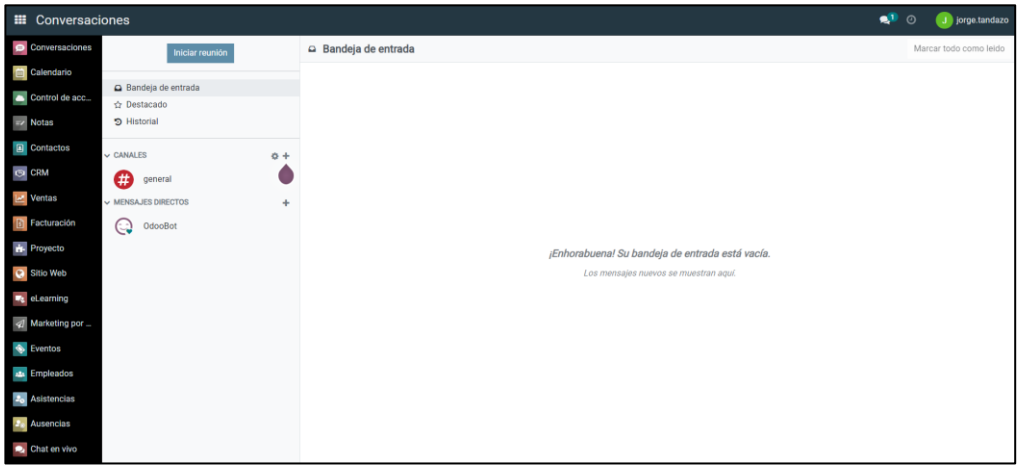
1. Establecer conexión con Aerobase **(CP01)**
2. Llenar el formulario con las credenciales registradas.
3. Dar Clic en el botón Iniciar Sesión.
4. Esperar visualizar la página de inicio de Odoo, SDLC y Quipux.

Resultado esperado:

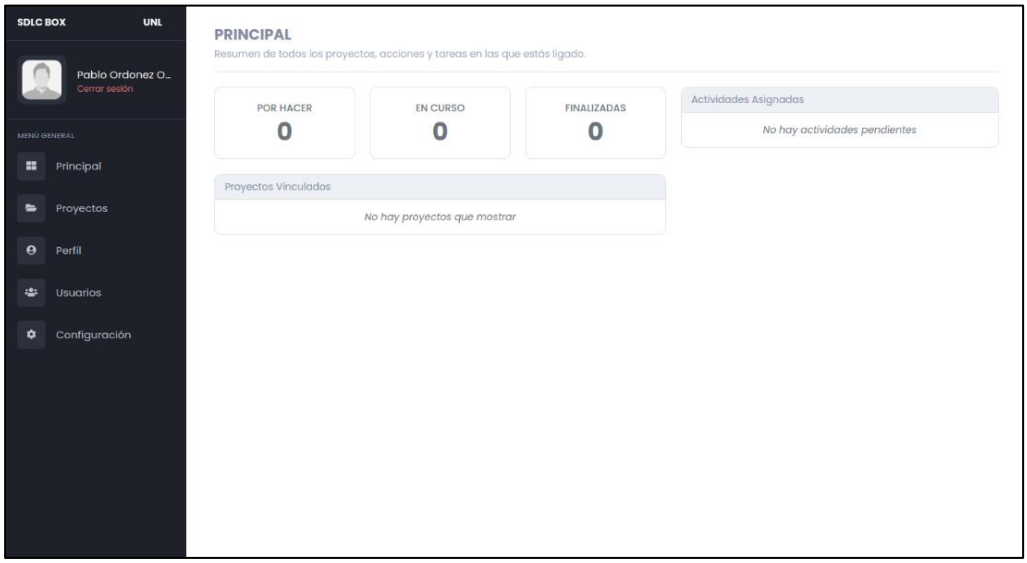
- Poder acceder a Odoo, SDLC y Quipux.
- Página de inicio de Odoo, SDLC y Quipux.

Resultado obtenido:

- Página de inicio de Odoo



- Página de inicio de SDLC



- Página de inicio de Quipux

Cerrar sesión Aerobase	CAS-03	
	¿Prueba de despliegue?	Sí

Descripción:
Se probará la conexión de Aerobase con Odoo, SDLC, Quipux.

Prerrequisitos

- Usuario con accesos a Odoo, SDLC, Quipux.
- Acceder a la página.
- Tener una sesión inicializada

Pasos:

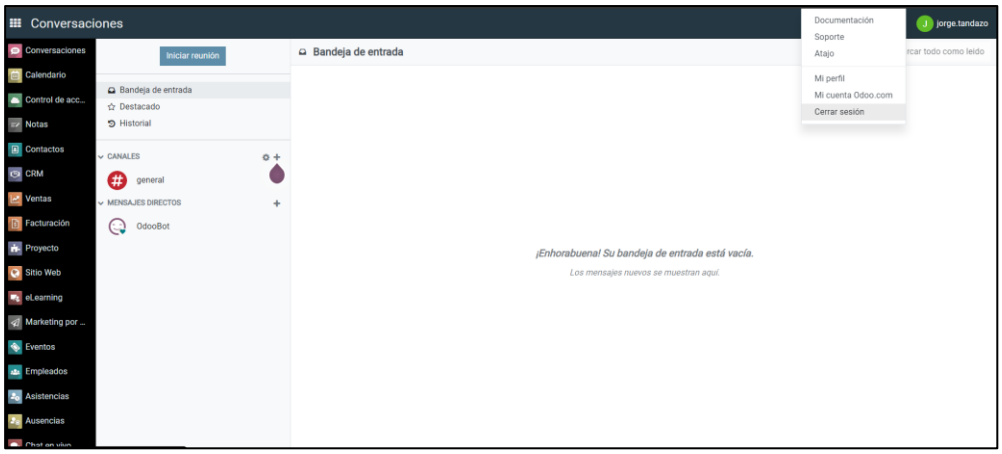
4. Ir al ítem de CERRAR SESION
5. Dar clic en el botón Cerrar Sesión
6. Esperar visualizar la página raíz de Odoo, SDLC, Quipux.

Resultado esperado:

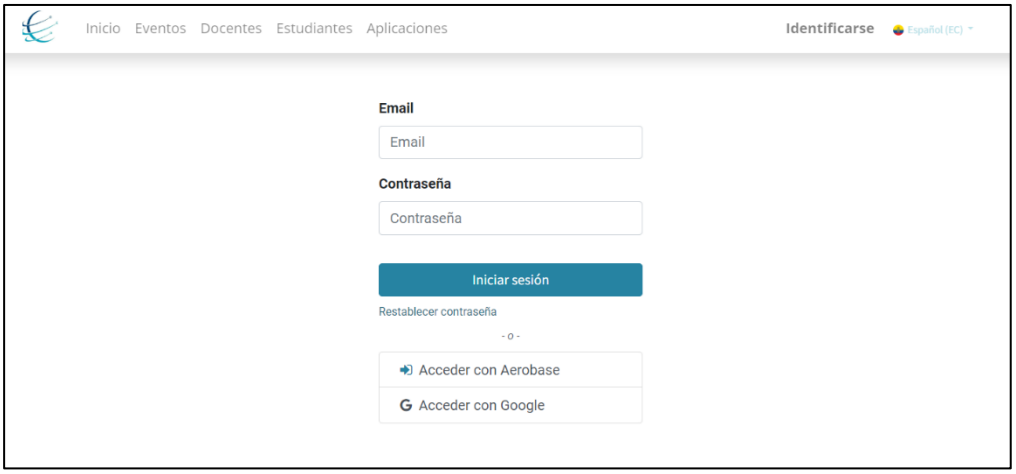
- Cerrar Sesión en Odoo, SDLC, Quipux.
- Visualizar la página raíz de Odoo, SDLC, Quipux.

Resultado obtenido:

