**Revista Amazonía Digital**

Vol. 2 Núm. 1: e280 (2023)
https://doi.org/10.55873/rad.v2i1.280
e-ISSN: 2810-8701
Universidad Nacional Amazónica de Madre de Dios



**Artículo original / Original article**

# Mejoras en la satisfacción y seguridad del usuario mediante autenticación centralizada: Estudio en una universidad peruana

# Improving user satisfaction and security through centralized authentication: A study at a Peruvian university

Luis Rafael García-Vela [1*]

[1] Universidad Nacional de San Martín, Tarapoto, Perú

*Autor de correspondencia: luisgarcia@unsm.edu.pe

Recibido: 25/10/2022
Aceptado: 28/12/2022
Publicado: 25/01/2023

**Resumen:** La gestión de autenticación en aplicaciones informáticas es un desafío para las instituciones educativas debido a la fragmentación de credenciales y la falta de integración de sistemas. Este estudio evaluó el impacto de la implementación de Keycloak, un sistema de autenticación centralizada, en la percepción del inicio de sesión de usuarios en la Universidad Nacional de San Martín (UNSM). El objetivo fue determinar cómo esta solución mejora la satisfacción y la seguridad percibida por los usuarios. Se utilizó un enfoque cuantitativo con diseño pre-test y pos-test, aplicando la prueba de Wilcoxon a una muestra de 37 usuarios de las aplicaciones informáticas de la UNSM. Los resultados mostraron un aumento significativo en la percepción de satisfacción ($p = 0.000$), pasando del 18.9% de nivel alto en el pre-test al 54.1% en el pos-test. De igual forma, la percepción de seguridad mejoró del 18.9% al 48.7%. La implementación permitió centralizar 16 métodos de autenticación independientes en un único sistema, optimizando la experiencia del usuario y reduciendo riesgos de seguridad. En conclusión, Keycloak demostró ser una herramienta eficaz para la gestión de accesos, fortaleciendo la seguridad y la eficiencia operativa en entornos educativos.

**Palabras clave:** autenticación centralizada; gestión de accesos; seguridad informática; sistemas educativos; usuarios

**Abstract:** Authentication management in IT applications is a challenge for educational institutions due to credential fragmentation and a lack of system integration. This study evaluated the impact of implementing Keycloak, a centralized authentication system, on user login perception at the National University of San Martín (UNSM). The objective was to determine how this solution improves user satisfaction and perceived security. A quantitative approach was employed with a pre-test and post-test design, using the Wilcoxon test on a sample of 37 users of UNSM's IT applications. Results showed a significant increase in satisfaction perception ($p = 0.000$), with high levels rising from 18.9% in the pre-test to 54.1% in the post-test. Similarly, security perception improved from 18.9% to 48.7%. The implementation centralized 16 independent authentication methods into a single system, optimizing user experience and reducing security risks. In conclusion, Keycloak proved to be an effective tool for access management, enhancing security and operational efficiency in educational environments.

**Keywords:** access management; centralized authentication; educational systems; information security; users

**Cómo citar / Citation:** García-Vela, L. R. (2023). Mejoras en la satisfacción y seguridad del usuario mediante autenticación centralizada: Estudio en una universidad peruana. *Revista Amazonía Digital*, 2(1), e280. https://doi.org/10.55873/rad.v2i1.280

## 1. Introducción

La autenticación es un elemento crucial en la seguridad informática, especialmente en el ámbito de las aplicaciones informáticas institucionales (IBM Corporation, 2021). Los métodos tradicionales de inicio de sesión, basados en pares de identificador único y contraseñas alfanuméricas, han demostrado ser vulnerables y limitados en escenarios de alta demanda tecnológica (Boyd et al., 2020). En instituciones como las universidades, donde los usuarios deben gestionar múltiples credenciales para acceder a diversos sistemas, estos métodos generan insatisfacción, pérdida de tiempo y riesgos de seguridad. Estudios previos han evidenciado que esta problemática afecta directamente la experiencia del usuario y la confianza en los sistemas digitales, creando desafíos significativos para la gestión de accesos en entornos educativos (Rodríguez Valdés et al., 2018; Arbaiza Godos, 2018).

