TECNICATURA UNIVERSITARIA EN CIBERSEGURIDAD

GESTION DE ACCESOS

Ejercicio 2: Esquema de Autenticación y Autorización basado en LDAP

Balbuena Atar Dante Gabriel

Tafí viejo Tucumán Argentina – 2025/05/30

Profesor: Marcelo Daniel Rossetti

Contenido

1. Introducción

En el contexto de una empresa dedicada a la comercialización de productos alimenticios, que basa su actividad en servicios clave como el sistema de ventas, logística, correo electrónico corporativo y una aplicación en desarrollo para compras en línea, se propone diseñar un esquema de autenticación y autorización basado en LDAP (Lightweight Directory Access Protocol). Este esquema permitirá gestionar de forma centralizada y segura el acceso de los usuarios a los distintos sistemas, aplicando una estructura jerárquica y basada en roles mediante el uso de unidades organizativas y atributos específicos definidos por el estándar LDAP...

2. Desarrollo

2.1 Descripción general del esquema sugerido

La empresa implementará un servidor LDAP como base central de autenticación y autorización. La estructura jerárquica del directorio será la siguiente:

- **Dominio raíz**: dc=empresa,dc=com

- **Unidades Organizativas (OU)**:
  - ou=Usuarios: Contiene todas las cuentas de empleados y clientes.
  - ou=Grupos: Agrupa usuarios según roles (Ventas, Logística, TI).
  - ou=Sistemas: Representa los distintos sistemas de la organización.
  - ou=ClientesExternos: Para usuarios de la aplicación en desarrollo.

Este diseño permite:

- Autenticación centralizada y segura.
- Autorización basada en pertenencia a grupos.
- Control de acceso granular y auditado.

2.2 Especificaciones técnicas y estándares LDAP

- **ObjectClasses**:

  - inetOrgPerson: Para usuarios.
  - groupOfNames: Para grupos.
  - organizationalUnit: Para unidades organizativas.

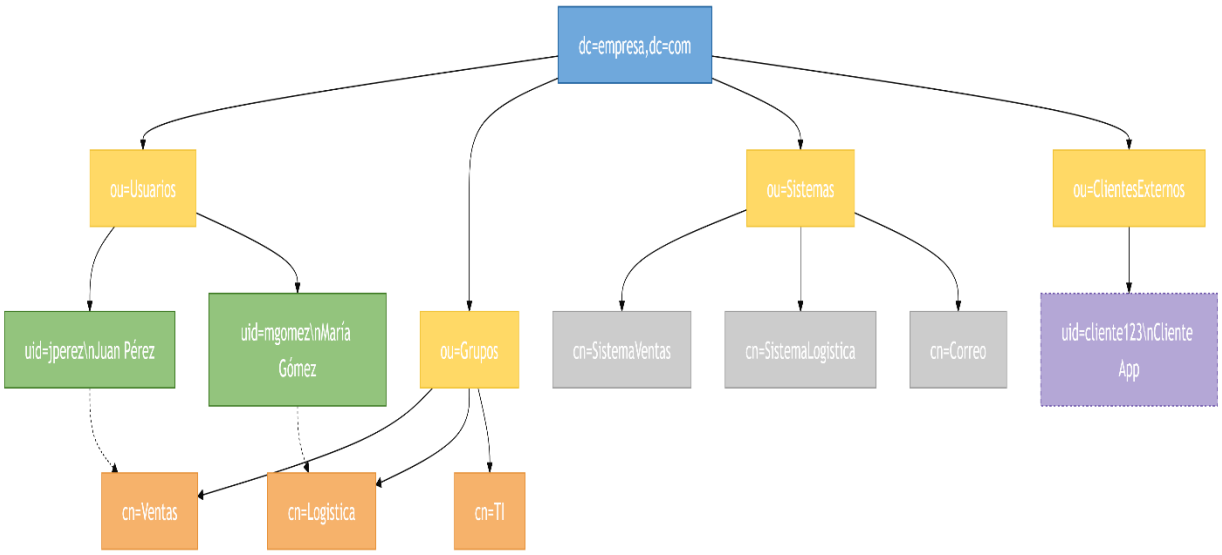
- **Atributos clave**:

  - uid: Identificador único.
  - cn: Nombre completo.
  - sn: Apellido.
  - userPassword: Contraseña cifrada (hash).
  - memberOf: Grupos a los que pertenece el usuario.
  - objectClass: Define el tipo de entrada.

- **Control de accesos (ACLs)**:

  Restringen o habilitan el acceso a recursos, según usuario o grupo.