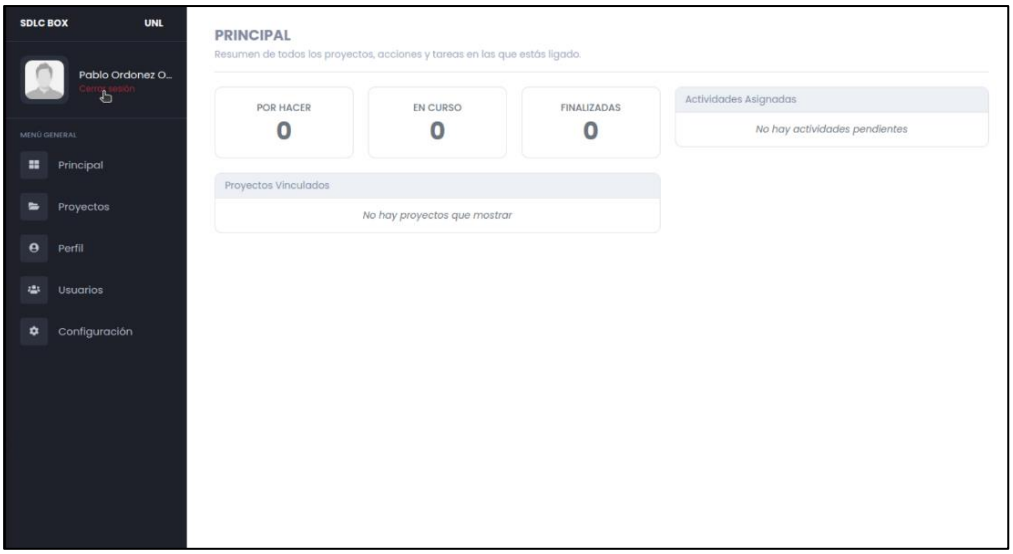
- Sección para Cerrar Sesión en Odoo



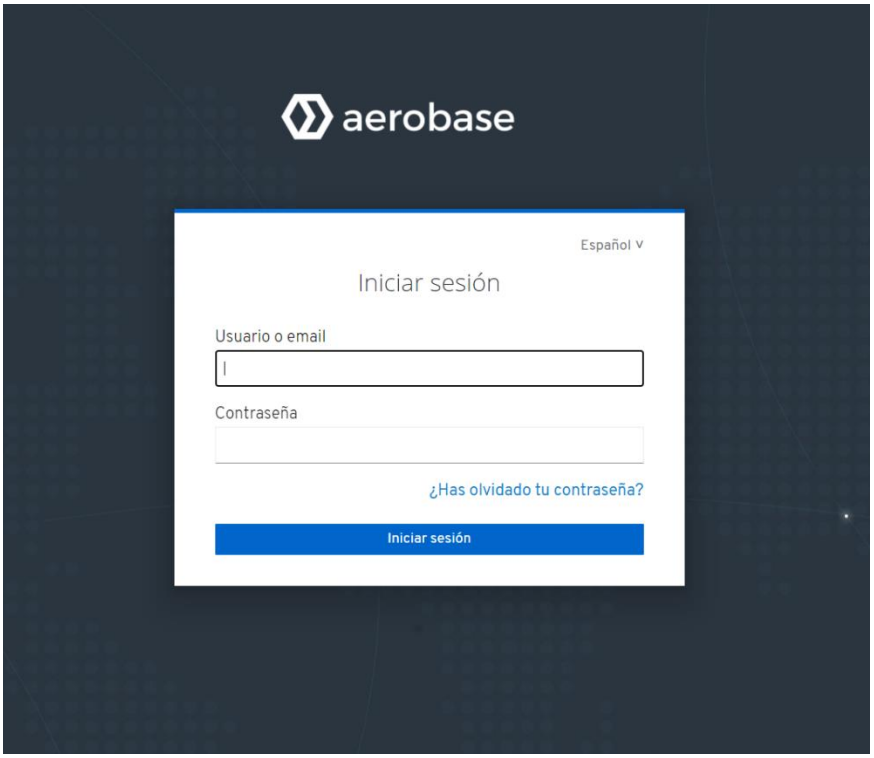
- Vista después de Cerrar Sesión en Odoo



- Sección para Cerrar Sesión en SDLC



- Vista después de Cerrar Sesión en SDLC

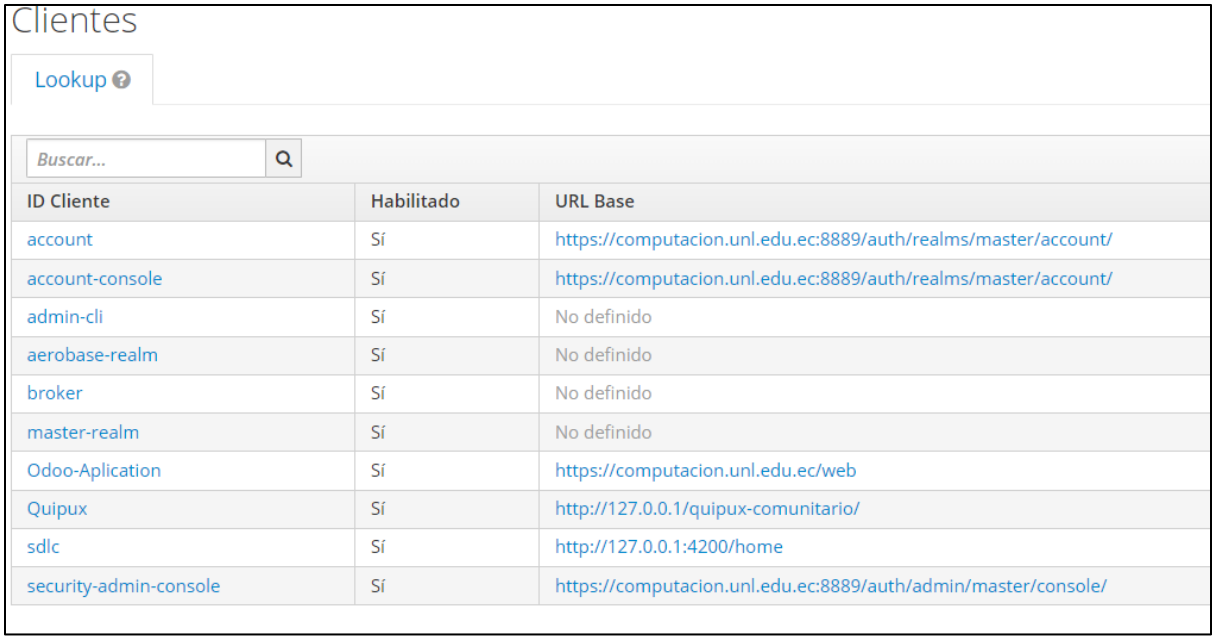


- Sección para Cerrar Sesión en Quipux

- Vista después de Cerrar Sesión en Quipux

Anexos

En la Figura se presenta los clientes que se han registrado en Aerobase para entablar conexión y permitir el acceso, entre ellos están los clientes para Odoo, SDLC y Quipux.



Bibliografía y referencias

Referencia	Título
Ref. 1	Anexo 5: Pruebas de Integración

Anexo 7: Pruebas de Rendimiento

Proyecto: Implementación de un Servicio Centralizado de Gestión de Identidades y Control de Acceso de usuarios en aplicaciones web para la Carrera de Ingeniería en Sistemas/Computación de la UNL: SmartLab

Versión: 1.0

Fecha: 08/02/2024

Hoja de control

Organismo	Universidad Nacional de Loja		
Proyecto	Implementación de un Servicio Centralizado de Gestión de Identidades y Control de Acceso de usuarios en aplicaciones web para la Carrera de Ingeniería en Sistemas/Computación de la UNL: SmartLab		
Entregable	Pruebas de rendimiento		
Autor	Josue Macas, Jorge Tandazo		
Versión/Edición	1.0	**Fecha Versión**	20/12/2023
Aprobado por	Ing. Pablo F. Ordoñez Ordoñez, Mg. Sc	**Fecha Aprobación**	26/12/2023
		Nº Total de Páginas	9

Introducción

Objetivo

El objetivo principal de las pruebas de rendimiento fue evaluar el comportamiento de IAM Computación bajo condiciones simuladas de carga de usuarios concurrentes, para determinar su capacidad para manejar un número creciente de usuarios.

Alcance

El alcance de las pruebas de rendimiento incluye la validación de casos de prueba por el Profesor Ing. Pablo F. Ordoñez Ordoñez, Mg. Sc., director del TT, con el aporte de su experiencia en ingeniería de sistemas y computación. Los escenarios de prueba serán elaborados por Josue Macas y Jorge Tandazo, estudiantes del TT, bajo la supervisión del Profesor Ordoñez. Se ejecutarán los escenarios bajo diversas cargas y se recopilarán datos relevantes para analizar y mejorar el rendimiento del sistema de autenticación IAM Computación, contribuyendo al éxito del TT.

Configuración de las Pruebas:

- Herramienta Utilizada: Apache JMeter
- Tipo de Prueba: Pruebas de Carga
- Número de Usuarios Simultáneos por caso: 100, 200, 800, 1600, 5000
- Métricas Evaluadas: Tiempo de Respuesta, Tasa de Error, Rendimiento del Sistema

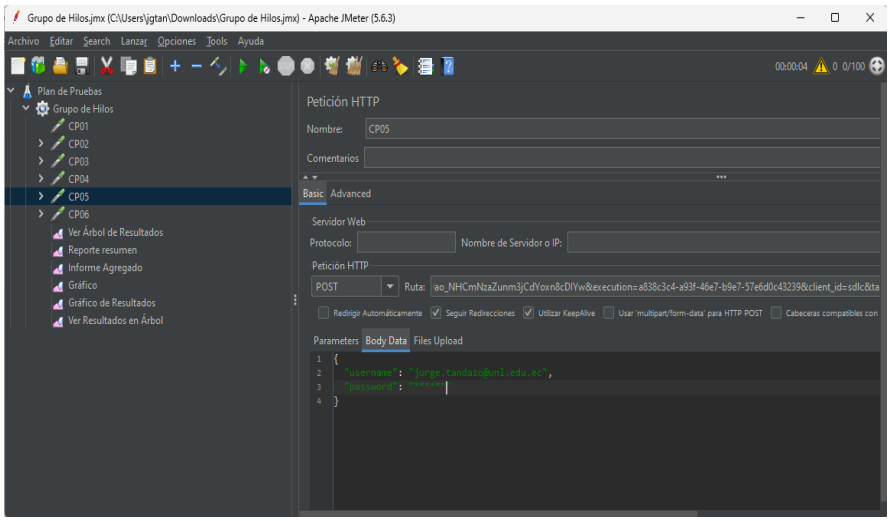


Figura 1: Configuración de los casos de prueba.

Resultados y Hallazgos:

Durante la evaluación de IAM Computación, se llevaron a cabo pruebas exhaustivas en su página de inicio de sesión, acceso a la cuenta mediante el inicio de sesión, información de perfil, actualización de credenciales, autenticación de clientes y cierre de sesión. Estas pruebas se realizaron utilizando muestras 100, 200, 800, 1600 y 5000 usuarios interactuando simultáneamente.

Resumen de los casos de prueba

Se simularon diferentes niveles de carga para evaluar la capacidad de respuesta del sistema.

Número del Caso de Prueba	Componente	Descripción de lo que se probará
CP01	IAM Computación	Página de inicio de sesión
CP02	IAM Computación	Acceso a la cuenta mediante el inicio de sesión
CP03	IAM Computación	Información de perfil
CP04	IAM Computación	Actualización de credenciales
CP05	IAM Computación	Autenticación de un cliente de IAM Computación
CP06	IAM Computación	Cerrado de sesión

Resultados obtenidos de JMeter

Los resultados obtenidos por la herramienta usada se presentan a continuación durante las primeras pruebas se puede visualizar en el grafico un rendimiento optimo:

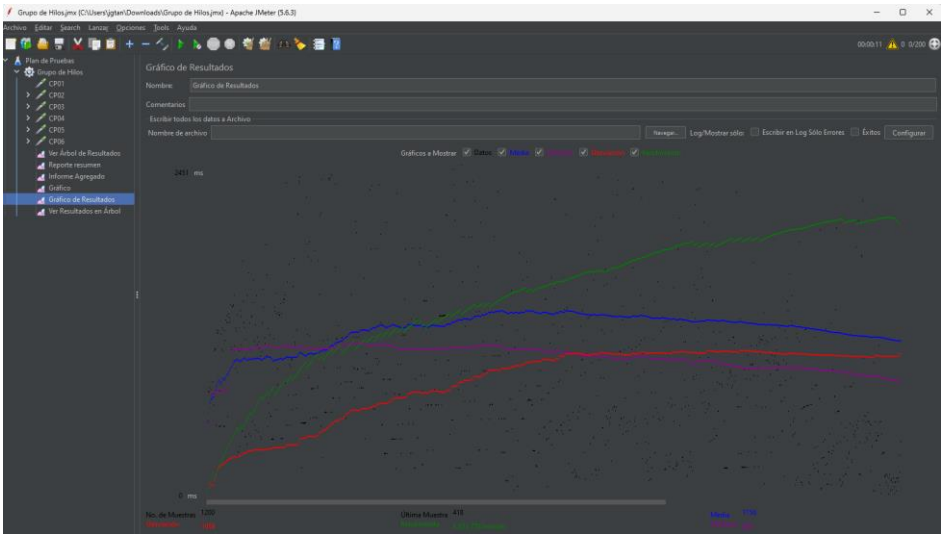


Figura 2: Rendimiento del sistema durante la ejecución de pruebas.

