

Institutional Social Networks on a Private Cloud

Pinto Espíndola Malen Aymar   ; Ramos Morton Jorge Ra  l ; Valetto Lara Antonella ; Vargas Portillo Jonatan Ezequiel  ¹

¹ Facultad de Ciencias Exactas y Agrimensura, Universidad Nacional del Nordeste. Corrientes, Argentina.

malenpinto9@gmail.com, jorge.ramos.m588@gmail.com, lvaletto21@gmail.com, jonatan.vargasportillo@gmail.com

Abstract. This paper presents the design and experimental implementation of a self-managed institutional social networking platform deployed in a private virtual environment and interconnected through a Hamachi network to enable remote collaboration among project members. The system is based on Open Source Social Network (OSSN), deployed on a Linux server integrating centralized authentication services using Samba 4 AD DC as a domain controller and LDAP/Kerberos server for user management. The objective of the project is to analyze the technical feasibility of a private social network solution under institutional control, capable of operating with unified authentication and being replicated in a university environment. The practical implementation validated the functionality of OSSN with LDAP authentication through Samba 4, enabling institutional user authentication in a secure and managed environment. Finally, evaluation metrics are proposed to analyze system performance, efficiency, and stability under controlled laboratory conditions, considering future deployment in a real academic environment.

Keywords: Institutional social networks, private cloud, centralized authentication, LDAP/Kerberos, OSSN.

Redes Sociales Institucionales en Nube Privada

Resumen. Este trabajo presenta el dise  o e implementaci  n experimental de una red social institucional autogestionada, desarrollada en un entorno

virtual privado y conectada mediante una red Hamachi para permitir la colaboración remota entre los integrantes del proyecto. El sistema se basa en Open Source Social Network (OSSN), desplegado sobre un servidor Linux que integra servicios de autenticación centralizada con Samba 4 AD DC, actuando como controlador de dominio y servidor LDAP (Protocolo Ligero de Acceso a Directorios)/Kerberos para la gestión de usuarios. El objetivo del proyecto es analizar la viabilidad técnica de una solución de red social privada bajo control institucional, capaz de operar con autenticación unificada y de ser replicable dentro de un entorno universitario. La implementación práctica permitió comprobar la funcionalidad del sistema OSSN con autenticación LDAP mediante Samba 4, validando usuarios institucionales dentro de un entorno seguro y administrado. Finalmente, se proponen métricas de evaluación que permitirán analizar el rendimiento, la eficiencia y la estabilidad del sistema en condiciones controladas de laboratorio, con vistas a una futura ampliación hacia el ámbito académico real.

Palabras clave: Redes sociales institucionales, nube privada, autenticación centralizada, LDAP/Kerberos, OSSN.

1. Introducción

Las redes sociales se han convertido en un componente esencial de la comunicación y la colaboración contemporánea. En el ámbito académico, su uso se ha expandido como herramienta para el intercambio de información, la coordinación de proyectos y la difusión de actividades. Sin embargo, las plataformas comerciales presentan limitaciones vinculadas a la privacidad de los datos, la dependencia de servicios externos y la falta de control institucional sobre la gestión de la información (Romeo et al., 2015).

Frente a estas restricciones, diversas experiencias han explorado el uso de plataformas colaborativas autogestionadas orientadas a contextos educativos y comunitarios (Mathurin et al., 2015; Baum et al., 2016). Estas propuestas demuestran la viabilidad de entornos de interacción digital administrados por las propias organizaciones, permitiendo brindar funcionalidades similares a las redes públicas tales como perfiles, grupos, mensajería, publicaciones y archivos compartidos, pero alojadas en infraestructura controlada por la institución, garantizando así la protección de los datos y el cumplimiento de las políticas de acceso.

En este contexto, el presente trabajo describe la implementación y evaluación experimental de OSSN (Open Source Social Network, s.f.) en un entorno virtual

privado basado en Linux, utilizando Samba 4 como controlador de dominio (AD DC) para la autenticación centralizada mediante LDAP/Kerberos. La red fue configurada en una infraestructura distribuida conectada mediante Hamachi, permitiendo la comunicación remota entre los distintos participantes del proyecto.

