ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

RENDIMIENTO DE LOS SISTEMAS DE AUTENTICACIÓN SINGLE SIGN ONE (SSO) WSO2 IDENTITY SERVER Y CAS EN AGROCALIDAD.

DAVID ALEXANDER RODRÍGUEZ FREIRE

Trabajo de Titulación modalidad: Proyectos de Investigación y Desarrollo, presentado ante el Instituto de Posgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de:

MAGÍSTER EN INTERCONECTIVIDAD DE REDES

Riobamba - Ecuador

Diciembre - 2019

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

CERTIFICACIÓN:

EL TRIBUNAL DE TRABAJO DE TITULACIÓN CERTIFICA QUE:

El Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, titulado **"RENDIMIENTO DE LOS SISTEMAS DE AUTENTICACIÓN SINGLE SIGN ONE (SSO) WSO2 IDENTITY SERVER Y CAS EN AGROCALIDAD "**, de responsabilidad del señor David Alexander Rodríguez Freire, ha sido prolijamente revisado y se autoriza su presentación.

Tribunal:

Ing. Raúl Marcelo Lozada Yánez; M.Sc.
PRESIDENTE

Ing. Paúl Xavier Paguay Soxo; M.Sc.
DIRECTOR

Ing. Gladys Lorena Aguirre Sailema; M.Sc.
MIEMBRO

Ing. Jonny Israel Guaiña Yungan; M.Sc.
MIEMBRO

Riobamba – diciembre 2019

DERECHOS INTELECTUALES

Yo, David Alexander Rodríguez Freire, declaro que soy responsable de las ideas, doctrinas y resultados expuestos en el Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, y que el patrimonio intelectual generado por la misma pertenece exclusivamente a la Escuela Superior Politécnica de Chimborazo.

David Alexander Rodríguez Freire

No. Cédula: 0201798907

DECLARACIÓN DE AUTENTICIDAD

Yo, **David Alexander Rodríguez Freire**, con cédula de identidad 0201798907, declaro que el presente proyecto de investigación, es de mi autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otras fuentes están debidamente referenciados

Como autor, asumo, la responsabilidad legal y académica de los contenidos de este trabajo de titulación de Maestría

David Alexander Rodríguez Freire
No. Cédula: 0201798907

DEDICATORIA

Dedico este trabajo de titulación a mi familia quienes han sido un pilar fundamental para buscar mi superación personal. A mis padres por haberme dado la vida, a mis hermanos(as), a mi esposa y mis hijos.

David

AGRADECIMIENTOS

Quiero expresar un sincero y profundo agradecimiento a la Escuela Superior Politécnica de Chimborazo, a mi tutor Ing. Mgs. Paúl Paguay Soxo por impartirme sus conocimientos en la elaboración de la investigación, a los miembros del tribunal de la tesis quienes supieron brindarme sus sabios concejos y la guía oportuna. A todas aquellas personas que han contribuido indirecta o directamente en este estudio, agradecer por sus valiosos comentarios, opiniones en el proceso de realización de este proyecto.

CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

RESUMEN

El objetivo de esta investigación fue realizar un análisis del rendimiento de los sistemas de autenticación SSO CAS y WSO2 Identity server, basados en plataformas Open Source analizando indicadores como: tiempo de respuesta, consumo de recursos (RAM, CPU) y capacidad, con una muestra de 292 usuarios, se creó un ambiente de test virtualizado en donde se simulo: servidor de base de datos, servidor de web con las misma configuraciones del ambiente de producción , se simularon los servidores para los sistemas de autenticación CAS y WSO2 Identity server. Se creo un plan de pruebas para el Sistema de autenticación centralizado (CAS) y WSO2 que se ejecutó mediante el software de test JMeter el cual simulo el acceso a cada sistema de autenticación con la muestra establecida de 292 usuarios, paralelo a cada plan se ejecutó el comando TOP para llevar una bitácora del consumo de recursos (RAM, CPU); los datos recopilados se los analizó con el software estadístico SPSS obteniendo los siguientes resultados: "Tiempo de Respuesta" existe una diferencia de 132.713,76 (milisegundos) a favor de CAS, "Consumo recurso CPU" existe una diferencia porcentual 17,1 % a favor de WSO2, "Consumo recurso RAM" existe una diferencia porcentual de 5,21 % a favor CAS y "Capacidad" existe una diferencia porcentual 36,13 % a favor de CAS. Finalmente aplicando el análisis multicriterio con el método de NAIADE se obtiene un ranking positivo de 0,92 a favor del sistema de autenticación CAS, por consecuencia se acepta la hipótesis alternativa y se rechaza la nula. Por cual se recomienda la implementación de sistema de autenticación CAS considerando los pasos descritos en el manual de buenas prácticas de los sistemas de autenticación único.

Palabras clave: <TECNOLOGÍA Y CIENCIAS DE LA INGENIERÍA>, <REDES>, <SISTEMAS DE AUTENTICACIÓN (SSO)>, <SISTEMA DE AUTENTICACIÓN CENTRALIZADO (CAS)>, <IDENTITY SERVER (WSO2)>, <RENDIMIENTO>, <MÉTODO DE CALIDAD DE SOFTWARE (FURPS)>, <NOVEL APPROACH TO IMPRECISE ASSEEMENT AND DECISIÓN ENVIROMENTS (NAIADE)>, <NORMA ISO/IEC 25010 >

ABSTRACT

The objective of this research work was to perform an analysis of the performance of the SSO CAS and WSO2 Identity server authentication systems, based on Open Source platforms analyzing indicators such as: response time, resource consumption (RAM, CPU) and capacity, with a sample of 292 users, a virtualized test environment was created where it was simulated: database server, web server with the same settings of the production environment, the servers for the CAS authentication systems and WSO2 Identity server were simulated. A test plan was created for the Centralized Authentication System (CAS) and WSO2 that was executed through the JMeter test software which simulated access to each authentication system with the established sample of 292 users, parallel to each plan was executed the TOP command to keep a log of resource consumption (RAM, CPU); The data collected was analyzed with the SPSS statistical software, obtaining the following results: "Response Time" there is a difference of 132,713.76 (milliseconds) in favor of CAS, "CPU resource consumption" there is a percentage difference 17.1% a In favor of WSO2, "RAM resource consumption" there is a percentage difference of 5.21% in favor of CAS and "Capacity" there is a percentage difference of 36.13% in favor of CAS. Finally, applying the multi-criteria analysis with the NAIADE method, a positive ranking of 0.92 is obtained in favor of the CAS authentication system, therefore the alternative hypothesis is accepted and the null is rejected. By which the implementation of CAS authentication system is recommended considering the steps described in the manual of best practices of single authentication systems.

Palabras clave: <TECNOLOGÍA Y CIENCIAS DE LA INGENIERÍA>, <REDES>, <SISTEMAS DE AUTENTICACIÓN (SSO)>, <SISTEMA DE AUTENTICACIÓN CENTRALIZADO (CAS)>, <IDENTITY SERVER (WSO2)>, <RENDIMIENTO>, <MÉTODO DE CALIDAD DE SOFTWARE (FURPS)>, <NOVEL APPROACH TO IMPRECISE ASSEEMENT AND DECISIÓN ENVIROMENTS (NAIADE)>, <NORMA ISO/IEC 25010 >

CAPÍTULO I

1 INTRODUCCIÓN

La globalización de la economía ha exigido que las empresas se actualicen constantemente e implementen plataformas tecnológicas que soporten una nueva forma de hacer negocios. El uso de Internet para este fin, conlleva a que se desarrollen proyectos de seguridad informática sin que esto conlleve a un declive en el rendimiento cuando el sistema se encuentre en producción. (Servicio Ecuatoriano de Normalizacion, 2003)

La seguridad informática concierne a la integridad, confidencialidad y disponibilidad de la información que se encuentra en la computadora o en una red de ellas, como también a la protección del acceso a todos los recursos del sistema (Baldeón, 2012).

Según Daniel Molina (legislacion Informática, 2016), experto de la empresa Kaspersky, en el Ecuador, las cifras de ataques cibernéticos podrían ir en aumento debido al crecimiento económico del país, que lo convierte en un blanco interesante para los ataques cibernéticos. *"Hay hackers que atacan desde Perú, Colombia o Europa occidental a los bancos ecuatorianos, lo que antes no sucedía, pues se trata es un delito importado"*, así también se afirma que la provincia de Pichincha es la que más registra este tipo de delitos, muy por encima de Guayas y del resto del país.

El inicio de sesión único (SSO) permite a un usuario usar un conjunto de credenciales de inicio de sesión (por ejemplo, nombre y contraseña) para acceder a múltiples aplicaciones. El servicio autentica al usuario final para todas las aplicaciones a las que el usuario tiene derechos y elimina otras solicitudes cuando el usuario cambia de aplicación durante la misma sesión reduciendo el tiempo de acceso. (UCO, 2010)

Entre los SSO que se encuentran en el mercado son los siguientes:

- Ubuntu Single Sign On
- IBM Enterprise Identity Mapping

- Active Directory Federation Services
- Authen2cate
- CA SSO (formerly CA Siteminder)
- CAS / Central Authentication Service
- Enterprise SSO, Web Access Manager
- WSO2 Identity Server
- Oracle Identity Management

Luego de una búsqueda bibliográfica y la utilización de la técnica de benchmarking, se comparó los diferentes sistemas SSO disponibles en el mercado, para lo cual de acuerdo a las necesidades de AGROCALIDAD se establecieron los siguientes criterios:

- Licencia: Free & Open Source (Apache 2.0) de libre distribución
- Protocolos: (SAML2, OAuth2, SCIM, OpenID y WS-Fed),
- Plataforma: (PHP, Java, .NET).
- Database: (JDBC, LDAP)

Una vez tabulada la información se evidencio que las dos alternativas más factibles para la implementación en la institución fueron WSO2 Identity Server (WSO2, 2019) y CAS (UNICON, 2019), como se observa en la tabla 1-1.

Tabla 1-1: Comparativa de SSO en base a los criterios de AGROCALIDAD.

SSO / **Criterio**	**CAS**	**Ubuntu Single Sign On**	**Enterprise SSO, Web Access Manager**	**WSO2 Identity server**	**SimplesamlPHP**
Licencia					
• Open source	X	X		X	X
Plataforma					
• PHP	X			X	X
• Java	X		X	X	
• .Net	X			X	
Protocolo					
• SAML	X		X	X	X
• OpenID	X	X		X	X

• OAuth2	X			X	X
Database					
• LDAP	X	X	X	X	
• JDBC	X			X	X
Total	**9**	**3**	**3**	**9**	**6**

Realizado por: David Rodríguez. 2019

Una vez determinado los sistemas más factibles, se hace necesario el analizar la mejor alternativa en cuanto a rendimiento (tiempo de respuesta, velocidad de procesamiento, consumo de recursos (RAM-CPU)), ya que el mismo repercute en la experiencia de usuario, debido a que una aplicación que tenga retardos muy amplios y que consuma muchos recursos puede provocar en algunas ocasiones que se deje de utilizar (Microsoft, 2016), o a su vez requiera de mayores capacidades de los servidores, repercutiendo en los costos de instalación y operación. Por tal motivo en este punto se plantea la pregunta ¿Cuál de los sistemas WSO2 Identity Server o CAS es más eficiente para la implementación de un sistema de autenticación en una organización?

AGROCALIDAD es una institución pública adscrita al Ministerio de Agricultura y Ganadería, que en sus facultades de Autoridad Fito zoosanitaria Nacional es la encargada de la definición y ejecución de políticas de control y regulación para la protección y el mejoramiento de la sanidad animal, sanidad vegetal e inocuidad alimentaria, dispone de una área denominada Dirección de Tecnología de Información y Comunicaciones (DTIC´S), cuya función principal corresponde a manejar sistemas que contribuyan a regular y mejorar los procedimientos relacionados con las funciones señaladas. (Agencia de regulación y control fito y zoosanitario, 2019)

Es importante recalcar que la información que maneja es absolutamente delicada y de alta confidencialidad; motivo por el cual se debe mejorar el acceso a esta información, en especial aplicando un sistema de autenticación de usuarios que ofrezca un funcionamiento eficaz.

El presente trabajo tiene por objetivo el análisis de la comparativa del rendimiento de los sistemas de autentificación single sign one (SSO); CAS y WSO2 Identity Server en AGROCALIDAD para determinar cual ofrece un mejor beneficio para la Institución por su calidad superior tanto en: tiempo de respuesta, consumo de recursos y capacidad; la estructura del presente trabajo de titulación está dividida en **CINCO** capítulos:

CAPÍTULO I: La introducción describe el planteamiento del problema y formulación del mismo con sus respectivas preguntas directrices y justificación de la investigación. Además del objetivo específico a alcanzar y objetivos generales con su respectiva hipótesis.

CAPÍTULO II: En este capítulo encontramos el marco referencial que comienza con la descripción del antecedente del problema el porqué del presente proyecto de investigación así como su respectivo marco teórico que recaba información sobre los sistemas de autentificación con clave única, definición, antecedentes de SSO, características y los diferentes sistemas SSO como: Open ID, OAuth, WSO2 Identity Server, CAS, comparativa entre los sistemas SSO antes descritos y por qué se realizó el presente estudio entre WSO2 Identity Server y CAS, los intrusos informáticos, seguridad informática, tipos de ataques presenta la información y herramientas para medir la carga y rendimiento en páginas web.

CAPÍTULO III: Detalla el diseño de la investigación, en este apartado se expone el tipo de diseño del estudio, métodos utilizados, como está enfocada la investigación, la población de estudio, como se seleccionó la muestra, recolección e instrumentos para procesar los datos. Variables, análisis, procesamiento de datos, formulas, herramientas, hardware cliente/ servidor y el software utilizado.

CAPÍTULO IV: En este capítulo se analizan los resultados obtenidos en la investigación y se discuten los mismos como el tiempo de respuesta, consumo de recursos y capacidad, además de la comprobación de la hipótesis.

CAPÍTULO V: Propuesta del proyecto.

1.1 Planteamiento del Problema.

El proceso de autenticación de los sistemas informáticos constituye una parte fundamental de la gestión de la seguridad informática de una organización. Uno de los principales inconvenientes del proceso de autenticación en las organizaciones es que al incrementarse el inventario de sistemas informáticos la cantidad de cuentas de acceso para cada usuario se incrementa de forma de forma proporcional, lo cual a su vez provoca otros problemas como: la utilización de recursos en los sistemas, dificultad en la administración de cuentas de usuario, dificultad en la recuperación de claves de acceso, repetición del proceso de loguearse para acceder a múltiples aplicaciones. (Consumoteca, 2009)

El inicio de sesión único (SSO) es un servicio de autenticación y sesión que permite a un usuario manejar un conjunto de credenciales de autenticación (por ejemplo, nombre y contraseña) para

acceder a múltiples aplicaciones. El servicio valida al usuario final su identidad para todas las aplicaciones a las que tiene derechos y elimina otras solicitudes cuando se cambia de aplicación durante la misma sesión. (Teravainen, 2019)

De entre las opciones en el mercado de sistemas SSO (Seguridad America, 2018), es importante analizar la mejor alternativa en cuanto a rendimiento del sistema para realizar el proceso de autenticación, ya que el mismo repercute en la experiencia de usuario, como lo indica (Microsoft, 2016) *"una aplicación que tenga retardos muy amplios y que consuma muchos recursos puede provocar en algunas ocasiones que se deje de utilizar, así como el incremento en los costos de capacidades de hardware".*

AGROCALIDAD dispone de un área denominada Dirección de Tecnología de Información y Comunicaciones (DTIC´S), cuya función principal corresponde a manejar sistemas que contribuyan a regular y mejorar los procedimientos relacionados con las funciones señaladas por la organización. Dentro de la organización existen cinco sistemas informáticos (GUIA, Zimbra, GLPI, SIZSE, SIFAE) a los que acceden aproximadamente 1200 usuarios, lo que ha generado la necesidad de implementar una solución informática para la centralización de la autenticación en los aplicativos, motivo por el cual se hace necesario realizar la comparativa del rendimiento de los sistemas CAS (UNICON, 2019) y SSO WSO2 Identity Server (WSO, 2019) , basado este análisis en métricas de calidad ya conocidos como el modelo de FURPS (1987) que establece indicadores como: tiempo de respuesta, velocidad de procesamiento, consumo de recursos y eficacia. (Pereira, Ayaach, Quintero, & Granadillo, 2019) y el modelo de calidad ISO/IEC 25010 que establece en eficiencia de desempeño indicadores como: comportamiento temporal, utilización de recursos, capacidad. (ISO, 2019)

1.2 Formulación del problema

¿Cuál de los sistemas de autenticación Single Sign One (SSO) CAS (sistema de autenticación central) y WSO2 Identity Server ofrece mejor rendimiento del proceso de autenticación de usuarios para los aplicativos de AGROCALIDAD (Agencia de regulación y control fito y zoosanitario)?

1.3 Sistematización del problema

- ¿Qué características tienen y cuál es el funcionamiento de los sistemas SSO CAS y WSO2 Identity Server?

- ¿Cuáles son los parámetros y herramientas de evaluación de rendimiento en los sistemas SSO CAS y WSO2 Identity Server?
- ¿Cuál es el rendimiento de los sistemas de autenticación SSO CAS Y WSO2 Identity Server para los aplicativos de AGROCALIDAD (Agencia de regulación y control fito y zoosanitario)?
- ¿Cuál es la propuesta de implantación de un SSO en AGROCALIDAD (Agencia de regulación y control fito y zoosanitario)?

1.4 Justificación de la investigación

El objetivo de los sistemas de identificación de usuarios, no suele identificar a una persona, sino autenticar que esa persona es quien dice ser realmente (Red IRIS, 2008), cuando el número de usuarios que accede es mayor, se requiere de un sistema SSO que permita mantener una única cuenta de usuario y que pueda ser utilizada para múltiples aplicaciones en la organización, lo cual a su vez contribuye en varios aspectos como: disminución en la utilización de recursos de los sistemas, mejorar la administración de cuentas de usuario, disminuir el número de peticiones de recuperación de claves de acceso, disminuir el número de procesos de loguearse para acceder a múltiples aplicaciones.

Los sistemas SSO seleccionados en la presente investigación CAS y WSO2 Identity Server, cada uno con varias características que ponen a disposición de las organizaciones para llevar un adecuado control de autenticación de sus usuarios, internamente estos sistemas utilizan modelos como OpenID, SAML2, OpenAuth lo cual estandariza y certifica el proceso.