Muestra de 100 usuarios por caso:

Tiempo Promedio de Respuesta	Tasa de Error	Rendimiento del Sistema
1878 milisegundos	0%	32.3 transacciones por segundo

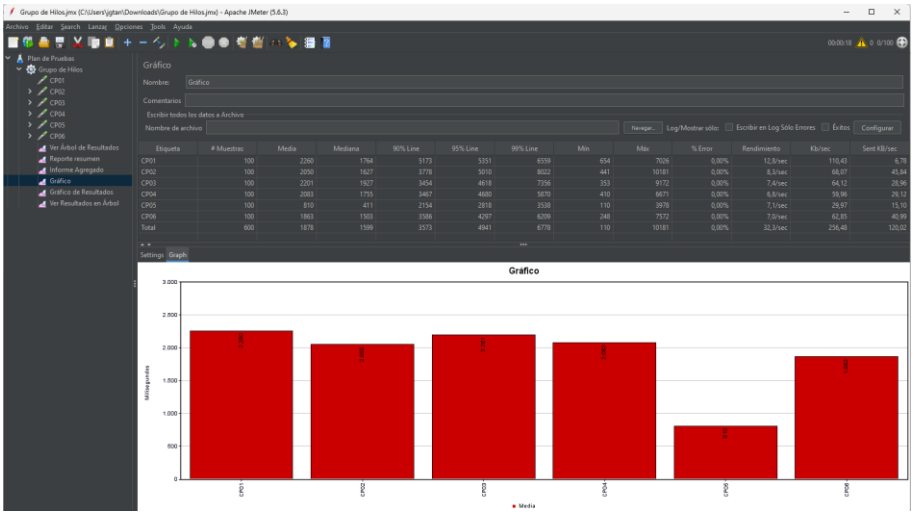


Figura 3: Pruebas de carga con 100 muestras por caso.

Durante la prueba con 600 usuarios, el sistema demostró un buen rendimiento con tiempos de respuesta aceptables y una tasa de error en 0%. La carga adicional generada por los usuarios simulados no afectó significativamente el rendimiento del sistema.

Muestra de 200 usuarios por caso:

Tiempo Promedio de Respuesta	Tasa de Error	Rendimiento del Sistema
1156 milisegundos	0%	105.4 transacciones por segundo

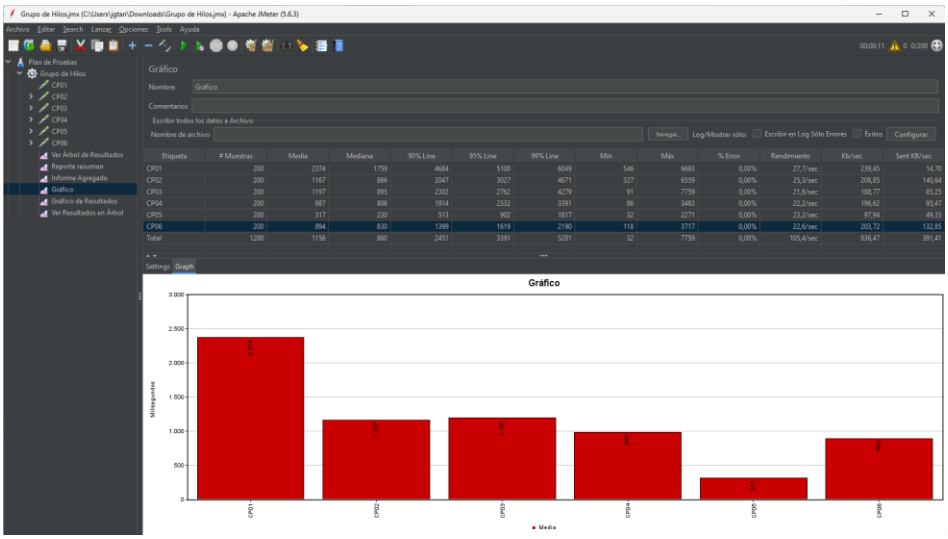


Figura 4: Pruebas de carga con 200 muestras por caso.

Con el doble de usuarios en comparación con la muestra anterior, el sistema experimentó un ligero aumento en los tiempos de respuesta, la tasa de error se mantuvo en 0%. Sin embargo, el rendimiento general se mantuvo dentro de límites aceptables y el sistema continuó respondiendo de manera eficiente.

Muestra de 800 usuarios por caso:

Tiempo Promedio de Respuesta	Tasa de Error	Rendimiento del Sistema
6409 milisegundos	0%	91.3 transacciones por segundo

Figura 5: Pruebas de carga con 800 muestras por caso.

Con el incremento de la carga a 4800 usuarios, se observó un aumento significativo en los tiempos de respuesta, por otro lado, la tasa de error se mantuvo en el 0%. El sistema se mantuvo en niveles óptimos sin presentar ninguna novedad.

Muestra de 1600 usuarios por caso:

Tiempo Promedio de Respuesta	Tasa de Error	Rendimiento del Sistema
9025 milisegundos	0%	75,1 transacciones por segundo

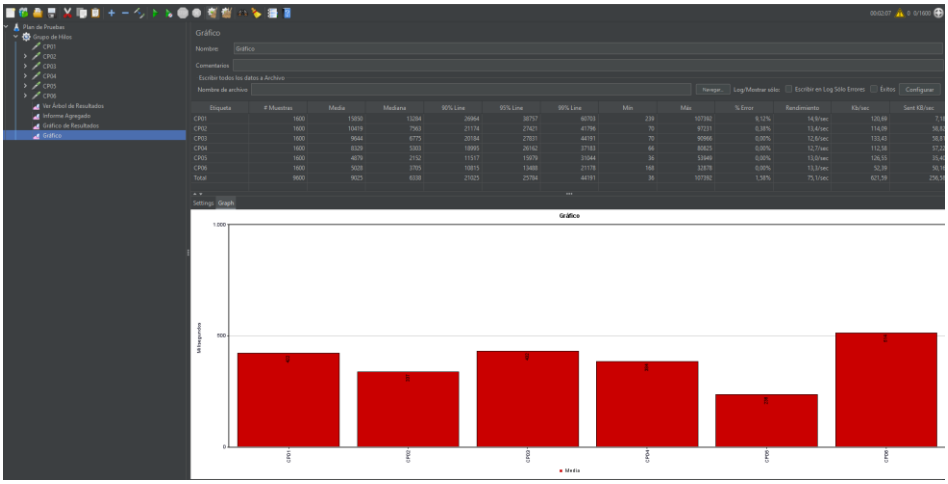


Figura 6: Pruebas de carga con 1600 muestras por caso.

Con el doble de usuarios en comparación con la muestra anterior, el sistema experimentó un ligero aumento considerable en los tiempos de respuesta, mientras que ya el sistema empezó a arrojar una taza de error del 1.58%. Sin embargo, pese a tener un porcentaje de error el sistema se puede mantener estable.

Muestra de 5000 usuarios por caso:

Tiempo Promedio de Respuesta	Tasa de Error	Rendimiento del Sistema
32101 milisegundos	16,65%	75,5 transacciones por segundo

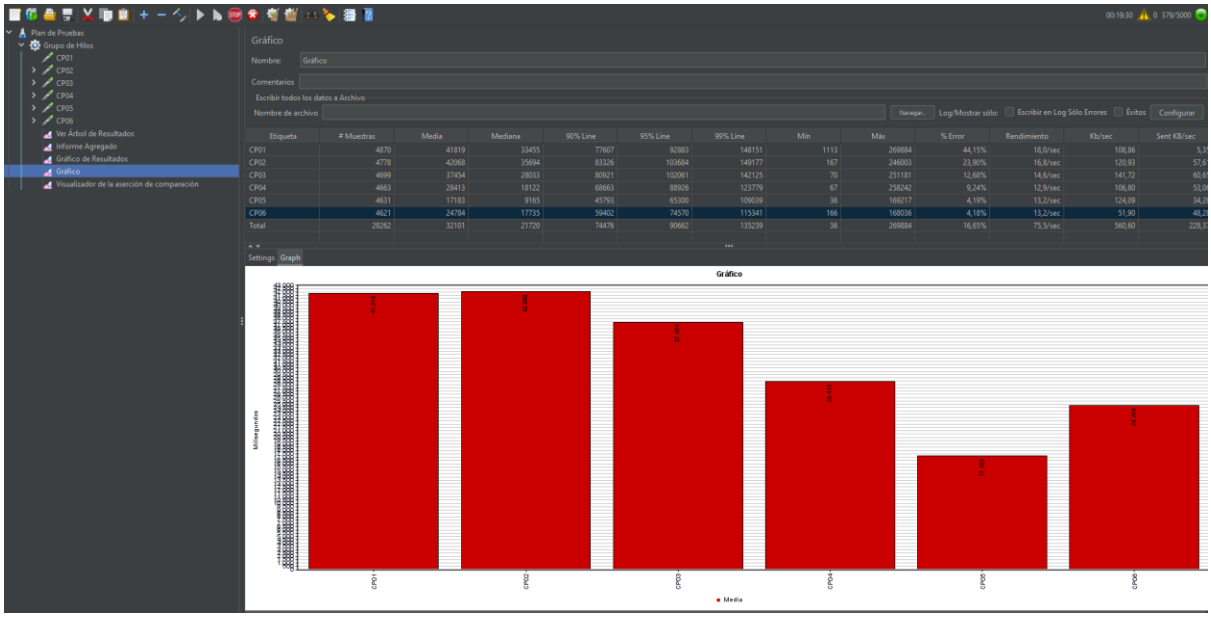


Figura 7: Pruebas de carga con 5000 muestras por caso.

