KnE Engineering

SIIPRIN-CITEGC
Ibero-American Symposium on Computer Programming jointly held with the International Congress on Technology Education and Knowledge Management
Volume 2018

Knowledge E
Engaging minds

Conference Paper

Systematic Literature Review on the LDAP Protocol As a Centralized Mechanism for the Authentication of Users in Multiple Systems

Revisión Sistemática de Literatura sobre el protocolo LDAP como mecanismo centralizado para la autentificación de usuarios en múltiples sistemas

Mario Cueva-Hurtado, Roberth Figueroa-Diaz, Wilmer Aguilar-Soto, and Manuel Armijos-Ordoñez

Universidad Nacional de Loja, Carrera de Ingeniería en Sistemas, Av. Pío Jaramillo Alvarado, La Argelia, Loja, Ecuador

Corresponding Author:
Mario Cueva-Hurtado
mecueva@unl.edu.ec

Received: 4 December 2018
Accepted: 5 December 2018
Published: 27 December 2018

Publishing services provided by Knowledge E

Selection and Peer-review under the responsibility of the SIIPRIN-CITEGC Conference Committee.

Abstract

The protocol LDAP (Lightweight Directory Access Protocol) allows centralized identity authentication, where the information of the directory is faster and easier to read. This article carries out a systematic literature review (SLR) according to what is proposed in the article by Bárbara Kitchenham [1], aimed to identify different methods for users' authentication in multiple systems using LDAP protocol, an analysis of criteria is carried out about different studies published in five digital libraries (Scopus, IEEEXplorer, Scientific.net, Google Scholar, DBLP), and two academic magazines (Revista Energía of UNL, Revista Científica of UTB), making relevant conclusions of the use of four mechanisms for the authentication of users of multiple systems such as: Languaje PHP, SSO (Single sign-on), IAM (Identity and Access Management), and T-RBAC (Access control based on roles and tasks), predominantly the use of the PHP language for its administrative tools for managing LDAP servers.

Resumen

El protocolo LDAP (Protocolo Ligero de Acceso a Directorios), permite la autentificación de identidad centralizada, donde la información del directorio es más rápida y fácil de leer. El presente artículo realiza una revisión sistemática de literatura (SLR) de acuerdo a lo propuesto en el artículo de Bárbara kitchenham [1], con el fin de identificar los diferentes métodos para la autentificación de usuarios en múltiples sistemas usando el protocolo LDAP, se realiza un análisis de criterios de diferentes estudios publicados en 5 bibliotecas digitales (Scopus, IEEEXplorer, Scientific.net, Google Scholar, DBLP), y 2 revistas académicas (Revista Energía de la UNL, Revista científica de la UTB), realizando conclusiones relevantes del uso de cuatro mecanismos para la autentificación de usuarios de múltiples sistemas como son: lenguaje PHP, SSO (Sistema de autentificación única), IAM (Sistema de gestión de identidades) y T-RBAC

OPEN ACCESS

(Control de acceso basado en tareas y roles); predominando el uso del lenguaje PHP por sus herramientas administrativas para la administración de servidores LDAP.

Keywords: LDAP, authentication, user management, systematic literature review, security

Palabras clave: LDAP, autentificación, gestión de usuarios, revisión sistemática de literatura, seguridad

1. Introduction

En los últimos años el uso y servicios de las tecnologías de la información y comunicación (TIC), han evolucionada constantemente, dichos servicios tienen su impacto directamente en la seguridad de la información, acceso a los recursos y datos personales.

En la actualidad cuando un usuario desea ingresar a una aplicación, sistema o información relevante, este debe autentificarse para poder verificar su identidad, generalmente ingresando un ID de usuario y una contraseña, mediante el cual se puede autorizar o denegar el permiso, pero el problema principal radica en que si un usuario utiliza o maneja varios sistemas o aplicaciones este deberá utilizar o manejar muchos ID de usuario y contraseñas, lo cual es bastante incómodo para los mismos.

LDAP (Protocolo Ligero de Acceso a Directorios), permite el acceso a un servicio de directorio ordenado y distribuido especialmente basado en el estándar X.500 para compartir directorios [2], LDAP se ejecuta sobre TCP/IP u otros servicios de transferencia orientados a conexión, utiliza un modelo de cliente - servidor. LDAP maneja su estructura de forma jerárquica, la forma de representar su directorio se llama DIT (Árbol de Información del Directorio) como lo indica [2] y se amplia en [3].

En la actualidad se usa LDAPv3 que se desarrolló a finales de la década de 1990 para reemplazar a LDAPv2. LDAPv3 agrega las siguientes características como se indica en [2]:

- Fuertes servicios de autenticación y seguridad de datos a través de SASL (Capa de Seguridad y Autenticación Simple)
- Certificación de autenticación y servicios de seguridad de datos a través de TLS (Seguridad de la Capa de Transporte)

- Internacionalización mediante el uso de Unicode
- Referencias y continuaciones
- Descubrimiento de esquema
- Extensibilidad (controles, operaciones extendidas entre otros).

