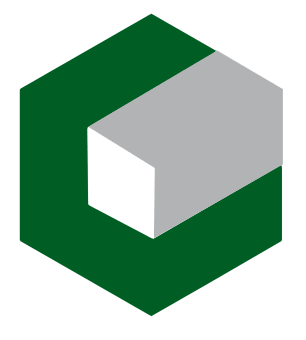
Universidad Tecnológica de La Habana “José Antonio Echeverría”

Facultad de Ingeniería Informática.



Aplicación web de código abierto para la gestión y autenticación de usuarios basada en Directorio Activo.

**Autor**: Carlos Daniel Vilaseca Illnait

**Tutores**: Dra. C. Raisa Socorro Llanes

Dra. C. Lisandra Bravo Ilisastigui

La Habana, Cuba

Julio,2024

Resumen

El documento presenta una solución propuesta para la gestión y autenticación de usuarios basada en Directorio Activo a través de LDAP. Se abordan temas como la historia detrás de esta propuesta, la selección del cliente LDAP que permita la comunicación con el directorio desde la aplicación, cómo se logra que la solución sea configurable y personalizable, las pruebas realizadas y los desafíos encontrados para lograr el despliegue de la solución.

**Palabras clave**: gestión de usuarios, código abierto, Directorio Activo, LDAP, personalización.

Abstract

The document presents a proposed solution for user management and authentication based on Active Directory through LDAP. It addresses topics such as the history behind this proposal, the selection of the LDAP client that allows communication with the directory from the application, how to make the solution configurable and customizable, the tests performed and the challenges encountered to achieve the deployment of the solution.

**Keywords**: user management, open source, Active Directory , LDAP, personalization.

Índice

[Introducción 1](#_Toc1)

[Capítulo 1 8](#_Toc2)

[Capítulo 2 10](#_Toc3)

[Capítulo 3 11](#_Toc4)

[Conclusiones 12](#_Toc5)

[Bibliografía 13](#_Toc6)

Índice de tablas

[Tabla 1 Comparación entre diversas herramientas para la gestión de directorios 1](#_Toc1)

# Introducción

En el mundo digital actual, la gestión de usuarios es un aspecto crucial para cualquier organización o negocio que opere en línea. Con el aumento del uso de plataformas en línea y servicios digitales, gestionar el acceso, los permisos y la seguridad de los usuarios se ha convertido en un desafío complejo y fundamental [1], [2], [3].

La gestión de usuarios implica la creación y mantenimiento de cuentas de usuario, la asignación de roles y permisos, y la garantía de que solo las personas autorizadas tengan acceso a la información y los sistemas adecuados. Esto es especialmente importante en entornos donde múltiples usuarios, con diferentes niveles de acceso, interactúan con sistemas sensibles o información confidencial. Una gestión de usuarios bien implementada puede mejorar la seguridad, proteger los datos y garantizar que los usuarios tengan una experiencia personalizada [1], [2], [3].

Los directorios activos son una solución robusta y ampliamente adoptada para la gestión de usuarios en diversidad de entornos. Proporcionan una forma centralizada y segura de gestionar las cuentas de usuario, los permisos y la autenticación. Al utilizar un directorio activo, las organizaciones pueden controlar y monitorear el acceso a sus recursos de red y aplicaciones, garantizando que solo los usuarios autorizados puedan acceder a la información confidencial [4], [5], [6].

Un directorio activo funciona como una base de datos central que almacena información sobre los usuarios, como nombres de usuario, contraseñas, direcciones de correo electrónico, roles y pertenencia a grupos. Esta base de datos se puede integrar con múltiples sistemas y aplicaciones, lo que proporciona un único punto de autenticación y gestión de acceso. Esto significa que los administradores de sistema pueden crear y administrar cuentas de usuario de forma eficiente, y los usuarios finales pueden acceder a los recursos que necesitan con un único conjunto de credenciales [4], [5], [6].

Una de las principales ventajas de los directorios activos es su capacidad para escalar y adaptarse a las necesidades de una organización en crecimiento. Pueden manejar fácilmente un gran número de usuarios y proporcionar una forma flexible de gestionar los cambios en los roles y permisos del personal. Los directorios activos también ofrecen una seguridad mejorada, con funciones de cifrado y la capacidad de aplicar políticas de contraseñas seguras.