Al manejarse con muestras superiores bastante considerable, el sistema empezó a mostrar signos de estrés, los usuarios experimentaron demoras en la respuesta y posterior a la caída del servicio. Se recomienda realizar ajustes en la infraestructura para mejorar la capacidad de manejo de cargas más altas en caso de ser necesaria.

Conclusiones:

- El sistema demostró ser robusto y capaz de manejar eficientemente los usuarios de la carrera de Ingeniería En Sistemas/ Computación, manteniendo tiempos de respuesta aceptables y una tasa de error en 0% dentro del límite de la cantidad de usuarios existentes.

Recomendaciones:

- Realizar pruebas de carga periódicas para monitorear el rendimiento del sistema y asegurar su óptimo funcionamiento en todo momento.

Anexo 8: Pruebas de Autenticación

Proyecto: Implementación de un Servicio Centralizado de Gestión de Identidades y Control de Acceso de usuarios en aplicaciones web para la Carrera de Ingeniería en Sistemas/Computación de la UNL: SmartLab

Versión: 1.0

Fecha: 08/02/2024

Hoja de control

Organismo	Universidad Nacional de Loja		
Proyecto	Implementación de un Servicio Centralizado de Gestión de Identidades y Control de Acceso de usuarios en aplicaciones web para la Carrera de Ingeniería en Sistemas/Computación de la UNL: SmartLab		
Entregable	Pruebas WSTG - Estable: Pruebas de Autenticación		
Autor	Josue Macas, Jorge Tandazo		
Versión/Edición	1.0	**Fecha Versión**	20/12/2023
Aprobado por	Ing. Pablo F. Ordoñez Ordoñez, Mg. Sc	**Fecha Aprobación**	26/12/2023
		Nº Total de Páginas	9

Introducción

Este informe presenta los resultados obtenidos durante las pruebas realizadas según el estándar OWASP en la sección de Pruebas de Autenticación. El propósito principal de estas pruebas es evaluar la robustez y seguridad del sistema de autenticación de la aplicación web en consideración.

Alcance de las Pruebas

Las pruebas se enfocaron en evaluar diez aspectos clave de la autenticación web, según lo establecido en la sección 4.4 de las Pruebas de Seguridad de Aplicaciones Web del WSTG - Estable.

Definición de los casos de pruebas

A continuación, se describe la metodología OWASP 4.0 para la realización de las pruebas de intrusión en IAM Computación, y se explica cómo realizar la comprobación de cada una de las vulnerabilidades.

Categoría	Numero de Referencia	Nombre de la Prueba	Vulnerabilidad
Pruebas de autenticación	OWASP-AT-001	Transporte de Credenciales sobre canal cifrado	Transporte de Credenciales sobre canal cifrado
	OWASP-AT-002	Credenciales predeterminadas	Credenciales predeterminadas
	OWASP-AT-003	Mecanismo de bloqueo débil	Mecanismo de bloqueo débil
	OWASP-AT-004	Omitir el esquema de autenticación	Omitir el esquema de autenticación
	OWASP-AT-005	Recordar contraseña vulnerable	Recordar contraseña vulnerable
	OWASP-AT-006	Debilidades de la caché del navegador	Debilidades de la caché del navegador
	OWASP-AT-007	Política de contraseñas débiles	Política de contraseñas débiles
	OWASP-AT-008	Respuesta débil a preguntas de seguridad	Respuesta débil a preguntas de seguridad
	OWASP-AT-009	Funcionalidades de cambio o restablecimiento de contraseña débil	Funcionalidades de cambio o restablecimiento de contraseña débil
	OWASP-AT-010	Autenticación más débil en un canal alternativo	Autenticación más débil en un canal alternativo

Resultados de las Pruebas

OWASP-AT-001: Transporte de Credenciales sobre Canal Cifrado: Se verificó la seguridad del canal de comunicación para garantizar que las credenciales de autenticación se transmitan de manera segura mediante cifrado SSL/TLS. Al ingresar a IAM Computación, se observó lo siguiente:

- En el inicio de sesión, las credenciales se cifran gracias a la URL de solicitud HTTPS.

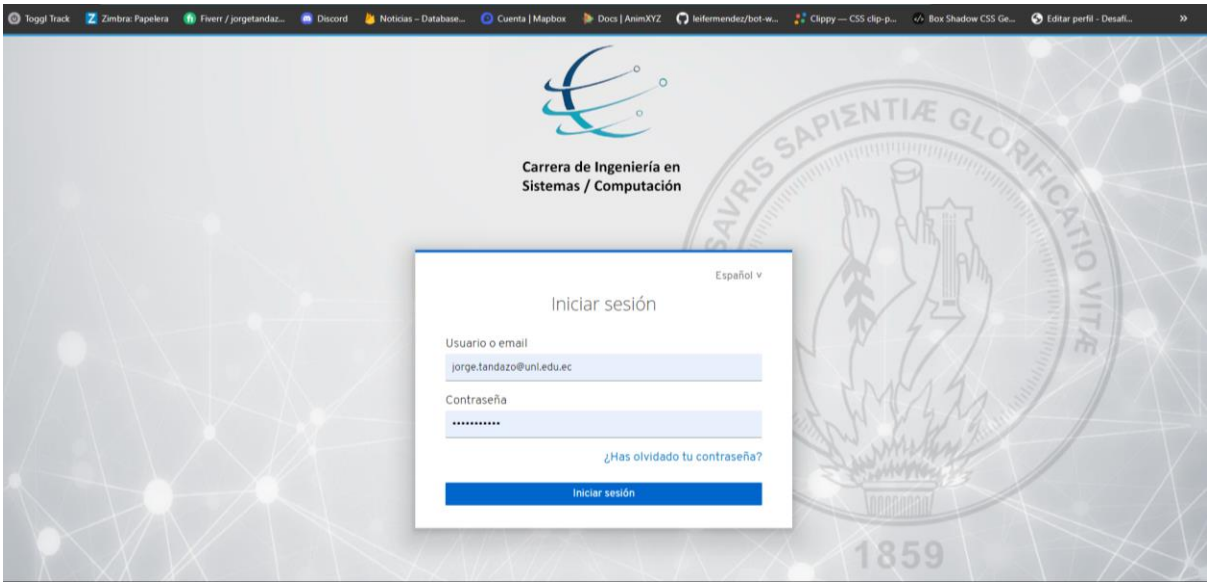


Figura 1: Transmisión por canal cifrado HTTP.

El servidor devuelve información de cookie para un token de sesión, incluyendo el atributo

"Secure" para evitar que el cliente exponga la cookie a través de canales no cifrados en el futuro.

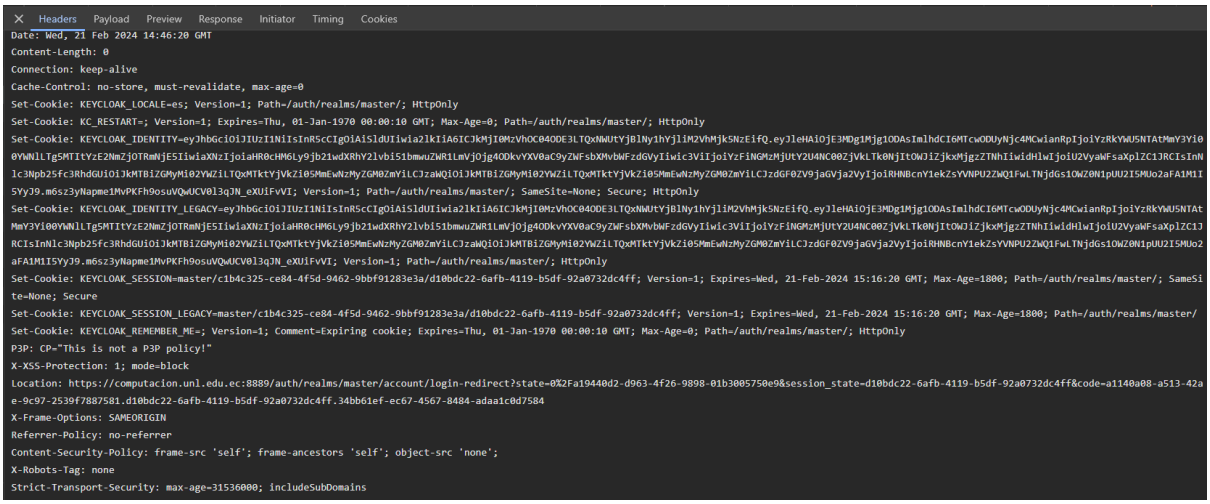


Figura 2: Response header solicitud POST.

OWASP-AT-002: Credenciales Predeterminadas: Se evaluó si existían credenciales predeterminadas que pudieran comprometer la seguridad del sistema. Se encontraron las siguientes observaciones:

- IAM Computación no acepta credenciales predeterminadas; para obtener acceso, es necesario registrarse por parte del administrador del sistema.