En este sentido en [2, 3] se amplia el protocolo LDAP como mecanismo centralizado, permitiendo la integración de diferentes sistemas con una autentificación única y brindando la proteccion a los datos confidenciales mediante protocolos de comunicación segura como: SASL (Capa de autenticación y seguridad), TLS (Seguridad de la capa de transporte) y SSL (Capa de conexión segura).

El propósito de este artículo muestra el resultado de una revisión sistemática de literatura, donde enfatiza principalmente la forma en que LDAP se integra a múltiples sistemas o aplicaciones, sin dejar de lado la seguridad que conlleva el proceso. Las siguientes secciones están organizadas de la siguiente manera: En la sección 2 se describe la metodología a seguir, en la sección 3 se presentan los resultados de la revisión sistemática de literatura, en la sección 4 se presenta la discusión e interpretación de los resultados y en la sección 5 se presentan las conclusiones que responden a nuestras preguntas de investigación.

2. Metodología

En el presente artículo se aplica la metodología propuesta por Bárbara Kitchenham [1], la cual parte del estudio de las pruebas disponibles sobre una determinada intervención, con el objeto de responder a cuestiones concretas, siguiendo una metodología explícita y rigurosa, descrita en la Tabla 1, donde se puede visualizar el esquema a seguir.

3. Resultados

3.1. Planificación de la Revisión Sistemática de Literatura

En esta etapa se identifica cuáles son las necesidades de la revisión, para lo cual es necesario plantear y responder algunos puntos claves descritos a continuación.

1. Objetivo de la Revisión Sistemática de Literatura

Tabla 1: Proceso de Revisión Sistemática de Literatura.

Fase	Paso
A. Planificación de la Revisión Sistemática de Literatura	1. Objetivo de la Revisión Sistemática de Literatura
	2. Formulación de la pregunta de investigación
	3. Palabras Claves
	4. Selección de fuentes y estrategias de búsqueda
	5. Cadena de búsqueda
	6. Criterios de inclusión
	7. Criterios de exclusion
B. Ejecución de la Revisión Sistemática de literatura	1.Criterios de selección de estudios
	2. Extracción de la información
C. Análisis de resultados y hallazgos	1. Hallazgos

El objetivo es poder identificar y seleccionar los artículos científicos que tengan relevancia sobre el protocolo LDAP y la autentificación de usuarios, que otorguen información fundamental al artículo de revisión.

2. Formulación de la pregunta de investigación

   A partir de tema de investigación "Protocolo LDAP como mecanismo centralizado para la autentificación de usuarios en múltiples sistemas", se plantea las siguientes preguntas de investigación referente al tema antes mencionado, descrita en la Tabla 2, donde P1 es la primera pregunta y P2 la segunda pregunta.

Tabla 2: Preguntas de investigación.

Preguntas
P1. ¿Por qué se utiliza el protocolo LDAP como mecanismo centralizado para la autentificación de usuarios en múltiples sistemas?
P2. ¿La autentificación con el protocolo LDAP, mejoró la seguridad y administración de usuarios?

3. Palabras claves

   Se identifican las palabras claves de los artículos científicos propuestos por el grupo de investigadores, las cuales servirán para poder plantear la cadena de búsqueda, descritos en la Tabla 3, que enumera los 10 artículos seleccionados.

4. Selección de fuentes y estrategias de búsqueda

   Se seleccionó un conjunto de bases de datos científicas y revistas académicas, en donde se procedió a buscar los artículos científicos descritos en la Tabla 4, visualizando el nombre y URL de cada una.

Tabla 3: Artículos Preliminares y Palabras Claves.

No.	Artículo	Palabras claves
A1	Profile Management and Authentication using LDAP. [4]	LDAP, client, server, SLADP, schemas, database, ACLs, authentication, LDIF, Web Server, VPN, RAS, SendMail.
A2	Inventions on LDAP-A study based on US Patents. [5]	LDAP, Directory Protocol, Inventions, Software Inventions, LDAP inventions, Software Patents.
A3	User Management with LDAP (Lightweight Directory Access Protocol) for access to technology and Information Services in Companies. [6]	LDAP, user management, integration, synchronization services.
A4	User identity & lifecycle management using LDAP directory server on distributed network. [7]	LDAP, authentication, security, policies, servers, internet, identity management systems, user access
A5	Intelligent agents applied to the management of LDAP user profiles. [8]	LDAP, interface, intelligent agents, Smart.
A6	Vulnerabilities of LDAP as an Authentication Service. [9]	LDAP, Authentication service, Denial.of-service, SYN Flooding.
A7	External authentication approach for virtual private network using LDAP. [10]	Authentication, LDAP, servers, protocolos, access protocol, external authentication, internet protocol security.
A8	Improve data security in cloud environment by using LDAP and two way encryption algorithm. [11]	Cloud computing, Encryption, Servers, Authentication, IP networks, Algorithm desing and analysis, LDAD, authorisation, security.
A9	Authentication using LDAP in Wireless Body Area Network. [12]	Authentication, security, Wireless Body Area Network, Attack.
A10	OCL Fault Injection-Based Detection of LDAP Query Injection Vulnerabilities.[13]	LDAP, Servers, authentication, detection, privilege, security.