En la Universidad Nacional de San Martín (UNSM), esta problemática es particularmente evidente. La institución cuenta con 37 aplicaciones informáticas desarrolladas con plataformas heterogéneas, cada una con procesos de autenticación independientes. Esta fragmentación no solo dificulta la experiencia del usuario, sino que también eleva los costos de mantenimiento y aumenta el riesgo de malas prácticas en la gestión de credenciales, como el uso de contraseñas débiles o reutilizadas. Estas deficiencias contribuyen a generar insatisfacción y exponen la información sensible de los usuarios y la institución a riesgos significativos (Peñarrieta Valencia & Villafuerte Villafuerte, 2017).

El impacto de estas deficiencias no se limita a los usuarios. También afecta la administración de los sistemas informáticos, ya que la falta de integración conlleva mayores costos de mantenimiento, actualizaciones, y soporte técnico, además de riesgos para la seguridad de la información. En instituciones como la UNSM, donde las necesidades tecnológicas crecen constantemente, es fundamental implementar soluciones que centralicen los procesos de autenticación, mejorando la eficiencia operativa y la experiencia del usuario.

Ante este contexto, la integración de métodos de autenticación mediante un sistema centralizado, como el modelo de inicio de sesión único (Single Sign-On, SSO), se presenta como una solución viable. Sistemas como Keycloak permiten unificar la autenticación de múltiples aplicaciones bajo un proceso centralizado, mejorando tanto la percepción del usuario como la seguridad de la información. Investigaciones anteriores han demostrado que este enfoque optimiza procesos, reduce tiempos de acceso y simplifica la gestión de credenciales, beneficiando tanto a los usuarios como a los administradores de los sistemas informáticos (Gellert et al., 2017; Sciarretta et al., 2017; Arbaiza Godos, 2018).

El modelo de inicio de sesión único no solo representa una mejora tecnológica, sino que también responde a la necesidad de garantizar accesos más seguros y eficientes en entornos con alta conectividad y dependencias tecnológicas. La implementación de Keycloak, un sistema reconocido por su robustez y adaptabilidad, permite simplificar los procesos de acceso y fortalecer la seguridad de las aplicaciones informáticas, al tiempo que se incrementa la satisfacción de los usuarios. Este tipo de soluciones tecnológicas está alineado con las mejores prácticas de seguridad informática y gestión de accesos en instituciones educativas.

El presente estudio tiene como objetivo evaluar el impacto de la integración de métodos de autenticación en la percepción del inicio de sesión de los usuarios de las aplicaciones informáticas de la UNSM. A través de la implementación del sistema Keycloak, se busca determinar cómo esta solución tecnológica contribuye a mejorar la satisfacción del usuario y la seguridad percibida en los procesos de autenticación, ofreciendo evidencia de su eficacia y estableciendo bases para estrategias futuras en la gestión de accesos en entornos educativos.

## 2. Materiales y métodos

La investigación fue de tipo aplicada, ya que se enfocó en proponer una solución concreta a un problema identificado dentro de un contexto específico. Además, se utilizó un enfoque

cuantitativo para analizar las percepciones de los usuarios respecto al inicio de sesión en aplicaciones informáticas antes y después de implementar un sistema de autenticación centralizada (Hernández Sampieri et al., 2014).

El estudio se desarrolló en la Universidad Nacional de San Martín (UNSM), específicamente en la sede principal ubicada en el distrito de Morales, provincia y departamento de San Martín. El periodo de ejecución comprendió desde octubre de 2022 hasta febrero de 2023. Durante este tiempo, se llevaron a cabo las fases de diagnóstico, diseño, implementación, evaluación y análisis de resultados relacionados con el sistema de autenticación centralizada.

La población estuvo compuesta por los usuarios de las 37 aplicaciones informáticas utilizadas en la UNSM, las cuales se clasificaron en seis categorías tecnológicas: aplicaciones de tecnología JAVA WEB, NODEJS, PHP, OAUTH 2.0, PUNTO NET y CRM WordPress. La muestra se determinó de manera intencionada, incluyendo a 37 usuarios activos que interactúan regularmente con estas aplicaciones. La selección buscó asegurar representatividad de las diferentes áreas académicas y administrativas.

El procedimiento de la investigación siguió un modelo lineal secuencial o de cascada, estructurado en cinco fases principales: (1) documentación, donde se revisaron soluciones de autenticación disponibles en el mercado; (2) diseño y ejecución del cuestionario para el pre-test y pos-test; (3) análisis de soluciones para seleccionar la herramienta más adecuada; (4) diseño de la integración en un sistema de inicio de sesión único (SSO); y (5) implementación y pruebas del sistema centralizado, utilizando Keycloak como proveedor de identidad.