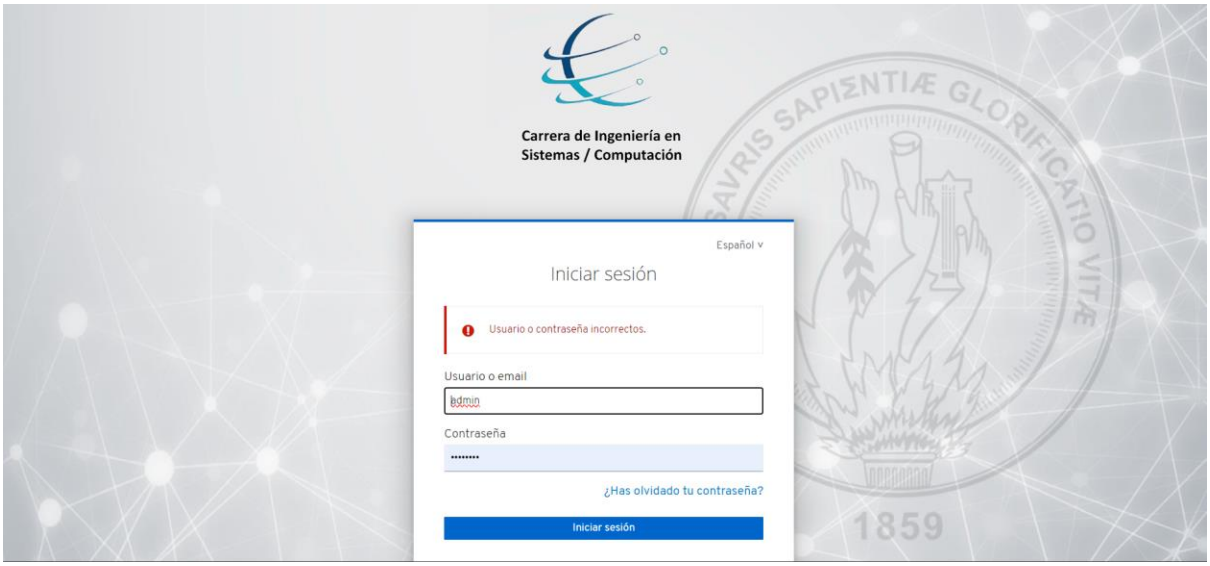


Figura 3: Solicitud de inicio de sesión con credenciales admin/admin.

OWASP-AT-003: Mecanismo de Bloqueo Débil: Se analizó la eficacia del mecanismo de bloqueo de cuentas luego de intentos de inicio de sesión fallidos. Se encontraron las siguientes observaciones:

- IAM Computación no bloquea la cuenta después de algún número de intentos de sesión fallidos.

OWASP-AT-004: Omitir el esquema de autenticación: Se verificó si era posible eludir el proceso de autenticación para acceder a funcionalidades restringidas. Se encontraron las siguientes observaciones:

- Al intentar acceder a http://mi.dominio.com/auth/realms/master/account sin una sesión activa, se redirigió automáticamente al inicio de sesión.

OWASP-AT-00005: Recordar Contraseña Vulnerable: Se revisó la implementación del mecanismo de "recordar contraseña" para identificar posibles vulnerabilidades. Se encontraron las siguientes observaciones:

- IAM Computación no mantiene habilitado el mecanismo de "recordar contraseña" para evitar posibles vulnerabilidades.

OWASP-AT-007: Política de Contraseñas Débiles: Se analizó la fortaleza de la política de contraseñas para garantizar que las contraseñas proporcionen un nivel adecuado de seguridad. Se encontraron las siguientes observaciones:

- Se implementa una política de contraseñas robusta en IAM Computación. Esto evita el riesgo de que se utilicen contraseñas débiles o fáciles de adivinar.

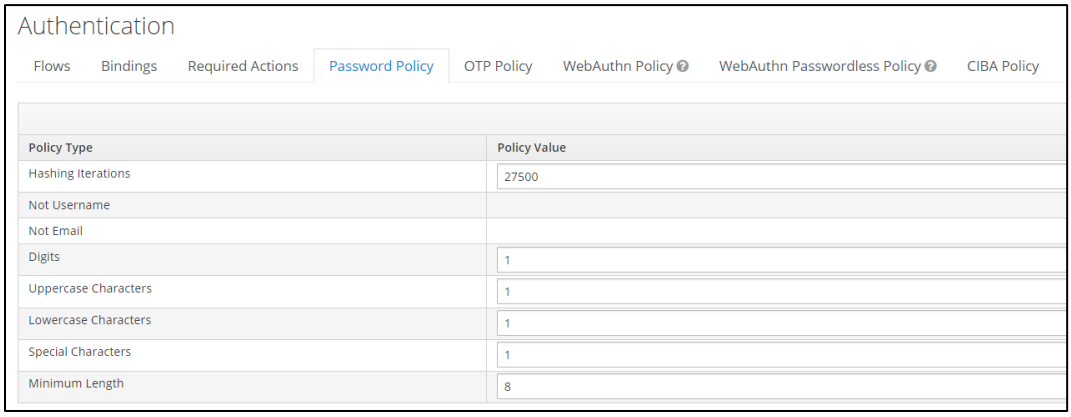


Figura 4: Políticas de contraseña.

OWASP-AT-008: Respuesta Débil a Preguntas de Seguridad: Se revisó la configuración de las preguntas de seguridad para asegurar que proporcionen una capa adicional de protección. Se observó lo siguiente:

- No se encontraron preguntas de seguridad o la configuración adecuada para una protección de la cuenta del usuario, ya que el registro lo maneja el administrador de IAM Computación.

OWASP-AT-009: Funcionalidades de Cambio o Restablecimiento de Contraseña Débil: Se evaluaron las funciones relacionadas con el cambio o restablecimiento de contraseñas para asegurar su robustez. Se encontraron las siguientes observaciones:

- Las funcionalidades recuperación de contraseña es adecuada ya que para llevar a cabo este proceso se debe pasar el filtro de un correo verificado por el sistema, al cual le llegara instrucciones para q pueda acceder a la recuperación de contraseña

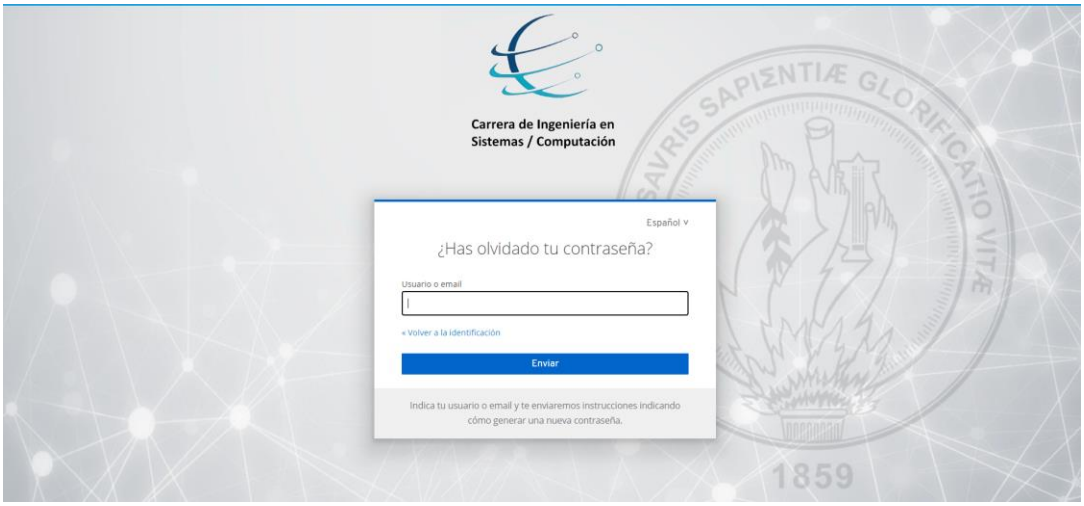


Figura 5: Formulario de solicitud de recuperación de contraseña.

- El correo que llega al usuario tiene un tiempo de caducidad

Figura 6: Respuesta a la solicitud de recuperación de contraseña.

- Para proceder a realizar el nuevo cambio de clave solicita una confirmación, para que el usuario este seguro de que clave ingresara

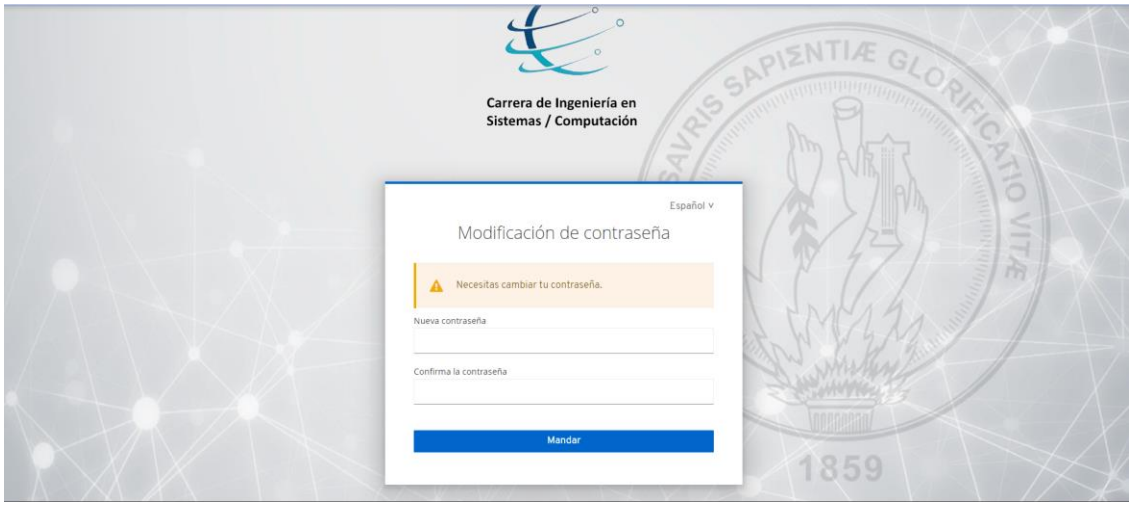


Figura 7: Formulario de ingreso de nueva contraseña.

OWASP-AT-010: Autenticación Más Débil en un Canal Alternativo: Se investigó la fortaleza de la autenticación en canales alternativos para evitar posibles puntos débiles. Se observó lo siguiente:

- Los canales alternativos de seguridad tienen un nivel complejo de acceso con el fin de evitar posibles vulnerabilidades.

Conclusiones

Basado en los resultados de las pruebas realizadas, se puede resumir que IAM Computación implementa una autenticación robusta y medidas de seguridad adecuadas para proteger las cuentas

de usuario y los datos sensibles. Sin embargo, se identificaron algunas áreas de mejora potencial, como el bloqueo de cuentas después de intentos fallidos de inicio de sesión y la implementación de preguntas de seguridad adicionales. Estas áreas pueden abordarse para fortalecer aún más la seguridad del sistema y garantizar la protección continua de la información del usuario.