Tabla 4: Fuentes de motores de búsqueda científica y revistas académicas.

Fuentes	URL
Scopus	https://www.scopus.com/
IEEEXPlore	http://ieeexplore.ieee.org/
Scientific.net	https://www.scientific.net
Scholar Google	http://scholar.google.es/
DBLP	http://dblp.uni-trier.de/
Revista Energía de la UNL	http://revistas.unl.edu.ec
Revista Científica de la UTB	http://revistas.utb.edu.ec

5. Cadena de Búsqueda

Para generar la cadena de búsqueda se utilizó los conectores lógicos “AND” y “OR”, descrita en la Tabla 5, donde se puede visualizar la cadena resultante.

Tabla 5: Cadena de búsqueda.

Cadena
((“LDAP”) AND (“Authentication”) AND (“User management OR User”) AND (“Security OR internet protocol security”)).

6. Criterios de Inclusión

   Se realizó un estudio de los artículos más relevantes, excluyendo a los demás, se tomó en cuenta los descritos en la Tabla 6, donde se puede visualizar los criterios de inclusión.

Tabla 6: Criterios de Inclusión.

Criterio	Valor
Idioma	Inglés, español.
Motores de búsqueda	Scopus, IEEEXplorer, Scientific.net, Google Scholar, DBLP, Revistas académicas.
Fecha de publicación	2013 – 2018.
Tipo de producciones	Artículos científicos.

7. Criterios de Exclusión

   Los estudios que no han sido relevantes se los descarta tomando en consideración el siguiente criterio: Título, abstract (resumen), texto completo del documento, palabras claves, resultados y conclusiones.

3.2. Ejecución de la Revisión Sistemática de literatura

A continuación, se describe los criterios de selección de los estudios más importantes, extracción de la información y las cadenas de búsqueda aplicadas en las fuentes científicas.

3.2.1. Ejecución en la base de datos Scopus

((“LDAP”) AND (“Authentication”) AND (“Security”)).

La ejecución de la cadena de búsqueda en Scopus arrojó 5459 resultados. Luego al aplicar el criterio de inclusión se obtuvo 18 documentos relevantes, de los cuales, aplicando el criterio de exclusión se consideran los descritos en la Tabla 7, que muestra los estudios primarios y sus referencias bibliográficas.

Tabla 7: Estudios primarios de Scopus.

#	art. cit.	Título y Publicación
1	[7]	User identity & lifecycle management using LDAP directory server on distributed network. 2015 International Conference on Pervasive Computing: Advance Communication Technology and Application for Society, ICPC 2015.
2	[10]	External Authentication Approach for Virtual Private Network using LDAP. 2014 First International Conference on Networks & Soft Computing (ICNSC2014).

3.2.2. Ejecución en la base de datos IeeeXplorer

(("LDAP") AND ("Authentication") AND ("Security")).

La ejecución de la cadena de búsqueda en IEEEXplorer arrojó 36 resultados. Luego al aplicar el criterio de inclusión se obtuvo 14 documentos relevantes, de los cuales, aplicando el criterio de exclusión se consideran los descritos en la Tabla 8, que muestra los estudios primarios y sus referencias bibliograficas.

Tabla 8: Estudios primarios de la IEEEXplorer.

#	art. cit.	Título y Publicación
3	[11]	Improve data security in cloud environment by using LDAP and two way encryption algorithm. 2016 Symposium on Colossal Data Analysis and Networking (CDAN).
4	[14]	Research on data and workflow security of electronic military systems. Proceedings of the 2013 International Conference on Intelligent Control and Information Processing, ICICIP 2013.
5	[15]	Study and design of enterprise public security platform based on PKI. Proceedings - 13th International Symposium on Distributed Computing and Applications to Business, Engineering and Science, DCABES 2014.
6	[16]	Classification of Lightweight Directory Access Protocol Query Injection Attacks and Mitigation Techniques. 978-1-4673-7648-8/15/$31.00 ©2015 IEEE
7	[17]	Linux PAM to LDAP Authentication Migration. 2017 International Conference on Soft Computing, Intelligent System and Information Technology (ICSIIT).

3.2.3. Ejecución de la selección de fuentes en Scientific.net

((LDAP) AND (Authentication)).