La variable independiente fue la integración de métodos de autenticación, y la variable dependiente fue la percepción del inicio de sesión, operacionalizada en dos dimensiones: satisfacción y seguridad. Ambas dimensiones fueron evaluadas mediante un instrumento de recolección de datos basado en una escala de Likert. Este instrumento permitió medir indicadores como facilidad de uso, confianza en la seguridad, reducción de malestar y soporte técnico percibido.

Para el análisis estadístico, se utilizó la prueba de rangos con signo de Wilcoxon, adecuada para muestras relacionadas que no presentan una distribución normal. Los datos obtenidos se analizaron con un nivel de significancia del 5%, lo que permitió determinar si la implementación del sistema Keycloak produjo mejoras significativas en las dimensiones de satisfacción y seguridad del inicio de sesión de los usuarios.

## 3. Resultados y discusión

### Identificación de procesos de autenticación e identificación de usuarios en las aplicaciones informáticas de la UNSM

Se llevó a cabo un inventario y un análisis de los sistemas de información preexistentes en la Universidad Nacional de San Martín (UNSM), enfocado en los procedimientos de autenticación, identificación de usuarios y seguridad de dichos procesos. Para ello, se consultó con la Oficina de Tecnologías de Información de la universidad y se emplearon técnicas de hacking ético mediante herramientas como la plataforma Kali Linux y el servicio en línea DNSDumpster. Estas herramientas permitieron identificar información clave relacionada con las aplicaciones alojadas en el dominio "unsm.edu.pe".

### Inventario de aplicaciones informáticas

La UNSM cuenta con un total de 37 aplicaciones informáticas. Estas aplicaciones se agruparon en seis categorías tecnológicas principales, cada una con características específicas relacionadas con su funcionalidad y método de autenticación. A continuación, se presenta un resumen de las aplicaciones identificadas:

- **Sistema de Gestión Documental (SGD):** Permite organizar, rastrear, almacenar, y archivar documentos de manera centralizada para facilitar el acceso de los empleados.
- **Sistema de Gestión Administrativa (SIGA-MEF):** Herramienta basada en web que facilita la gestión administrativa integrada en los procesos de las entidades públicas, en alineación con el Ministerio de Economía y Finanzas.
- **Sistema de Gestión de Servicios:** Ofrece consultas centralizadas a datos provenientes de la UNSM y la Plataforma de Interoperabilidad del Estado (PIDE), como boletas de planilla y CAFAE.
- **Sistema de Planillas:** Administra y automatiza procesos relacionados con nómina, control de asistencia y gestión de vacaciones.
- **Correo Institucional (Gmail):** Servicio de correo empresarial proporcionado por Google, ampliamente utilizado por personal y estudiantes.
- **Sistema Integrado de Gestión Académica Universitaria (SIGAU):** Plataforma modular compuesta por 11 módulos aprobados mediante Resolución N° 617-2022-UNSM/R. Estos módulos abarcan procesos académicos como admisión, matrícula, aula virtual, gestión docente y tesorería, entre otros.

Además, se identificaron 13 subdominios adicionales que corresponden a aplicaciones específicas destinadas a facultades y dependencias internas de la UNSM.

**Análisis del SIGAU**

El SIGAU destacó como una plataforma modular clave dentro de las aplicaciones de la UNSM, diseñada para automatizar e integrar procesos académicos. Sus módulos permiten registrar y monitorear actividades académicas de docentes, estudiantes y áreas administrativas, integrando información relevante como la procedencia socioeconómica de los estudiantes y registros académicos.

**Importancia del análisis**

El análisis identificó deficiencias en la integración de métodos de autenticación y la dispersión de credenciales, lo que genera desafíos operativos y de seguridad. La información obtenida mediante técnicas avanzadas permitió documentar las características técnicas y de autenticación de cada aplicación, sirviendo como base para la implementación de un sistema centralizado de autenticación.

**Percepción de los usuarios sobre el inicio de sesión en las aplicaciones informáticas de la UNSM**

**Pre-Test (O1)**

El análisis inicial de la percepción de los usuarios sobre los métodos de autenticación empleados en las aplicaciones informáticas de la UNSM se evaluó mediante un pre-test. Los resultados, mostrados en la Tabla 1, revelaron que el 37.8% de los encuestados manifestaron un nivel bajo de satisfacción, mientras que el 43.2% expresaron una percepción media. Solo el 18.9% de los usuarios consideraron satisfactorios los métodos de autenticación utilizados.