2.3 Diagrama del árbol LDAP

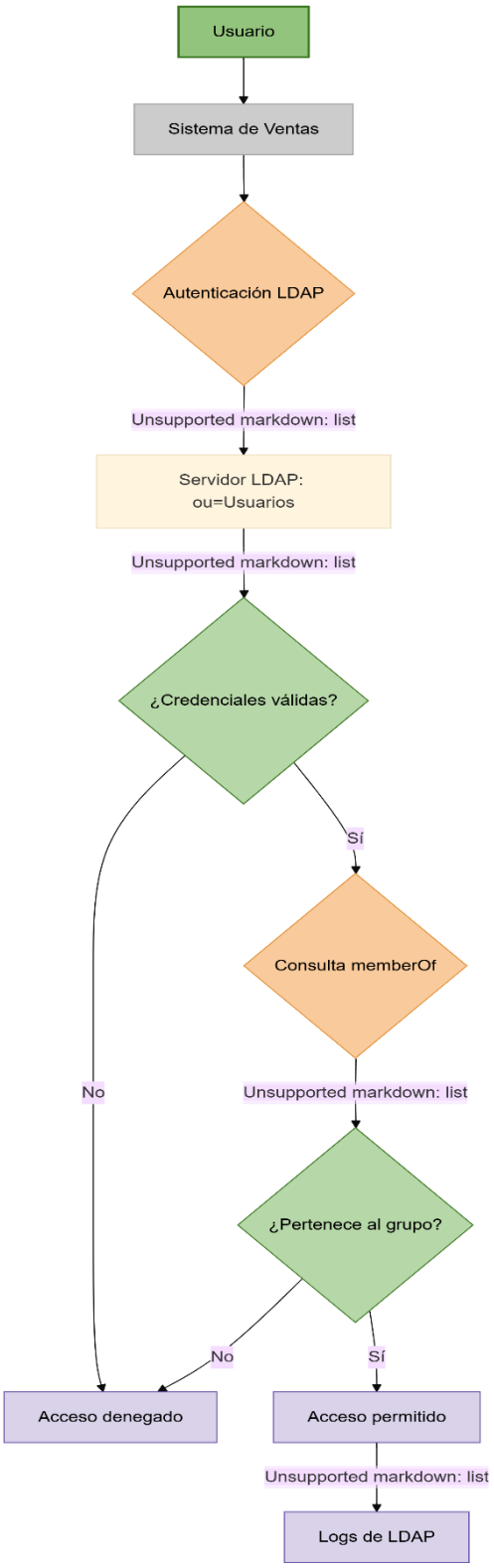


2.4 Lista mínima de atributos

Atributo	Descripción
uid	Identificador único (ej.: "jperez")
cn	Nombre completo del usuario (ej.: "Juan Pérez")
sn	Apellido del usuario (ej.: "Pérez")
userPassword	Contraseña almacenada en formato hash seguro
memberOf	Grupos a los que pertenece el usuario
objectClass	Clase del objeto (ej.: inetOrgPerson para usuarios)

2.5 Interacción: Usuario ↔ Sistema de Ventas

Diagrama de flujo simplificado



Descripción narrativa

- **Autenticación**:
  Juan Pérez (uid=jperez) inicia sesión en el Sistema de Ventas. El sistema envía las credenciales al servidor LDAP, que verifica su existencia en ou=Usuarios y la

validez de su contraseña.

- **Autorización**:
  El sistema consulta el atributo memberOf. Si Juan pertenece al grupo cn=Ventas, se le otorga acceso. En caso contrario, se lo deniega. Toda la actividad queda registrada.
- **Clientes externos**:
  Usuarios como cliente123 se ubican en ou=ClientesExternos y solo tienen permisos restringidos para acceder a la aplicación específica.

---

3. Conclusiones

El esquema propuesto permite una gestión centralizada de identidades con controles de acceso precisos, alineados con políticas de seguridad. Su estructura jerárquica y modular facilita la escalabilidad y la auditoría. Además, garantiza que usuarios internos y externos accedan exclusivamente a los recursos permitidos, reduciendo el riesgo de accesos no autorizados.

4. Referencias

Mermaid. (s.f.). *Live editor*. https://mermaid.live/edit#pako:eNpVjbFugzAQhl_FugmVSETAEPBQgSFtlkjtkKmQwQoHRg02MkZpCrx7DVHU9qY7fd__Xw8nlSMwKM7qchJcG3LYZpLYeU4ToavW1Lw9ksXiadihIbWSeB3I5mGnSCtU01SyfLz5m0kiSb-fNCRGVPJzvKFkzr9JHMq23fPGqOb4lxwuaiAvafUubP1_IjTa1GtacFbwxYlrknA9K-BAqascmNEdOlCjrvl0Qj_RDIzAGjNgds2x4N3ZZJDJ0cYaLj-Uqu9JrbpSqK0_t_bqmpwb3Fa81PxXQZmjTlQnDbBVOFcA6-ELmE-9pR97qyigQRytqOfAFRgNlzENPY-6oRutXZeODnzPP91lGAeuH_gBjb0oWEfB-APEr3a4

Wahl, M., Howes, T., & Kille, S. (2006). *RFC 4511 - Lightweight Directory Access Protocol (LDAP): The Protocol*. Internet Engineering Task Force. https://datatracker.ietf.org/doc/html/rfc4511

Instituto Nacional de Ciberseguridad (INCIBE). (s.f.). *Auditoría de sistemas*. https://www.incibe.es

National Institute of Standards and Technology. (2020). *Digital Identity Guidelines (SP 800-63-3)*. https://csrc.nist.gov/publications

OWASP Foundation. (s.f.). *Authentication Cheat Sheet*. https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html