



*Comparación de la eficiencia de los sistemas de inicios de sesión único (SSO)
WSO2 Identity Server y CAS en AGROCALIDAD*

*Performance comparison of WSO2 Identity Server and CAS single sign-on (SSO)
systems in AGROCALIDAD*

*Comparaçãõ da eficiênciã dos sistemas single sign-on (SSO) WSO2 Identity
Server e CAS no AGROCALIDAD*

David Alexander Rodríguez-Freire ^I
davidalex786@hotmail.com
<https://orcid.org/0000-0003-2903-8398>

Paúl Xavier Paguay-Soxo ^{II}
ppaguay@esPOCH.edu.ec
<http://orcid.org/0000-0002-0262-9844>

Gladys Lorena Aguirre-Sailema ^{III}
gaguirre@esPOCH.edu.ec
<https://orcid.org/0000-0001-5096-1844>

Jonny Israel Guaiña-Yungán ^{IV}
jguaina@esPOCH.edu.ec
<http://orcid.org/0000-0003-0456-7429>

Pamela Alexandra Buñay Guisñan
pbunay@unach.edu.ec
<http://orcid.org/0000-0002-4320-6899>

Correspondencia: davidalex786@hotmail.com

Ciencias Técnicas y Aplicadas
Artículo de Investigación

***Recibido:** 20 de enero de 2022 ***Aceptado:** 14 de febrero de 2022 * **Publicado:** 02 marzo de 2022

- I. Agencia de Regularización y Control Fito y Zoonosanitario – AGROCALIDAD, Ecuador.
- II. Escuela Superior Politécnica de Chimborazo (ESPOCH) Sede Orellana, Grupo de Investigación INFOSO, Ecuador.
- III. Escuela Superior Politécnica de Chimborazo (ESPOCH), Grupo de Investigación GRIISOFT, Ecuador.
- IV. Escuela Superior Politécnica de Chimborazo (ESPOCH), Ecuador.
- V. Universidad Nacional de Chimborazo, Ecuador.

Resumen

La autenticación y autorización de los servicios informáticos en cualquier organización es el método más básico y se podría considerar la característica mínima de seguridad a tomar en cuenta, en una entidad de cualquier índole el aumento del inventario software junto con la cantidad de credenciales de acceso para cada uno de estos converge en problemas como fatiga de la clave o almacenamientos inadecuados de sus credenciales, incrementando el riesgo de divulgación de contraseñas y posibles accesos no autorizados. Los sistemas de inicio de sesión único (SSO) permiten solucionar este inconveniente al administrar un solo punto de acceso para diferentes aplicativos instalados. En el mercado dos de los más importantes servidores de inicio de sesión son CAS y WSO2 Identity Server, los cuales se han implementado en diferentes tipos de escenarios. Por otro lado, la eficiencia de desempeño es un requerimiento no funcional importante que de acuerdo con varios estándares de calidad del software tiene implícitos subindicadores como tiempos de respuesta, consumo de recursos y capacidad. La presente investigación estableció como escenario de pruebas una simulación del entorno de producción de la institución AGROCALIDAD donde se analizó mediante pruebas de rendimiento utilizando la norma de calidad ISO 25010, el desempeño de cada alternativa. Mediante la aplicación de pruebas estadísticas y análisis multicriterio, los resultados evidencian que CAS obtiene un mejor desempeño que WSO2 Identity Server en la mayoría de los indicadores, a excepción del consumo de recursos donde no se encontró una diferencia significativa.

Palabras clave: Inicio de sesión único; Autenticación; WSO2 Identity Server; CAS

Abstract

Authentication and authorization of IT services in any organization is the most basic method and could be considered the minimum security feature to be taken into account. In an organization of any kind, the increase in software inventory together with the number of access credentials for each of these converges in problems such as key fatigue or inadequate storage of credentials, increasing the risk of password disclosure and possible unauthorized access. Single sign-on (SSO) systems solve this problem by managing a single access point for different installed applications. Two of the most important single sign-on servers are CAS and WSO2 Identity Server, which have been implemented in different types of scenarios. On the other hand, performance efficiency is an important non-functional requirement that according to several software quality standards has

implicit sub-indicators such as response times, resource consumption and capacity. This research established as a test scenario a simulation of the production environment of the AGROCALIDAD institution where the performance of each alternative was analyzed by means of performance tests using the ISO 25010 quality standard. Through the application of statistical tests and multicriteria analysis, the results show that CAS performs is better than WSO2 Identity Server in most of the indicators, with the exception of resource consumption, where no significant difference was found.