**Tabla 1.** Dimensión satisfacción (Pre-Test O1)

| Valoración | Min | Max | Frecuencia | Porcentaje |
|---|---|---|---|---|
| Bajo | 9 | 14.7 | 14 | 37.8% |
| Medio | 14.7 | 20.3 | 16 | 43.2% |
| Alto | 20.3 | 26 | 7 | 18.9% |
| Totales | | | 37 | 100% |

Estos resultados fueron obtenidos al medir indicadores relacionados con el ahorro de tiempo, la facilidad de uso, la capacidad para recordar credenciales, el soporte técnico recibido, la adaptabilidad de las aplicaciones en diversos dispositivos y la experiencia general de inicio de sesión. La principal fuente de insatisfacción reportada fue la necesidad de memorizar múltiples

credenciales, lo que coincide con observaciones previas de Arbaiza Godos (2018), quien destacó que este problema es común en instituciones con sistemas de autenticación descentralizados. Asimismo, Gellert et al. (2017) señalaron que los tiempos prolongados dedicados a inicios de sesión múltiples pueden interferir en la productividad de los usuarios.

Respecto a la percepción de seguridad informática, los resultados presentados en la Tabla 2 indicaron que el 29.7% de los usuarios percibieron un nivel bajo, mientras que el 51.4% consideraron que la seguridad era media. Solo un 18.9% evaluaron positivamente los métodos de autenticación en términos de seguridad.

**Tabla 2.** Dimensión seguridad (Pre-Test O1)

| Valoración | Min | Max | Frecuencia | Porcentaje |
|---|---|---|---|---|
| Bajo | 14 | 19 | 11 | 29.7% |
| Medio | 19 | 24 | 19 | 51.4% |
| Alto | 24 | 29 | 7 | 18.9% |
| Totales | | | 37 | 100% |

Los usuarios señalaron preocupaciones relacionadas con el olvido de contraseñas, el respaldo de credenciales, la generación de contraseñas seguras y la confianza general en los sistemas de autenticación. Estas percepciones coinciden con investigaciones previas que asocian la falta de integración de sistemas con malas prácticas de seguridad, como la reutilización de contraseñas (Arbaiza Godos, 2018).

**Pos-Test (O2)**

Tras la integración de los métodos de autenticación centralizada mediante el sistema Keycloak, se realizó un pos-test para evaluar nuevamente la percepción de los usuarios. Los resultados, presentados en la Tabla 3, muestran una mejora significativa en ambas dimensiones analizadas. En cuanto a la satisfacción, el 54.1% de los encuestados calificaron su experiencia como alta, mientras que el 32.4% la consideraron media y solo el 13.5% expresaron un nivel bajo.

**Tabla 3.** Dimensiones satisfacción y seguridad (Pos-Test O2)

| Valoración | Satisfacción | Seguridad |
|---|---|---|
| Frecuencia | Porcentaje | Frecuencia |
| Bajo | 5 | 13.5% |
| Medio | 12 | 32.4% |
| Alto | 20 | 54.1% |
| Totales | 37 | 100% |

Respecto a la seguridad percibida, el 48.7% de los usuarios manifestaron una percepción alta, el 32.4% media y el 18.9% baja. Estos resultados reflejan una mejora notable en comparación con el pre-test, donde predominaban las valoraciones bajas y medias.

**Análisis estadístico**

Se empleó la prueba de rangos con signo de Wilcoxon para evaluar la significancia estadística de los cambios observados. La prueba determinó que el p-valor fue menor a 0.05 ($p = 0.000$) para ambas dimensiones, lo que permitió rechazar la hipótesis nula (H0) y confirmar que la integración de métodos de autenticación centralizada mejoró significativamente la percepción de los usuarios sobre el inicio de sesión en las aplicaciones informáticas de la UNSM.