Recomendaciones

Se sugiere implementar las siguientes medidas para mejorar la seguridad de la autenticación web:

- Bloqueo de cuentas después de intentos fallidos de inicio de sesión.
- La implementación de preguntas de seguridad adicionales.

Bibliografía y referencias

Referencia	Título
Ref. 1	https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/

Anexo 9: Pruebas de Aceptación

Proyecto: Implementación de un Servicio Centralizado de Gestión de Identidades y Control de Acceso de usuarios en aplicaciones web para la Carrera de Ingeniería en Sistemas/Computación de la UNL: SmartLab

Versión: 1.0

Fecha: 08/02/2024

Hoja de control

Organismo	Universidad Nacional de Loja		
Proyecto	Implementación de un Servicio Centralizado de Gestión de Identidades y Control de Acceso de usuarios en aplicaciones web para la Carrera de Ingeniería en Sistemas/Computación de la UNL: SmartLab		
Entregable	Pruebas de aceptación		
Autor	Josue Macas, Jorge Tandazo		
Versión/Edición	1.0	**Fecha Versión**	25/12/2023
Aprobado por	Ing. Pablo F. Ordoñez Ordoñez, Mg. Sc	**Fecha Aprobación**	26/12/2023
		Nº Total de Páginas	9

Introducción

Objetivo

El objetivo de este documento es recopilar datos para evaluar la utilidad del Servicio Centralizado de Gestión de Identidades y Control de Acceso de Usuarios (IAM) mediante una encuesta de utilidad percibida.

Propósito

Mediante el uso de encuestas y una muestra de estudiantes de la Carrera de Sistemas/Computación, elegidas mediante muestreo por conveniencia, para verificar que la utilidad del Servicio IAM tiene la aceptación necesaria.

Difusión de la Encuesta

Para esta encuesta se trabajó con una muestra de 55 estudiantes de la Carrera de Sistemas/Computación de la UNL, los cuales pertenecen a 8vo y 9no ciclo, a los mismos que se les envió un correo electrónico explicando el propósito de la encuesta y proporcionándoles un enlace para acceder a la encuesta en línea.

Consideraciones Especiales

- Para esta encuesta se garantiza la confidencialidad y anonimato de las respuestas de los usuarios para fomentar la honestidad y la franqueza.
- Los encuestadores están disponibles para responder preguntas y aclarar dudas de los usuarios durante el período de aplicación de la encuesta.

Preparación de la Encuesta

El diseño de la encuesta de utilidad percibida se basa en la pregunta de investigación y los objetivos específicos, posteriormente se revisa y valida el cuestionario con el equipo para asegurar la claridad y relevancia de las preguntas. Para el análisis de resultados se dividirá la encuesta en 5 secciones, la primera para datos generales, la segunda para exponer ítems referentes al funcionamiento y utilidad de la aplicación, la tercera para conocer la experiencia del usuario, la cuarta ayudará a conocer sobre la seguridad y privacidad de los datos del usuaria y finalmente la última parte corresponderá a sugerencias, por parte de los usuarios, para mejorar la aplicación.

Parámetros de Evaluación

Nro.	Pregunta
*	Edad
*	Genero
1	¿Con qué frecuencia utiliza la aplicación de gestión de identidad y acceso centralizado?
2	¿Cuál es el propósito principal de utilizar esta aplicación?
3	¿Cómo calificaría la actualización de credenciales proporcionado por IAM Computación?
4	Respecto a la recuperación de contraseña, ¿Considera que IAM Computación ofrece un proceso claro y eficiente para recuperar contraseñas olvidadas o perdidas?
5	¿Qué tan efectiva considera usted la implementación de la autenticación de doble factor en IAM Computación para garantizar la seguridad de las cuentas de usuario?
6	En general, ¿Cómo calificaría la utilidad del servicio proporcionado por IAM Computación en relación con la gestión de credenciales y accesos a los aplicativos webs?
7	¿Cómo evalúa la experiencia de acceso a las aplicaciones web mediante el Servicio IAM incorporado en la Carrera de Ingeniería en Sistemas/Computación de la UNL?
8	¿Qué características de la aplicación encuentras más útiles?
9	¿Qué características de la aplicación cree que podrían mejorarse para que sea más útil?
10	¿Confía en la seguridad de la aplicación para proteger sus datos personales y contraseñas?
11	¿Siente que sus datos personales están adecuadamente protegidos mientras utiliza esta aplicación?
12	¿Ha experimentado algún problema significativo al utilizar IAM Computación en cualquiera de los aspectos mencionados?

Respuestas de cada pregunta

- **Datos demográficos**

Edad

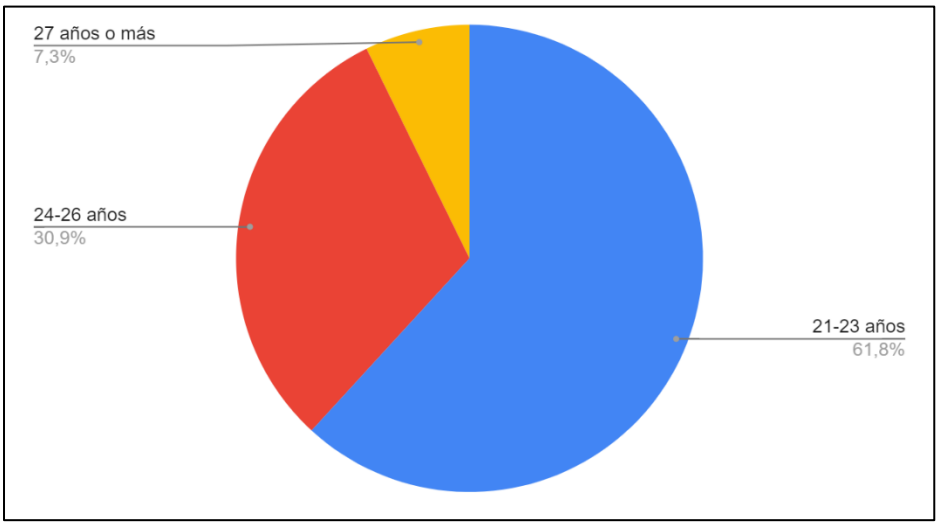


Figura 1. *Resultados de la edad de los encuestados*

Genero

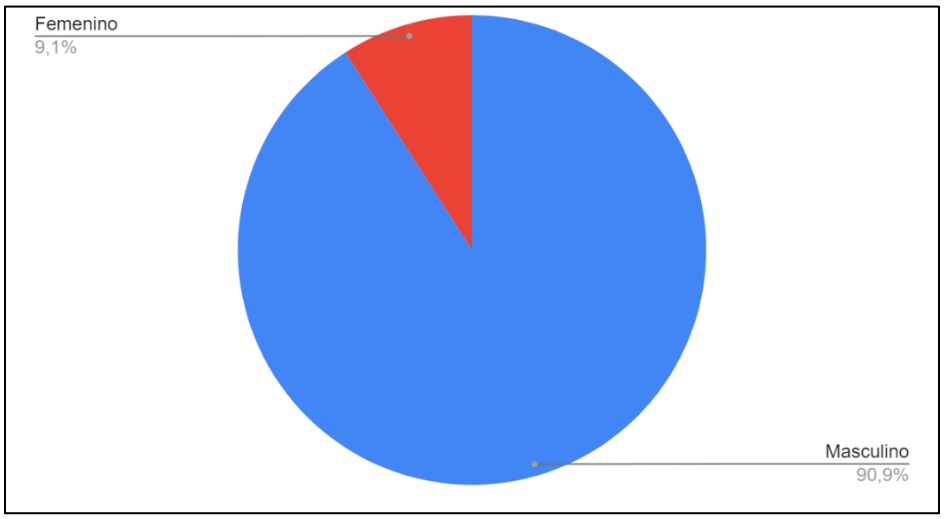


Figura 2. *Resultados del género de los encuestados*

- **Sobre la aplicación de gestión de identidades y acceso**

Pregunta 1: ¿Con qué frecuencia utiliza la aplicación de gestión de identidad y acceso centralizado?

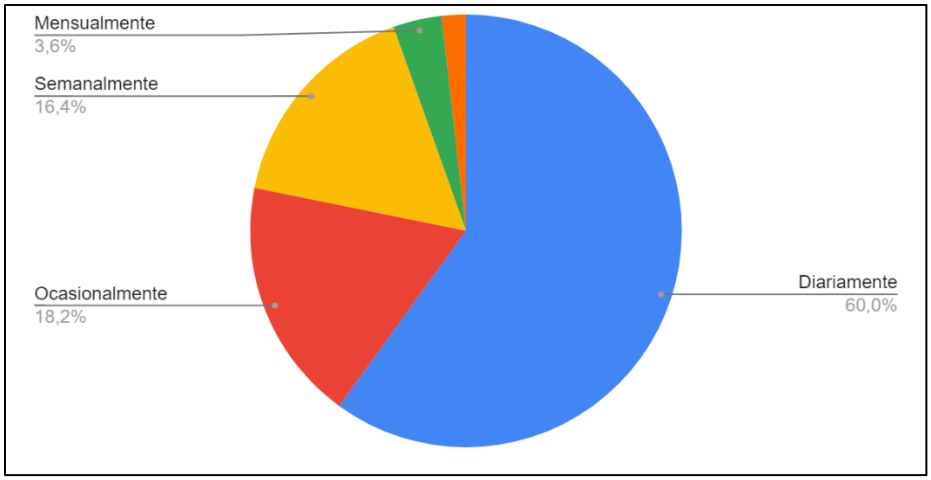


Figura 3. *Resultados de la pregunta 1*

Pregunta 2: ¿Cuál es el propósito principal de utilizar esta aplicación?