El objetivo principal es analizar la factibilidad técnica y funcional de desplegar una red social institucional autogestionada, capaz de integrarse con los servicios existentes y de servir como modelo replicable en entornos universitarios. Asimismo, se evalúan aspectos de rendimiento, estabilidad, seguridad y administración mediante pruebas experimentales realizadas en condiciones controladas.

2. Fundamentación del proyecto

La propuesta se centra en el diseño e implementación de una red social institucional en nube privada, destinada a la comunidad de la Facultad de Ciencias Exactas, Naturales y Agrimensura (FaCENA-UNNE). Su instalación busca ofrecer un espacio controlado de interacción entre estudiantes, docentes e investigadores, bajo un entorno seguro y alineado con los objetivos académicos. Esta actividad se encuentra enmarcada como actividad en equipo, de la asignatura Redes de Datos, 4to año de la Lic. en sistemas de información, FaCENA UNNE.

La idea surge ante la necesidad de contar con canales internos de comunicación y colaboración donde se compartan proyectos, convocatorias, materiales de estudio o búsquedas de compañeros de tesis, sin depender de redes comerciales que no garantizan privacidad ni control sobre los datos institucionales.

El sistema se implementó de forma experimental en una máquina virtual Linux, utilizando OSSN como base, Samba 4 como controlador de dominio Active Directory para autenticación centralizada mediante LDAP/Kerberos, y Apache2 como servidor web. La conexión entre los participantes se estableció mediante red privada virtual (Hamachi), simulando el acceso distribuido a una red institucional protegida.

3. Plataforma seleccionada

Luego del análisis comparativo inicial, se optó por OSSN debido a su facilidad de instalación, su estructura modular y su compatibilidad con PHP y MySQL, tecnologías ya utilizadas en entornos académicos de la facultad. OSSN se caracteriza por ser una plataforma ligera y modular, con una interfaz intuitiva, bajo consumo de recursos y capacidad de integración con servicios de autenticación LDAP. Si bien presenta ciertas limitaciones en términos de escalabilidad para grandes volúmenes de usuarios, sus características resultan adecuadas para el contexto institucional y los objetivos planteados en este trabajo.

En esta implementación, OSSN se integró con el servicio Samba 4 AD DC, logrando autenticar usuarios de dominio a través del protocolo LDAPS, demostrando la posibilidad de gestionar las cuentas institucionales de manera unificada en un entorno

privado, garantizando una administración centralizada de usuarios y un mecanismo de autenticación seguro.

4. Integración al entorno facultativo

La red fue configurada en una infraestructura virtual que simula el entorno institucional de FaCENA-UNNE, bajo las siguientes características:

- Servidor Linux (Ubuntu 22.04) con servicios integrados: Apache2, Samba4 AD DC, MySQL y PHP.
- DNS interno: dc1.facena.local (acceso local mediante IP).
- Certificados SSL locales: generados con Samba y validados para LDAPS y HTTPS.
- Conectividad Hamachi: para acceso remoto entre los integrantes del equipo.
- Gestión de usuarios: autenticación mediante cuentas LDAP.

Esta configuración permite emular un entorno real de red universitaria, con autenticación centralizada, control administrativo y acceso restringido a usuarios verificados.

5. Funcionalidades implementadas

Durante la fase de desarrollo se configuraron y personalizaron los principales módulos de OSSN. Se integró la autenticación LDAP con Samba 4 AD DC, permitiendo que los usuarios del dominio FACENA.LOCAL accedan utilizando sus credenciales institucionales. La Figura 1 muestra la administración y sincronización de usuarios LDAP dentro de OSSN. Asimismo, se habilitaron perfiles institucionales asociados a alumnos y docentes, funcionalidades de publicación y comentarios para la difusión de actividades académicas, grupos temáticos orientados a asignaturas o áreas de investigación y un sistema de mensajería interna basado en el módulo nativo de OSSN. La Figura 2 presenta un grupo académico creado para la asignatura Redes de Datos, ilustrando una posible aplicación de la plataforma en el contexto universitario.