Keyword: Single Sign One; Authentication; WSO2 Identity Server; CAS

Resumo

A autenticação e autorização de serviços de informática em qualquer organização é o método mais básico e pode ser considerado o recurso mínimo de segurança a ser levado em conta, em uma entidade de qualquer tipo, o aumento do inventário de software juntamente com o número de credenciais de acesso para cada destes converge em problemas como fadiga de chaves ou armazenamento inadequado de suas credenciais, aumentando o risco de divulgação de senha e possível acesso não autorizado. Os sistemas de logon único (SSO) permitem que você resolva esse problema gerenciando um único ponto de acesso para diferentes aplicativos instalados. No mercado, dois dos servidores de login mais importantes são o CAS e o WSO2 Identity Server, que foram implementados em diferentes tipos de cenários. Por outro lado, a eficiência de desempenho é um importante requisito não funcional que, de acordo com diversos padrões de qualidade de software, possui subindicadores implícitos como tempos de resposta, consumo de recursos e capacidade. A presente investigação estabeleceu como cenário de teste uma simulação do ambiente de produção da instituição AGROCALIDAD onde foi analisado o desempenho de cada alternativa através de testes de desempenho utilizando o padrão de qualidade ISO 25010. Através da aplicação de testes estatísticos e análise multicritério, os resultados mostram que o CAS obtém um desempenho melhor que o WSO2 Identity Server na maioria dos indicadores, exceto no consumo de recursos, onde não foi encontrada diferença significativa.

Palavras-chave: Logon único; Autenticação; Servidor de identidade WSO2; CAS

Introducción

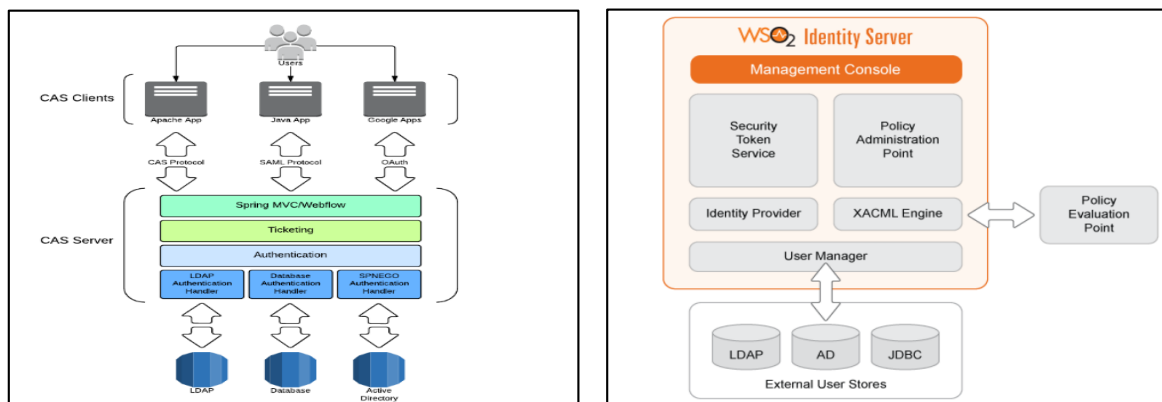
La constante demanda de servicios informáticos y el incremento de sus implementaciones en las organizaciones sean estas de cualquier propósito requieren de la incorporación de un mínimo de seguridad en su estructura.

Para (Carretero et al., 2018), es necesario contar con mecanismos de autenticación de usuarios enfocados a proveer accesos personalizados y confidencialidad de información. Los protocolos de autenticación son la base de cualquier sistema de validación de identidad del usuario del sistema.

Ahora bien, cuando el número de aplicaciones crece, el usuario debe proveer y mantener diferentes credenciales (usuarios/contraseñas) para acceder a cada servicio (Lee & Lai, 2015). Esto podría resultar en otros problemas como la fatiga de la contraseña y conducir a que el usuario opte por apuntar en un lugar no seguro sus claves con lo que puede existir el riesgo de divulgación de la contraseña (Hu et al., 2010).

Según (Han et al., 2020), el inicio de sesión único (SSO) es un mecanismo que permite a un usuario acceder a múltiples servicios utilizando una sola credencial. Las soluciones SSO existentes incluyen OpenID, SAML, y Kerberos, etc. Los sistemas SSO pueden reducir la carga del usuario en el mantenimiento de credenciales de autenticación.

Para (Mainka et al., 2017), SSO es un concepto para delegar la identificación de un usuario final en un proveedor de servicios (SP) a un tercero, el denominado proveedor de identidad (IdP).



Normalizado en 2014.