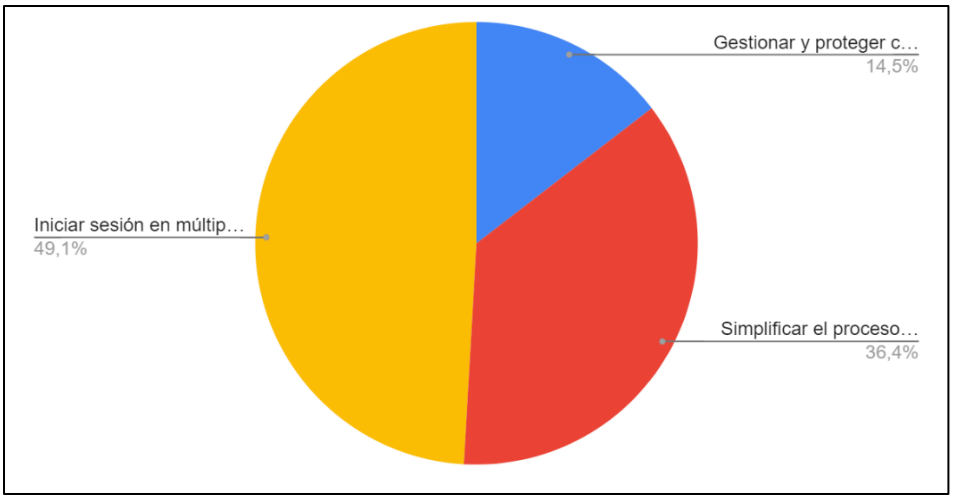


Figura 4. *Resultados de la pregunta 2*

Pregunta 3:¿Cómo calificaría la actualización de credenciales proporcionado por IAM Computación?

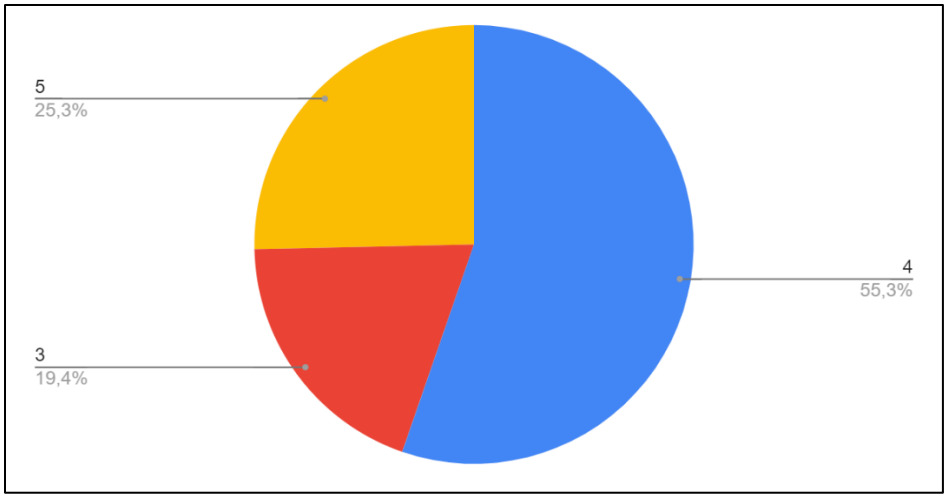


Figura 5. *Resultados de la pregunta 3*

Pregunta 4: Con respecto a la recuperación de contraseña ¿Considera que IAM Computación ofrece un proceso claro y eficiente para recuperar contraseñas olvidadas o perdidas?

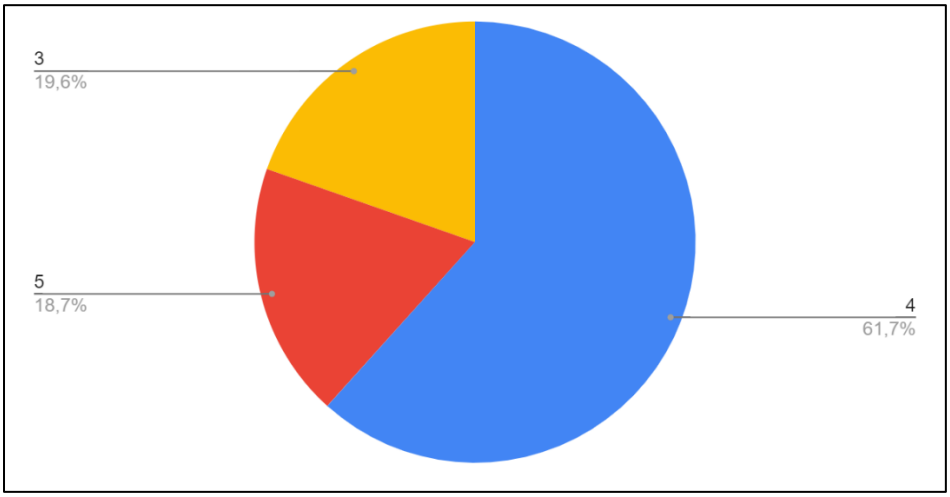


Figura 6. *Resultados de la pregunta 4*

Pregunta 5:¿ Qué tan efectiva considera usted la implementación de la autenticación de doble factor en IAM Computación para garantizar la seguridad de las cuentas de usuario?

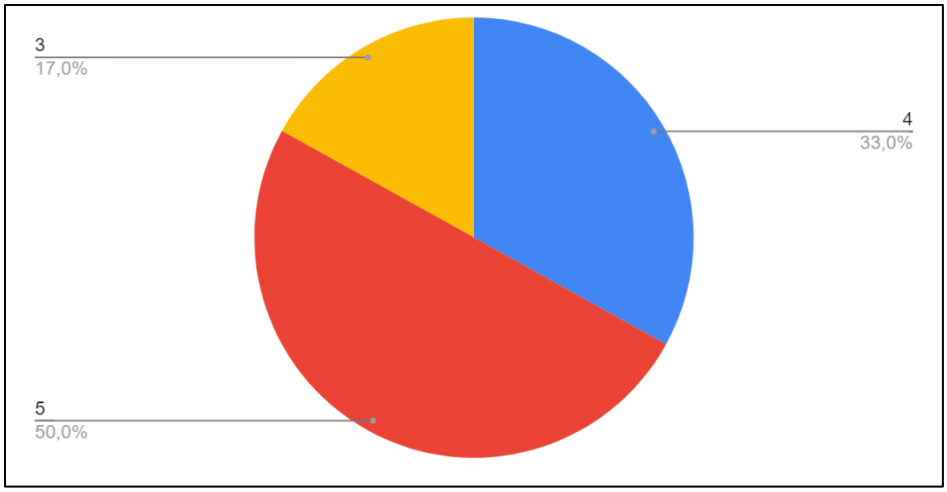


Figura 7. *Resultados de la pregunta 5*

Pregunta 6: En general, ¿Cómo calificaría la utilidad del servicio proporcionado por IAM Computación en relación con la gestión de credenciales y accesos a los aplicativos webs?

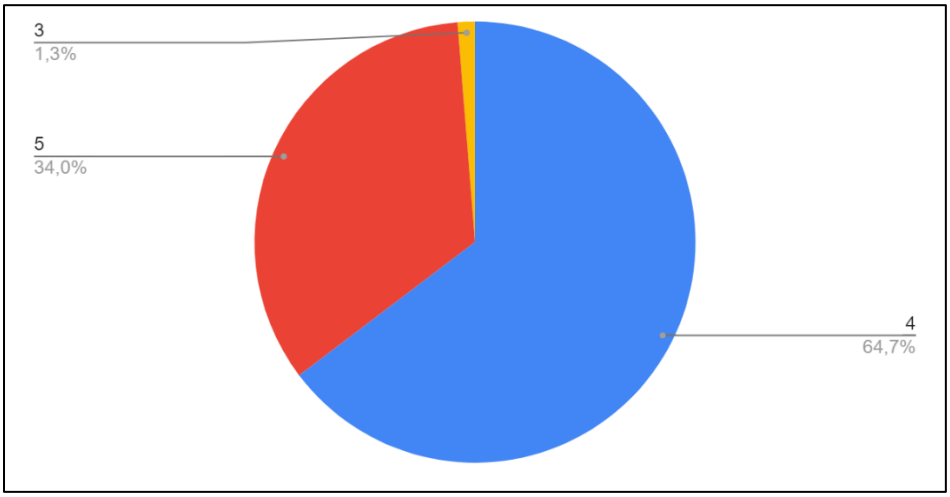


Figura 8. *Resultados de la pregunta 6*

- **Experiencia del usuario**

Pregunta 7: ¿Cómo evalúa la experiencia de acceso a las aplicaciones web mediante el Servicio IAM incorporado en la Carrera de Ingeniería en Sistemas/Computación de la UNL?

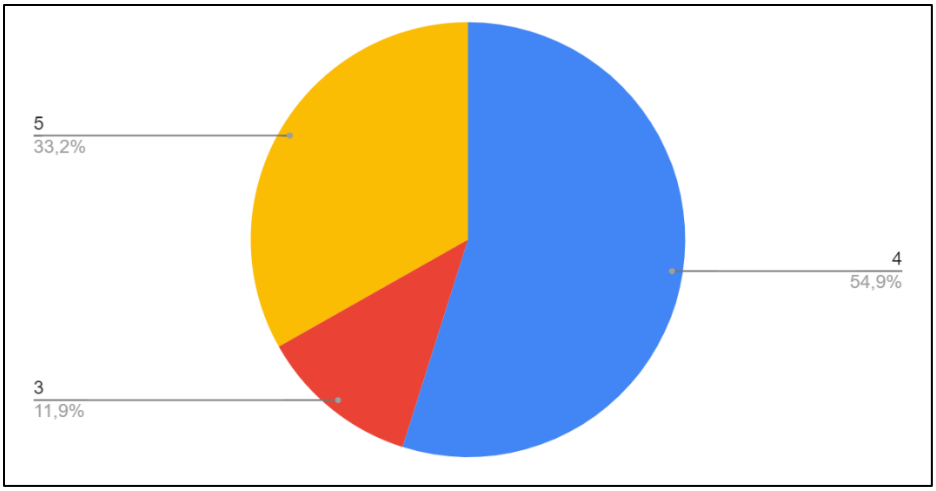


Figura 9. *Resultados de la pregunta 7*

Pregunta 8: ¿ Qué características de la aplicación encuentras más útiles?