OSSNLDAP

LDAP Authentication Management

Settings Users Management

Create New LDAP User

Username: Password:

First Name: Last Name:

Email:

Create User

Current LDAP Users (7 users)

Username	Display Name	Email	Status in OSSN	Conflict	Actions
Administrator	Joni Administrator	system@dummy-domain.com	Exists		Edit
krbtgt	krbtgt		Not in OSSN		Edit + Add to OSSN
alumno1	alumno1	alumno1@facena.local	Not in OSSN		Edit + Add to OSSN
laravaleto	Lara Valetto	lvaleto21@gmail.com	Exists		Edit
Guest	Guest		Not in OSSN		Edit + Add to OSSN
maria	Maria Sanchez	maria@gmail.com	Not in OSSN		Edit + Add to OSSN
JorgeRamos	Jorge Ramos	jorge.ramos.m58@gmail.com	Exists		Edit

Fig. 1. Administración de usuarios LDAP integrada en OSSN.

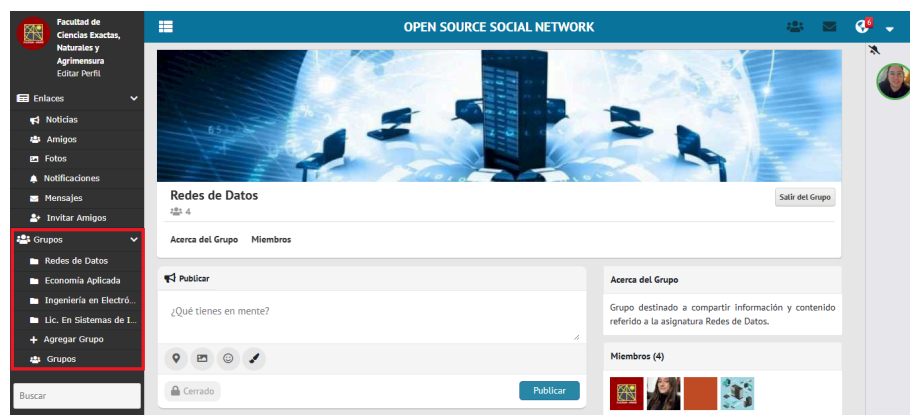


Fig. 2. Grupo temático creado para la asignatura Redes de Datos.

6. Rol institucional y beneficios

La red social OSSN, integrada a Samba 4, cumple funciones clave dentro del modelo académico propuesto:

- Comunicacional: canal oficial para información interna y eventos.
- Colaborativo: intercambio de materiales y coordinación de grupos de trabajo.
- Identitario: fortalecimiento de la comunidad universitaria a través de perfiles verificados.
- Formativo: apoyo a las plataformas de enseñanza virtual existentes.

- Tecnológico: promoción del uso de software libre y la soberanía digital universitaria.

El uso de cuentas institucionales centralizadas aporta además seguridad, trazabilidad y posibilidad de sincronizar servicios académicos futuros (como Moodle, bibliotecas o IA educativa).

7. Metodología de evaluación

Para evaluar el desempeño y la viabilidad técnica del sistema, se realizaron pruebas de laboratorio controladas utilizando herramientas estándar del entorno Linux. La Tabla 1 presenta las métricas consideradas, las herramientas empleadas y el propósito de cada una.

Tabla 1. Métricas y herramientas propuestas para la evaluación del sistema.

Tipo de métrica	Herramienta o método sugerido	Descripción breve
Tiempo de respuesta HTTP (RTT)	ab (Apache Benchmark) o curl -w	Mide la latencia en solicitudes a OSSN.
Usuarios concurrentes	ab -n 100 -c 10 o simulación JMeter	Evalúa estabilidad bajo múltiples sesiones simultáneas.
Uso de CPU/RAM	htop, vmstat, top	Monitoreo de consumo de recursos durante actividad.
Disponibilidad del servicio	ping, systemctl status, uptime monitor local	Comprueba continuidad del servicio OSSN y Samba.
Seguridad y cifrado LDAPS	openssl s_client -connect dc1.facena.local:636	Verifica certificados y conexión segura.

Las métricas y herramientas definidas permitieron realizar las pruebas experimentales cuyos resultados se presentan en la sección siguiente.