A través de la investigación que se llevará a cabo se logrará determinar cuál de los dos sistemas de autenticación CAS y WSO2 Identity Server ofrece un mejor rendimiento del proceso de autenticación para los aplicativos de AGROCALIDAD, a su vez el estudio se basará en métricas de calidad ya conocidos como el modelo de FURPS (1987) para el análisis del rendimiento de sistemas informáticos, que establece indicadores como: tiempo de respuesta, velocidad de procesamiento, consumo de recursos y eficacia (Pereira, Ayaach, Quintero, & Granadillo, 2019); el modelo de calidad ISO/IEC 25010 que establece en eficiencia de desempeño indicadores como: comportamiento temporal, utilización de recursos, capacidad. (ISO, 2019)

1.5 Objetivos de la investigación

1.5.1 Objetivo General

Comparar el rendimiento de los sistemas de autenticación SINGLE SIGN ONE (SSO) CAS y WSO2 Identity Server para el proceso de autenticación de los aplicativos de AGROCALIDAD.

1.5.2 Objetivos Específicos

- Analizar las características de los sistemas de autenticación Single Sign One (SSO) CAS y WSO2 Identity Server.
- Diseñar escenarios de evaluación de los sistemas SSO CAS y WSO2 Identity server para la autenticación de usuarios en el sistema GUIA de AGROCALIDAD.
- Evaluar los resultados cuantitativos del rendimiento de los sistemas SSO CAS y WSO2 Identity Server obtenidos durante el trabajo de recolección de información.
- Proponer un sistema guía de buenas prácticas para la implementación de un sistema SSO en AGROCALIDAD que permita proteger la institucionalidad de la información.

1.6 Planteamiento de la hipótesis

A continuación, se plantean la hipótesis alternativa y la hipótesis nula.

Ha: El sistema de autentificación de sesión único. CAS ofrece mejor rendimiento en cuanto a tiempo de respuesta, consumo de recursos y capacidad en comparación con WSO2 Identity server.

Ho: El sistema de autentificación de sesión único CAS NO ofrece mejor rendimiento en cuanto a tiempo de respuesta, consumo de recursos y capacidad en comparación con WSO2 Identity server.

CAPÍTULO II

2 MARCO DE REFERENCIA

2.1 Antecedentes del Problema

Como antecedente del tema propuesto de investigación se considera la vulnerabilidad que tienen los sistemas en el inicio de sesión, dada a partir de la necesidad de proteger la privacidad de la información, se considera los SSO como una alternativa, se presenta investigaciones realizadas en artículos científicos desde diferentes puntos de vista.

- En el mundo digital actual, los usuarios deben acceder a múltiples sistemas para llevar a cabo su día a día de actividades de negocio.

  El inicio de sesión único indudablemente lo hace más fácil y seguro al reducir a una sola cuenta por usuario para todos los servicios, número de contraseñas, administración central de roles para definir el control de acceso a los recursos. Eso puede ser muy beneficioso para los usuarios finales, los administradores y el servicio de ayuda. El inicio de sesión único puede ganar mucha más importancia con la emergente tecnología de computación en la nube, que proporciona servicios de TIC y también reduce las posibilidades de ataques de phishing, sin embargo, como el inicio de sesión único da acceso con un inicio de sesión, debe ser implementado de forma segura. El inicio de sesión único tiene sus fortalezas y debilidades y uno debe estimar el uso del sistema y los recursos disponibles para su implementación y administración antes elegir la solución SSO o puede crear una gran vulnerabilidad en la seguridad de una organización si no es implementado correctamente. (Hitha Reddy, 2012)
- Single Sign On (SSO) es un mecanismo de autenticación que permite a los usuarios legales con una sola credencial ser autenticados por múltiples proveedores de servicios en una red informática distribuida. SSO obtiene credenciales de autoridades de confianza, es decir, Centro de producción de tarjetas inteligentes (SCPC) y Privacidad de credenciales de

confianza (TCP) que se utiliza para la autenticación mutua y la autorización de usuarios legales. (Anithadevi, 2015)

El mecanismo de inicio de sesión único (SSO) permite a un usuario legal con una sola credencial ser autenticado y autorizado por múltiples proveedores de servicios que hacen uso de autoridades de confianza, producción de tarjetas inteligentes Center (SCPC) y Trusted Credential Privacy (TCP). El esquema de SSO mejorado se centra en la seguridad de la autenticación del usuario y, por lo tanto, el cifrado basado en atributos (ABE) se utiliza para una política de seguridad estricta. (Surya, 2015)

- La insatisfacción de los médicos con los registros electrónicos de salud (EHR) en la era del uso significativo ha sido significativa [1-3]. Para muchos médicos, los EHR y la entrada de pedidos de proveedores computarizados (CPOE) se encuentran entre los cambios más grandes y más dislocantes en la práctica clínica y el flujo de trabajo en una generación.

  En base a esta evaluación del impacto de la implementación de SSO, SSO está entregando un valor clínico sustancial, ROI anual recurrente y ahorros netos de costos en las primeras 6 instalaciones implementadas dentro de nuestro sistema hospitalario. La tecnología de inicio de sesión único parece ser un método eficaz y rentable para liberar tiempo clínico de inicios de sesión repetitivos y lentos a aplicaciones de software clínico. Además, nuestra experiencia fue que la introducción de la tecnología SSO facilitó la adopción de funcionalidades y aplicaciones de componentes clave dentro de nuestro EHR según lo informado por los usuarios médicos, lo que se alinea con la experiencia de implementación de otros hospitales. La implementación de SSO y su mejor rendimiento pueden exigir y se facilita mucho cuando se combina con la migración a un dispositivo de cliente ligero y VDI. Esto reduce la necesidad de costosas sustituciones y actualizaciones de PC, y produce ahorros considerables en el gasto de hardware. (George A. Gellert, 2017)

2.2 Definición de SSO

Permite a los usuarios tener acceso a múltiples aplicaciones ingresando solo con una cuenta a los diferentes sistemas y recursos. El SSO es de gran utilidad cuando existen diferentes sistemas a los que es posible acceder mediante una única contraseña y se desea evitar el ingreso repetitivo de estas cada vez que el usuario se desconecte del servicio. Para los usuarios supone una gran comodidad ya que identificándose solo una vez es posible mantener la sesión válida para el resto de las aplicaciones que hacen uso del SSO. (chakray, 2019)

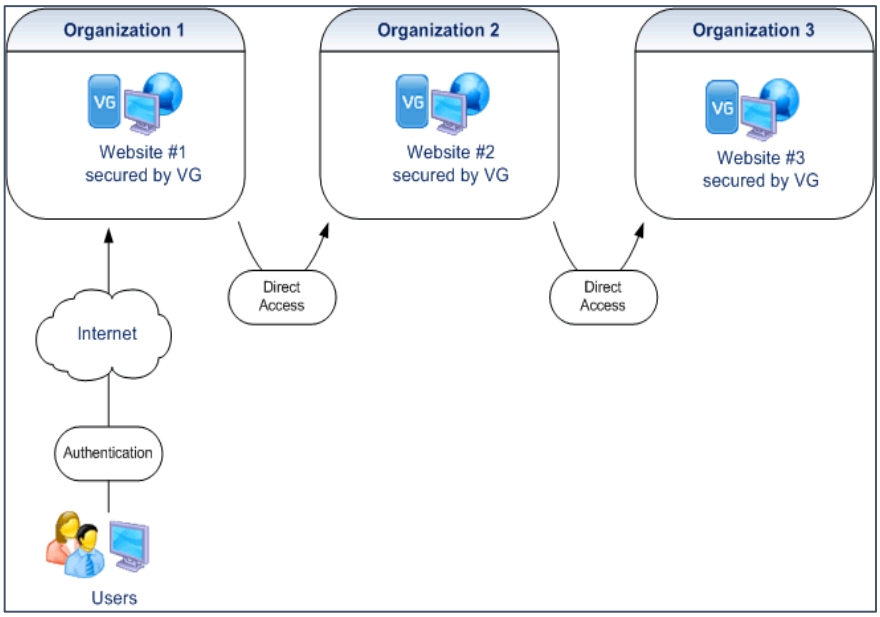

Figura 1-2: Autenticación única a través de varios sitios web independientes.
Fuente: isual-guard-web-portal.html.

Como ventajas inherentes a este mecanismo se puede encontrar:

- Descenso del número de procesos de login en los sistemas asociados, disminuyendo la *"fatiga"* del propio proceso de autenticación (el uso de varias combinaciones de usuario/password para una misma identidad). (Martín, 2019)
- Aceleración del proceso de acceso (autenticado) a los sistemas, evitando tener que volver a introducir las credenciales de usuario (Martín, 2019).
- Gestión centralizada de usuarios y autorizaciones, evitando que sean las propias aplicaciones las que tengan que implementar estos mecanismos (se delega al propio SSO) agilizando el proceso de aprovisionamiento de credenciales de usuarios (altas) para las diferentes aplicaciones, y automatizando los procesos de actualización y baja, reduciendo considerablemente la probabilidad de error (Martín, 2019).
- Seguridad el sistema de autenticación mejora la seguridad de la red y de las aplicaciones. Single Sign On puede identificar inequívocamente a un usuario por lo que cumple con normas más exigentes respecto a la seguridad (Martín, 2019).

Un ejemplo claro de cómo funcionan los sistemas de autentificación de contraseña o clave única sería:

Una persona X, usuario típico de la web que utiliza a diario algunas cuentas como Facebook, twitter, Outlook, Gmail etc. De esta manera esta esta persona X realiza sus actividades cotidianas

y negocios, pero todas estas aplicaciones requieren que se autentifique el usuario es decir que se identifique como usuario y una contraseña asociada a este usuario cada vez que inicie sesión en cada una de estas cuentas ya que son aplicaciones independientes y utilizan sus propios sistemas de autentificación y gestión de datos.

La persona X empieza a tener inconvenientes cuando crece su número de cuentas por que tiene varias en distintos servidores o plataformas y la persona debe recordar el usuario y contraseña de cada una de estas aplicaciones para poder autentificarse e ingresar a ellas si no lo hace no tendrá acceso a su cuenta. El problema no es tanto con el computador personal ya que la mayoría de veces uno tiene guardadas las cuentas de usuario y contraseñas de cada una de estas plataformas

El problema la mayoría de veces radica cuando se utiliza un computador ajeno ya sea alquilado, prestado o del trabajo y no recuerda la contraseña o el usuario de la cuenta. Cuenta a la que desea acceder, la cuenta se bloquea después de varios intentos le solicita preguntas de autentificación o códigos con lo cual se pierde tiempo y recursos. Entonces los usuarios se incomodan porque tienen que recordar varias cuentas y varias contraseñas y la forma más fácil para ellos es utilizar generalmente el mismo usuario y contraseñas para todas las cuentas generando inseguridad.

Se debe tener en cuenta la diferencia entre autentificación y autorización:

Autentificación: Es un sistema para certificar que el usuario es quien dice ser; es la combinación de identificador de usuario único y contraseña el sistema single-sign-on consiste en un protocolo de autentificación que funciona en más de un sistema. (Sanchez, 2019)

- **Single Sign on federado:** Es si el sistema responsable de la autentificación puede ser cualquier estándar definido.
- **Single Sing on delegado:** Es en si el sistema que autentifica predeterminado.

Autorización: Consiste en dar acceso a un conjunto de recurso a un usuario o sistema para ello el usuario o sistema previamente se tenían que haber autentificado. (Sanchez, 2019)

Atendiendo a la arquitectura de un sistema SSO, se pueden clasificar de la siguiente manera:

Simple: En el que el sistema SSO es único (esté o no clusterizado), y otorga acceso a los usuarios de un único dominio de seguridad.

Complejo: Es una arquitectura propia de sistemas federados, en los que existe más de un sistema de autenticación (SSO), y entre los que existe algún mecanismo de interrelación o confianza.

Generalmente este tipo de sistemas están compuestos por varios dominios de seguridad, habiendo un mecanismo SSO en cada uno de ellos.

Autenticación centralizada: En este tipo de arquitectura, el usuario es identificado a través de un elemento (Token o certificado) que es el que intercambia con las entidades de autenticación. (Martín, 2019)

- **Basada en PKI**: En este caso no se asigna token al usuario, sino que, este, usa un certificado PKI que es validado contra una CA de confianza para todos los SSO federados. (Martín, 2019)
- **Basada en Tokens:** La entidad de autenticación inicial es la que proporciona un token de sesión al usuario (token de kerberos o una cookie, etc.), y es el que, de forma transparente usa el cliente para acceder al resto de recursos, de la primera entidad o del resto de la federación. El resto de entidades validarán el token contra la primera. (Martín, 2019)

Autentificación Centralizada

Basado en	Ventajas	Desventajas
Token	• Tiene un único conjunto de credenciales simplifica la vida al administrador y al usuario. • El software normalmente viene incorporado con el Sistema.	• Requiere una infraestructura de autentificación homogénea. • Se basa en criptografía simétrica.
PKI	• Tiene un único conjunto de credenciales simplifica la vida al administrador y al usuario. • El software normalmente viene incorporado con el Sistema. • Se basa en criptografía asimétrica.	• Solo puede trabajar con un único conjunto de credenciales. • Algoritmo complejo de validación de certificado. Requiere mucho cálculo en el lado del cliente. • Requiere una infraestructura de autentificación homogénea (todos los servicios deben tener activado el mecanismo PKI)

Figura 2-2: Autentificación Centralizada ventajas y desventajas Token y PKI
Fuente: Single Sign-On Miquel Trilla

Autenticación Múltiple: En este tipo de mecanismos, las credenciales son cacheadas, ya sea en el lado del cliente, o ya sea en el servidor, y son independientes para cada autoridad de autenticación. Se trata de sistemas más pesados porque requieren mecanismos muy seguros para las cachés de credenciales, así como software adicional para la gestión y sincronización de credenciales en la parte cliente o servidor. En esta arquitectura, realmente se produce la autenticación en las diferentes entidades de autenticación (múltiple autenticación), ya que el cliente utiliza la información de sus credenciales que tiene cacheadas (ya sean en el servidor o en el propio cliente) en cada recurso al que desea acceder. (Trilla, 2019)

Y atendiendo al alcance del ámbito de operación del sistema SSO, podemos diferenciar dos tipos:

- **ESSO**: Enterprise Single Sign-On, es un sistema SSO completamente heterogéneo, que es capaz de gestionar los procesos de autenticación de los usuarios en cualquier sistema de un entorno IT (que esté integrado en el SSO).

  Microsoft introduce una variante, denominada Integrated Windows Authentication, en la que proporciona todos los mecanismos de autenticación de usuario basado en Directorio Activo a cualquier sistema Microsoft, y hace extensión de este mecanismo a entornos Linux, Unix y Macs.

- **WSSO**: Web Single Sign On Es una especialización de los sistemas ESSO, que centran la gestión de autenticación en sistemas Web, generalmente, de acceso público. En definitiva, como podemos intuir, todo el trabajo de un sistema Single Sign On se centra en el establecimiento y posterior mantenimiento de la sesión de usuario (propio o de un entorno federado) a lo largo de todo el entorno SSO, así como la identificación y autorización (local o a través de terceros) de dicha sesión en cada uno de los accesos (exitosos o no) del usuario a los recursos gestionados por el entorno SSO. (microsoft.com, 2006)

Autentificación Múltiple

Basado en	Ventajas	Desventajas
Caché Cliente	• Puede trabajar con diferentes gestores de credenciales. • No requiere una infraestructura de autentificación homogénea. • Tiene un impacto importante en el cliente (requiere software extra o un SO que lo soporte).	• Requiere una caché "segura" de credenciales en el lado del cliente – no recomendado su uso en dispositivos portatiles. • Múltiples gestores de credenciales complica la vida al usuario y al administrador.
Caché Servidor	• Puede trabajar con diferentes gestores de credenciales. • No requiere una infraestructura de autentificación homogénea. • Tiene un impacto importante en el cliente (requiere software extra).	• Requiere un mecanismo de sincronización de credenciales (puede formar parte del producto SSO). • Múltiples gestores de credenciales complica la vida al usuario y al administrador. • Requiere software extra en el lado del servidor.

Figura 3-2: Autentificación múltiple cache cliente vs cache servidor ventajas y desventajas

Fuente: Single Sign-On Miquel Trilla

2.2.1 Antecedentes de SSO

El protocolo HTTP, en el que se basa la comunicación entre el navegador de usuario y los sitios web, carece de mecanismos de control y gestión de sesión, lo cual implica que no es posible, sin ningún otro elemento de apoyo, relacionar los diferentes mensajes HTTP que puedan enviarse desde el navegador de un usuario cuando este esté, por ejemplo, actualizando su perfil en un sitio web de Internet.

Para solucionar este problema, se emplean las cookies (creadas por Lou Montull en 1994).

Cookie: se trata de un conjunto de datos enviados por el servidor web al navegador del usuario en el momento que este accede por primera vez al mismo (aplicación web). El cliente almacenará estos datos en local y serán reenviados al servidor cada vez que el usuario, de nuevo, vuelva a acceder al sitio web. Este conjunto de datos almacena información de estado que debe mantenerse a lo largo de la actividad de navegación del usuario. Además, permite almacenar otros elementos que pueden ser usados por los sitios web para recabar información de la actividad web del usuario para tareas de customización, etc.

Pero esta ventaja que dan los Cookie de recordar contraseñas e historial de navegación también tienen sus desventajas entre las cuales podemos citar:

Sin embargo, no todo es positivo. A pesar de que las cookies pueden ayudar a facilitar la navegación de los usuarios una de sus principales desventajas es la protección a la privacidad. Debido a que almacenan cualquier tipo de información, los datos personales pueden ser utilizados para fines ilegales. Esta es una de las principales causas de su desactivación. (Softevolution, 2018)

RFC 6265: Norma que específica cómo se han de implementar las cookies para establecer mecanismos de gestión de estado el uso del protocolo HTTP. Esta norma establece que los elementos que debe almacenar una cookie para gestión del estado son:

- **Domain:** Dominio donde podrá ser transmitida la cookie, y de no existir, se utilizará como cookie basada en el host. Es decir, si la cookie tiene el dominio "*tfmuoc.edu"*, estará disponible para cualquier subdominio de este dominio (es decir, por ejemplo, estará disponible para apps1.tfmuoc.edu y apps2.tfmuoc.edu). El dominio ha de ser válido en modo FQDN, cualquier otra opción, como *"localhost"* o la dirección IP será rechazada (la cookie).
- **Max-Age:** indica el tiempo de validez máximo de la cookie, y la cookie será válida al menos durante este tiempo o hasta que el navegador del usuario se cierre.
- **Path:** contiene la URL de aplicación de la cookie (dónde es válida).
- **Secure:** si se usa este parámetro, la cookie sólo puede ser transmitida por HTTP Seguro (HTTPS/443), en caso contrario, esta cookie no podrá ser incluida en la transmisión.
- **HttpOnly:** Si se usa, indica que no se podrá usar desde JavaScripts, lo cual ofrece una protección contra ataques de tipo XSS.