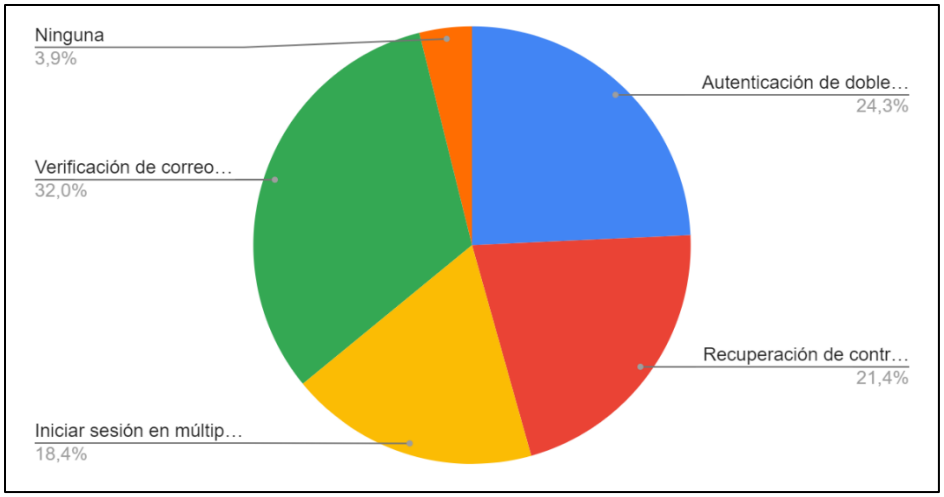


Figura 10. *Resultados de la pregunta 8*

Pregunta 9: ¿Qué características de la aplicación cree que podrían mejorarse para que sea más útil?

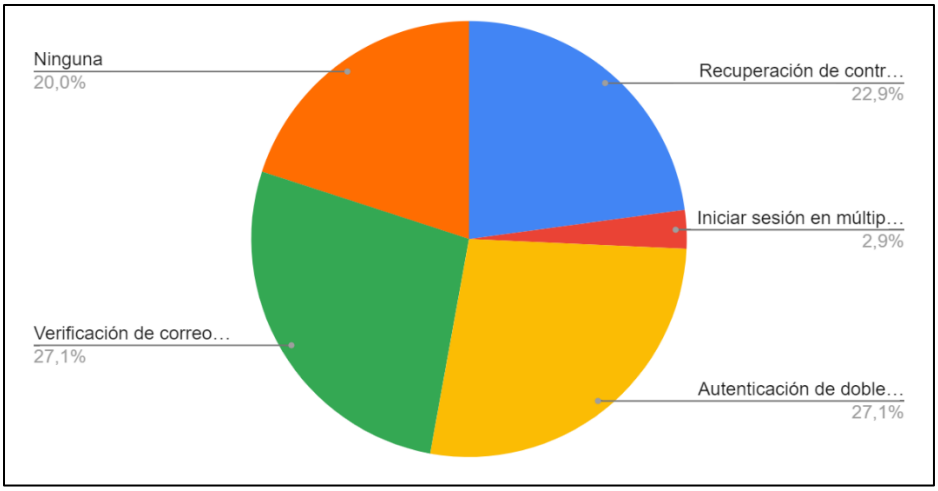


Figura 11. *Resultados de la pregunta 9*

- **Seguridad y Privacidad**

Pregunta 10: ¿Confía en la seguridad de la aplicación para proteger sus datos personales y contraseñas?

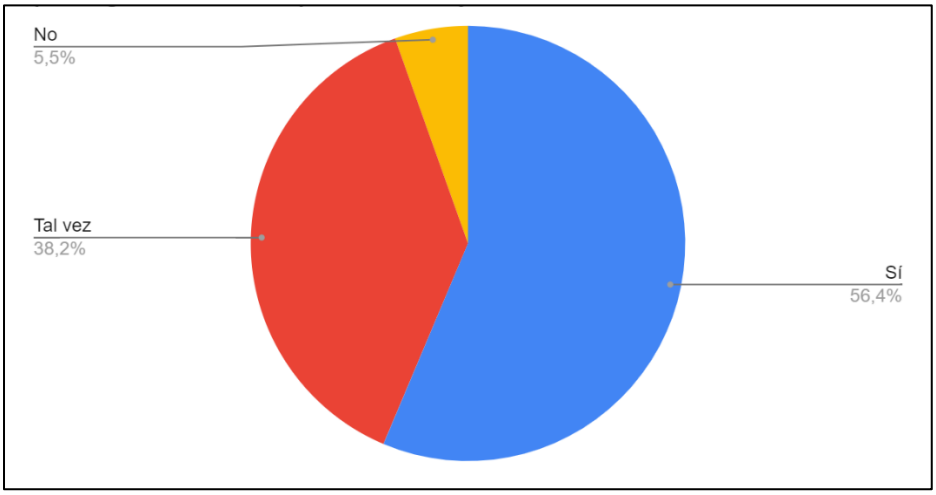


Figura 12. *Resultados de la pregunta 10*

Pregunta 11: ¿Siente que sus datos personales están adecuadamente protegidos mientras utiliza esta aplicación?

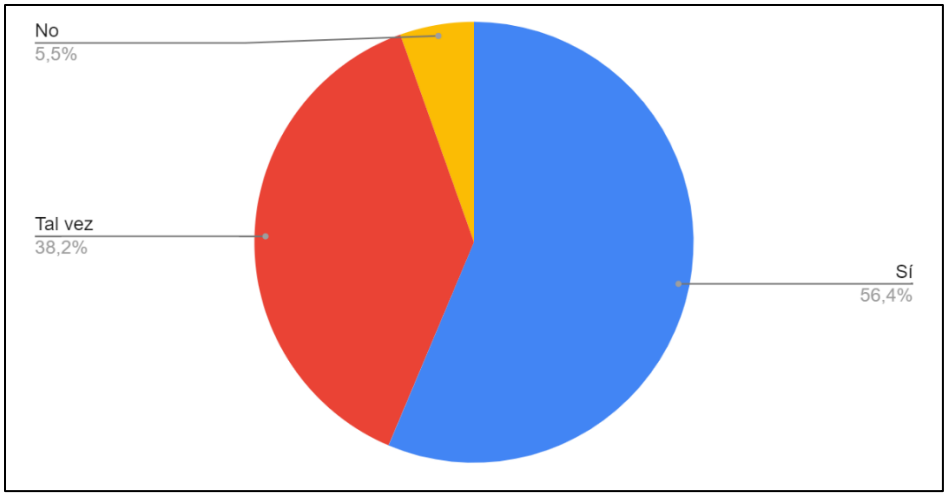


Figura 13. *Resultados de la pregunta 11*

- **Sugerencias y Comentarios Adicionales:**

Pregunta 12:¿Ha experimentado algún problema significativo al utilizar IAM Computación en cualquiera de los aspectos mencionados?

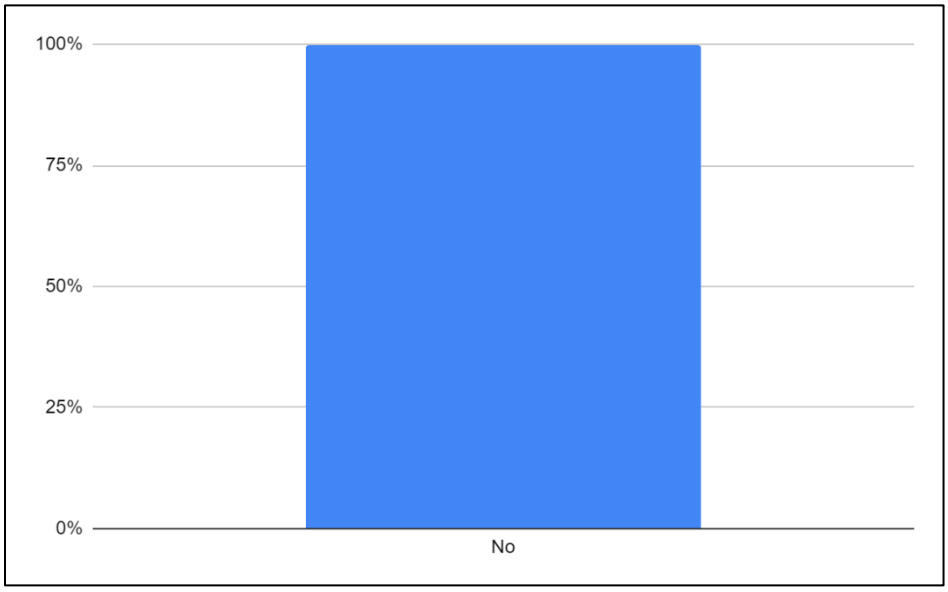


Figura 14. *Resultados de la pregunta 12*

Anexo 10: Certificación de traducción de resumen

Yo, Fernando Joel Lara Carrera, portador de la cédula de ciudadanía número 0106975196, y titular del grado académico de Máster Universitario en Enseñanza de Inglés como Lengua Extranjera por la Universidad internacional de la Rioja (UNIR)

CERTIFICO:

Que el documento aquí compuesto, del resumen de la Tesis titulada: **"Implementación de un Servicio Centralizado de Gestión de Identidades y Control de Acceso de usuarios en aplicaciones web para la Carrera de Ingeniería en Sistemas/Computación de la UNL: SmartLab"**, es fiel traducción del idioma español al idioma inglés, y cumple con las características propias del idioma extranjero.

Proyecto de Tesis que se encuentra bajo la dirección del **Ing. Pablo Fernando Ordoñez Ordoñez Mg. Sc.** De la autoría de los estudiantes: **Josue Andres Macas Caraguay**, con CI. **1104123425** y **Jorge Gustavo Tandazo Cueva**, con CI. **0705637965**, egresados de la de **Carrera de Sistemas/Computación**, de la **Facultad de la Energía, las Industrias y los Recursos Naturales No Renovables** de la **Universidad Nacional de Loja**.

Es en cuanto puedo certificar en honor de la verdad, facultando a los interesados hacer uso de la presente en lo que estime conveniente.

Fernando Joel Lara Carrera
0106975196
Máster Universitario en Enseñanza de Inglés como Lengua Extranjera