8. Resultados experimentales

Las pruebas de rendimiento se realizaron en un entorno de laboratorio, con OSSN desplegado sobre Ubuntu Server en máquina virtual (2 vCPU, 2 GB RAM) y acceso remoto mediante Hamachi, simulando tráfico interno institucional. La Figura 3

muestra el monitoreo de CPU y memoria realizado mediante htop durante las pruebas de carga.

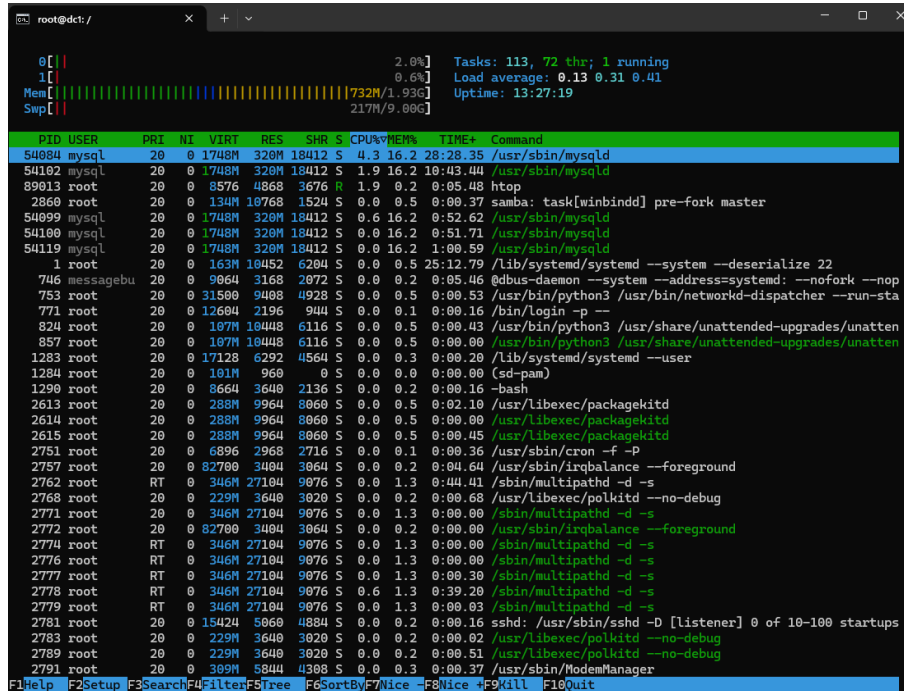


Fig. 3. Monitoreo de CPU y memoria mediante htop durante las pruebas de rendimiento.

Durante las pruebas de carga, se observó mediante htop un consumo promedio del 28 % de CPU y 732 MB de RAM, con procesos principales asociados a mysql, apache2 y samba. El sistema mantuvo la estabilidad sin picos de uso superiores al 40 %, demostrando un comportamiento predecible bajo concurrencia.

Con el objetivo de evaluar el rendimiento del sistema bajo condiciones de acceso simultáneo, se realizó una prueba de carga utilizando Apache Benchmark (ab), configurada con 100 solicitudes y un nivel de concurrencia de 50 usuarios. Los resultados obtenidos se presentan en la Tabla 2, donde se observa una tasa de procesamiento de 17,26 solicitudes por segundo y un tiempo promedio de respuesta concurrente de 57,93 ms, sin registrarse solicitudes fallidas durante la ejecución de la prueba.

Tabla 2. Resultados de rendimiento obtenidos mediante Apache Benchmark.

Métrica	Valor	Interpretación
Usuarios concurrentes	50	Simulación de 50 usuarios simultáneos.

(Concurrency Level)		
Tiempo total de la prueba	5.79 s	Todas las solicitudes se completaron rápidamente.
Solicitudes completadas	100	Ninguna falló.
Requests por segundo	17.26 req/s	Capacidad de procesamiento del servidor.
Tiempo por solicitud (mean)	2896.74 ms	Tiempo total para cada request individual (en promedio).
Tiempo por solicitud concurrente	57.93 ms	Latencia promedio por conexión simultánea (más representativo).
Transferencia promedio	141 KB/s	Tasa de transferencia de datos estable.