(Torres & Gonz, n.d.) Señala que con los SSO el usuario ya no se cansa, mejora la productividad y la seguridad informática se ve fortalecida. Mientras que entre las desventajas indica que si el

servidor SSO deja de funcionar se produciría una caída completa de todos los sistemas asociados, por lo tanto, se requiere asumir minuciosamente las medidas necesarias para que se cuente con un sistema tolerante a fallos y de alta disponibilidad.

Existen varias opciones de sistemas SSO en el mercado como: Keycloak, JOSSO (Sign-On abierto de Java solo), Ubuntu Single Sign On, Open AM, Authen2cate, CA SSO (formerly CA Siteminder), CAS / Central Authentication Service, Enterprise SSO, Web Access Manager, WSO2 Identity Server. De entre las opciones antes mencionadas dos de las más utilizadas son CAS y WSO2, los cuales han sido citadas e instaladas como es el caso de (Jenderal et al., 2016) con su implementación de CAS en la Universidad de Bina Darma o en (Fremantle et al., 2014) en su investigación sobre la utilización de WSO2 para autenticación utilizando Internet de las cosas.

CAS

Desarrollado por la Universidad de Yale, CAS (Central Authentication Service) fue desarrollado en 2002 y en conjunto con la Universidad de Rutgers en 2004 se puso a dominio público bajo la supervisión de Jasig, más tarde Apereo (Yale University, 2004). Implementa un servidor de autenticación accesible por W3, compuesto por servlets java, que se ejecuta en cualquier motor de servlet (Tomcat por ejemplo) (Aubry et al., n.d.).

Figura 1: Arquitectura de CAS

WSO2 Identity Server

El Servidor de Identidad de WSO2, es una identidad de código abierto y un servidor de gestión de acceso que soporta una amplia variedad de protocolos de gestión de identidad y acceso, incluyendo OAuth 2.0 y OpenID Connect entre muchos otros.

Figura 2: Arquitectura de WSO2 Identity server

El servidor ofrece una consola basada en la web fácil de usar que permite a los administradores proveer a los usuarios, configurar las aplicaciones OAuth y otras tareas que se necesitaban como parte de esta exploración (Fremantle et al., 2014).

El rendimiento de los sistemas

La incorporación de medidas de seguridad, así como de sistemas de autenticación que permitan mayor productividad requieren de procesamiento adicional para su ejecución, esto conlleva a buscar alternativas que sean eficientes y que permita obtener adecuados tiempos de respuesta con aceptable utilización de recursos.

Un requerimiento no funcional que constituye una prioridad al momento de poner en producción servicios informáticos es la eficiencia de desempeño que según normas de calidad como la ISO 25010 establecen como indicadores al tiempo de respuesta, consumo de recursos y capacidad.

La presente investigación tiene como objetivo comparar el rendimiento de las dos alternativas de servidores SSO, CAS y WSO2 Identity Server aplicado a un entorno de producción que para el experimento se lo ha realizado con la institución Agrocalidad. El resultado obtenido constituye una herramienta para el personal del área informática para decidir la mejor alternativa de aplicación en el control del acceso a los servicios informáticos de la institución donde es prioridad la eficiencia en el desempeño ya sea por contar con infraestructura de bajas prestaciones o a su vez por una alta concurrencia de usuarios.

En la siguiente parte del documento se aborda la metodología utilizada para el experimento de comparación, la cual está basada en la Norma ISO/IEC 25010, posterior se detallan los resultados obtenidos con cada servidor SSO y finalmente se establecen las conclusiones de la investigación.

Metodología

La calidad de una solución informática no únicamente viene definida por el cumplimiento de requerimientos funcionales sino además de requerimientos no funcionales como la seguridad, rendimiento, usabilidad, entre otros. En el siguiente apartado se aborda la metodología utilizada para medir el rendimiento en los servidores SSO motivo del presente estudio.

Pruebas de rendimiento

Las pruebas del sistema son el mecanismo imprescindible si se desea contar con sistemas confiables y estándares de calidad, en ese sentido. las pruebas de rendimiento son una parte del extenso proceso de pruebas como: pruebas unitarias, de integración, de regresión, de campo, beta, etc. (Mera Paz et al., 2017).

Las pruebas de rendimiento tienen que diseñarse para asegurar que el sistema pueda procesar su carga esperada. Al igual que otras pruebas estas deben demostrar que el sistema satisface los requerimientos así como descubrir problemas y defectos del proyecto (Sommerville, 2006).

Las pruebas de rendimiento no se centran en verificar únicamente un requerimiento funcional sino más bien como lo indica (Verona Marcos et al., 2016), estas pruebas tienen un enfoque transversal, ya que una llamada o petición puede involucrar sub llamadas a otras funciones, esto se lo puede interpretar en la figura 3.