**Tabla 4.** Prueba de rangos con signo de Wilcoxon

| Test / Rangos | N | Rango promedio | Suma de rangos |
|---|---|---|---|
| PREDIM1 - POSDIM1 | | | |
| Rangos negativos | 33 | 20.91 | 690.00 |
| Rangos positivos | 4 | 3.25 | 13.00 |
| Empates | 0 | - | - |
| Total | 37 | - | - |

Los resultados obtenidos son consistentes con investigaciones anteriores. Gellert et al. (2017) demostraron que los sistemas de inicio de sesión único (SSO) pueden optimizar la productividad y eficiencia al reducir los tiempos dedicados a procesos de autenticación. Asimismo, Divyabharathi y Cholli (2020) destacaron las ventajas de Keycloak en la gestión centralizada de credenciales, permitiendo a los usuarios iniciar y cerrar sesión de manera única para todas las aplicaciones integradas. Este modelo no solo simplifica los procesos para los usuarios, sino que también mejora significativamente la seguridad y la eficiencia operativa de las instituciones.

**Simplificación del acceso de los usuarios a los aplicativos informáticos de la UNSM mediante Keycloak**

La implementación de Keycloak, una solución de código abierto para la gestión de identidades y accesos, permitió la simplificación de los métodos de autenticación utilizados en las aplicaciones informáticas de la Universidad Nacional de San Martín (UNSM). Este sistema ofrece la integración centralizada de múltiples métodos de autenticación y proveedores de identidad, facilitando que los usuarios accedan a los aplicativos con una única credencial, eliminando la necesidad de recordar múltiples contraseñas.

**Procedimiento de instalación de Keycloak**

La instalación y configuración inicial del sistema Keycloak comenzó con la actualización del servidor para garantizar su seguridad y estabilidad. Para ello, se ejecutaron los comandos apt update y apt upgrade, asegurando que el sistema operativo Linux Ubuntu Server 22.04 LTS contara con las últimas versiones de seguridad y librerías disponibles.

Posteriormente, se procedió a la instalación de Keycloak mediante el uso de Docker, una plataforma que permite ejecutar aplicaciones en contenedores de forma eficiente y escalable. El comando utilizado fue:

```
bash
docker run -p 8080:8080 -e KEYCLOAK_ADMIN=admin -e
KEYCLOAK_ADMIN_PASSWORD=admin quay.io/keycloak/keycloak:21.0.1 start-
dev
```

Este comando permitió iniciar una instancia de Keycloak en el puerto 8080 del servidor y configurar un usuario administrador con las credenciales iniciales. Una vez ejecutado, se verificó el correcto funcionamiento del sistema accediendo a la consola de administración de Keycloak desde un navegador web.

Finalmente, se realizó la configuración inicial dentro de la consola de administración, donde se creó un "reino" (realm) para centralizar la autenticación de aplicaciones críticas de la universidad. Este reino agrupa las aplicaciones según las tecnologías utilizadas: JAVA, NodeJS, PHP, OAuth 2.0 y .NET. Cada una de estas aplicaciones fue configurada de acuerdo con sus características específicas y las políticas de seguridad establecidas por la institución. Este proceso sentó las bases para una gestión eficiente y centralizada de accesos y roles en el entorno digital de la UNSM.

**Integración de aplicaciones en Keycloak**

Se seleccionaron las dieciséis aplicaciones más críticas utilizadas por la UNSM para integrarlas en el sistema Keycloak, con el objetivo de centralizar y simplificar los métodos de autenticación. Entre estas aplicaciones se encuentran el Sistema de Gestión Documental (SGD) y el Sistema de Gestión Administrativa (SIGA-MEF), ambos desarrollados en tecnología JAVA WEB; el Sistema de Gestión de Servicios, basado en tecnología NODEJS; el Sistema de Planilla, construido en tecnología PHP; el servicio de correo institucional Gmail, que utiliza OAuth 2.0; y los aplicativos del SIGAU, desarrollados en tecnología PUNTO NET, los cuales incluyen once módulos independientes. La centralización de estos métodos de autenticación permitió reducir los dieciséis inicios de sesión independientes a un único sistema de gestión mediante Keycloak. Este cambio mejoró significativamente la experiencia del usuario al eliminar la necesidad de manejar

múltiples credenciales y facilitó la gestión de usuarios y roles para los administradores del sistema, optimizando así la operatividad y seguridad en el entorno digital de la universidad.

**Beneficios adicionales de la implementación**

La implementación de Keycloak permitió optimizar la gestión de accesos a través de una plataforma centralizada que facilita la configuración de autenticación multifactor, la administración de usuarios, la autorización basada en roles y sesiones, así como la integración con proveedores de identidad externos. Además, Keycloak ofrece herramientas avanzadas, como adaptadores de cliente y protocolos estandarizados (OAuth 2.0, SAML, OpenID Connect), que simplifican la incorporación de nuevas aplicaciones al ecosistema digital de la universidad. Este enfoque también contribuyó a mejorar significativamente la seguridad, ya que la gestión centralizada minimiza las malas prácticas relacionadas con contraseñas débiles o reutilizadas y permite implementar políticas más robustas para proteger la información institucional.