La ejecución de la cadena de búsqueda en Scientific.net arrojó 44 resultados. Luego al aplicar el criterio de inclusión se obtubo 25 documentos relevantes, de los cuales, aplicando el criterio de exclusión se consideran los descritos en la Tabla 9, que muestra los estudios primarios y sus referencias bibliograficas.

Tabla 9: Estudios primarios de Scientific.net.

#	art. cit.	Título y Publicación
8	[18]	Research of Unified Authentication System Based on LDAP. Published by Atlantis Press, Paris, France.
9	[19]	Design and Implementation of unified Identity Authentication System Based on LDAP in Digital Campus. Advanced Materials Research

3.2.4. Ejecución en el motor de búsqueda científico Google Scholar

Para realizar la consulta en esta fuente, seleccionamos la búsqueda por título introduciendo palaras claves como (Autentificación con LDAP), el cuál dio como resultado 2.800 documentos, aplicando el criterio de inclusión se obtubo 1.290 documentos relevantes y aplicando el criterio de exclusión y página de referencia se considera el descrito en la Tabla 10, que muestra el estudio primario y su referencia bibliografica.

Tabla 10: Estudios primarios de Google Scholar.

#	art. cit.	Título y Publicación
10	[20]	Sistem Autentikasi Hotspot Menggunakan LDAP dan Radius pada Jaringan Internet Wireless Prodi Teknik Sistem Komputer. Jurnal Teknologi dan Sistem Komputer

3.2.5. Ejecución en la base de datos DBLP

(LDAP).

La ejecución de la cadena de búsqueda en DPLB arrojó 163 resultados. Luego al aplicar el criterio de inclusión se obtuvo 8 documentos relevantes, de los cuales, aplicando el criterio de exclusión se considera el descrito en la Tabla 11, que muestra el estudio primario y su referencia bibliografica.

Tabla 11: Estudios primarios de DBLP.

#	art. cit.	Título y Publicación
11	[21]	Selective LDAP Multi-Master Replication. Proceedings Open Identity Summit 2013. Open Identity Summit (OID-2013), September 9-11, Kloster Banz, Germany.

3.2.6. Ejecución en las revistas académicas de la UNL y UTB.

La ejecución de la cadena de búsqueda en las revistas académicas, aplicando el criterio de inclusión y exclusión arrojó 3 resultados relevantes descritos en la Tabla 12, que muestra los estudios primarios y sus referencias bibliograficas.

Tabla 12: Estudios primarios de Revista Energía de la UNL y Revista Científica de la UTB.

#	art. cit.	Título y Publicación
12	[8]	Intelligent agents applied to the management of ldap user profiles. Revista Energía ISSN: 1390-9037.
13	[22]	Implemetation of Eduroam as Wireless Infraestructure on the Campus of National University of Loja. Revista Energía ISSN: 1390-9037.
14	[6]	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 Investigación, E-Issn: 2528-8083, Vol. 1, Citt, Pp. 10-15.

1. Criterios de selección de estudios

   Para el cumplimiento del objetivo principal, los resultados de búsqueda deben cumplir el siguiente criterio de selección: Los artículos deben destacar la importancia y beneficios del uso del protocolo LDAP para la autenticación de usuarios.

2. Extracción de la información

   Los criterios dados de inclusión, exclusión y de selección, permitieron identificar los diferentes artículos con el fin de cumplir el objetivo planteado en esta investigación. Para la extracción importante de cada estudio se utilizó los siguientes elementos:

   - Características claves de la autentificación de LDAP
   - Mecanismos de interrelación con diferentes sistemas.

3.3. Análisis de resultados y hallazgos

Se realizó un análisis previo donde se evalúa cada estudio, discriminando artículos que tienen criterios comunes e información no trascendental, estos fueron descartados quedándose con los artículos más relevantes.

Se enlistan 14 artículos con las etiquetas A1 a A14, que son los estudios seleccionados de acuerdo a los criterios indicados, presentados en la Tabla 13.

Tabla 13: Estudios seleccionados de la Revisión Sistemática de Literatura.