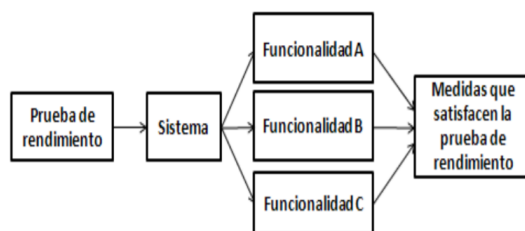


Figura 3: Transversalidad de una prueba de rendimiento

Población y muestra

El experimento se realizó utilizando una simulación del entorno de producción de la institución Agrocalidad que cuenta con varios sistemas informáticos y en su planta laboral participan un total de 1200 empleados que tienen el rol de usuarios repartidos en las diferentes direcciones y coordinaciones a lo largo del país.

Utilizando la fórmula del tamaño de la muestra se calculó el número de usuarios con los que se realizará el experimento, con una confianza del 95% y un error del 5%. Dando un total de 292 usuarios.

$$n = \frac{N * Z\alpha^2 * p * q}{d^2 * (N - 1) + Z\alpha^2 * p * q} \quad (1)$$

Donde:

n= Tamaño de la muestra

N = Tamaño de la población 1200

Zα2 = seguridad del 95% 1.962

p = proporción esperada (5%) 0,05

q = 1 –p (en este caso 1-0,05) 0.95

d = precisión (3%) 0.03

$$n = \frac{1200 * 1,96^2 * 0,05 * 0,95}{0,03^2 * (1200 - 1) + 1,96^2 * 0,05 * 0,95}$$

Tamaño de la muestra = n = 292

Norma ISO/IEC 25010

El modelo de calidad representa la piedra angular en torno a la cual se establece el sistema para la evaluación de la calidad del producto.

La norma ISO 25010 provee un marco de referencia para medir la calidad del producto software y describe 8 características y 38 subcaracterísticas de calidad de producto software (Pardo & Pino, 2009).

En este modelo se determinan los atributos de calidad que se van a tener en cuenta a la hora de evaluar las propiedades de un producto software determinado. Una característica es la eficiencia de desempeño que determina la cantidad de recursos utilizados bajo determinadas condiciones que se subdivide en:

- Comportamiento temporal,
- Utilización de recursos y
- Capacidad.

A continuación, se abordará cada una:

Comportamiento temporal

Para varios autores este indicador es de lo más importantes como es el caso de (Diaz et al., 2012) que aclara que en lo referente a los sitios web el tiempo está correlacionado con la velocidad del sistema y cita además a Jakob Nielsen considerado el padre de la usabilidad, quien señala que existen tres límites importantes en el tiempo de respuesta:

- 0,1 segundo: límite de tiempo en el que el usuario siente que esta “manipulando” los objetos de la interfaz de usuario.
- 1 segundo: límite en el cual el usuario siente que está navegando adecuadamente sin percibir que el sistema es lento.
- 10 segundos: límite en el cual el usuario pierde la atención. Si la respuesta toma más de este tiempo el usuario deberá contar con la opción de cancelar la tarea.

Por lo tanto, contar con unos adecuados tiempos de respuesta, repercutirá en otro parámetro de calidad como la usabilidad, muy importante para esperar una aceptación del sistema por parte del usuario.

Utilización de recursos

En todo proyecto donde se involucre a la informática sin duda se piensa en la instalación de servidores que puedan alojar a los diferentes servicios. En ese sentido se debe estimar el costo de la inversión para este importante requerimiento.

Pero ¿Cómo estimar?, nuevamente viene a la palestra las pruebas de rendimiento en las cuales se estima con una cantidad de usuarios esperados o con diferentes cargas de trabajo, simulando entornos de funcionamientos reales. Mientras más recursos requieran un aplicativo esto se traducirá en mayor inversión de equipo hardware.

En la norma ISO, el indicador de utilización de recursos se enfoca a analizar, las cantidades y tipos de recursos utilizados cuando el software lleva a cabo su función bajo condiciones determinadas.

Capacidad

Según la ISO este indicador se enmarca en el “grado en que los límites máximos de un parámetro de un producto o sistema software cumplen con los requisitos” (ISO, n.d.).

En este experimento la herramienta con la que se llevará a cabo las pruebas entrega el resultado del número de errores que se generan al ejecutar la carga de peticiones, con lo cual se estima este indicador.