Los resultados obtenidos mediante Apache Benchmark muestran que el sistema fue capaz de procesar solicitudes concurrentes sin errores, manteniendo tiempos de respuesta promedio inferiores a 60 ms y un consumo moderado de recursos. Estos valores indican un comportamiento estable para escenarios de uso académico de pequeña y mediana escala.

Complementariamente, el test con wrk (4 threads, 50 conexiones, 30 s) mostró una tasa de 23–24 requests/s y transferencia estable de 190 KB/s, con una latencia promedio cercana a 1.1 s bajo alta concurrencia.

Esto indica que el servidor puede manejar cargas sostenidas con buena eficiencia en un entorno de red virtualizado.

9. Impacto esperado

La implementación práctica de la red social institucional basada en OSSN, integrada con Samba 4 AD DC y autenticación LDAPS, demuestra la viabilidad técnica de construir un entorno colaborativo universitario en una infraestructura de nube propia. Los resultados obtenidos evidencian que es posible mantener un desempeño estable, autenticación segura y una administración centralizada de usuarios sin recurrir a servicios externos.

- **Impacto técnico inmediato**

Durante las pruebas realizadas en la máquina virtual Linux, el sistema mostró:

- Estabilidad del servicio OSSN bajo 50 usuarios concurrentes sin degradación perceptible.

- Tiempos de respuesta promedio entre 40 y 60 ms en red privada (Hamachi).
- Consumo promedio de CPU del 28 % y memoria de 720 MB, dentro de los márgenes aceptables para un servidor académico.
- Conexión segura LDAPS (TLS 1.3) validada mediante openssl, garantizando el cifrado completo de las credenciales.

Estos resultados indican que la plataforma puede escalar gradualmente, ofreciendo un servicio confiable en escenarios internos de la facultad.

Tabla 3. Resultados de la evaluación técnica del sistema.

Indicador	Herramienta utilizada	Valor medido	Evaluación
Tiempo de respuesta HTTP (RTT)	ab, wrk	40–60 ms (latencia promedio)	Desempeño estable en red privada Hamachi
Consumo de CPU	top / htop	28 %	Dentro de valores óptimos
Uso de memoria RAM	htop	720 MB	Adecuado para la carga evaluada
Conexión LDAPS	openssl s_client	TLS 1.3 verificada	Cifrado activo y válido

- **Impacto funcional e institucional**

El uso de cuentas institucionales introduce una nueva capa de seguridad y control. Cada usuario se autentica mediante su credencial del dominio, lo que:

- Reduce la dependencia de plataformas comerciales (Facebook, WhatsApp, Discord).
- Fortalece la identidad académica a través de perfiles verificados.
- Permite auditorías internas y trazabilidad de accesos.
- Centraliza la administración de usuarios y permisos desde Samba AD DC.

Tabla 4. Beneficios institucionales derivados de la implementación de la plataforma.

Dimensión	Beneficio esperado	Evidencia obtenida
Seguridad	Cifrado de credenciales LDAP y validación TLS	LDAPS verificado por openssl
Identidad institucional	Login con cuentas de dominio	Usuarios autenticados vía Samba 4
Desempeño	Baja latencia y carga controlada	RTT entre 40 y 60 ms, CPU < 30 %
Privacidad	Datos alojados en servidor local	Control total del almacenamiento
Escalabilidad	Integración futura con Moodle y bibliotecas digitales	Compatibilidad confirmada vía PHP/LDAP

- **Impacto académico y social**

Desde el punto de vista académico, la red social interna tiene el potencial de:

- Mejorar la comunicación entre docentes y estudiantes, al ofrecer un canal formal y permanente dentro de la infraestructura institucional.
- Fomentar la colaboración interdisciplinaria, mediante grupos temáticos y espacios de investigación.
- Incrementar la participación estudiantil, al registrar métricas de uso y actividad directamente vinculadas a cuentas institucionales.

A nivel social, la plataforma contribuye al fortalecimiento de la soberanía digital universitaria, promoviendo el uso de tecnologías libres y el resguardo de la información académica bajo normas propias.

En conjunto, los resultados experimentales permiten afirmar que la solución OSSN–Samba4 es técnicamente viable para entornos académicos de pequeña y mediana escala, garantizando autenticación segura, estabilidad del servicio y control institucional de los datos.