Los directorios activos usan un protocolo de comunicación llamado Protocolo Ligero de Acceso a Directorios, conocido como LDAP (*Lightweight Directory Access Protocol*); un protocolo de red abierto y estándar para acceder y mantener información en un servicio de directorio. LDAP juega un papel crucial en la gestión de usuarios y la autenticación en muchos sistemas y aplicaciones [5], [7], [8], [9], [10], [11].

Para la gestión de Directorios, existen herramientas como *Remote Server Administration Tools* [14], Webmin [15], samba4-manager [12] y ADwebmanager [13], que usan LDAP para la conexión y gestión del directorio. Sin embargo estas pueden resultar insuficientes en términos de personalización y facilidad de despliegue a necesidades organizacionales o de la comunidad (Tabla 1).

Tabla 1 Comparación entre diversas herramientas para la gestión de directorios

|  |  |  |
| --- | --- | --- |
| **Herramienta** | **Capacidad de personalización (interfaz y apariencia)** | **Simplicidad de despliegue** |
| RSAT | Limitada, la personalización se limita a ajustes mínimos dentro del entorno de Windows | Compleja, requiere conocimientos técnicos específicos y sólo disponible para ciertas versiones de Windows |
| Webmin | Moderada, permite cierta personalización a través de temas y ajustes de interfaz, pero con limitaciones en la profundidad de las modificaciones | Relativamente fácil de instalar, pero la configuración inicial puede ser confusa y tiene una curva de aprendizaje |
| Sambabox | Limitada, centrada principalmente en la gestión de Samba, con poca atención a la personalización de la interfaz | Complicado, requiere conocimientos profundos de Samba y su configuración |
| samba4-manager | Limitada, diseñada específicamente para la gestión de Samba4, con opciones de personalización limitadas | Tedioso, especialmente en entornos grandes o complejos |
| ADwebmanager | Limitada, diseñada para funciones comunes de Directorio Activo, con mínimas opciones de personalización de interfaz | Sencillo para usuarios con experiencia en Directorio Activo, pero puede presentar desafíos para usuarios sin experiencia |

La gestión de Directorio Activo a menudo se encuentra con obstáculos en términos de personalización y simplicidad debido a su enfoque en satisfacer necesidades específicas, manejar complejidades técnicas, priorizar seguridad y estabilidad, enfrentar restricciones arquitectónicas, y evolucionar a partir de diseños que no consideraron la personalización y la facilidad de despliegue. A partir de esta **situación problemática** se formula el siguiente **problema**: ¿Cómo puede desarrollarse una herramienta de gestión para Directorio Activo que ofrezca una mayor personalización y facilidad de despliegue, sin sacrificar la seguridad, estabilidad y capacidad para manejar las complejidades técnicas inherentes?. Para solucionar el problema se tienen como objeto de estudio los directorios activos y la comunicación a través de LDAP; el campo de acción serían las herramientas de gestión de directorio activo.

Como hipótesis se plantea que desarrollar una aplicación web de código abierto, con archivos de configuración que permitan la personalización de la solución; con un proceso de despliegue documentado, es una mejora en comparación con soluciones de gestión de Directorio Activo ya existentes.

Para demostrar esta hipótesis se plantea como objetivo general crear una consola de administración de código abierto adaptable, y fácil de desplegar para la gestión de Directorio Activo, ofreciendo una solución práctica y flexible para diferentes contextos.

A partir de este objetivo general, se derivan los siguientes objetivos específicos y tareas:

1. Analizar los requisitos de la aplicación y la personalización del sistema:
   1. Documentar los requisitos funcionales y no funcionales que debe cumplir la aplicación.
   2. Analizar diferentes casos de uso para identificar las opciones de personalización.
   3. Documentar los requisitos de personalización, incluyendo la interfaz de usuario y ajustes de seguridad.
2. Seleccionar tecnologías adecuadas:
   1. Evaluar diferentes clientes LDAP disponibles en el mercado, considerando factores como compatibilidad, rendimiento y facilidad de integración.
   2. Elegir el cliente LDAP que mejor se alinee con los requisitos funcionales y no funcionales previamente definidos.
3. Implementar la arquitectura y funciones básicas de la aplicación:
   1. Establecer la arquitectura base del proyecto y configurar el ambiente de desarrollo necesario.
   2. Configurar el cliente LDAP seleccionado y las herramientas asociadas para iniciar el desarrollo.
   3. Desarrollar mecanismos de autenticación que interactúen con el Directorio Activo utilizando el cliente LDAP seleccionado.
   4. Implementar funcionalidades críticas para la gestión de usuarios y grupos utilizando el cliente LDAP, incluyendo operaciones de lectura, eliminación y actualización.
   5. Realizar pruebas unitarias y funcionales para garantizar la confiabilidad y corrección de estas funciones básicas.
4. Realizar pruebas para asegurar el correcto funcionamiento del sistema:
   1. Diseñar y ejecutar pruebas de integración que verifiquen el correcto funcionamiento del sistema en su conjunto, desde la autenticación hasta la gestión de recursos.
   2. Documentar los resultados de las pruebas y realizar los ajustes necesarios basados en los hallazgos.
   3. Extender el conjunto de pruebas de integración para abarcar nuevas funcionalidades y garantizar la estabilidad y compatibilidad del sistema ante cambios y actualizaciones futuras.