Herramientas

Las herramientas para demostrar el rendimiento de los sistemas de autenticación (SSO) CAS y WSO2 IDENTITY SERVER son:

- Software de test JMeter
- Monitor del sistema operativo Linux (TOP)
- Software estadístico SPSS
- Software de evaluación multicriterio NAIADE

Equipos y software

Los escenarios para las pruebas se realizaron utilizando virtualización cuyo equipo anfitrión contaba con las siguientes características hardware:

- Laptop Toshiba C45-C4205K
- Procesador: Intel Core i5-5200U @ 2.20 GHz (4 CPUs)
- Memoria: 12 GB RAM

Las características software del equipo anfitrión son:

- Sistema Operativo: Windows 10 Enterprise 64 bits
- JDK 1.8-221
- JMeter 5.1.1
- Oracle Virtual Box 6.0.8
- Putty, Filezilla

En la figura 3, se observa los servidores virtualizados en el equipo anfitrión:

- 1 servidor de base de datos
- 2 servidores SSO:
 - 1 CAS
 - 1 WSO2
- 1 servidor web con dos aplicaciones conectadas al servidor SSO CAS
- 1 servidor web con dos aplicaciones conectadas a servidor SSO WSO2 Identity Server.
- 1 PC cliente para pruebas de rendimiento

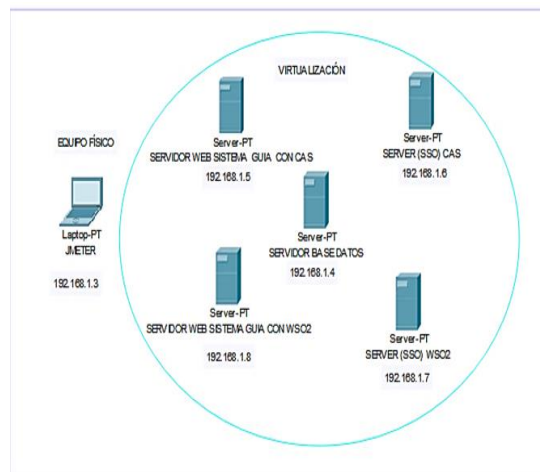


Figura 3: Infraestructura virtualizada

Escenario:

Las conexiones del escenario implementado con cada servidor SSO está conformado por el servidor SSO (WSO2 Identity Server y CAS), un servidor web que cuenta con dos servicios web y que están conectados al servidor SSO por último se tiene una PC cliente que mediante la

utilización del software JMeter realiza las peticiones concurrentes, todo este esquema se observa en la figura 4.

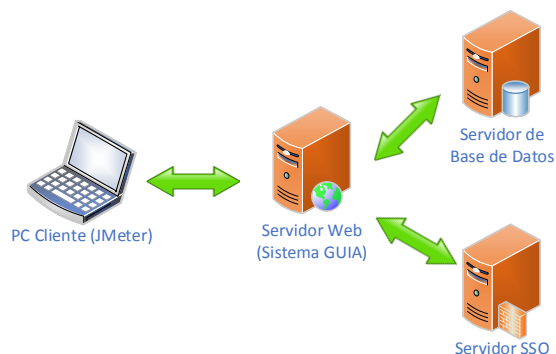


Figura 4: Escenario de pruebas con cada servidor SSO

El hardware virtualizado en cada escenario se estableció con las mismas características las cuales se detallan en tabla 1.

Tabla 1: Características hardware virtualizado para los escenarios configurados con cada SSO (CAS y WSO2 Identity Server)

<i>Descripción</i>	<i>Características</i>
Servidor Web GUIA	Memoria RAM: 1447MB Disco Duro: 40 GB Procesador: 1
Servidor SSO	Memoria RAM: 1447MB Disco Duro: 40 GB Procesador: 1
Servidor de base de datos	Memoria RAM: 1447MB Disco Duro: 40 GB Procesador: 1

El software utilizado en las máquinas virtuales de cada escenario fue el que se muestra en la tabla 2:

Tabla 2: Características software para los escenarios configurados con cada SSO (CAS y WSO2 Identity Server)

<i>Software</i>	<i>Característica / Versión</i>
Servidor SSO	SSO CAS 4.0, SSO WSO2 IDENTITY SERVER 5.3.0
Sistema operativo	CentOS 7
Java	Java 1.8.0_151
Servidor WEB	Httpd 2.4.6
Servidor Base de datos	PostgreSQL 9.6.15
Librerías de monitoreo	ServerAgent-2.2.3
Conexión remota	ssh

Plan de pruebas

En Agrocalidad se cuenta con un sistema informático que provee los servicios informáticos a la institución, se publicó dos sistemas GUIA en el servidor web que se conectan a cada servidor SSO. Con este sistema se creó un “trabajo programado” que consta de varias “tareas”, que a su vez mediante la creación de hilos de procesamiento (subprocesos), estos se enviarán en lotes simulando de esta manera el acceso concurrente de usuarios en un sistema de producción, de igual manera se puede simular escenarios de concurrencia máxima y promedio.