A1. User identity & lifecycle management using LDAP directory server on distributed network. [7]	
Características claves del uso del protocolo LDAP	Almacena y gestiona datos de roles asignados como: identidades de usuario, contraseñas y políticas.
Mecanismos de interrelación con otros sistemas.	Utiliza un sistema de gestión de identidades (IAM), el cual determina quién puede ingresar a sus sistemas protegidos, a qué nivel puede acceder el usuario y también asegurará que los usuarios accedan sólo a lo que necesitan para sus tareas comerciales mediante un protocolo DAML (Lenguaje de marcado de acceso al directorio), para transferir datos entre el servidor de Identity Manager y los servicios de LDAP.
A2. External Authentication Approach for Virtual Private Network using LDAP. [10]	
Características claves del uso del protocolo LDAP	-Inicio de sesión con credenciales de administrador. -Almacena y gestiona datos de roles asignados como identidades de usuario, contraseñas y políticas. -Para la autenticación utiliza los protocolos: SSL (Capa de sockets seguros) y TLS (Seguridad de la capa de transporte). -Autenticación externa mediante VPN.
Mecanismos de interrelación con otros sistemas.	Se implementa una Red privada virtual (VPN), utilizando el protocolo de tunelización punto a punto (PPTP) para mejorar la seguridad de las credenciales del administrador, enviando una solicitud al servidor LDAP para una correcta conexión a los sistemas.
A3. Improve data security in cloud environment by using LDAP and two way encryption algorithm. [11]	
Características claves del uso del protocolo LDAP	-Almacena y gestiona datos de roles asignados como: identidades de usuario, contraseñas y políticas. -Protocolos de Autenticación. -Multiplataforma (puede ejecutarse en varios sistemas operativos).
Mecanismos de interrelación con otros sistemas.	Se implementan 2 métodos descritos a continuación: El primer método lo realiza mediante un enlace simple y TLS (Seguridad de la capa de transporte), para evitar la divulgación de contraseñas en la red. El segundo método lo realiza mediante la autenticación simple y capa de seguridad SASL (Capa de seguridad y autenticación simple), que junto con los certificados del lado del cliente y TLS (Seguridad de la capa de transporte) proporcionan la protección más completa.
A4. Research on data and workflow security of electronic military systems. [14]	
Características claves del uso del protocolo LDAP	-Protocolos de Autenticación -Almacena y gestiona datos de roles asignados como: identidades de usuario, contraseñas y políticas.
Mecanismos de interrelación con otros sistemas.	Para conectarse al servidor LDAP se implementa un mecanismo de control de acceso T-RBAC (control de acceso basado en tareas y roles), y un componente de autenticación independiente basado en PKI (Infraestructura de clave pública), obteniendo así una conexión segura. T-RBAC es el mecanismo encargado de las funciones de envío, edición y composición de roles y tareas, garantizando un acceso correcto en la conexión con el LDAP y la seguridad del mismo.
A5. Study and design of enterprise public security platform based on PKI. [15]	

Características claves del uso del protocolo LDAP	-Almacena y gestiona datos de roles asignados como: identidades de usuario, contraseñas y políticas. -Eficiencia de consulta -Marco de despliegue distribuido -Control de acceso flexible y preciso.
Mecanismos de interrelación con otros sistemas.	Para la conexión de las aplicaciones móviles con el servidor LDAP, utiliza KMC SERVER Y CA SERVER que permiten la autenticación segura de las apps, las cuales son compatibles con el certificado digital X.509 de tecnología PKI (Infraestructura de Clave Pública) y el certificado digital X.509 de WPKI (Infraestructura de clave pública inalámbrica).
A6. Classification of Lightweight Directory Access Protocol Query Injection Attacks and Mitigation Techniques. [16]	
Características claves del uso del protocolo LDAP	-LDAP se puede usar para agregar, modificar y borrar información junto con operaciones de búsqueda. -Almacena y gestiona datos de roles asignados como: identidades de usuario, contraseñas y políticas. -Restringir el acceso mediante el uso de IP
A7. Linux PAM to LDAP Authentication Migration. [17]	
Características claves del uso del protocolo LDAP	-Almacena y gestiona datos de roles asignados como: identidades de usuario, contraseñas y políticas. -Para la encriptación de mensajes se utiliza los protocolos: SSL (Capa de sockets seguros) y TLS (Seguridad de la capa de transporte). -Multiplataforma (Puede ejecutarse en varios sistemas operativos). -LDIF (Formato de intercambio de datos en LDAPv3). -LDAP acepta métodos de almacenamiento de contraseñas y transformación de claves con valores hash MD5 que son: SMD5, - Crypt, SHA y SSHA este es el más seguro. -Sistema de base de datos backend -OID Identificador único de objeto para asignar los atributos. -LDAP utiliza AC que es la configuración de permiso para cuenta existente. -Apache Bench herramienta para determinar el tiempo de respuesta del servidor LDAP.
Mecanismos de interrelación con otros sistemas.	-LDAP cuenta con una biblioteca adicional para PHP el cual tiene un módulo de conexión a las aplicaciones creadas en PHP estás pueden acceder a la información de los usuarios que se encuentran en el servidor LDAP, para las nuevas contraseñas utiliza una función de PHP que incorpora un generador SHA1 (Algoritmo de Hash Seguro 1). -Para la migración de contraseñas de un servidor a otro se utiliza la herramienta Migrationtools que permite trabajar con LDAP.
A8. Research of Unified Authentication System Based on LDAP. [23]	
Características claves del uso del protocolo LDAP	-Almacena y gestiona datos de roles asignados como: identidades de usuario, contraseñas y políticas. -Directorio centralizado -Protocolos de autenticación. -Directorio Base de la Información (DIB) ofrece acceso a directorios estándar para todo tipo de aplicaciones basada en LDAP. -LDIF (Formato de intercambio de datos)