El alcance de las prácticas profesionales 2 es del objetivo 1 al 4; de cara a la tesis se proponen los siguientes objetivos y tareas:

1. Simplificar y documentar el proceso de despliegue:
   1. Identificar y documentar estrategias y herramientas que simplifiquen el proceso de instalación y configuración inicial de la aplicación.
   2. Utilizar contenedores Docker para simplificar el proceso de puesta en marcha de la aplicación.
   3. Elaborar documentación detallada del proceso de despliegue.
2. Desplegar documentación:
   1. Crear y estructurar la documentación técnica que incluya la descripción del sistema, la arquitectura, y las guías de desarrollo.
   2. Documentar referencias de API y/o archivos de configuracion que sean claras y accesibles.
   3. Publicar la documentación en un sitio web accesible.
3. Desplegar demo:
   1. Configurar el servidor donde se va a desplegar.
   2. Configurar Docker para simplificar el despliegue.
   3. Configurar CI/CD para despliegues automáticos.
   4. Ejecutar el primer despliegue exitoso.

Como valor práctico con la realización de este trabajo se espera un diseño de software de una herramienta para la gestión de directorio activo que sea personalizable y fácil de desplegar.

La estructura del informe se organiza de la siguiente manera:

Capítulo 1 Fundamentación teórica. En este capítulo se presenta una explicación teórica sobre los conceptos y tecnologías fundamentales para la gestión de usuarios y Directorio Activo. Se analizarán en profundidad temas como la importancia de la gestión de usuarios en entornos digitales, los principios de seguridad y autenticación, y el funcionamiento de los directorios activos y LDAP. También se abordarán las diferentes herramientas existentes para la gestión de Directorio Activo, sus ventajas y limitaciones, y se establecerá el marco teórico que sustenta la propuesta de solución planteada en este trabajo.

Capítulo 2 Descripción de la propuesta de solución. Este capítulo aporta una explicación detallada sobre la propuesta de solución a los problemas identificados en la gestión de Directorio Activo. Se describirá la arquitectura de la aplicación web de código abierto propuesta, sus funcionalidades principales, y cómo se abordarán los requisitos de personalización y simplicidad de despliegue. Además, se explicarán las decisiones de diseño y las tecnologías seleccionadas para el desarrollo de la herramienta, así como los beneficios esperados en términos de seguridad, estabilidad y facilidad de uso.

Capítulo 3 Validación de la propuesta de solución. Este capítulo está dedicado a la validación de la propuesta de solución mediante la realización de pruebas exhaustivas. Se diseñarán y ejecutarán pruebas de integración para verificar el correcto funcionamiento del sistema en su conjunto, desde la autenticación hasta la gestión de recursos. Los resultados de estas pruebas se documentarán y se realizarán los ajustes necesarios basados en los hallazgos.

# Capítulo 1: Fundamentación teórica

El propósito de este capítulo es proporcionar una base sólida sobre los conceptos y tecnologías fundamentales para la gestión de usuarios y Directorio Activo, que sustentan la propuesta de solución planteada. Se explorará la importancia de una gestión eficaz de usuarios en entornos digitales, abordando los principios clave de seguridad y autenticación que son esenciales para proteger la integridad y confidencialidad de los datos. Asimismo, se detallarán los conceptos de Directorio Activo y LDAP, explicando su funcionamiento y relevancia en la administración de identidades y accesos. Además, se realizará un análisis exhaustivo de las herramientas existentes para la gestión de Directorio Activo, evaluando sus ventajas y limitaciones, con el objetivo de establecer un marco teórico robusto que guíe el desarrollo de una solución personalizable y fácil de desplegar.

## 1.1 Introducción a la Gestión de Usuarios y Directorio Activo

* Importancia de la gestión de usuarios en entornos digitales.
* Principios de seguridad y autenticación en sistemas informáticos.
* Conceptos básicos de Directorio Activo y LDAP.