Trabajo Programado

El trabajo programado constó de varias tareas realizadas en el sistema GUIA registrado y almacenado la herramienta JMeter. Estas tareas fueron:

1. Ingresar al sistema (GUIA)
2. Autenticación en el sistema
3. Ingresar a varias páginas del sistema GUIA, obteniendo información (3 páginas)
4. Terminar sesión y salir del sistema

Una vez registrada toda la secuencia de tareas se procede a replicar las mismas con lo cual se simula accesos concurrentes al sistema.

Simulación con JMeter

Jmeter es una herramienta open source muy completa, implementada en Java que permite realizar test de comportamiento funcional y medir el rendimiento de sistemas informáticos. También se puede utilizar para realizar pruebas de estrés, por ejemplo, en un servidor, y poner a prueba su rendimiento (Diaz et al., 2012).

Utilizando esta herramienta se construyó el “trabajo programado” que constó de 6 pasos lo que resulta en 6 peticiones al servidor web (http request).

Utilizando la muestra obtenida con la fórmula (1) correspondiente a 292 usuarios se creó esa cantidad de hilos de procesamiento (subprocesos), lo cual luego de multiplicar por la cantidad de peticiones se obtiene un total de 1752 peticiones concurrentes.

El envío de este lote de peticiones del trabajo programado, se lo realizó en tres momentos en un día normal escogido por el investigador.

Resultados y Discusión

En el siguiente apartado se detallan los resultados obtenidos de las pruebas realizadas con la muestra, escenarios y plan de pruebas establecido.

Antes de proceder con las pruebas de contraste se analizó la normalidad de los datos arrojados por parte del software JMeter, para lo cual se utilizó la prueba estadística de Kolmogorov-Smirnov recomendada para conjuntos de datos mayores a 30 con cada uno de los indicadores, lo que evidenció, que los datos no seguían una distribución normal.

Con este resultado se procedió a realizar las pruebas de contraste utilizando la prueba no paramétrica U de Mann-Whitnev con el cual se comprobó que en todos los casos existe una diferencia significativa entre los dos sistemas servidores SSO.

A continuación, se muestra las gráficas comparativas de las medias estadísticas halladas en cada indicador.

Tiempo de respuesta

Se evidencia en la figura 5, que el sistema WSO2 Identity Server necesita más tiempo de procesamiento para obtener el resultado de la tarea, por lo tanto, CAS ofrece un mejor tiempo de respuesta.

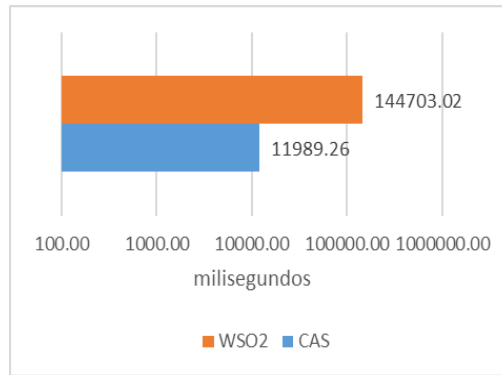


Figura 5: Medias estadísticas del tiempo de respuesta

Consumo de CPU

La figura 6 muestra los resultados correspondientes al consumo de recursos, en esta se evidencia que WSO2 consume menor porcentaje de CPU al procesar los trabajos programados

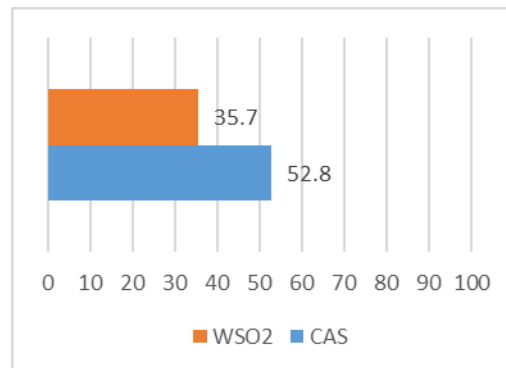


Figura 6: Medias estadísticas del consumo de CPU

Consumo de RAM

Con respecto al indicador de consumo de memoria RAM, la figura 7 demuestra que CAS requiere menos recurso RAM para ejecutar el mismo trabajo programado.