Mecanismos de interrelación con otros sistemas.	-Se puede acceder a las diferentes aplicaciones con SSO (Sistema de autenticación única). -Para importar y exportar la información de los usuarios, utiliza ICE Novel que es un kit de herramientas para la importación y exportación de datos de código abierto (como el Navegador JXplore de interfaz gráfica), que se incorporan con LDAP. -Utiliza un IDM (Novell Identity Management) que es una guía de identidad sincronizada con la base de datos, directorio y aplicación estándar.
A9. Design and Implementation of unified Identity Authentication System Based on LDAP in Digital Campus. [24]	
Características claves del uso del protocolo LDAP	-Estándar de información unificada -Plataforma de aplicaciones unificada -LDAP trabaja con 4 modelos básicos: modelo de información (representa la información), modelo de organización de datos, modelo de acceso-operación de datos y modelo de seguridad. -Bloquear y desbloquear cuentas de usuario. -Bloqueo y desbloqueo de tiempo. -Restablecer contraseñas. -Creación y eliminación de grupos de usuarios. -Estándar x.500 -LDAPv3
Mecanismos de interrelación con otros sistemas.	-Se utiliza ApacheDS (Servidor de Directorios) para conectarse con el servidor LDAP y se puede acceder a las diferentes aplicaciones con SSO (Sistema de autenticación única). -LDAP simplifica operaciones utilizando el patrón Spring's JdbcTemplat para la gestión de operaciones y base de datos al conectar los sistemas con LDAP, este patrón utiliza el Interprete de Ordenes Seguro SSH2 (Struts2 + Spring + Hibernate) que es una estructura de 3 niveles y sirve para una conexión segura.
A10. Sistem Autentikasi Hotspot Menggunakan LDAP dan Radius pada Jaringan Internet Wireless Prodi Teknik Sistem Komputer. [20]	
Características claves del uso del protocolo LDAP	-Almacena y gestiona datos de roles asignados como: identidades de usuario, contraseñas y políticas. - Interfaz phpLdapadmin. - Protocolo de autenticación. - Directorio centralizado
Mecanismos de interrelación con otros sistemas.	Para la conexión de diversas computadoras mediante la red inalámbrica Wireless se utiliza FreeRADIUS este incluye un servidor RADIUS, cuenta con un archivo de configuración llamado users donde se agregan los usuarios para acceso a la red wireless con el servidor LDAP.
A11. Selective LDAP Multi-Master Replication. [21]	
Características claves del uso del protocolo LDAP	-Coherencia de datos duplicados -Almacena y gestiona datos de roles asignados como: identidades de usuario, contraseñas y políticas.
A12. Intelligent agents applied to the management of ldap user profiles. [8]	
Características claves del uso del protocolo LDAP	-LDAPv3 -Multiplataforma (Puede ejecutarse en varios sistemas operativos). -Almacena y gestiona datos de roles asignados como: identidades de usuario, contraseñas y políticas. -Protocolos de autenticación.
Mecanismos de interrelación con otros sistemas.	LDAP cuenta con una biblioteca adicional para PHP el cual tiene un módulo de conexión a las aplicaciones creadas en PHP estás pueden acceder a la información de los usuarios que se encuentran en el servidor LDAP.

A13. Implemetation of Eduroam as Wireless Infraestructure on the Campus of National University of Loja. [22]	
Características claves del uso del protocolo LDAP	-Para la autenticación se utiliza los protocolos: SSL (Capa de sockets seguros) y TLS (Seguridad de la capa de transporte). -Almacena y gestiona datos de roles asignados como: identidades de usuario, contraseñas y políticas. -Multiplataforma (Puede ejecutarse en varios sistemas operativos).
Mecanismos de interrelación con otros sistemas.	Para la conexión de diversas computadoras mediante la red inalámbrica Wireless se utiliza FreeRADIUS este incluye un servidor RADIUS, cuenta con un archivo de configuración llamado users donde se agregan los usuarios para acceso a la red wireless con el servidor LDAP.
A14. User Management with LDAP (Lightweight Directory Access Protocol) for access to technology and Information Services in Companies. [6]	
Características claves del uso del protocolo LDAP	-Almacena y gestiona datos de roles asignados como: identidades de usuario, contraseñas y políticas. -Proporciona seguridad que impide el acceso no autorizado mediante protocolos de comunicación segura como: SSL (Capa de sockets seguros) y TLS (Seguridad de la capa de transporte). -Permite realizar replicas permitiendo tener varios servidores LDAP que almacenan contenido del mismo directorio. -Multiplataforma (Puede ejecutarse en varios sistemas operativos).
Mecanismos de interrelación con otros sistemas.	-LDAP cuenta con una biblioteca adicional para PHP, el cual tiene un módulo de conexión para los CRM, ERP y aplicaciones. Estás pueden acceder a la información de los usuarios que se encuentran en el servidor LDAP. El módulo desarrollado en PHP requiere lo siguiente para la conexión: *La URL del servidor LDAP *Definir el puerto que va a usar para la comunicación (Puerto 389 por defecto). -Para la integración de correo electrónico y LDAP se utiliza un servidor de correos ZIMBRA y se lo configura de la siguiente manera para poder establecer la conexión con el servidor LDAP: *Se define la URL del servidor LDAP y el puerto que va a utilizar para la comunicación (Por defecto 389 por defecto). *Se debe marcar en usar SSL (Capa de sockets seguros). -Para la conexión de diversas computadoras mediante la red inalámbrica Wireless se utiliza FreeRADIUS este incluye un servidor RADIUS, cuenta con un archivo de configuración llamado *users* donde se agregan los usuarios para acceso a la red wireless con el servidor LDAP.