Los sistemas de Single Sign On, por tanto, requieren una buena gestión de cookies HTTP de sesión de usuario, a través de las cuales poder hacer un seguimiento para mantener las sesiones en todas las aplicaciones que se encuentren bajo el control del SSO. (Martín, 2019)

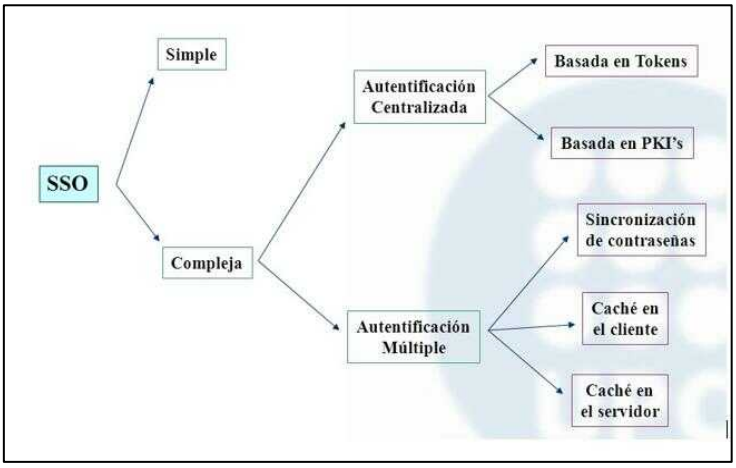

Figura 4-2: Clasificación De Las Arquitecturas Del SSO
Fuente: Single Sign-On Miquel Trilla

2.2.2 Características SSO

- **Multiplataforma:** Puesto que facilita las tareas de inicio de sesión en cada uno de las plataformas a las que se acede con una sola clave ahorrando el tiempo y recursos de la persona que lo emplea ya que no tiene que ingresar usuario y contraseña en cada uno de los sitios visitados.
- **Fácil Uso:** El usuario se autentifica una sola vez y acede a los recursos evitando interrupciones producidas por solicitud de contraseña y usuario en cada uno de los sitios.
- **Transparencia:** el acceso a recursos de sistemas se efectúa de forma trasparente al usuario.
- **Gestión Sencilla:** el uso de SSO sincroniza las contraseñas e información del o los usuarios simplificación la gestión de recurso, el memorizar gran cantidad de contraseñas simplificando la gestión del administrador.
- **Control de acceso:** no se afecta los sistemas no modifica los permisos de los recursos solo implica un cambio en el mecanismo de autentificación del servidor o administrador.
- **Seguridad:** la seguridad del sistema no es vulnerada fácilmente debido a que la información es cifrada por varios sistemas como SSL, certificado etc.

2.2.3 OpenID

Figura 5-2: Logo Open ID
Fuente: http://openid.net/

OpenID fue creado en el verano de 2005 por una comunidad de código abierto que intentaba resolver un problema que no era fácilmente resuelto por otras tecnologías de identidad existentes. Como tal, OpenID está descentralizado y no es propiedad de nadie, ni debería serlo. Hoy, cualquiera puede elegir usar un OpenID o convertirse en un proveedor de OpenID gratis sin tener que registrarse o ser aprobado por ninguna organización. (OpenID, 2018)

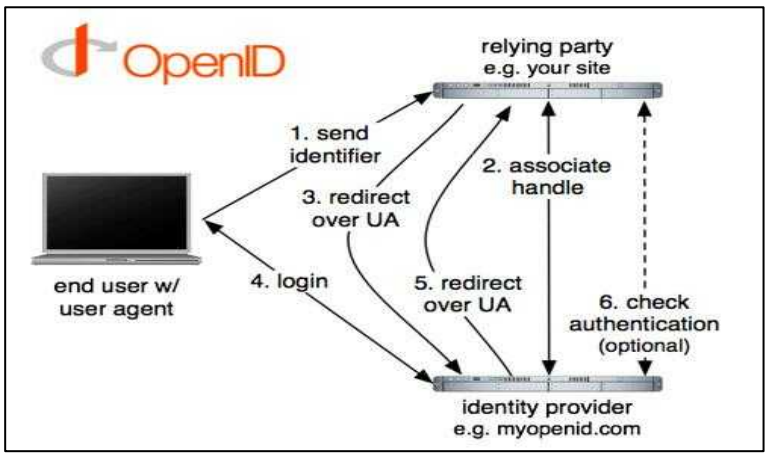

Figura 6-2: Acceso con Open ID
Fuente: flickr.com

La Fundación OpenID se formó para ayudar al modelo de código abierto al proporcionar una entidad legal para ser el administrador de la comunidad al proporcionar la infraestructura necesaria y, en general, ayudar a promover y apoyar la adopción ampliada de OpenID.

OpenID le permite usar una cuenta existente para iniciar sesión en varios sitios web, sin la necesidad de crear nuevas contraseñas. Puede optar por asociar información con su OpenID que se puede compartir con los sitios web que visita, como un nombre o dirección de correo electrónico. Con OpenID, usted controla qué parte de esa información se comparte con los sitios web que visita.

Con OpenID, su contraseña solo se le otorga a su proveedor de identidad, y ese proveedor luego confirma su identidad en los sitios web que visita. Además de su proveedor, ningún sitio web ve su contraseña, por lo que no debe preocuparse por un sitio web inescrupuloso o inseguro que comprometa su identidad (OpenID, 2018).

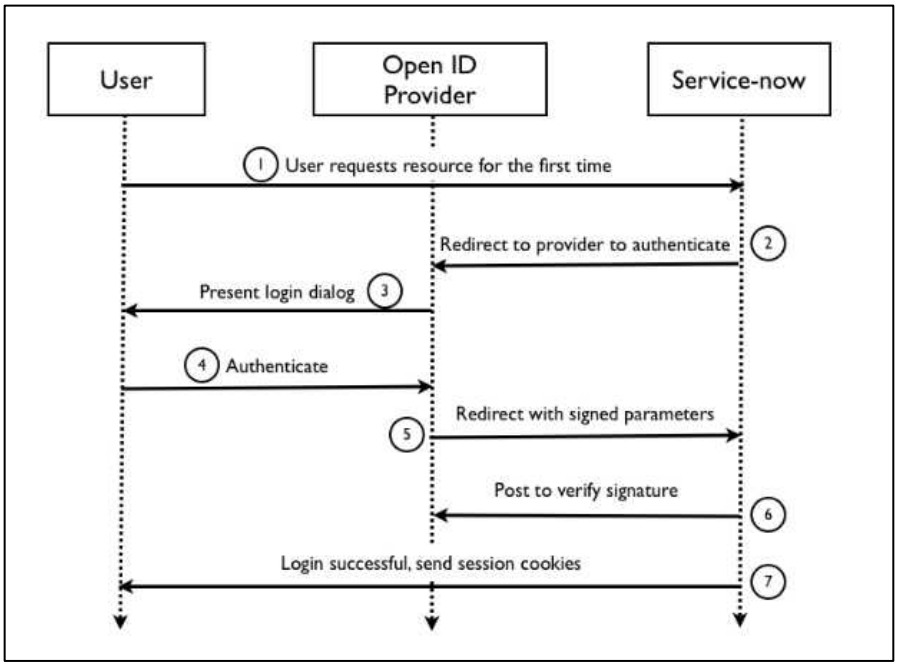

Figura 7-2: Protocolo de autentificación del OpenID
Fuente: https://jordisan.net/proyectos/Autent_y_auth-J_Sanchez.pdf?3eb125

2.2.3.1 Protocolo de autentificación del OpenID

- Si el servidor soporta el protocolo Open id (es "Consumidor" de OpenID), solicita al usuario su OpenID (la URL externa de "proveedor" de OpenID).
- El usuario introduce su OpenID.
- El servidor redirige al usuario al proveedor de OpenID.
- El usuario se autentica contra el proveedor de OpenID.
- El proveedor de OpenID redirige al usuario de nuevo al servidor, validando su identidad.
- Si el usuario utiliza siempre el mismo proveedor de OpenID solo necesitaría recordar su Identificador de OpenID y una única contraseña de validación.

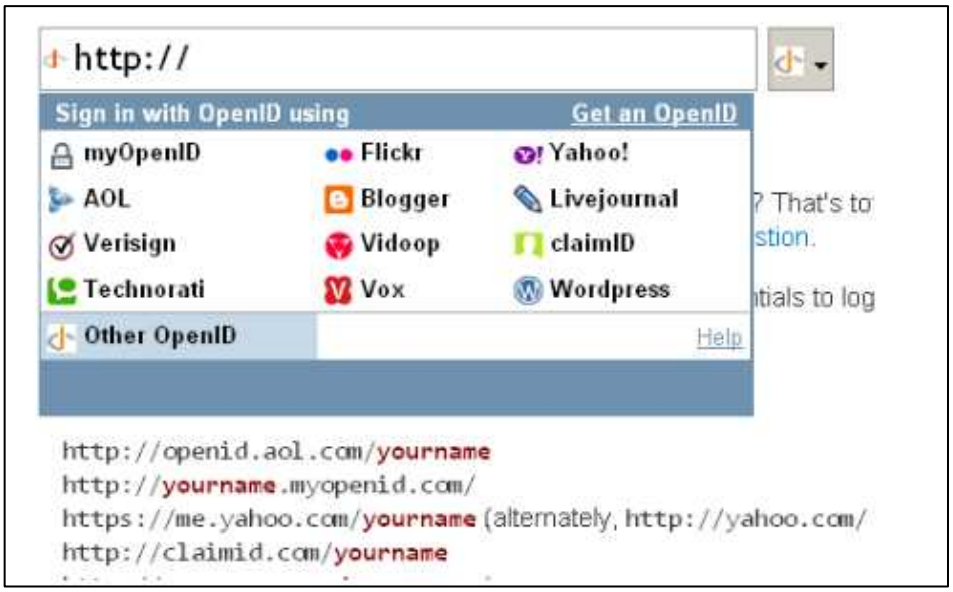

Figura 8-2: Pantalla de ejemplo de selección de OpenID
Fuente: https://jordisan.net/proyectos/Autent_y_auth-J_Sanchez.pdf?3eb125

2.2.3.2 Problemas del OpenID

Complejidad: No es fácilmente implementable por su complejidad.

Seguridad: Es vulnerable al phishnig que consiste en la suplementación maliciosa de una página de autentificación con el objetivo de conseguir el usuario y contraseña de un usuario esto lo hace mediante enlaces en correos electrónicos en un servidor que utiliza OpenID el cual abre los enlaces lo redirigen a una página falsa que suplanta la página del proveedor de OpenId para de esta manera conseguir la contraseña.

Privacidad: los proveedores de OpenID tendrán mucha información de las actividades en la red de los usuarios lo que lleva a problemas de privacidad.

Confianza: El protocolo ofrece un mismo sistema de autentificación para diferentes servicios, pero no ofrece ninguna garantía de la identidad real del usuario nada impide que Spam creen y validen identidades mediante OpenID.

Uso: Puede ser complejo el uso al momento de elegir el proveedor de OpenID y autentificarse en un servidor diferente al de la aplicación puede resultar confuso e incluso complejo para el usuario.

Proveedores: El número de proveedores de servicios como mecanismo de autentificación es bajo esto se debe a que las personas u organizaciones les resulta beneficioso tener cuentas de los usuarios en sus servidores, por tanto, siempre estarán más interesados que los usuarios utilicen las cuentas en sus servidores para autentificase en otros.

2.2.4 OAuth

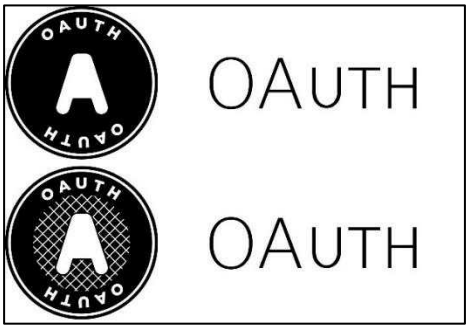

Figura 9-2: Logo OAuth
Fuente: openam.jp/wp-content

Empezó a definirse en 2006 ante las carencias de OpenID y en 2007 se lanzó su primera versión oficial Es un estándar abierto que permite flujos simples de autorización para sitios web o aplicaciones informáticas. Se trata de un protocolo propuesto por Blaine Cook y Chris Messina, que permite autorización segura de una API de modo estándar y simple para aplicaciones de escritorio, móviles y web.

OAuth permite a un usuario del sitio A compartir su información en el sitio A (proveedor de servicio) con el sitio B (llamado consumidor) sin compartir toda su identidad. Para desarrolladores de consumidores, OAuth es un método de interactuar con datos protegidos y publicarlos. Para desarrolladores de proveedores de servicio, OAuth proporciona a los Usuarios un acceso a sus datos al mismo tiempo que protege las credenciales de su cuenta. Este mecanismo es utilizado por compañías como Google, Facebook, Microsoft, Twitter y Github para permitir a los usuarios compartir información sobre sus cuentas con aplicaciones de terceros o sitios web. (David Lozano, 2017).

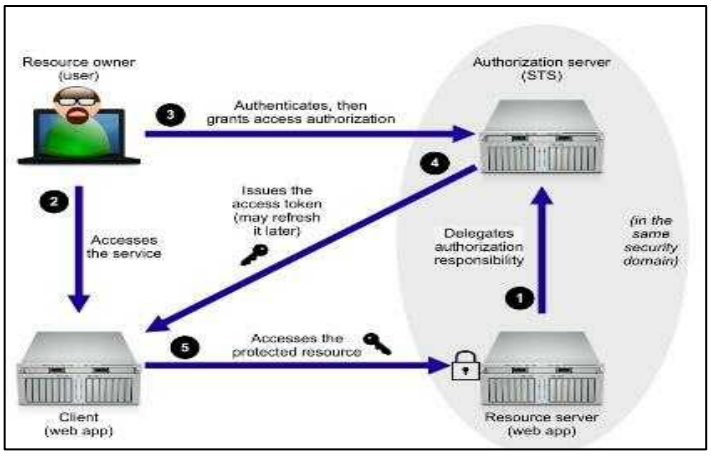

Figura 10-2: Arquitectura del SSO OAuth
Fuente: openam.jp/wp-content

2.2.4.1 Protocolo de autorización de OAuth

- El usuario dispone de una serie de recursos propios en un servidor que es el proveedor.
- Un servidor externo ósea el consumidor desea acceder a un subconjunto de esos recursos.
- El consumidor dirige al usuario hacia el proveedor.
- El usuario se autentifica en el proveedor sino lo ha hecho previamente.
- El proveedor pregunta al usuario si autoriza al consumidor a que utilice esos determinados recursos.
- El usuario autoriza al consumidor a utilizar esos recursos.
- El servidor externo ósea el consumidor consigue acceso a esos recursos

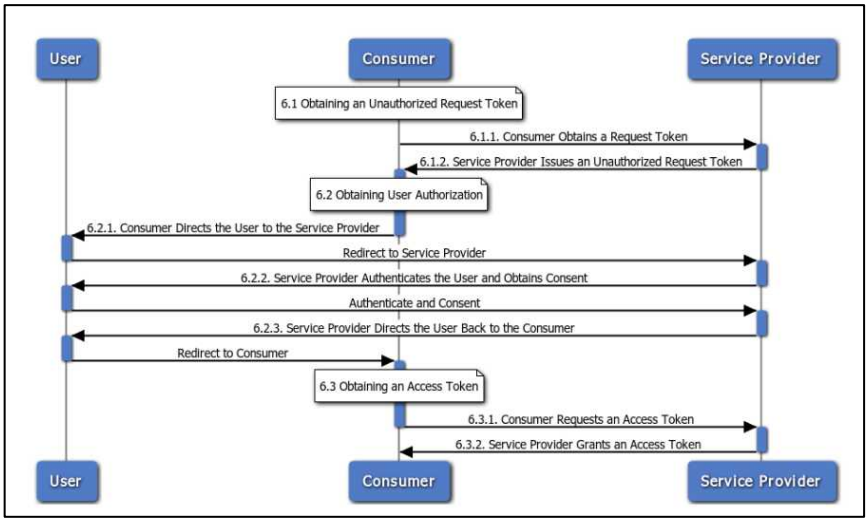

Figura 11-2: Protocolo de Autorización de OAuth
Fuente: https://jordisan.net/proyectos/Autent_y_auth-J_Sanchez.pdf?3eb125

2.2.4.2 Problemas del OAuth

Complejidad: difícil de implementar eso hace que exista diversas implementaciones y librerías que realizan implementaciones poco robustas y poco documentadas.

Orientación a Navegadores: Está orientado a su uso en navegadores de internet de modo que su uso en otras aplicaciones es problemático por el uso de redirecciones entre URLs.

Seguridad: Posee problemas y falencias en sus protocolos de seguridad.

No es un sistema de autentificación: es un protocolo de autorización de delegación de acceso; permite definir como un tercero va a acceder a los recursos propios.