## 1.2 Tecnologías y Herramientas Existentes

* Herramientas actuales para la gestión de Directorio Activo.
* Ventajas y limitaciones de las soluciones existentes.
* Marco teórico que sustenta la propuesta de solución planteada.

## 1.3 Requisitos de la Aplicación y Personalización del Sistema

* Documentación de requisitos funcionales y no funcionales.
* Análisis de diferentes casos de uso para identificar opciones de personalización.
* Requisitos de personalización incluyendo interfaz de usuario y ajustes de seguridad.

# Capítulo 2: Solución propuesta

## 2.1 Arquitectura de la Aplicación Web de Código Abierto

* Descripción de la arquitectura base del proyecto.
* Configuración del ambiente de desarrollo necesario.
* Selección de tecnologías y herramientas para el desarrollo.

## 2.2 Implementación de Funciones Básicas

* Configuración del cliente LDAP seleccionado.
* Desarrollo de mecanismos de autenticación que interactúen con el Directorio Activo.
* Implementación de funcionalidades críticas para la gestión de usuarios y grupos.

# Capítulo 3: Validación de la solución

## 3.1 Pruebas de Integración

* Diseño y ejecución de pruebas de integración que verifiquen el funcionamiento del sistema desde la autenticación hasta la gestión de recursos.
* Documentación de resultados de las pruebas y ajustes necesarios basados en los hallazgos.

# Conclusiones

# Bibliografía

[1]M. A. Thakur and R. Gaikwad, “User identity and Access Management trends in IT infrastructure- an overview,” in 2015 International Conference on Pervasive Computing (ICPC), Pune, India: IEEE, 2015, pp. 1–4. doi: 10.1109/PERVASIVE.2015.7086972.  
   
   
 [2]A. Josang et al., “Local user-centric identity management,” J Trust Manag, vol. 2, no. 1, p. 1, 2015, doi: 10.1186/s40493-014-0009-6.  
   
   
 [3]J. M. Kizza, “Access Control and Authorization,” in Guide to Computer Network Security, Cham: Springer International Publishing, 2024, pp. 195–214. doi: 10.1007/978-3-031-47549-8\_9.  
   
   
 [4]G. Carter, LDAP System Administration. O’Reilly Media, Inc., 2003.  
   
   
 [5]R. Harrison, “Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms.” IETF, Jun. 2006. Accessed: May 15, 2024. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc4513  
   
   
 [6]M. A. Thakur and R. Gaikwad, “User identity and lifecycle management using LDAP directory server on distributed network,” in 2015 International Conference on Pervasive Computing (ICPC), Pune, India: IEEE, 2015, pp. 1–3. doi: 10.1109/PERVASIVE.2015.7086970.  
   
   
 [7]J. Sermersheim, “Lightweight Directory Access Protocol (LDAP): The Protocol,” www.rfc-editor.org, Jun. 2006, doi: 10.17487/RFC4511.  
   
   
 [8]A. Bartlett, “Samba 4 -Active Directory.” 2005. [Online]. Available: https://www.samba.org/samba/news/articles/abartlet\_thesis.pdf  
   
   
 [9]R. E. Voglmaier, The ABCs of LDAP. CRC Press, 2003.  
   
   
 [10]RedHat, “What is LDAP authentication?” RedHat, Jun. 03, 2022. [Online]. Available: https://www.redhat.com/en/topics/security/what-is-ldap-authentication  
   
   
 [11]R. Janice, “LDAP authentication with Microsoft Entra ID - Microsoft Entra.” Accessed: Jun. 28, 2024. [Online]. Available: https://learn.microsoft.com/en-us/entra/architecture/auth-ldap  
   
   
 [12]S. Graber, stgraber/samba4-manager. 2024. Accessed: Jun. 28, 2024. [Online]. Available: https://github.com/stgraber/samba4-manager  
   
   
 [13]V. S. G. Jerez, VicentGJ/AD-webmanager. 2024. Accessed: Jun. 28, 2024. [Online]. Available: https://github.com/VicentGJ/AD-webmanager  
   
   
 [14]D. Han, “Remote Server Administration Tools - Windows Server.” Microsoft, May 03, 2024. Accessed: Jun. 10, 2024. [Online]. Available: https://learn.microsoft.com/en-us/troubleshoot/windows-server/system-management-components/remote-server-administration-tools  
   
   
 [15]M. Karzyński, Webmin Administrator’s Cookbook. Packt Publishing Ltd, 2014.