4. Discusión

A continuación, se presentan los principales hallazgos que se encontraron al realizar la Revisión Sistemática:

Los artículos A1, A2, A3, A4, A5, A6, A7, A8, A9, A10, A11, A12, A13 y A14 que se detallan en la Tabla 13, presentan las características claves de la autentificación con el protocolo LDAP, las cuales son: Almacenamiento y gestión de perfiles de usuario asignados, multiplataforma (puede ejecutarse en varios sistemas operativos); encriptación de

mensajes en la autentificación mediante los protocolos SSL (Capa de sockets seguros) y TLS (Seguridad de la capa de transporte). Las características claves de LDAP en los artículos revisados para mecanismos de interrelación con diferentes sistemas son: Biblioteca adicional de PHP incorporada en LDAP para una correcta conexión; FreeRADIUS que incluye un servidor RADIUS para la conexión inalámbrica con el servidor LDAP. Estos artículos especifican a LDAP como un mecanismo centralizado para compartir directorios y acceso a un servicio distribuido.

Los artículos A8 y A9 recomienda la utilización de un SSO (Sistema de Autenticación única) para acceder a las diferentes aplicaciones conectadas al servidor LDAP.

El artículo A7, menciona además que para mejorar la seguridad hace uso del algoritmo SHA-1(actualmente ya es obsoleto) para generar contraseñas mediante una función de PHP. A partir del año 2017 las comunicaciones usan el algoritmo SHA-2.

El artículo A6 indica la importancia de usar ICE Novel que es un kit de herramientas para la importación y exportación de datos que se incorporan con LDIF (Formato de intercambio de datos), el cual contiene los registros que se envían a un servidor LDAP.

El artículo A9 sugiere un aspecto alternativo para la simplificación de operaciones utilizando el patrón Spring's JdbcTemplat para la gestión de operaciones y base de datos al conectar los sistemas con LDAP.

Los artículos A7, A12 y A13 puntualizan la importancia que tiene LDAP al contar con una biblioteca adicional para PHP el cual tiene un módulo de conexión a las aplicaciones, estás pueden acceder a la información de los usuarios que se encuentran en el servidor LDAP.

Los artículos A2, A3, A7, A13 y A14 precisan el mérito de LDAP al trabajar con protocolos de seguridad en la autentificación y encriptación de mensajes como son: SSL (Capa de sockets seguros) y TLS (Seguridad de la capa de transporte).

El artículo A2 indica que el uso del protocolo LDAP mejoró la seguridad mediante una red virtual privada VPN, junto al protocolo de tunelización punto a punto (PPTP), así mismo el artículo A4 puntualiza la seguridad al conectarse al servidor LDAP, referente a un mecanismo de control de acceso T-RBACK y un componente de autenticación independiente basado en PKI.

5. Conclusiones

La utilización del protocolo LDAP, permite la integración de múltiples sistemas o aplicaciones desarrollados en diferentes lenguajes de programación, mediante librerías y módulos que cuentan con métodos para su integración con el servidor OpenLDAP.

El protocolo LDAP, garantiza la seguridad de los datos mediante la encriptación de mensajes asegurando la confidencialidad, integridad y autentificación en la comunicación usando protocolos SSL (Capa de sockets seguros) y TLS (Seguridad de la capa de transporte).

El uso del protocolo LDAP, como mecanismo centralizado para la integración de distintos sistemas o aplicaciones, ofrece varios mecanismos de conexión como son: lenguaje PHP, SSO (Sistema de autentificación única), IAM (Sistema de gestión de identidades) y T-RBAC (Control de acceso basado en tareas y roles); siendo más relevante el uso del lenguaje PHP por sus herramientas de gestión para la administración de servidores OpenLDAP.

El protocolo LDAP mejoró la administración y almacenamiento de la información de usuarios, debido a su mecanismo centralizado y jerárquico, el cual optimiza las operaciones de lectura rápida y de gran volumen; respecto a una base de datos relacional que se encuentra optimizada para manejo de transacciones.