Figura 12-2: Pantalla de autorización a recursos de twitter mediante OAuth
Fuente: https://jordisan.net/proyectos/Autent_y_auth-J_Sanchez.pdf?3eb125

2.2.5 SAML2

SAML (Security Assertions Markup Language) está guiado en XML para servicios Web que permite el intercambio de información de autorización y autenticación entre diferentes sitios Web. Este está desarrollado por los comités técnicos de servicios de seguridad de OASIS (Organization for the Advancement of Structured Information Standards). Es flexible y extensible y está diseñado para ser utilizado por otros estándares. Integra protocolos y entornos de mensajería ya presentes en la industria, como XML Signature, XML Encryption y SOAP. La especificación puede integrarse en entornos de estándares como HTTP y navegadores Web estándares, por ejemplo, ya incorporaron este protocolo, Liberty Alliance, Internet2 Shibboleth. OASIS Web Services Security (WS-Security), etc. (Oliva Mateos, 2016)

2.2.5.1 Historia de SAML y su versión 2.O

La versión SAML 1.0 fue un estándar de OASIS en noviembre de 2002. Y a continuación apareció la versión SAML 1.1 en septiembre de 2003 en la que se ha visto un éxito relevante dentro de la industria, recabando fuerza en servicios financieros. La versión definitiva, SAML 2.0, se publicó el 15 de marzo de 2005 SAML ha sido puesto en ejecución ampliamente por todos los vendedores importantes de la gestión del acceso Web. La versión SAML 2. junta los bloques dispares de construcción de identidad federados antiguas de SAML 1.1, con la entrada en la iniciativa de Shibboleth y el marco de la federación de identidad de Liberty Alliance. Como tal, SAML 2.0 es un paso crítico hacia la convergencia total de los estándares de identidad federados. (Oliva Mateos, 2016)

2.2.5.2 Ventajas SAML 2.0

- **Plataforma neutral**: SAML abstrae el marco de la seguridad lejos de puestas en práctica y de arquitecturas particulares de vendedores.
- **Acoplador flojo de directorios:** SAML no requiere la información del usuario para ser mantenido y sincronizado entre principales.
- **Experiencia en línea mejorada para usuarios finales**: las aserciones de la autentificación de SAML permiten "single sign-on" consintiendo que los usuarios se autentifiquen en un proveedor de identidad y después tengan acceso a servicios/recursos en los proveedores de servicio sin autentificación adicional.
- **Costes administrativos reducidos para los proveedores de servicio**: el uso de SAML para la federación entre los dominios de identidad puede reducir el coste de mantenimiento de la información de la cuenta (por ejemplo, el nombre de usuario y la contraseña).
- **Transferencia del riesgo:** SAML puede ceder la responsabilidad de la gestión de las identidades al proveedor de identidad, que es a menudo más compatible con su modelo de negocios que el de un proveedor de servicios. (Oliva Mateos, 2016)

2.2.5.3 Características SAML2.0

Uno de los motivos por los que se ha producido un incremento en el uso de SAML 2.0 son las características nuevas que reúne, que junto a sus ventajas le proporcionan unas potencialidades muy importantes para ser el estándar más usado en cuestiones de autentificación e información de identidad. SAML 2.0 incorpora las siguientes ventajas:

- **Seudónimos:** SAML 2.0 define como un identificador pseudo-aleatorio opaco sin correspondencia discernible con los identificadores significativos (por ejemplo, el e-mail o los nombres de cuenta) se puede utilizar entre los proveedores para representar a los principales. Los seudónimos son una llave privada que permite la tecnología porque inhiben la colusión entre proveedores múltiples (cuando sea posible con un identificador global como en direcciones de e-mail).
- **Gestión de la federación:** SAML 2.0 define cómo dos proveedores pueden establecer y manejar posteriormente el seudónimo(s) para los principales para quienes están funcionando.
- **Gestión de la sesión:** El protocolo "single logout" (SLO) en SAML 2.0 proporciona un medio por el cual todas las sesiones proporcionadas por una autoridad particular de sesión puedan ser cercanas y simultáneamente terminadas.

- **Móvil:** SAML 2 introduce un nuevo soporte para el mundo móvil, tanto por los desafíos introducidos por los dispositivos y las limitaciones del ancho de banda como por las oportunidades hechas posibles al surgir los dispositivos activos o inteligentes.
- **Mecanismos de Privacidad:** SAML 2 incluye mecanismos que permiten que los proveedores se comuniquen, de unos a otros, las políticas de privacidad establecidas. (Oliva Mateos, 2016)

SimpleSAMLphp: El protocolo estándar SimpleSAML, suministra una infraestructura de autenticación repartida que facilita la autenticación en múltiples entornos a través de un proceso de autenticación único. Esto quiere decir que el usuario sólo tiene que introducir sus credenciales una única vez lo que implica al mismo tiempo, que no existe redundancia de datos de autenticación, ni, por otra parte, inconsistencia de datos por duplicación de la información de un mismo usuario.

Esta aplicación de origen PHP se encarga de las funciones de autenticación. Este programa se basa en proveer un soporte para el tipo de autenticación conocido como SAML 2.0 tanto como proveedor de servicio como proveedor de identidad. SAML2.0 es un estándar de OASIS basado en XML para el intercambio de información de autenticación y autorización entre dominios seguros. (Gómez A. , 2011)

2.2.6 WSO2

Figura 13-2: logo WSO2
Fuente: https://wso2.com/

La suite WSO2 es una plataforma Open Source encaminada hacia el diseño de arquitecturas y la misma se apoya en los productos (SOA - Service-oriented architecture). WSO2 se encarga de resguardar cada paso del ciclo de vida en un proyecto de desarrollo y se basa en los siguientes servicios:

- Construcción de Servicios.
- Documentación de APIs para equipos de Desarrollo.
- Publicación y Routing.
- Monitorización del tráfico.
- Securizar el acceso y consumo inadecuado.
- Balanceo de carga.

- Reporting y Monetización de los servicios.
- Suministrar la integración con dispositivos móviles.

WSO2, según se verifica en su página web, fue fundada por Sanjiva Weerawarana, y se enfoca en abastecer una arquitectura para desarrolladores profesionales que se orienta hacia los servicios SOA. Esta plataforma surge desde que Collax, un proveedor de servidores linux de código abierto adquiriera una inversión millonaria por parte de Intel Capital, una corporación global de USA (Mountain View CA), UK (Emsworth, Hampshire) y Sri Lanka. WSO2 también ha realizado contribuiciones esenciales en los servicios web de Apache, Apache Axis2, Apache de Rampart, Apache Synapse, Apache Axiom. (WSO2, 2018)

2.2.6.1 Elementos de la plataforma WSO2

Con los avances tecnológicos que ha sufrido la plataforma WSO2, se ha ido incorporando nuevos productos en los mercados que se adaptan de mejor manera a los requerimientos de las empresas según el informe presentado por Sebastián Sanz. (Sanz, 2016).

WSO2 API Manager: Gestiona la publicación de APIS a sistemas terceros a los mismos a los cuales garantiza la seguridad de la información y disminuye los lapsos de integración.

WSO2 Identity Server: Este producto permite el manejo de credenciales y protocolos para que puedan acceder a los recursos y servicios corporativos mediante un exclusivo punto de gestión. Identity Server administra a los servidores de autenticación internos de forma única. WSO2-IS suministra los protocolos de acceso más manejados en el mercado como el OAuth2.

WSO2 Data Services Server: Este producto permite encasillar en un API aquellos recursos que se encuentran almacenados en sistemas de ficheros o bases de datos de una manera sencilla asegurando la integridad de la información. Como puede ser la creación de un API de consulta a partir de un conjunto de ficheros Microsoft Excel.

WSO2 Enterprise Service Bus: Gestiona la dirección de servicios y acceso a recursos en procesos de negocio. WSO2-ESB otorga la integración de los productos de la plataforma WSO2.

WSO2 Data Analytics Server: Delinea cuadros de mando a medida y muestra la información a Sistemas de Inteligencia de Negocio (Business Intelligence) o Big Data mediante un API-REST.

WSO2 IoT Server: Suministra la integración y gestión de dispositivos. La versión 1.0 será liberada en el Q3 de 2016.

WSO2 Microservices Framework for Java: Framework y Runtime genera microservicios con un rendimiento superior a otros frameworks similares como Spring Boot, optimizando el uso de recursos. (Sanz, 2016)

En la siguiente imagen se representa la composición de los productos descritos anteriormente, en este contexto de desarrollo:

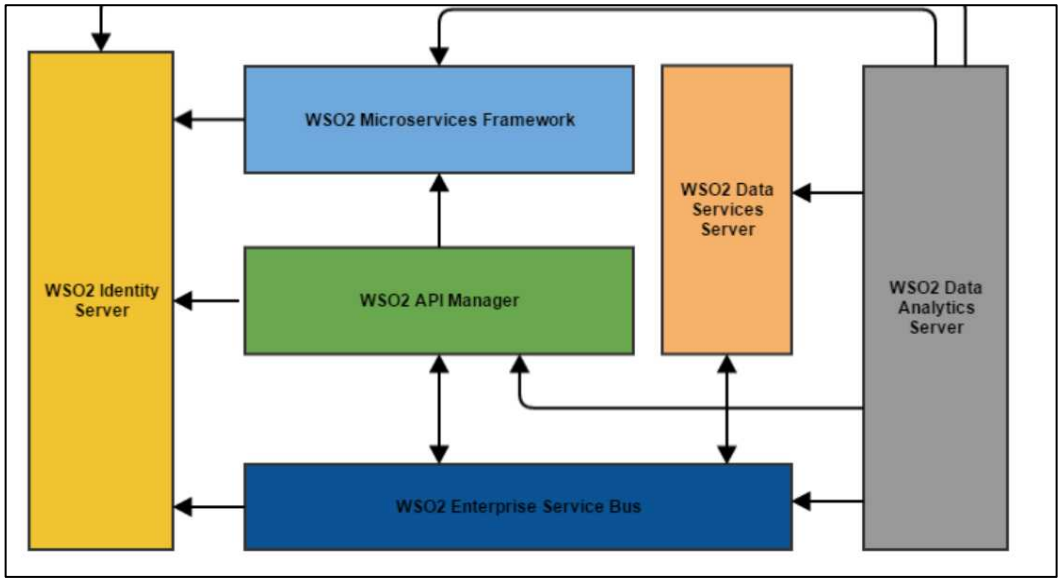

Figura 14-2: Productos de la plataforma WSO2
Fuente: https://wso2.com/

El servidor WSO2, facilita la posibilidad de poder observar los logs que se crean a cada instante, para verificar los eventos de conexión y desconexión para determinar que los procesos se cumplan satisfactoriamente.

2.2.7 WSO2 Identity Server

Figura 15-2: Logo WSO2 identity server
Fuente: https://wso2.com/

Considerando que WSO2 maneja gran parte de los escenarios que gestionan identidades y direccionan procesos de autorización y autenticación. WSO2 Identity Server, al ser un producto de la plataforma WSO2 cumple con todos los requerimientos de seguridad en los Sistemas de Información.

WSO2 Identity Server se puede utilizar para simplificar las actividades relacionadas con la gestión de identidad y acceso (IAM) en la empresa. El producto se basa en estándares abiertos y principios de código abierto. WSO2 Identity Server viene con capacidades de integración integrada y fácil de usar que ayudan a conectar aplicaciones, tiendas de usuarios, directorios y sistemas de administración de identidades. Una de las herramientas más sencillas que puede usar para administrar identidades y resolver problemas relacionados con la identidad. Facilita la administración centralizada, la administración, el monitoreo y la detección de actividades relacionadas con la identidad. En el mundo conectado de las aplicaciones empresariales, donde las aplicaciones deben construirse rápidamente al tiempo que se garantiza la seguridad de los datos y sistemas asociados, es fundamental que tenga un conjunto de herramientas fácil de usar para establecer y mantener políticas de gestión de acceso e identidad adecuadas (WSO, 2019).

Figura 16-2: Requisitos de seguridad WSO2 IDENTITY SERVER
Fuente: https://es.slideshare.net/wso2.org/implementacin-de-autenticacin-federada-con-wso2-identity-server-51

WSO2 IS, administra la identidad para aplicaciones web, ofreciendo seguridad óptima y disminuyendo los tiempos de despliegue. Este producto, soporta SAML, OpenID y XACML.

Su distribución es libre y se distribuye en resguardo a los términos de la licencia de Apache 2.0. Además, sobrelleva varios almacenes de usuarios como LDAP externo, Microsoft Active Directory, Apache Cassandra o cualquier base JDBC.

Posee una interfaz de administración, interfaces gráficas, y una para el usuario final que permite a la vez el manejo de perfiles, recuperación de cuentas y administración de aplicaciones autorizadas.

Al ser un servidor de administración de código abierto y a la vez ser compatible con tarjetas de información y autenticación OpenID, provee una completa solución de identidad que se integra fácilmente en los servicios de usuarios existentes, como LDAP o Active Directory. Este producto responde a los crecientes desafíos de la administración de identidades y seguridad de las aplicaciones Web empresariales. Facilita a los arquitectos de la empresa y a los desarrolladores a mejorar la experiencia del cliente garantizando las interacciones en línea seguras dentro y fuera de SOA-Service oriented architecture.

La Solución de Identidad WSO2 trabaja actualmente con los directorios empresariales de identidad, como Lightweight Directory Access Protocol (LDAP) y Microsoft Active Directory, lo que les permite aprovechar su infraestructura existente. Aparte del proveedor de identidad y de la solución de identidad WSO2, *brinda "un conjunto de elementos que se conectan a los servicios de la Web más comunes para añadir soporte en la autenticación OpenID y CardSpace"* (Chakray.com, 2019)

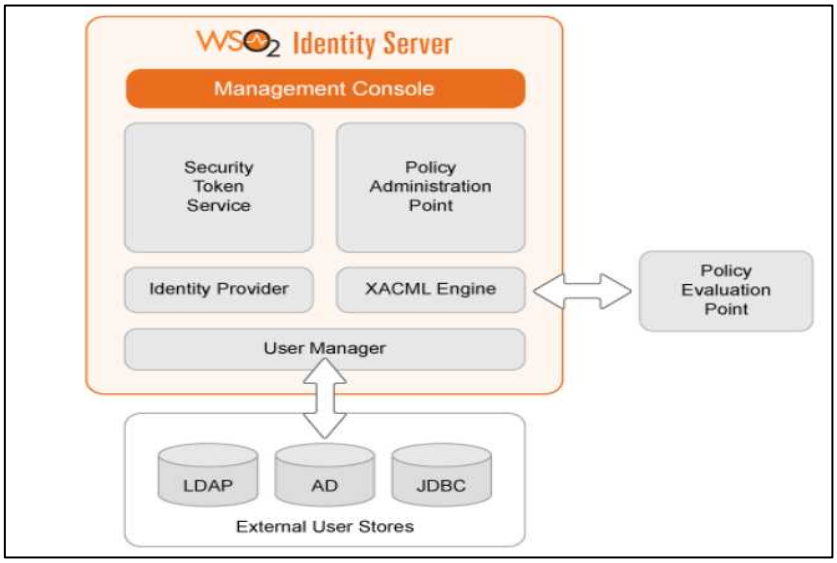

Figura 17-2: Arquitectura WSO2 Identity server
…Fuente: https://es.slideshare.net/wso2.org/implementacin-de-autenticacin-federada-con-wso2-identity-server-51

2.2.7.1 Características WSO2 Identity Server

- WSO2 Identity Server proporciona gestión de identidades para aplicaciones web, servicios y Apis

- Identity Server actúa como un Bus Empresarial de Identidad (BEI), una red troncal centralizada para conectar y gestionar múltiples identidades.
- Soporta múltiples User Store.
- Soporta los estándares XACML 2.0/3.0 y SAML.
- Soporta control de acceso basado en roles (RBAC).
- Permite el control de políticas de acceso y derechos mediante interfaces de usuario.
- Proporciona un Api de servicios para la gestión de identidades que puede ser utilizado por aplicaciones.
- Soporta Single Sign-On (SSO) via OpenID, SAML2, y Kerberos KDC
- Provee servicios de delegación vía OAuth 1.0a, OAuth 2.0, y WS-Trust
- Soporta Federación vía OpenID, SAML2, y WS-Trust STS. • Soporta políticas de control de acceso fino vía XACML
- Implementa seguridad sobre servicios REST con OAuth 2.0 y XACML. • Permite despliegues en HA y Dockerizados.
- Integrado con WSO2 Enterprise Service Bus para autorización y todos los productos WSO2 Carbon.
- Políticas de validación/expiración de passwords
- Recuperación de cuentas vía email.
- Preguntas secretas. (Chakray, 2004)

2.2.7.2 WSO2 IS – Conjunto de componentes Open Source

- WSO2 Carbon
- Apache Axis2 (SOAP)
- Apache Axiom (High performance XML Object Model)
- Apache Rampart/Apache WSS4J (WS-Security, WS-SecureConversation)
- Apache Rahas (WS-Trust) • WS-Addressing implementation in Axis2, Apache Neethi (WS-Policy)
- WS-SecurityPolicy implementation in Axis2
- Apache XML Schema
- OpenID4Java
- SunXACML
- OpenSAML2
- Apache Directory Server

- Apache Oltu (Chakray, 2004)

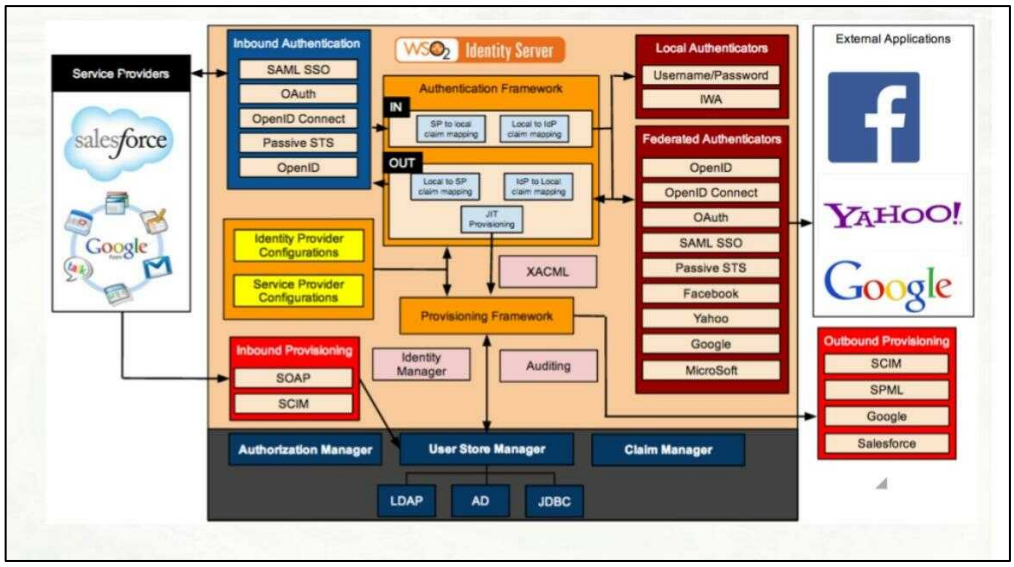

Figura 18-2: Arquitectura WSO2 IDENTITY SERVER

Fuente: https://es.slideshare.net/wso2.org/implementacin-de-autenticacin-federada-con-wso2-identity-server-51

Tabla 1-2: Fases de aplicación de la seguridad a una organización

APLICACIÓN DE LA SEGURIDAD A UNA ORGANIZACIÓN			
Primera fase:	**Segunda fase:**	**Tercera fase**:	**Cuarta fase:**
Gestión de Accesos e Identidades (IAM). User credential lifecycle Management Modelo de usuarios servicio de Autenticación Servicio de Autorización Servicio de SSO	Seguridad de la Información PKI, Firma Digital Gestión Centralizada de Documentos	Security Compliance: Gestión de Riesgos de activos de la empresa Continuidad de Negocio	Auditabilidad y "no repudio"

Realizado por: David Rodríguez. 2019

2.2.7.3 Beneficios y recomendaciones de uso de WSO2 Identity server

Tabla 2-2: Beneficios y recomendaciones de uso de WSO2 Identity server.