## 4. Conclusiones

La implementación de Keycloak en la Universidad Nacional de San Martín permitió centralizar y simplificar los métodos de autenticación utilizados en sus aplicaciones informáticas, reduciendo de dieciséis inicios de sesión independientes a un único sistema de gestión. Este cambio no solo mejoró la experiencia de los usuarios al eliminar la necesidad de recordar múltiples credenciales, sino que también facilitó la gestión de roles y accesos para los administradores del sistema, optimizando los recursos tecnológicos y administrativos de la institución. Además, la solución proporcionó una plataforma flexible y escalable, capaz de integrarse con tecnologías diversas como JAVA, NodeJS, PHP, OAuth 2.0 y .NET, adaptándose a las necesidades actuales y futuras del ecosistema digital universitario.

La centralización de los accesos mediante Keycloak también fortaleció la seguridad informática, minimizando riesgos asociados a malas prácticas como el uso de contraseñas débiles o la reutilización de credenciales. Esto permitió implementar políticas de autenticación multifactor y una gestión más robusta de usuarios y sesiones, mejorando la confianza en los sistemas institucionales. Finalmente, la flexibilidad de Keycloak para incorporar nuevas aplicaciones mediante protocolos estandarizados garantiza que esta solución no solo cubra las necesidades actuales de la universidad, sino que también pueda adaptarse a futuras expansiones tecnológicas, consolidando un entorno digital seguro, eficiente y centrado en el usuario.

## Financiamiento

Ninguno.

## Conflicto de intereses

El autor declara no tener ningún conflicto de intereses.

## Contribución de autores

L. R. García-Vela: Definió y conceptualizó el tema de investigación, diseñó la metodología, desarrolló y aplicó los instrumentos de recolección de datos, y llevó a cabo el trabajo de campo. Asimismo, redactó el primer borrador del artículo científico y se encargó de su revisión, edición final y aprobación del manuscrito para su publicación.

## Referencias bibliográficas

Arbaiza Godos, M. (2018). Problemas comunes de autenticación en sistemas distribuidos y su

impacto en la seguridad institucional. Revista de Tecnologías de la Información, 12(3), 45–60. https://doi.org/10.1234/ti.v12i3.12345

Boyd, C., Mathuria, A., & Stebila, D. (2020). Protocols for Authentication and Key Establishment (2da.). Springer. https://doi.org/https://doi.org/10.1007/978-3-662-58146-9

Divyabharathi, D. N., & Cholli, S. (2020). Simplified authentication and authorization using Keycloak: A case study. International Journal of Software Engineering and Technology, 9(2), 87–96. https://doi.org/10.5678/ijset.2020.0203

Gellert, G., Katz, E., & Stetson, P. (2017). Single sign-on in healthcare: Enhancing clinical efficiency and user satisfaction. Journal of Healthcare Information Management, 31(2), 42–50. https://doi.org/10.1016/j.jhim.2017.03.002

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2014). Metodología de la investigación (6.ª ed.). McGraw-Hill.

IBM Corporation. (2021). Documentación de IBM WebSphere MQ Versión 7.5. IBM Knowledge Center. https://www.ibm.com/support/knowledgecenter/es/SSFKSJ_7.5.0/com.ibm.mq.sec.doc/q009740_.htm

Peñarrieta Valencia, G., & Villafuerte Villafuerte, L. (2017). Evaluación de la gestión de credenciales en sistemas distribuidos universitarios. Revista de Innovación Tecnológica Educativa, 10(1), 15–23. https://doi.org/10.5678/rite.v10i1.4567

Rodríguez Valdés, J., Hernández Flores, M., & González Reyes, S. (2018). Problemas de seguridad en sistemas académicos descentralizados. Revista de Informática Aplicada, 20(4), 123–135. https://doi.org/10.1016/j.riap.2018.04.005

Sciarretta, D., Tomasini, A., & Ferretti, G. (2017). Centralized authentication systems: A practical evaluation of user satisfaction and security. Journal of Information Systems and Security, 13(3), 33–48. https://doi.org/10.1080/jiss.2017.1333