Referencias

[1] Kitchenham, B.: Procedures for performing systematic reviews. Keele, UK, Keele Univ. 33, 28 (2004).

[2] OpenLDAP Software 2.4 Administrator's Guide, http://www.openldap.org/doc/admin24/guide.html#What is a directory service.

[3] Butcher, M.: Mastering OpenLDAP. (2007).

[4] Qadeer, M.A., Salim, M., Sana Akhtar, M.: Profile management and authentication using LDAP. Proc. - 2009 Int. Conf. Comput. Eng. Technol. ICCET 2009. 2, 247–251 (2009).

[5] Mishra, U.: Inventions on LDAP-A study based on US Patents. 1–15 (2014).

[6] Jose, M., Gonzáles, M., Epaña, Á.: User Management with LDAP (Lightweight Directory Access Protocol) for access to technology and Information Services in Companies ´. J. Sci. Res. Rev. Cienc. E Investig. ´ ON, E-ISSN 2528-8083, VOL. 1, CITT, PP. 10-15. 1, 10–15 (2016).

[7] Thakur, M.A., Gaikwad, R.: User identity & lifecycle management using LDAP directory server on distributed network. 2015 Int. Conf. Pervasive Comput. Adv. Commun. Technol. Appl. Soc. ICPC 2015. 00, 1–3 (2015).

[8] Espinoza, G., Ortega, P., Palacios, C., Junior, S.: Intelligent agents applied to the management of ldap user profiles, https://issuu.com/universidadnacionaldeloja/docs/revista_energ__a/91, (2014).

[9] Obimbo, C.: Vulnerabilities of LDAP As An Authentication Service. J. Inf. Secur. 02, 151–157 (2011).

[10] Shrivastava, A., Rizvi, M.A.: External authentication approach for virtual private network using LDAP. In: 2014 First International Conference on Networks & Soft Computing (ICNSC2014). pp. 50–54. IEEE (2014).

[11] Raipurkar, K. V., Deorankar, A. V.: Improve data security in cloud environment by using LDAP and two way encryption algorithm. In: 2016 Symposium on Colossal Data Analysis and Networking (CDAN). pp. 1–4. IEEE (2016).

[12] Dharme, W.S.: Authentication using LDAP in Wireless Body Area Network. 4, 235–239 (2017).

[13] Shahriar, H., Haddad, H.M., Bulusu, P.: OCL Fault Injection-Based Detection of LDAP Query Injection Vulnerabilities. Proc. - Int. Comput. Softw. Appl. Conf. 2, 455–460 (2016).

[14] Wang, W., Luo, H., Deng, H.: Research on data and workflow security of electronic military systems. Proc. 2013 Int. Conf. Intell. Control Inf. Process. ICICIP 2013. 705–709 (2013).

[15] Xiao, Y., Zhao, Y.: Study and design of enterprise public security platform based on PKI. Proc. - 13th Int. Symp. Distrib. Comput. Appl. to Business, Eng. Sci. DCABES 2014. 258–262 (2014).

[16] Bulusu, P., Shahriar, H., Haddad, H.M.: Classification of Lightweight Directory Access Protocol Query Injection Attacks and Mitigation Techniques. 337–344 (2015).

[17] Andjarwirawan, J., Palit, H.N., Salim, J.C.: Linux PAM to LDAP Authentication Migration. 2017 Int. Conf. Soft Comput. Intell. Syst. Inf. Technol. 155–159 (2017).

[18] Ming, J.: Research of Unified Authentication System Based on LDAP. 1044–1047 (2012).

[19] Zhiyuan Wu1, Z. edu. c., Weiping Huang1, H. edu. c., Lei Yu1, Y. edu. c.: Design and Implementation of unified Identity Authentication System Based on LDAP in Digital Campus. Adv. Mater. Res. 1213–1217 (2014).

[20] Muttaqin, A.H., Rochim, A.F., Widianto, E.D.: Sistem Autentikasi Hotspot Menggunakan LDAP dan Radius pada Jaringan Internet Wireless Prodi Teknik Sistem Komputer. J. Teknol. dan Sist. Komput. 4, 282–288 (2016).

[21] Bauereiß, T., Gohmann, S., Hutter, D., Kläser, A.: Selective LDAP Multi-Master Replication. Proc. Open Identity Summit 2013. Open Identity Summit (OID-2013), Sept. 9-11, Kloster Banz, Ger. 94–105 (2013).

[22] Loayza J, J., Castillo, J, F., Chamba, L, A.: Implemetation of Eduroam as Wirelless Infraestructure on the Campus of National University of Loja., https://issuu.com/universidadnacionaldeloja/docs/revista_energ__a/91, (2014).

[23] Ming, J.: Research of Unified Authentication System Based on LDAP. 1044–1047 (2012).

[24] Wu, Z., Huang, W., Yu, L.: Design and Implementation of unified Identity Authentication System Based on LDAP in Digital Campus. 1213–1217 (2014).