BENEFICIOS	RECOMENDACIONES
– Permite la conformación de un proveedor único de identidad para la autenticación y autorización. – Se fomenta la utilización de un sistema basado en el reconocimiento, eliminando por completo el modelo de nombre de usuario / contraseña.	– Utilizar una estrategia de implementación soportada por Role-Based Access Control (RBAC) en conjunto con el estándar XACML. Ambos sistemas son gestionados por el WSO2 Identity Server. Utilizar el estándar XACML para proporcionar políticas de autorización de grano fino, la cual incluye servicios de administración de políticas de autorización, de intercepción, evaluación e información de solicitudes.

– Elimina el riesgo creado a partir de múltiples nombres de usuario y contraseñas. – Soporta los estándares para el inicio de sesión único como (SSO): OpenID, OAuth, SAML2 y Kerberos. – Se fomenta el uso de autenticación basada en tokens y certificados. – Soporte de federación, en la cual las instituciones del Ecuador pueden abrir sus servicios de autenticación y autorización de forma segura utilizando protocolos como SAML2, OpenID, OAuth, Seguridad Token Service (STS) e InfoCards. – Soporta la delegación de Identidad mediante OAuth. – Soporta políticas de autorización mediante los tipos de control de acceso basado en roles y atributos. – Soporte del estándar de facto para la autorización XACML mediante dos asistentes de políticas.	– Utilizar el estándar XACML sobre los protocolos OpenID, SAML2 o Kerberos. – Conformar un API transversal de servicios que estandarice la administración de servicios de autenticación y autorización en el estado del Ecuador mediante un middleware de soluciones WSO2 Open Source sólido, ágil y pragmático. – Utilizar un modelo de políticas de acceso a recursos dinámico, flexible y basado en la web para autenticación y autorización basado en WSO2 IS. – Interoperar con el Bus de Servicios de la Organización. – Utilizar las interfases ya disponibles en WSO2 IS para soportar los requerimientos de control de políticas y roles. – De cara a abordar el Proyecto desde una visión global, considerar siempre que los Proyectos de Gestión de Identidades son Proyectos de "INTEGRACIÓN" donde las funcionalidades relacionadas a la IdM deben ser expuestas como "APIs" para distintos "CANALES", donde el uso y la salud de la plataforma debe ser "MONITORIZADO" para tomar las mejores decisiones basado en "MÉTRICAS". (Chakray, 2004)

Realizado por: David Rodríguez. 2019

2.2.8 CAS (Central Authentication Service)

CAS fue desarrollado en la universidad de Yale por Shawn Bayenr y fue mantenido por Drew Mazurek en Yale CAS 1.0 implementó el inicio de sesión única, CAS 2.0 introdujo la autentificación de múltiples niveles proxy y en mayo del 2014 se lanzó CAS 3.0.

CAS fue desarrollado por la constante problemática de solicitudes de contraseña y autentificación en cada sitio web o programa esto creo la necesidad de un programa que valide todos estos sitios con solo una contraseña esto proporciona comodidad al usuario y sobre ahorro de recursos en empresas e instituciones.

CAS es muy beneficioso en entornos donde varias aplicaciones web diferentes comparten un conjunto de usuarios comunes. Si todas las aplicaciones web se *"validaran"*, un usuario podría

iniciar sesión una vez y luego podría moverse entre las diversas aplicaciones web sin tener que presentar credenciales de autenticación nuevamente. (docs.moodle.org, 2017)

Numerosas solicitudes de contraseña y diferentes credenciales requeridas para cada sistema han creado la necesidad de que las instituciones y organizaciones adopten un proceso de autenticación de inicio de sesión único seguro en la web. El inicio de sesión único proporciona comodidad al usuario, ya que protege contra la proliferación de credenciales y la exposición de contraseñas, y centraliza la experiencia de inicio de sesión. El Apereo Central Authentication Service (CAS) de código abierto crea una forma segura para que los usuarios accedan a múltiples servicios con un inicio de sesión único empresarial. CAS ha ganado amplia adopción dentro de las instituciones de educación superior y las empresas para la autenticación empresarial (UNICON, 2019).

CAS tiene la ventaja de compatibilidad con IdP e integraciones de SP, soporte para OpenID SAML 2.0, autentificación multifactorial

2.2.8.1 Protocolo de autentificación CAS

Se divide en tres partes el protocolo de CAS el Navegador web del cliente: al cliente visitar una aplicación o página web que necesita autentificación:

- La aplicación web que solicita la autentificación: es redirigida a CAS
- Y el Servidor (CAS) que es quien valida la autenticidad del cliente verifica el nombre de usuario o contraseña contenido en una base de datos ya sea Active Directory, LDAP, Kerberos, etc.
- Al ser autenticado el cliente. CAS devuelve al cliente a la plataforma o aplicación.

2.2.8.2 Componentes CAS: (CAS client and CAS server)

CAS es un sistema SSO web empresarial de código abierto y fue desarrollado en Java, usando el framework Spring MVC, Spring Webflow y los componentes de Java. La arquitectura de este sistema se comprende de dos componentes físicos que son el CAS Clients y CAS Server, como se puede visualizar en la imagen siguiente. (Vargas, 2016)

El CAS Clients comprenden dos significados distintos en su uso común:

- Es cualquier aplicación habilitada para el CAS que pueden comunicarse con el servidor mediante un protocolo soportado o compatible.

- Es un paquete de software que puede ser integrado con diversas plataformas y aplicaciones con el fin de comunicarse con el CAS Server mediante de algunos protocolos de autenticación que son soportados por CAS server.

Por otro lado, en el CAS Server su característica principal es legitimar a los usuarios y consentir el acceso a los servicios habilitados para CAS, usualmente llamados CAS Clients, a través de la emisión y validación de tickets. Una sesión SSO se crea cuando el servidor emite un ticket de acceso (TGT) al usuario a través de un login óptimo. Un Ticket de Servicio (ST) es emitido para

servicio a petición del usuario mediante un navegador que redirecciona utilizando el TGT como un token. (Vargas, 2016).

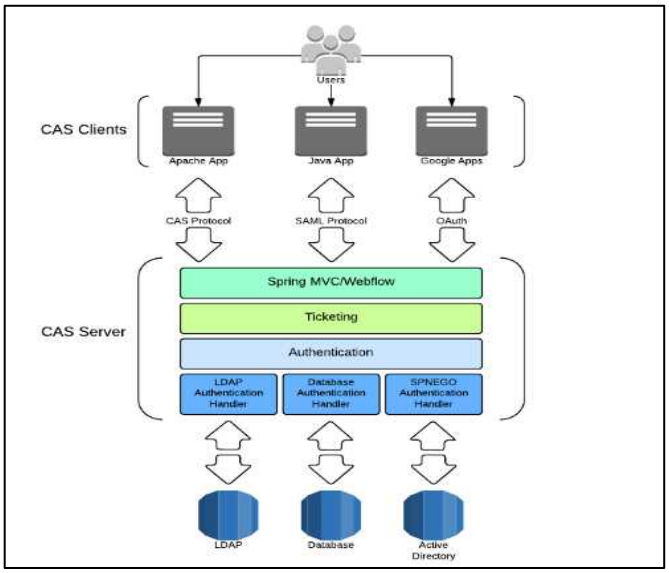

Figura 19-2: Arquitectura de CAS
Fuente: Página oficial de CAS

2.2.8.3 Características CAS:

- Soporte para la autenticación de los usuarios una o múltiples conexiones a LDAP, Bases de datos (Ej: Mysql, Postgresql, etc.), X.509, SPNEGO, etc.

- Soporte para múltiples protocolos como CAS (Protocolo implementado que es propio de este sistema), SAML, OAuth, OpenID, Protocolo REST, etc. Soporte de clientes MultiPlataformas (Java, .Net, PHP, Perl, Apache, etc). Se integra con uPortal, Liferay, BlueSocket, Moodle y Google Apps para nombrar unos pocos. También puede integrarse con una plataforma de SSO federada con Shibboleth.

- Además, tiene una aplicación web aparte para la administración de registros de los servicios que se desean integrar con este sistema llamado CAS Services Management
- Soporte de SSO
- Basado en estándares: XML, HTTP, SOAP, SAML.
- Multiplataforma.
- Soporte para los lenguajes de programación web más utilizados (Java, PHP, ASP).
- Open source.
- Soporte para LDAP (Vargas, 2016)

2.2.8.4 Beneficios CAS:

- Integra varios servidores de base de datos o de directorios activos como MySQL y LDAP.
- Admite integrar múltiples aplicaciones en distintas tecnologías o ambientes de desarrollo.
- Proporciona una agradable comunidad de código fuente abierto que apoya y contribuye activamente al proyecto.
- La familiaridad y la facilidad en la forma de instalación, configuración y extensión de los componentes de CAS. También su documentación es mucho más clara y esta
- Constantemente actualizada por su comunidad. (Vargas, 2016)

2.2.9 Comparativa entre los SSO

Tabla 3-2: Comparativa entre los SSO.

Protocolo	Propósito	Ventajas	Desventajas
Ubuntu Single Sign On	Autentificación	Funciona bajo protocolo OpenID	Sistema únicamente valido para los sitios relacionados con Ubuntu
Enterprise SSO, Web Access Manager	Autentificación	No está basado en tecnologías J2EE, .NET, ASP o PHP, ni en sistemas de usuario (como Windows, Linux, Solaris, AIX, etc.) ni en mecanismos de autenticación específicos o	Licencia no open free membresía de contrato

		especializados (Autenticación HTTP básica, formas de todo tipo y dinámica), o autenticación integrada de Microsoft (por ejemplo, NTLM, Kerberos)).	
WSO2 Identity server	Autentificación	Compatibilidad con la mayoría de sistemas operativos licencia Free & Open Source (Apache 2.0) de libre distribución y funcionan bajo los mismos protocolos (SAML2, OAuth2, SCIM, OpenID y WS-Fed)	
CAS	Autentificación	licencia Free & Open Source (Apache 2.0) de libre distribución y funcionan bajo los mismos protocolos (SAML2, OAuth2, SCIM, OpenID y WS-Fed) fácil de instalar, usar y seguro Soporte de SSO Basado en estándares: XML, HTTP, SOAP, SAML. Multiplataforma. Soporte para los lenguajes de programación web más utilizados (Java, PHP, ASP). Open source. Soporte para LDAP.	Construido en java Configurable vía XML

Realizado por: David Rodríguez. 2019

2.2.10 Los intrusos informáticos

Se puede resumir en pocas palabras como una persona que intenta acceder a un sistema informático sin autorización.

El acceso al sistema puede ser de diversas formas y el propósito final es invadir la privacidad del ordenar llegando incluso a dañar o alterar el software entre ellos están los spyware, malware, virus, troyanos oct.

Se puede hablar de infinidad de intrusos informáticos y sus clasificaciones como lo menciona **Sergio Hernández en su blog:**

"Tales como los *"script-kiddies"*. El nombre hace referencia a la forma habitual en que estos intrusos comprometen los sistemas que atacan, mediante el uso de herramientas desarrolladas por otros y que aprovechan indiscriminadamente contra todos los sistemas que encuentran. La mayoría de este tipo de intrusos son personas

inmaduras ya sea en edad o mentalidad que hacen todo lo posible para no pasa desapercibidos otro tipo de intruso que podemos encontrar Uber-hackers' **Cuya motivación habitual es el robo de información, desde planos de diseño de prototipos hasta tarjetas de crédito, pasando por contraseñas de plataformas de televisión digitales e información privilegiada de bolsa." (Hernandez, 2010)**

2.2.10.1 Hackers

Destaca por su excelencia en programación y electrónica, un conocimiento avanzado en ordenadores y redes informáticas. Su objetivo principal es comprender los sistemas y el funcionamiento de ellos. Buscan y descubren las debilidades de una computadora o red informática. En seguridad informática se diferencian tres tipos: (Hernandez, 2010)

- **Sombreros negros o Black Hats**
  Utilizan sus conocimientos para realizar actividades ilegales, normalmente con ánimo de lucro y para aumentar su reputación. Suelen ser creadores de tipo de malware.
- **Sombreros blancos o White Hats**
  A los sombreros blancos también se les llama hackers éticos. Estos expertos en informática utilizan sus conocimientos para buscar vulnerabilidades y hacer test de penetración, para estudiar y corregir fallos de seguridad y mejorar los sistemas en materia de seguridad. Alertan de un fallo en algún programa comercial, comunicándoselo al fabricante. Pueden formar parte de un equipo de seguridad empresarial o gubernamental. Se pueden dedicar a detectar y localizar a sombreros negros.
- **Sombreros grises o Grey Hats**.
  Como su color indica, tienen una ética ambigua. Suelen utilizar las mismas técnicas que los sombreros negros para encontrar vulnerabilidades y luego venderlas a quién esté dispuesto a pagar por ellas. Su clientela abarca gobiernos, servicios militares y otros hackers. Además, se pueden presentar como expertos en seguridad para resolver los fallos encontrados. Su enfoque suele estar en el lucro más que en perjudicar a las empresas de manera directa. (conectasoftware.com, 2019)

2.2.10.2 *Sniffers*

Sniffers se dedican a rastrear, reconocer y descifrar todos los mensajes que se encuentra o circulan por las redes, hay aplicaciones que no solo se dedican a capturar paquetes de manera indiscriminada, sino que pueden analizar topología de las redes entre las funciones que poseen los sniffers se puede citar.

- Capacidad de obtener información de forma indiscriminada.
- Ver la información del remitente.
- El destino de la información.
- Servidores y procesos que ocupa.
- Tipo de datos que está transmitiendo.
- Los Sniffers pueden ser utilizados de manera legal e ilegal.

Manera ilegal: utilizada por hackers e informáticos con intenciones maliciosas ver información privada, conversaciones, estafar, extorsionar, atacar redes empresariales y de compañías incluso convertirse en un arma de espionaje industrial.

Manera legal: utilizada por empresas en sus redes para controlar la red LAN que se haya organizado en la empresa de esta forma el informático tendrá el control completo sobre la red de una forma efectiva y máxima, se puede hacer auditorias, comprobar el tráfico de la red. (universidadviu.es, 2017)

2.2.10.3 Piratas informáticos

Los piratas informáticos son personas que se dedican al pirateo de programas y contenidos digitales tales como música video juegos películas etc. Estas personas se apropian y distribuyen con fines lucrativos sin permiso ni licencia del autor.

Un pirata informático no necesariamente tiene que ser un experto en informática puede ser una persona común que consume o utiliza estos contenidos digitales son pagar por ellos o sin permiso de su autor existe países donde se bloquea la conexión a internet cuando una persona intenta obtener o copiar esto contenidos digitales de forma ilegal. Por supuesto este no es el caso en nuestro país que se venden programas video juegos música, de forma indiscriminada. (Urban, 2015)

2.2.10.4 Creadores de virus y programas dañinos

Son expertos en informática que buscan ser notados en el sistema y demostrar su conocimiento construyendo programas que daña el software de los computadores y la forma más fácil y rápida es propagarlas a través del internet al cabo de los últimos años se han vuelto más meticulosos para desarrollar virus con fines delictivos ahora no solo desarrollan virus para dañar el software sino que también para robar cuestas bancarias de tarjetas de crédito información corporativa, empresarial y sabotaje industrial todo esto con el fin de estafar o cometer actos fraudulentos entre los distintos tipos de virus podemos mencionar:

- **Residentes:** Este tipo de virus se ocultan en la memoria RAM de forma permanente de este modo interceptan y controlan las operaciones realizadas y llevadas a cabo por el sistema operativo, infectando los ficheros y programas que fueron ejecutados, cerrados, abiertos, copiados, renombrados entre algunos de los virus de este tipo están: Meve, Mrklunky, Randex, etc.
- **De acción directa:** Estos no permaneces en la memora RAM el objetivo primordial de este tipo de virus es reproducirse y actuar en el momento de ser ejecutados se activan y buscan ficheros ubicados dentro de un mismo directorio para contagiarlos.
- **De sobre escritura**: Se caracteriza por destruir la información contenida en un fichero al infectar al fichero escribe dentro de su contenido dañando total o parcialmente el contenido de forma irreversible.
- **De arranque o boot:** Este tipo de virus dañan una sección muy importante del disco como su nombre lo dice la sección de arranque que es la parte donde se guarda toda la información esencial del disco y se encuentra el programa que permite que arranque el computador al prenderlo este tipo de virus no infecta los ficheros sino el disco que los contiene y al momento de ser introducido a un ordenador este infectara al disco duro del ordenador donde se introduzca el disco infectado.
- **Macro:** Los virus macro infecta ficheros de aplicaciones que contengan macros: Documentos de Word, Excel power point ficheros Corel draw, AutoCAD, etc. todos estos ficheros contienen extensiones (DOC, XLS; PPS, ACAD, etc) entonces los macros son micro. Programas asociados a un fichero que sirven para automatizar conjuntos de operaciones.
- **De enlace:** Los virus de enlace o directorio se ubican en determinadas partes de una unidad de disco o directorio que el sistema operativo conoce para poder localizar y trabajar así con ellos.
- **Polimórficos:** son virus que constantemente están cambiando se cifran en diferentes algoritmos de esta forma se generan grandes cantidades de copias de sí mismo y cada vez el antivirus los localizas a través de la búsqueda de cadenas o firmas estos ya han cambiado y no son encontrado siendo los virus más difíciles de detectar por sus características.
- **Multipartites:** Son virus avanzados que realizan múltiples infecciones combinando varias técnicas para ello el objetivo de este tipo de virus es infectar todo lo que encuentre a su paso: discos, programas, macros, archivos, etc.
- **Ficheros:** infecta ficheros y programas ejecutables con extensiones EXE y COM y al ejecutar el programa infectado el virus es activado produciendo diferentes efectos.