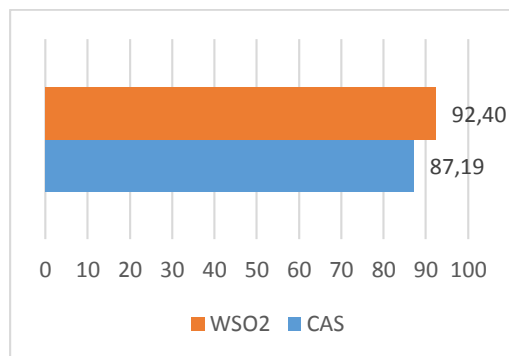


Figura 7: Medias estadísticas del consumo de CPU

Los resultados obtenidos en los indicadores de consumo de recursos evidencian que ambos servidores muestran una ventaja en un indicador y desventaja en otro, por lo que se puede considerar que existiría un empate en el parámetro “consumo de recursos” de la ISO 25010.

Capacidad

Para este indicador se contabilizó el error que arroja el sistema JMeter correspondiente a la carga de los lotes de procesamiento, evidenciado que el sistema CAS presentó un menor porcentaje de error de carga de lotes.

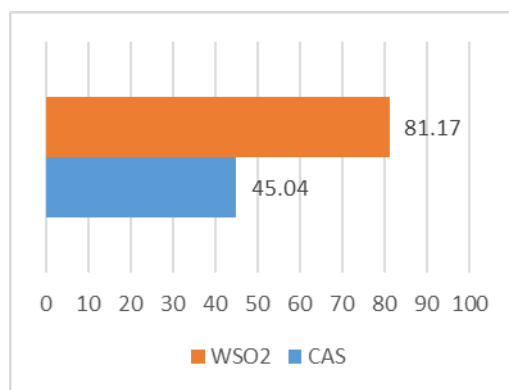


Figura 8: Medias estadísticas de la capacidad

Análisis multicriterio

Hasta este punto anterior, se puede evidenciar las fortalezas que cada sistema presenta en los diferentes indicadores analizados, adicionalmente se realiza un análisis multicriterio con el fin de aplicando conceptos de operación de procesos y técnicas de maximización y minimización de

funciones objetivo se procedió en primer lugar a construir la matriz de impacto la cual se observa en la tabla 3, en la cual se observan los cuatro indicadores utilizados en la presente investigación, la unidad de medida utilizada, el objetivo del indicador (maximizar / minimizar) y las medias estadísticas encontradas en cada indicador. En este caso los cuatro indicadores, las funciones objetivo corresponden minimizar ya que mientras menor valor tengan será mejor.

Tabla 3. Matriz de impacto de indicadores del rendimiento

<i>Dimensio nes y Variables</i>	<i>Unida d de medid a</i>	<i>Ob jeti vo</i>	<i>CAS</i>	<i>WSO 2</i>
Tiempo de respuesta	ms	Mí n.	1198 9	14470 3
Consumo de recurso (CPU)	%	Mí n.	53	36
Consumo de recurso (RAM)	%	Mí n.	87	92
Capacida d	%	Mí n.	45	81

Utilizando el software de NAIADE, estableciendo un alfa por defecto (α) de 0,5; el sistema arroja un valor de ranking (Φ^+) de 0.92, lo que corresponde a la opción del servidor SSO CAS un mejor resultado en comparación con WSO2, de acuerdo a los criterios y valores establecidos.

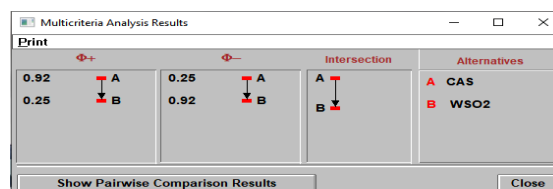


Figura 9: Prueba de multicriterio con el software NAIADE

Conclusiones

Los resultados obtenidos con cada uno de los indicadores de rendimiento establecidos se evidenció que en cuanto al tiempo de respuesta que para varios autores es el más importante CAS requiere menos tiempo para completar la tarea de autenticación lo que constituye mayor rapidez de todo el sistema, en cuanto al consumo de recursos WSO2 obtiene un mejor porcentaje de CPU al requerir menos uso del mismo si embargo en cuanto al porcentaje de uso de memoria RAM, CAS obtiene un mejor resultado, por lo tanto se podría considerar que no existe una diferencia en cuanto a este indicador (Consumo de recursos). Para el indicador de capacidad el mismo que tiene relación con el porcentaje de errores de cada lote cargado para la prueba, CAS nuevamente vuelve a obtener un mejor resultado siendo un 36,13% mejor.