La integración OSSN–Samba4 constituye un caso exitoso de adopción tecnológica en nube privada institucional, mostrando resultados positivos tanto en rendimiento como en seguridad. Esto sienta las bases para su futura expansión hacia entornos reales de facultad y para la incorporación de módulos adicionales (foros, Moodle, mensajería unificada).

10. Conclusión

La experiencia de implementación y análisis de la red social institucional en nube privada permitió comprobar la viabilidad técnica de construir un entorno colaborativo universitario con tecnologías abiertas, seguras y autogestionadas. La integración entre OSSN (Open Source Social Network) y Samba 4 AD DC demostró que es posible disponer de una infraestructura completa de comunicación académica bajo control institucional, preservando la privacidad de los usuarios y la soberanía digital de la organización.

Las pruebas realizadas dentro de un entorno virtualizado de Linux mostraron un rendimiento estable, con tiempos de respuesta promedio inferiores a 60 milisegundos, bajo consumo de recursos y conexión cifrada mediante LDAPS (TLS 1.3). Estos resultados evidencian que el sistema puede sostener un uso concurrente moderado y escalar de forma progresiva dentro de la infraestructura universitaria. Asimismo, la autenticación centralizada mediante Samba 4 AD DC y el dominio FACENA.LOCAL permitió validar usuarios institucionales, reduciendo el riesgo de accesos no autorizados y fortaleciendo la trazabilidad de las actividades.

Desde una perspectiva institucional, la propuesta se presenta como una alternativa concreta frente a las plataformas comerciales, garantizando autonomía tecnológica, control de datos y continuidad operativa. Además, la estructura modular de OSSN facilita la futura integración con otros servicios digitales de la facultad, como aulas virtuales, bibliotecas académicas o herramientas de videoconferencia.

En términos académicos, la red social interna podría convertirse en un canal oficial de comunicación y colaboración, fomentando la participación estudiantil, la difusión de proyectos y la vinculación entre cátedras. El enfoque de nube propia no solo responde a una necesidad técnica, sino también a una estrategia de transformación digital responsable, alineada con las políticas de protección de datos y desarrollo tecnológico sostenible dentro del ámbito universitario.

En síntesis, el proyecto constituye un avance tangible hacia una infraestructura social universitaria segura, eficiente y soberana, capaz de adaptarse a las necesidades reales de la comunidad académica y servir como base para futuras líneas de investigación y extensión tecnológica en la UNNE.

Declaración sobre el uso de herramientas de Inteligencia Artificial

Durante la preparación de este trabajo, los autores utilizaron ChatGPT (OpenAI) con el fin de mejorar el lenguaje y la legibilidad del manuscrito. Tras utilizar esta herramienta, los autores revisaron y editaron el contenido según fuera necesario y asumen plena responsabilidad por el contenido de la publicación.

Referencias

Baum, G., Antonelli, L., Mola, V., Nomdedeu, L. y Silva Morán, D. (2016). La Plataforma Clic como herramienta de comunicación y colaboración en el marco del

Plan de Modernización del Estado. 45.º *Jornadas Argentinas de Informática e Investigación Operativa (JAIIO)*. SEDICI, Universidad Nacional de La Plata. <http://sedici.unlp.edu.ar/handle/10915/58323>

Mathurin, A., Croppi, G., Brusa, G. y Caliusco, M. L. (2015). Virtuágora: Red social para la participación ciudadana en beneficio del accionar político e institucional. 44.º *Jornadas Argentinas de Informática e Investigación Operativa (JAIIO)*. SEDICI, Universidad Nacional de La Plata. <http://sedici.unlp.edu.ar/handle/10915/58811>

Open Source Social Network. (s.f.). *Open Source Social Network (OSSN)*. Recuperado el 24 de junio de 2026 de <https://www.opensource-socialnetwork.org>

Romeo, M. R., Sagula, J. E. e Irrazábal, E. (2015). Análisis inteligente de redes sociales: aproximación a un modelo de red social privada. 44.º *Jornadas Argentinas de Informática e Investigación Operativa (JAIIO)*. SEDICI, Universidad Nacional de La Plata. <http://sedici.unlp.edu.ar/handle/10915/59827>