- **De FAT:** Los virus FAT afecta a la tabla de asignación de ficheros esta sección es utilizada por el disco para enlazar la información contenida en este. Los virus que atacan esta sección son potencialmente dañinos ya que bloquean el acceso a ciertas partes del disco, donde son almacenados los ficheros críticos para el funcionamiento normal del computador.

2.2.10.5 Crackers

Ser un Crack es ser muy bueno en algo. Ser un cracker es saber romper algo, en este caso sistemas y software. Tienen un conocimiento profundo de programación y electrónica. Nos pueden sonar de los cracks que permiten utilizar un software sin haber pagado por la licencia. Dicho en otras palabras, la edición desautorizada de software de propiedad. La fascinación de un cracker por romper sistemas y software suele ser motivado por una multitud de razones, desde el lucro, pasando por actos de protesta hasta el simple desafío. Siempre encuentran el modo de romper una protección y estas roturas se suelen filtrar o difundir en la red para el conocimiento de los demás.

2.2.11 Seguridad de la información

La seguridad informática se encarga de resguardar los recursos de los sistemas informáticos, como el hardware y software, es decir, toda la infraestructura computacional que puede ser de una organización y a la cual se puede acceder bajo estándares, parámetros y métodos restrictivos que disminuyen las amenazas informáticas.

Dentro de los elementos fundamentales que deben protegerse en los sistemas informáticos se encuentran el software, el hardware y los datos.

Hardware, proviene de la fusión de dos vocablos de la lengua anglosajona: *hard* que puede significar *"duro"* y *ware* que es sinónimo de *"cosas"*. Este elemento es el conjunto de los componentes que conforman la parte material o física de una computadora y pueden ser dispositivos físicos internos como el disco duro, placa madre, microprocesador, circuitos, cables, etc, y también los periféricos como (escáners, impresoras). Por otro lado, por ***software*** se entiende a los componentes lógicos o intangibles de una computadora. Este conjunto de programas son los que se ligan a un sistema de cómputo. El software es la herramienta para que un sistema o programa se efectúe efectivamente y su desenvolvimiento sea viable y sencillo.

Y finalmente los ***datos***, son el conjunto de información lógica que opera el software y el hardware y que pueden ser los paquetes que circulan por un cable de red o entradas de una base de datos.

2.2.11.1 Áreas principales que cubre la seguridad informática

Los componentes de un sistema informático pueden ser vulnerables frente a una infiltración ilegal o a un ataque; en el que la confidencialidad, la integridad, o la disponibilidad de la información quedan expuestas a una tergiversación o robo.

Considerando la premisa anterior, la seguridad de los datos y la información, se comprendería entonces 3 aspectos fundamentales:

- **Confidencialidad:** Se refiere a que todo archivo debe tener la facultad de poder ser leído, procesado y entendido por la persona o sistema que lo autorice, como por ejemplo la utilización de un cifrado de clave simétrica dentro de un intercambio de mensajes.
- **Integridad:** Esta característica permite verificar si el documento o archivo ha sido modificado o alterado por personas que hayan tenido autorización y así también si fuesen usuarios que no la han tenido.
- **Disponibilidad:** La disponibilidad se refiere a que los servicios o bases de datos deben mantenerse disponibles para el acceso de los usuarios cuando sea requerido. También trata de la capacidad de que la información perdida pueda ser recuperada. Dentro de la disponibilidad encontramos la alta disponibilidad o Hight *Availability*, este sistema está disponible durante todo el día, los siete días de la semana, y los 365 días de un año.

Se puede percibir la disponibilidad en varios niveles:

- **Base*:*** Ocurre en paradas previstas e imprevistas.
- **Alta*:*** Se adquiere tecnologías que reducen el número y el tiempo de interrupciones imprevistas.
- **Operaciones continuas*:*** Detecta y asegura que no se presenten las interrupciones planificadas.
- **Sistemas de disponibilidad continua*:*** Se incluyen tecnologías que verifiquen que no se suscitarán paradas imprevistas, ni previstas.
- **Sistemas de tolerancia al desastre*:*** Son sistemas que están separados entre sí para poder acaparar y tomar el control en una interrupción provocada por un desastre.

Los aspectos descritos son los generales para mantener una seguridad óptima, y cada uno será priorizado dependiendo el contexto en el que se desenvuelva el sistema. Además, de la mano de estos elementos fundamentales, es muy probable que también se genere la necesidad de estudiar

y aplicar conjuntamente los siguientes conceptos: *autenticación* y el *no repudio,* mismos que serán desglosados a continuación.

2.2.11.1.1 Autenticación

Este elemento permite verificar que la información, el archivo o documento que está en mira sea realizado por quién se mencione. La autenticación de los sistemas informáticos se produce mediante códigos, comandos o contraseñas y radica en la ratificación de la identidad de un usuario. Es decir, brinda la certeza para que cada una de las partes asegure que se está comunicando con el interlocutor que se supone ser. Este control viabiliza el acceso único a los recursos e información solamente a las personas autorizadas.

2.2.11.1.2 No repudio

La irrenunciabilidad o el no repudio de información hace referencia a que después de realizada una operación sistemática ninguna de las dos partes implicadas puede negar su participación en la comunicación.

Se tienen dos posibilidades para manejar el ***No repudio:***

No repudio en origen: El destinatario adquiere una prueba infalsificable del envío de la comunicación por parte del receptor, por lo tanto, este último no puede negar lo que se suscitó en el proceso informativo.

No repudio de destino: El receptor no puede negar que fue parte de la comunicación porque el emisor tiene evidencias de la recepción.

Si la autenticidad prueba quien es el autor y cuál es su destinatario, el no repudio prueba que el autor envió la comunicación (en origen) y que el destinatario la recibió (en destino).

Al conjunto de características mencionadas anteriormente se les denomina CIDAN, por la inicial de cada una de las mismas.

Cuando se habla de seguridad se asocia a la falta de riesgo, contingencia y a la certeza de la información, por lo cual se debe entender a través de sus niveles, ya que una seguridad absoluta no es posible, pero si puede tener un rango alto de probabilidades de no ser interceptada o violada. La seguridad considerada como un problema integral, provoca que sus elementos no puedan ser tratados aisladamente, ya que la seguridad de todo el sistema es igual a su punto más débil. El uso de sofisticados algoritmos y métodos es inútil si no garantizamos la confidencialidad de las

estaciones de trabajo y a la vez, existe algo que los hackers llaman *ingeniería asociada*. La ingeniería asociada se refiere a que se puede conseguir mediante un engaño que los usuarios que si son autorizados develen sus passwords, por lo tanto, una educación en seguridad informática de los usuarios es fundamental para que la tecnología pueda efectuarse exitosamente.

2.2.11.2 Formas de protección de un sistema de información:

Para proteger un sistema informático se realiza un rastreo de las amenazas potenciales, las pérdidas que podrían suscitarse y la probabilidad de que se efectúen. Por lo tanto, es necesario diseñar una política de seguridad que diferencie las reglas y responsabilidades que se deben seguir para esquivar y sobrellevar los efectos de una amenaza si esta llegara a consumarse.

Estos mecanismos de seguridad que brindan protección a los sistemas y a la red, se pueden clasificar en activas o pasivas.

- **Activas** evitan daños en los sistemas informáticos mediante empleo de contraseñas adecuadas en el acceso a sistemas y aplicaciones, encriptación de los datos en las comunicaciones, filtrado de conexiones en redes y el uso de software específico en seguridad informática.
- **Pasivas:** minimizan el impacto y los efectos causados por accidentes mediante uso de hardware adecuado, protección física, eléctrica y ambiental, realización de copias de seguridad.

2.2.11.3 Criptografía

El aparecimiento de nuevas redes comunicativas, sobre todo de Internet, ha viabilizado nuevas posibilidades para el intercambio de información. Así como también, las amenazas a la seguridad de la información que ascienden intempestivamente. Por lo tanto, para suplir las necesidades actuales de información se deben crear otros mecanismos, que garanticen la confidencialidad y autenticidad de los documentos electrónicos. A este proceso se denomina Criptografía.

La Criptografía se inclina al paisaje de los mensajes digitales, suministrando los materiales adecuados para solucionar los problemas ligados a la autenticidad y la confiabilidad. El problema de la confidencialidad se vincula comúnmente con técnicas denominadas de *"encripción"* y la autenticidad con técnicas denominadas de "firma digital". Este nuevo método, se encarga de enviar información confidencial por un medio inseguro, que garantice la confidencialidad.

Según el autor Bradanovic la Criptografía encripta la información de manera que, aun cuando se encuentre disponible para cualquiera, no pueda utilizarla, a menos que alguien autorizado la descifre. (vcd.cl, 2003)

- La diferencia entre criptografía y seguridad informática:
- En un modelo criptográfico típico, existen dos puntos: "a" y "b", que se consideran fiables y, entre ellos, se transmite información mediante un canal no fiable. La Criptografía se ocupa de los problemas relacionados con la transmisión confidencial y segura por el medio no fiable, en tanto la seguridad informática se ocupa de asegurar la fiabilidad de los nodos "a" y "b".
- La Criptografía se divide en dos grandes ramas: Clave privada o simétrica y la Criptografía de clave pública o asimétrica.
- La primera se refiere al conjunto de métodos que permiten una comunicación segura entre las partes siempre que, con anterioridad, se intercambie la clave correspondiente, que se denomina clave simétrica. La simetría se refiere a que las partes tienen la misma llave, tanto para cifrar como para descifrar. (criptored.upm.es, 2003)
- Los sistemas criptográficos se clasifican en:
  - El número de claves usadas
  - El tipo de operación utilizado para transformar el texto claro en texto cifrado
  - La forma de procesar el texto claro

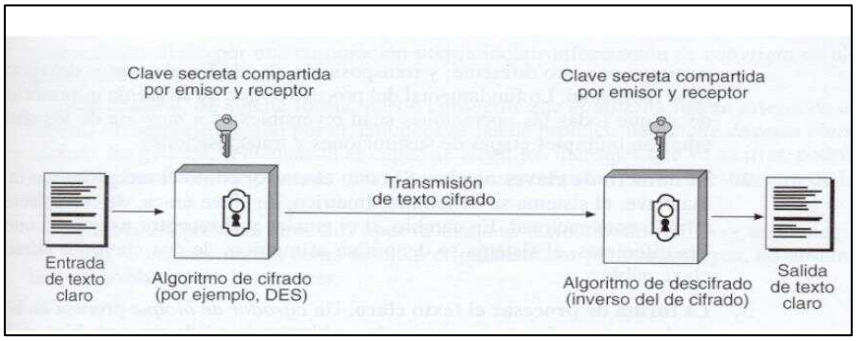

Figura 20-2: Esquema de cifrado simétrico
Fuente: http://www.criptored.upm.es/guiateoria

- Criptología**:** Es la unión de criptografía y criptoanálisis:
  - Criptografía**:** Es la disciplina referente a la construcción de sistemas de cifrado; estudia las técnicas para hacer que la información en un mensaje sea más fácil de entender para el destinatario que tiene una clave secreta para el uso y acceso de ella.

- Criptoanálisis**:** Es la disciplina referente al rompimiento de sistemas de cifrado, que busca recuperar la información sin necesidad de un código o clave. El resultado es, que siempre que avanza una, su contraparte necesita ser revisada. Una vez que se logró romper una técnica criptográfica, ésta necesitará aumentar su complejidad. (Itzcoatl, 2010)

- Sistemas de cifrado DES Y AES (Algoritmos de Encriptación): Cuando surgieron los primeros computadores apareció a la vez la necesidad de cifrar la información en los diversos sistemas informáticos, y las organizaciones de seguridad de los países buscaron algoritmos de cifrado que sean fuertes, accesibles y rápidos para poder manejarlos. Estos algoritmos eran de clave privada lo que quiere decir que existe una clave en la que para acceder a la información se debía tener el conocimiento de la misma. (Luz, 2010)
- DES (Data Encryption Standard): Es un método antiguo de la encriptación de los datos, lo que no facilita que la información sea leída por otras personas que podrían interceptar el tráfico. Desde entonces ha sido sustituida por AES (Advanced Encryption Standard), este algoritmo se suplantó debido a las debilidades que resultaba de DES porque permitía que el cifrado se rompa cuando aparecían ataques.
- Con el aparecimiento de AES hasta la actualidad, las aplicaciones de uso más comunes, siguen siendo impermeable a cualquier forma de craqueo, lo que hace que sea una opción adecuada inclusive para información secreta. (Carrada, 2014)
- AES (Advanced Encryption Standard - AES): Es entendido también como Rijndael. Esquema de cifrado por bloques, que fue acogido como estándar de cifrado por el gobierno de Estados Unidos. Sustituye progresivamente a su antecesor (DES y Triple DES). Este algoritmo fue instaurado como estándar por la NSA y desde ese momento ha sido el algoritmo más utilizado en gran diversidad de ámbitos, tanto en el sector privado como en el público y en los gobiernos. (Carrada, 2014)
- Seguridad de AES. La seguridad de AES se fundamenta en la longitud de la clave, cuanto mayor es el tamaño de clave mayor es el número de rondas que debe realizar el cifrador y por tanto mayor número de operaciones.

Comparación DES Y AES

- DES es obsoleto, mientras que AES es prácticamente nuevo
- DES es delicado mientras que AES es hasta hoy indestructible
- DES maneja un tamaño de clave mucho más pequeño en comparación con AES
- DES utiliza un tamaño de bloque más pequeño en comparación con AES

- DES ocupa una estructura de Feistel equilibrada, mientras que AES utiliza sustitución-permutación. (Chovis, 2016)

La debilidad de DES es producida por características que ya están cubiertas por AES:

- La clave de cifrado es muy corta, tiene 56 bits. La clave es una contraseña que es necesaria para descifrar la información. 56bits tiene un máximo de 256 combinaciones, lo que podría parecer mucho, pero es bastante fácil para un equipo porque no puede soportar un ataque de fuerza bruta.
- AES puede utilizar una clave de cifrado de 128 bits, 192, o 256 con 2 ^ 128, 2 ^ 192, 2 ^ 256 combinaciones respectivamente. Las claves de cifrado más largas hacen que sea mucho más difícil de romper, dado que el sistema no tiene otros puntos débiles.
- También existe otro problema que es el tamaño de bloque pequeño utilizado por DES, ya que se fija en 64 bits.
- En comparación, AES utiliza un tamaño de bloque que es el doble de largo a 128 bits. El tamaño de bloque determina la cantidad de información que puede enviar antes de empezar a tener bloques idénticos, que se filtran información. Las personas pueden interceptar estos bloques y su utilización.
- Para DES con 64 bits, la cantidad máxima de datos que se pueden transferir con una sola clave de cifrado es de 32 GB; en este punto otra clave necesita ser utilizado. Con AES, es a 256 exabytes o 256 mil millones de gigabytes. (Chovis, 2016)

2.2.12 Tipos de ataques a la información

Tipos de ataques:

- **Ingeniería social**: Estos ataques están basados en la interacción humana porque obtienen información de una organización o sus sistemas computacionales. Un atacante podría parecer inocente, tan solo si aduce que es un nuevo empleado, una persona del servicio técnico, o un investigador, inclusive puede ofrecer credenciales que avalen su identidad. De tal manera, solamente realizando preguntas simples, una persona podría recabar suficiente información para infiltrar la red de una organización. Si un atacante no puede adquirir información de una fuente, podría contactar a otra persona dentro de la misma organización y usar la información parcial, obtenida de la primera fuente para tratar de acreditar su identidad El Phishing es una forma de ingeniería social.

a) **Ingeniería social inversa**: la ingeniería social: de persona a persona, teléfono, sitio web, correo electrónico, red social, etc…), sin saberlo con la persona que desea obtener información de él y una vez establecido el contacto ésta obtiene la información necesaria para realizar el ataque o la intrusión.

b) **Monitorización:** Se realiza para observar a la víctima y su sistema, con el objetivo de establecer sus vulnerabilidades y posibles formas de acceso futuro.

c) **Ataque de autenticación:** Tiene como finalidad traicionar al sistema de la víctima para ingresar al mismo. Generalmente este engaño se realiza tomando las sesiones ya establecidas por la víctima u obteniendo su nombre de usuario y password.

d) **Análisis del tráfico**: Estos ataques tratan de observar los datos y el tipo de tráfico transmitido a través de redes informáticas, utilizando para ello herramientas como los "sniffers". Así, se conoce como "eavesdropping" a la interceptación del tráfico que circula por una red de forma pasiva, sin modificar su contenido.