Con el fin únicamente de obtener un resultado consolidado se optó por realizar un análisis multicriterio utilizando el software NAIADE que aplica algoritmos de análisis operacional con el que se obtuvo que con un 92% CAS ofrece mejores prestaciones con los indicadores establecidos. En un entorno en producción los analistas informáticos deben decidir por soluciones que se encuentran en el mercado ya sea de software libre o propietario siendo varios de los requerimientos no funcionales un criterio para seleccionar una u otra opción.

A futuro se recomienda analizar otros indicadores de calidad como usabilidad, seguridad, etc., los cuales en otros escenarios pueden constituir una mayor prioridad.

Conflicto de Interés

Los autores no presentan ningún conflicto de interés ya que la presente investigación ha sido el resultado de un trabajo de titulación de maestría de autoría de los mismos autores del presente trabajo.

Agradecimiento Acknowledgment

Un agradecimiento a la institución AGROCALIDAD donde se realizaron las pruebas correspondientes, simulando un escenario de pruebas lo más cercano a un ambiente en producción.

Referencias

1. Aubry, P., Mathieu, V., & Marchal, J. (n.d.). *ESUP-Portail : open source Single Sign-On*

- with CAS (Central Authentication Service).
2. Carretero, J., Izquierdo-Moreno, G., Vasile-Cabezas, M., & Garcia-Blas, J. (2018). Federated identity architecture of the European eID System. *IEEE Access*, 6, 75302–75326. <https://doi.org/10.1109/ACCESS.2018.2882870>
 3. Diaz, F. J., Banchoff, C. M. T., & Soria, V. (2012). *Usando Jmeter para pruebas de rendimiento*. January, 1–14.
 4. Fremantle, P., Aziz, B., & Kopeck, J. (2014). *Federated Identity and Access Management for the Internet of Things*. 10–17. <https://doi.org/10.1109/SIoT.2014.8>
 5. Han, J., Chen, L., Schneider, S., Treharne, H., Wesemeyer, S., & Wilson, N. (2020). Anonymous Single Sign-On With Proxy Re-Verification. *IEEE Transactions on Information Forensics and Security*, 15(1), 223–236. <https://doi.org/10.1109/TIFS.2019.2919926>
 6. Hu, J., Sun, Q., & Chen, H. (2010). *APPLICATION OF SINGLE SIGN-ON (SSO) IN*. 725–727.
 7. ISO. (n.d.). *ISO/IEC 25010*. <https://iso25000.com/index.php/normas-iso-25000/iso-25010>
 8. Jenderal, J., Yani, A., & Palembang, N. (2016). *ANALISIS TEKNOLOGI SINGLE SIGN ON (SSO) DENGAN PENERAPAN CENTRAL AUTHENTICATION SERVICE (CAS) PADA UNIVERSITAS BINA*. 2013.
 9. Lee, C. C., & Lai, Y. M. (2015). Toward a secure single sign-on mechanism for distributed computer networks. *Computer Journal*, 58(4), 934–943. <https://doi.org/10.1093/comjnl/bxu014>
 10. Mainka, C., Mladenov, V., Schwenk, J., & Wich, T. (2017). SoK: Single Sign-On Security - An Evaluation of OpenID Connect. *Proceedings - 2nd IEEE European Symposium on Security and Privacy, EuroS and P 2017*, 251–266. <https://doi.org/10.1109/EuroSP.2017.32>
 11. Mera Paz, J., Miranda Gómez, M. Y., & Cuaran Rosas, S. (2017). Análisis sistemático de información de la Norma ISO 25010 como base para la implementación en un laboratorio de Testing de software en la Universidad Cooperativa de Colombia Sede Popayán. *Memorias de Congresos UTP*, 149–154. <https://revistas.utp.ac.pa/index.php/memoutp/article/view/1483%0Ahttp://revistas.utp.ac.pa/index.php/memoutp/article/view/1483>

12. Pardo, C., & Pino, F. J. (2009). Analizando el apoyo de marcos SPI a las características de calidad del producto ISO 25010. *REICIS. Revista Española de Innovación, Calidad e Ingeniería Del Software*, 5(2), 6–16.
13. Sommerville, I. (2006). *Ingeniería de Software*. Pearson Education.
14. Torres, G., & Gonz, A. (n.d.). *Implantación de un sso*.
15. Verona Marcos, S., Pérez Díaz, Y., Torres Pérez, L., Delgado Dapena, M., & Yáñez Márquez, C. (2016). Pruebas de rendimiento a componentes de software utilizando programación orientada a aspectos. *Ingeniería Industrial*, 37(3), 278–285.
16. Yale University. (2004). *CAS - Central Authentication Service*.
<https://developers.yale.edu/cas-central-authentication-service>