- **Ataques de suplantación de la identidad:**
  a) **IP Spoofing** ("enmascaramiento de la dirección IP"): Mediante la cual un atacante obtiene modificar la cabecera de los paquetes enviados a un determinado sistema informático para simular que proceden de un equipo distinto al que verdaderamente los ha originado.
  b) **DNS Spoofing:** Los ataques de falsificación de DNS procuran provocar un direccionamiento erróneo en los equipos afectados, debido a una traducción errónea de los nombres de dominio a direcciones IP, facilitando de este modo la redirección de los usuarios de los sistemas afectados hacia páginas Web falsas o bien la interceptación de sus mensajes de correo electrónico.
  c) **SMTP Spoofing:** El envío de mensajes con remitentes falsos ("masquerading") para tratar de engañar al destinatario o causar un daño en la reputación del supuesto remitente es otra técnica frecuente de ataque basado en la suplantación de la identidad de un usuario.
  e) **Conexión no autorizada a equipos y servidores:** Existen varias posibilidades para establecer una conexión no autorizada a otros equipos y servidores, entre las que podríamos destacar las siguientes:
     - **Violación de sistemas de control de acceso.**
     - **Explotación de "agujeros de seguridad" ("exploits").**

- **Utilización de "puertas traseras" ("backdoors"),** conjunto de instrucciones no documentadas dentro de un programa o sistema operativo, que permiten acceder o tomar el control del equipo saltándose los controles de seguridad.
- **Utilización de "rootkits",** programas similares a los troyanos, que se instalan en un equipo reemplazando a una herramienta o servicio legítimo del sistema operativo.
- **"Wardialing":** conexión a un sistema informático de forma remota a través de un módem. (Gómez Á. , 2018)

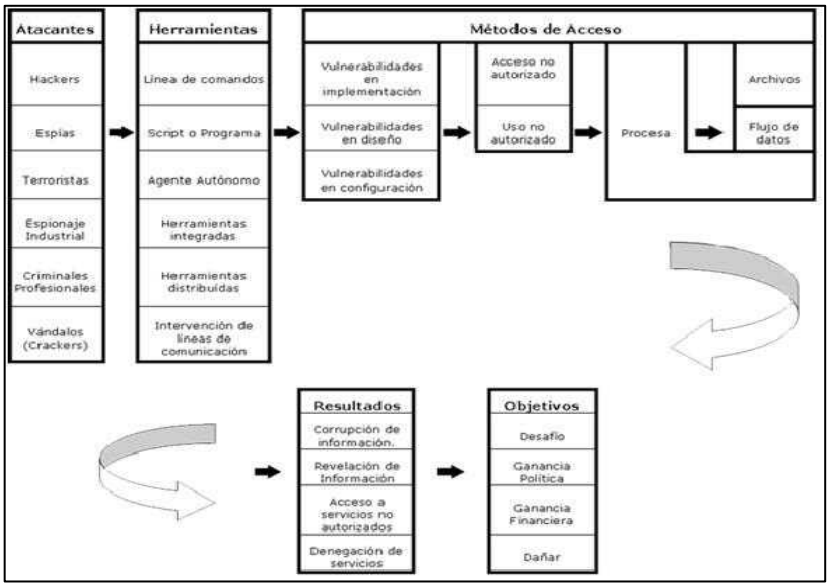

Figura 21-2: Tipos de atacantes informáticos
Fuente: http://blanca-pke20je.blogspot.com/2010/11/tipos-de-intrusos-informaticos.html

2.2.13 Herramientas para prueba de carga y rendimiento

Entre las herramientas utilizadas tenemos:

- FWPTT load testing
- Jmeter

FWPTT load testing: Es un programa de pruebas de carga de aplicaciones web, permite al usuario importar las sesiones de navegación grabadas con Fiddler. Estas solicitudes http se pueden importar y usar para generar una clase c que llama a todas las solicitudes http que el usuario haya registrado previamente. Luego de usar el corrector de pruebas, el usuario podrá ejecutar el código de su clase de prueba; para funcionar requiere de .net 4.7.2 de Microsoft. (fwptt, 2018)

JMeter: La aplicación Apache JMeter es un software de código abierto, una aplicación Java 100% pura diseñada para cargar el comportamiento funcional de la prueba y medir el rendimiento. Se puede usar para probar el rendimiento tanto en recursos estáticos como dinámicos, aplicaciones

dinámicas web. Se puede usar para simular una carga pesada en un servidor, grupo de servidores, red u objeto para probar su resistencia o para analizar el rendimiento general bajo diferentes tipos de carga. (Foundation, 2019)

JMeter se basa en "Elementos" y en una estructura en árbol, al crear un plan de pruebas se crea una "lista ordenada" de peticiones (Request http) utilizando "samplers" que representan los pasos a ejecutar. Podemos especificar el número de threads (hilos de ejecución) en paralelo, así como el tiempo de arranque de cada uno, y número de iteraciones que hará cada uno de ellos.

Las características de Apache JMeter incluyen:

- Capacidad de carga
- Prueba de rendimiento de muchos tipos diferentes de aplicaciones / servidor / protocolo
- Web: HHTP, HTTPS (Java, NodeJS, PHP, ASP.NET)
- SOAP / REST Webservices
- FTP
- Database vía JDBC
- LDAP
- Message-oriented middleware (MOM) vía JMS
- Mail – SMTP (S) y IMAP (s)
- Comandos nativos o scripts de shell
- TCP
- Java Objects

2.2.14 Software estadístico

La plataforma del software de IBM SPSS® ofrece análisis estadístico avanzado, una vasta biblioteca de algoritmos de machine learning, análisis de texto, extensibilidad de código abierto, integración con big data e implementación continua en las aplicaciones. Su facilidad de uso, flexibilidad y escalabilidad hacen que IBM SPSS sea accesible para los usuarios con todos los niveles de habilidades y los proyectos conjuntos de todos los tamaños y complejidad, para ayudarle a usted y a su organización a encontrar nuevas oportunidades, mejorar la eficiencia y minimizar el riesgo. (IBM, 2018)

2.2.15 Comando TOP

El comando **TOP** proporciona una vista dinámica en tiempo real de un sistema en ejecución. Puede mostrar información resumida del sistema, así como una lista de procesos o subprocesos

actualmente gestionados por el kernel de Linux. Los tipos de información de resumen del sistema que se muestran y los tipos, orden y tamaño de la información que se muestra para los procesos. (linux, 2019)

Ejecutar el comando

Abrir la consola y ejecutar el comando: top

```
[root@serverWebGuia ~]# top
```

Nos aparece una interfaz en modo texto que se actualiza cada 3 segundos, muestra un resumen del estado de nuestro sistema y la lista de procesos que se están ejecutando.

```
top - 19:35:13 up 3 min,  1 user,  load average: 0,11, 0,30, 0,15
Tasks: 100 total,   2 running,  98 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0,3 us,  1,0 sy,  0,0 ni, 98,7 id,  0,0 wa,  0,0 hi,  0,0 si,  0,0 st
KiB Mem :  1439928 total,  1162416 free,   132756 used,   144756 buff/cache
KiB Swap:  2883580 total,  2883580 free,        0 used.  1145060 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
 3518 root      20   0  161876   2216   1560 R  1,6  0,2   0:00.16 top
   25 root      20   0       0      0      0 S  0,3  0,0   0:00.60 kworker/0:1
 3236 root      20   0  573920  17088   6012 S  0,3  1,2   0:00.99 tuned
    1 root      20   0  128028   6524   4132 S  0,0  0,5   0:03.19 systemd
    2 root      20   0       0      0      0 S  0,0  0,0   0:00.01 kthreadd
    3 root      20   0       0      0      0 S  0,0  0,0   0:00.12 ksoftirqd/0
    4 root      20   0       0      0      0 S  0,0  0,0   0:00.00 kworker/0:0
    5 root       0 -20       0      0      0 S  0,0  0,0   0:00.00 kworker/0:0H
```

Gráfico 1-2: Interfaz de consumo de recurso del comando TOP
Realizado por: David Rodríguez. 2019

2.2.16 Análisis multicriterio

La "teoría de evaluación multicriterio" comprende en realidad un conjunto de teorías, modelos y herramientas de apoyo a la toma de decisiones, aplicable no sólo al análisis de inversiones sino a una amplia gama de problemas en la gestión tanto privada como pública tales como: análisis de posicionamiento de marcas en el mercado, medición de percepciones de clientes y selección de tecnologías. (Sara Arancibi, 2019)

Método discreto multicriterio, cuya matriz de impacto que puede incluir medidas nítidas, estocásticas o difusas del rendimiento de una alternativa con un respecto a un criterio de juicio, por lo que es flexible para aplicaciones del mundo real. Esto lo hace particularmente útil para estudios donde se incluyen parámetros con varios grados de precisión de las variables establecidas.

CAPÍTULO III

3 DISEÑO DE LA INVESTIGACIÓN

3.1 Tipo y diseño de investigación

La perspectiva por la que se encaminará este estudio será cuasi-experimental, teniendo en cuenta que debe verificarse si la hipótesis dispone de validez que todo trabajo de investigación debe tener. Para realizar el análisis de las técnicas aplicadas en el sistema informático, será necesario explicar y describir cada uno de los procesos metodológicos empleados por los usuarios, con el propósito de evaluar sí son correctas.

3.1.1 Tipo de investigación

La siguiente investigación presenta los siguientes tipos de investigación:

Aplicativa: Se utiliza el conocimiento de tecnologías ya existentes basadas en algoritmos, secuencias y programación ya dadas. Y se compara cuál de los sistemas de sesión único CAS o WSO2 Identity server es mejor en cuanto a rendimiento, velocidad, tiempo de repuesta y consumo de recursos.

Cuantitativa: ya que en el presente estudio se analiza datos obtenidos de los servidores de AGROCALIDAD de la comparación de rendimiento, capacidad, tiempo de respuesta y consumo de los recursos entre los sistemas de inicio de sesión único CAS y WSO2 Identity server de los cuales obtenemos un resultado y podemos comparar cual es mejor en los parámetros antes expuestos.

Longitudinal: la investigación se la realiza con un seguimiento de los procesos a lo largo de un tiempo determinado con el cual observamos la evolución y resultado del estudio realizado.

Experimental: Se utiliza el conocimiento en sistemas de inicio de sesión único para realizar la comparación entre rendimiento, capacidad, tiempo de respuesta y uso de recurso de los sistemas CAS y WSO2 Identity server.

3.1.2 Diseño de investigación

El presente trabajo de investigación es cuasi- experimental, cuantitativo, aplicativo y longitudinal ya que se ha propuesto comparar el rendimiento de dos sistemas de inicio de sesión único (SSO) CAS y WSO Identity server en los servidores de AGROCALIDAD en un universo de 292 servidores y comprobar cuál de los dos es mejor en cuanto a tiempo de respuesta, capacidad y uso de recursos (RAM, CPU).

3.2 Métodos de investigación

El método que se empleará durante el transcurso de la investigación será el inductivo-deductivo por lo que se trata de elaborar una guía de buenas prácticas para la implementación de un sistema SSO en AGROCALIDAD que permita proteger la institucionalidad de la información, actividad posterior a su análisis.

3.2.1 Método experimental y de observación

Método científico: el cual consta de algunas etapas para obtener un conocimiento valido desde el punto de vista científico, y para que estos resultados sean confiables consta de varias etapas:

- El planteamiento del problema que es la base de la investigación
- El proceso previo a la formulación de la hipótesis
- Recopilación de la información necesaria
- Análisis e interpretación de los resultados
- El proceso de comprobación de la Hipótesis e interpretación de resultados

Método hipotético deductivo: se utilizó este método al estudiar de forma general todos los tipos de sistema de inicio de sesión único, y se intentó encontrar el más adecuado para la presente investigación reducidos a dos el CAS y WSO2 IDENTITY SERVER.

Método comparativo: después del estudio de un conjunto de plataformas solo se tomó dos CAS y WSO2 IDENTITY SERVER para la comparación, en igualdad de condiciones en una misma institución y comparar cuál de los dos es mejor en cuanto a rendimiento, tiempo de respuesta, consumo de recursos y capacidad.

Método analítico: el cual nos permite desarticular la variable dependiente en cuanto a sus diferentes características o indicadores: tiempo de respuesta, uso de recursos y capacidad, para después mediante el análisis y síntesis de los resultados se llegue a la conclusión.

3.3 Enfoque de la investigación

En lo que se refiere al enfoque de la investigación se analizará de manera cualitativa, por lo que se busca es diseñar un sistema que reúna la aplicación de técnicas de autenticación y protocolos de cifrado, exponiendo los diversos beneficios.

El alcance de la investigación permitirá plantear los siguientes interrogantes: el porqué de la investigación, para qué y a quiénes podría beneficiar.

El cual se lo realizara en la provincia Pichincha, cantón Quito (Av. Eloy Alfaro N30-350 y Av. Amazonas, Ministerio de Agricultura y Ganadería – MAG, piso 9).

3.4 Alcance de la Investigación

Se realizará una investigación correlacionar porque se realizará una comparación entre las dos variables. Se realizará una guía metodológica del proceso realizado en la comparativa de los sistemas de autenticación SSO.

3.5 Población de estudio

AGROCALIDAD actualmente cuenta con 1200 usuarios como se muestra en la tabla 1-3, los cuales acceden a los diferentes aplicativos de la organización, la población de estudio utilizada para la presente investigación está conformada por el número de inicio de sesión exitosos en el sistema SSO para cada usuario de AGROCALIDAD que corresponde a 1200.

Tabla 1-3: Usuarios de AGROCALIDAD

Coordinación / Dirección	Usuarios
Coordinación General de Inocuidad de Alimentos	16
Coordinación de laboratorios	58
Coordinación General de Registro de Insumos Agropecuarios	28
Coordinación General de Sanidad Animal	32
Coordinación General de Sanidad Vegetal	33
Dirección de Comunicación Social	15

Direccionamiento Estratégico	6
Dirección General Administrativo Financiero	51
Dirección General de Asesoría Jurídica	13
Dirección General de Administración de Talento Humano	18
Dirección de Gestión Documental y Archivo	20
Dirección General de Planificación y Gestión Estratégica	19
Dirección de Tecnologías de la Información y Comunicación	21
Dirección Distrital y Articulación Territorial 1 – Sucumbíos	99
Dirección Distrital y Articulación Territorial 2 – Pichincha	124
Dirección Distrital y Articulación Territorial 3 – Tungurahua	101
Dirección Distrital y Articulación Territorial 4 – Santo Domingo	91
Dirección Distrital y Articulación Territorial 5 – Guayas	237
Dirección Distrital y Articulación Territorial 6 – Cañar	88
Dirección Distrital y Articulación Territorial 7 – El Oro	130
Total	**1200**

Realizado por: David Rodríguez. 2019

En la tabla 1-3 se muestra la cantidad de servidores que existe en cada coordinación, dirección de AGROCALIDAD.

3.6 Unidad de análisis

Los objetivos de estudio involucrados en la presente investigación son, un universo total de 1200 servidores de AGROCALIDAD con los SSO (CAS y WSO2 Identity server).

3.7 Selección de la muestra

En base a los escenarios propuestos para la comparativa de los sistemas de autenticación Single Sign One CAS y WSO2 Identity server se calcula la muestra con una población finita en **292** según la fórmula que se muestra a continuación:

$$Tamaño\ de\ la\ muestra = \frac{N * Z\alpha^2 * p * q}{d^2 * (N-1) + Z\alpha^2 * p * q}$$

Dónde:

N = Tamaño de la población	1200
$Z\alpha^2$ = seguridad del 95%	1.96^2
p = proporción esperada (5%)	0,05
q = 1 –p (en este caso 1-0,05)	0.95
d = precisión (3%)	0.03

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

$$Tamaño\ de\ la\ muestra = 292$$

3.8 Técnica de recolección de datos

Las técnicas que serán utilizadas en la presente investigación son:

- Búsqueda de información: permite obtener la información necesaria acerca del objeto de estudio de la investigación para su desarrollo, utilizando las fuentes secundarias disponibles.
- Pruebas: permite realizar las pruebas de rendimiento entre los sistemas SSO WSO2 Identity Server y CAS.
- Observación: permite determinar resultados de las pruebas realizadas entre los sistemas SSO WSO2 Identity Server y CAS.
- Análisis: permite determinar los resultados de la investigación.

Las fuentes que se tomarán como base para esta investigación serán:

Primarias

- Papers y Revistas científicas
- Investigaciones realizadas
- Libros

Secundarias

- Observaciones

- Textos

3.9 Instrumentos de recolección de datos primarios y secundarios

Para la variable independiente se utilizará el sistema de autenticación planteado, permitiendo así evaluar los indicadores planteados.

En cuanto a la variable dependiente se usará un software para probar el rendimiento de cada sistema SSO.

3.10 Instrumentos para procesar datos recopilados

Los instrumentos para procesar los datos de los indicadores son los siguientes:

- Software estadístico SPSS para realizar el procesamiento de los datos recopilados.
- La presentación de los datos se dará a través de gráficos cuadros para analizar e interpretarlos.
  - Redactar una síntesis general de los resultados.

3.11 Variables e indicadores

3.11.1 Variable independiente

El sistema de autenticación utilizado.

3.11.2 Variable dependiente

Rendimiento del proceso de autenticación de usuarios para los aplicativos de AGROCALIDAD.

3.12 Operacionalización de variables

Tabla 2-3: Operacionalización de Variables

Hipótesis	Variables	Conceptualización
Los sistemas de autenticación (SSO) CAS y WSO2 IDENTITY SERVER presentan una diferencia significativa en cuanto al rendimiento del proceso de autenticación de usuarios para los aplicativos de AGROCALIDAD (Agencia de regulación y control fito y zoosanitario).	**Independiente:** El sistema de autenticación utilizado.	• SSO (Inicio de sesión único) Procedimiento de autenticación que habilita al usuario para acceder a varios sistemas con una sola instancia de identificación • CAS (servicio de autenticación central) los usuarios accedan a múltiples servicios con un inicio de sesión único. • WSO2 Identity Server facilita la seguridad al conectar y gestionar múltiples identidades en diferentes aplicaciones.
	Dependiente: Rendimiento del proceso de autenticación de usuarios para los aplicativos de AGROCALIDAD.	• La medida o cuantificación de la velocidad / resultado con que se realiza una tarea o proceso

Realizado por: David Rodríguez. 2019

3.12.1 Matriz de consistencia

Para realizar la matriz de consistencias se están estableciendo los indicadores e índices que permitirán estudiar las variables dependiente e independiente y de esta forma obtener resultados a partir de mediciones, este proceso se lleva a cabo con descripciones en tablas donde se ingresó objetivo general, hipótesis, variables, indicadores, técnicas e instrumentos de medición.

Tabla 3-3: Matriz de Consistencia

Formulación del problema	Objetivo General	Hipótesis	Variables	Indicadores	índices	Técnicas	Instrumentos
¿Cuál de los sistemas de autenticación Single Sign One (SSO) CAS (sistema de autenticación central) y WSO2 IDENTITY SERVER ofrece mejor rendimiento del proceso de autenticación de usuarios para los aplicativos de AGROCALIDAD (Agencia de regulación y control fito y zoosanitario)?	Comparar el rendimiento de los sistemas de autenticación SINGLE SIGN ONE (SSO) CAS y WSO2 IDENTITY SERVER para el proceso de autenticación de los aplicativos de AGROCALIDAD	Los sistemas de autenticación (SSO) CAS y WSO2 IDENTITY SERVER presentan una diferencia significativa en cuanto al rendimiento del proceso de autenticación de usuarios para los aplicativos de AGROCALIDAD (Agencia de regulación y control fito y zoosanitario).	**Independiente** El sistema de autenticación utilizado			• Experimentación • Observación • Evaluación	• JMeter
			Dependiente Rendimiento del proceso de autenticación de usuarios para los aplicativos de AGROCALIDAD	• Tiempo de respuesta	• Cantidad de segundos por tarea	• Experimentación • Observación • Test de rendimiento • Análisis de rendimiento • Comprobación	• JMeter • Herramientas del sistema operativo
				• Consumo de recursos	• Porcentaje de uso de CPU. • Porcentaje de uso de RAM		
				• Capacidad	• Cantidad de peticiones		

Realizado por: David Rodríguez. 2019

3.13 Procesamiento y análisis

La información recopilada en la investigación es analizada y presentada en barras y aplicando la inferencia con la prueba z con una muestra de 292 servidores para determinar la comprobación o anulación de la hipótesis.

3.13.1 Método de FURPS

Modelo desarrollado por Hewlett-Packard (HP) en 1987, desarrollando un conjunto de factores de calidad de software y sus respectivos atributos. Se utilizan para establecer métricas de la calidad para todas las actividades del proceso de desarrollo de un software, inclusive de un sistema de información. (Pereira, Ayaach, Quintero, & Granadillo, 2019)

Atributos:

- Velocidad de Procesamiento (VR)
- Tiempo de respuesta (TR)
- Consumo de Recurso (CR)
- Eficiencia (E)

3.13.2 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. En este modelo se determinan las características de calidad que se van a tener en cuenta a la hora de evaluar las propiedades de un producto software determinado (ISO, 2019). Una característica es eficiencia de desempeño que determina la cantidad de recursos utilizados bajo determinadas condiciones que se subdivide en:

- **Comportamiento temporal**. - Los tiempos de respuesta y procesamiento y los ratios de throughput de un sistema cuando lleva a cabo sus funciones bajo condiciones determinadas en relación con un banco de pruebas (benchmark) establecido.
- **Utilización de recursos. -** Las cantidades y tipos de recursos utilizados cuando el software lleva a cabo su función bajo condiciones determinadas.
- **Capacidad. -** Grado en que los límites máximos de un parámetro de un producto o sistema software cumplen con los requisitos.

3.13.3 Definición de Variables

Basado en las métricas de calidad citadas anteriormente se aplicará el análisis estadístico inferencial del tiempo de respuesta por lo que se define la siguiente tabla.

Tabla 4-3: Variables para el análisis de datos

Variables	Unidad	Modelo	Definición
Tiempo de respuesta (TR)	Milisegundos(ms)	FURPS, ISO/IEC 25010	El tiempo transcurrido entre el momento que se envía la petición y el momento que se recibe la respuesta.
Consumo de Recurso (RAM)	Megabyte (Mb)	FURPS, ISO/IEC 25010	Memoria en uso durante la ejecución del plan de pruebas.
Consumo de Recurso (CPU),	Porcentaje (%)	FURPS, ISO/IEC 25010	Es una medida sobre cuanto procesador se utiliza en un momento dado.
Capacidad	Peticiones(numero)	ISO/IEC 25010	Grado en que los límites máximos de un parámetro de un producto o sistema software cumplen con los requisitos

Realizado por: David Rodríguez. 2019

3.14 Planteamiento de fórmulas.

3.14.1 Promedio o media

Se obtendrá el promedio o media de los tiempos de respuesta de las peticiones realizadas a los sistemas de autenticación (SSO) CAS y WSO2 IDENTITY SERVER, por medio del software de análisis estadístico SPSS.

3.14.2 Mediana

Se obtendrá la mediana de los tiempos de respuesta de las peticiones realizadas a los sistemas de autenticación (SSO) CAS y WSO2 IDENTITY SERVER, por medio del software de análisis estadístico SPSS.

3.14.3 Desviación estándar

Se obtendrá la desviación estándar de los tiempos de respuesta de las peticiones realizadas a los sistemas de autenticación (SSO) CAS y WSO2 IDENTITY SERVER, por medio del software de análisis estadístico SPSS.

3.14.4 Tiempos de respuesta

Se obtendrá el tiempo de respuesta de las peticiones realizadas a los sistemas de autenticación (SSO) CAS y WSO2 IDENTITY SERVER, por medio del software de análisis estadístico SPSS.

3.14.5 Consumo de recursos

Se obtendrá el consumo de recursos de la bitácora de monitoreo de recursos en los test realizados a los sistemas de autenticación (SSO) CAS y WSO2 IDENTITY SERVER, por medio del software de análisis estadístico SPSS.

Tabla 5-3: Variables del uso de recursos.

Consumo de recursos	**Definición**
Memoria RAM	Es una memoria de lectura y escritura rápida, almacena momentáneamente conjunto de instrucciones que la CPU debe procesar.
CPU	Procesa los datos e interpreta las instrucciones que se le envía por medio de un software.

Realizado por: David Rodríguez. 2019

3.14.6 Capacidad

Se obtendrá del número de peticiones máximas realizada en la prueba de stress a los sistemas de autenticación (SSO) CAS y WSO2 IDENTITY SERVER.

3.15 Herramientas

Se empleo las siguientes herramientas:

3.15.1 Para evaluación del rendimiento

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 (TOP)
- Software estadístico SPSS
- Software de evaluación multicriterio NAIADE

3.15.2 Para tabulación y análisis estadísticos

Herramienta para calcular la hipótesis: Se utilizo software estadístico SPSS.

3.16 Diseño de los escenarios

Para el diseño de los escenarios se utilizó un equipo con las siguientes características:

- Equipo: Laptop Toshiba C45-C4205K
- Procesador: Intel Core i5-5200U @ 2.20 GHz (4 CPUs)
- Memoria: 12 GB RAM
- Sistema Operativo: Windows 10 Enterprise 64 bits
- Tarjeta de red: Realtek PCIe FE Family Controller

Utilizando el software Oracle WM Virtual Box en su versión 6.0.8, se crearon las 5 máquinas virtuales para la instalación del sistema operativo CentOS 7 sobre el cual se procedió con la instalación y configuración de los sistemas de autenticación (SSO), el servidor WEB, servidor de base de datos, herramientas de testeo, las mismas que se encuentran conectadas a través de una red (Adaptador Puente) para realizar los test necesarios, ver **Gráfico 1-3**.

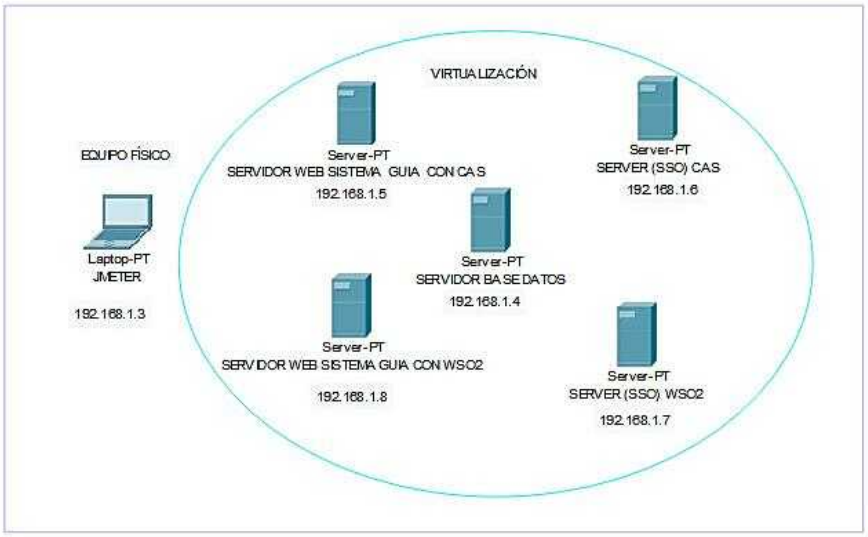

Gráfico 1-3: Esquema lógico del escenario de simulación
Realizado por: David Rodríguez. 2019

3.16.1 Escenario propuesto

Escenario 1

Para el primer escenario se utilizó la arquitectura descrita en la siguiente tabla, en donde se incluye la instalación de las herramientas necesarias para realizar el test, ver **Tabla 6-3.**

Tabla 6-3: Arquitectura del escenario 1

Descripción	Red	Características	Sistema Operativo
Servidor Web GUIA (SSO) CAS	Adaptador Puente	Memoria RAM: 1,447GB Disco Duro: 40 GB Procesador: 1	CentOS 7
Servidor (SSO) CAS	Adaptador Puente	Memoria RAM: 1,447GB Disco Duro: 40 GB Procesador: 1	CentOS 7
Servidor de base de datos	Adaptador Puente	Memoria RAM: 1,447GB Disco Duro: 40 GB Procesador: 1	CentOS 7
Pc Anfitrión	Interna / Externa	Memoria RAM: 12 GB Disco Duro: 1TB Procesador: 1	Windows 10

Realizado por: David Rodríguez. 2019

En el escenario 1, en todas las máquinas virtuales se procede a instalar el sistema operativo CentOS 7, una vez finalizada la instalación, se procede a instalar y configurar el servicio de autenticación (SSO) CAS 4.0 de acuerdo con el anexo A, finalizada su instalación, se procede a instalar y configurar el servidor WEB y su base de datos con las configuraciones que se tiene levantado en el ambiente de producción de la institución, se agrega la configuración para la conexión con el servicio de autenticación, de acuerdo con el anexo B.

Escenario 2

En el segundo escenario, se utilizó la arquitectura descrita en la siguiente tabla, en donde incluye la instalación de las herramientas necesarias para realizar el test, ver **Tabla 7-3.**

Tabla 7-3: Arquitectura del escenario 2

Descripción	Red	Características
Servidor Web GUIA - (SSO) WSO2	Adaptador Puente	Memoria RAM: 1447MB Disco Duro: 40 GB Procesador: 1
Servidor (SSO) WSO2	Adaptador Puente	Memoria RAM: 1447MB Disco Duro: 40 GB Procesador: 1
Servidor de base de datos	Adaptador Puente	Memoria RAM: 1447MB Disco Duro: 40 GB Procesador: 1
Pc Anfitrión	Interna / Externa	Memoria RAM: 12 GB Disco Duro: 1TB Procesador: 1

Realizado por: David Rodríguez. 2019

En el escenario 1, en todas las máquinas virtuales se procede a instalar el sistema operativo CentOS 7, una vez finalizada la instalación, se procede a instalar y configurar el servicio de autenticación (SSO) WSO2 IDENTITY SERVER 5.6.0 de acuerdo con el anexo C, finalizada su instalación, se procede a instalar y configurar el servidor WEB y su base de datos con las configuraciones que se tiene levantado en el ambiente de producción de la institución, se agrega la configuración para la conexión con el servicio de autenticación, de acuerdo con el anexo D.

3.16.2 Software utilizado

En la tabla 8-3 se muestra el software utilizado para el desarrollo de los dos escenarios propuestos.

Tabla 8-3: Características Software

Características	SSO CAS 4.0	SSO WSO2 IDENTITY SERVER 5.3.0	Pc Anfitrión
Sistema operativo	CentOS 7	CentOS 7	Windows 10
Java	Java 1.8.0_151	Java 1.8.0_151	Java 8-221
Servidor WEB	Httpd 2.4.6	Httpd 2.4.6	N/A
Servidor Base de datos	PostgreSQL 9.6.15	PostgreSQL 9.6.15	N/A
Software de Monitoreo	N/A	N/A	Jmeter 5.1.1
Librerías de monitoreo	ServerAgent-2.2.3	ServerAgent-2.2.3	N/A
Virtualizador	N/A	N/A	Virtual Box 6.0.8
Conexión remota	ssh	ssh	Putty, Filezilla

Realizado por: David Rodríguez. 2019

3.17 Plan de pruebas de rendimiento con JMeter

Para realizar el plan de pruebas se sigue los siguientes puntos:

3.17.1.1 Instalación del software JMeter.

Para instalar JMeter se sigue los siguientes pasos:

1. Instalar Java
2. Descargar e instalar JMeter

3.17.1.2 Instalación del plugin BlazeMeter en el navegador Chrome.

Para instalar el plugin BlazeMeter se sigue los siguientes pasos:

1. Abrir el navegador Chrome
2. Buscar el plugin BlazeMeter para instalar
3. Hacer clic en agregar a Chrome
4. Reiniciar el navegador

3.17.1.3 Crear el plan de pruebas.

Se elaboró 6 pasos que vamos a seguir en el proceso de autenticación, los que se describen a continuación:

1. Abrir navegador Chrome
2. Ingresar a la URL del sistema web (GUIA)
3. Ingresar las credenciales de acceso
4. Realizar el proceso de login
5. Navegar en la página web del sistema GUIA
6. Salir del sistema GUIA

Este proceso se lo capturó con el plugin BlazeMeter el cual genera un archivo (test.jmx) con todo el procedimiento descrito anteriormente, tanto para el sistema de autenticación SSO CAS y WSO2, como se muestra en el gráfico 2-3.

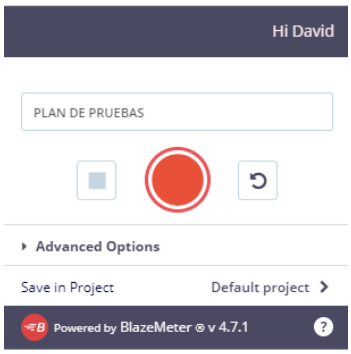

Gráfico 2-3: Interfaz BlazeMeter
Realizado por: David Rodríguez. 2019

3.17.1.4 Configurar plan de pruebas en JMeter.

Se sigue el siguiente procedimiento:

- Abrir el software JMeter
- Abrimos el archivo (test.jmx)

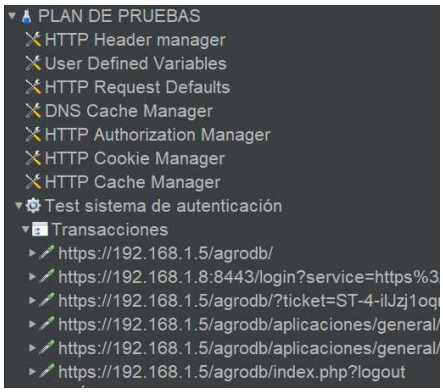

Gráfico 3-3: Plan de pruebas
Realizado por: David Rodríguez. 2019

En el gráfico 3-3 se muestra como está compuesto el plan de pruebas, el cual se generó en el paso anterior.

- Configurar los parámetros de ejecución:

a) Peticiones a ejecutar según la muestra obtenida anteriormente (292).

b) Periodo de subida de cada petición (1 segundo).

c) Numero de ciclos a ejecutar (1).

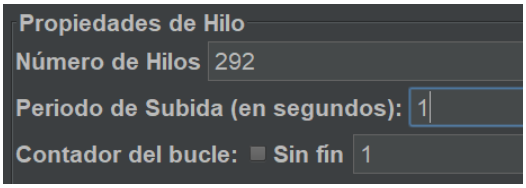

Gráfico 4-3: Configurar parámetros JMeter
Realizado por: David Rodríguez. 2019

En el gráfico 4-3 se presenta las configuraciones de ejecución del plan de pruebas.

- Añadir reportes

a) Clic derecho sobre plan de pruebas

b) Seleccionar Añadir

c) Seleccionar Receptor

d) Seleccionar Ver resultados en arbol

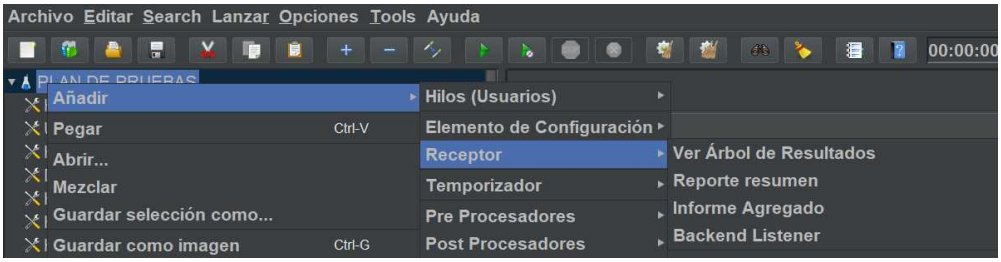

Gráfico 5-3: Configurar reportes JMeter
Realizado por: David Rodríguez. 2019

En el gráfico 5-3 se presenta como seleccionar los diferentes tipos de reportes que presenta la herramienta JMeter.

En el plan de pruebas se definió 6 pasos a seguir, lo que nos permite realizar 6 peticiones (Request http) en cada petición se crean 292 threads (hilos de ejecución) según la muestra calculada anteriormente, lo cual nos retorna como resultado 1752 muestras, se simuló tres veces al día obteniendo un total de 5256 muestras.

CAPÍTULO IV

4 RESULTADOS Y DISCUSIÓN

4.1 Recolección y análisis de datos por cada indicador

En el presente capítulo se discuten los resultados obtenidos de los planes de prueba realizados a cada sistema de autenticación SSO CAS y WSO2 Identity Server, en el anexo C se presentan los datos utilizados para el estudio.

4.1.1 Tiempo de respuesta

A continuación, se procederá a realizar el análisis de tiempo de respuesta, que en este caso el objetivo de esta variable es de minimizar la cantidad de milisegundos utilizados para ejecutar la tarea, una vez procesados los datos de las pruebas realizadas, en la tabla 1-4 se observan los resultados estadísticos del conjunto de datos correspondientes al indicador, preliminarmente para el conjunto de datos existe una alta desviación estándar.

Tabla 1-4: Estadísticos descriptivos del tiempo de respuesta.

	Plataforma SSO			Estadístico	Error estándar
Tiempo de Respuesta	CAS	Media		11989,2574	281,52537
		95% de intervalo de confianza para la media	Límite inferior	11437,3507	
			Límite superior	12541,1641	
		Media recortada al 5%		8976,5354	
		Mediana		4544,0000	
		Varianza		416572334,1	
		Desviación estándar		20410,10373	
		Mínimo		23,00	
		Máximo		151384,00	
		Rango		151361,00	
		Rango intercuartil		,00	
		Asimetría		2,971	,034
		Curtosis		9,776	,068
	WSO2	Media		144703,0225	3410,38174
		95% de intervalo de confianza para la media	Límite inferior	138017,2572	
			Límite superior	151388,7877	
		Media recortada al 5%		110616,5530	
		Mediana		28702,0000	
		Varianza		6,113E+10	
		Desviación estándar		247246,7958	
		Mínimo		19,00	
		Máximo		1,45E+6	
		Rango		1446404,00	
		Rango intercuartil		133457,25	
		Asimetría		2,070	,034
		Curtosis		3,416	,068

Realizado por: David Rodríguez. 2019

4.1.1.1 Normalidad del tiempo de respuesta

La comprobación de la normalidad del indicador "Tiempo de respuesta" se realizó en el software estadístico SPSS, una vez configurado las variables se procedió a agregar los datos recopilados, y se analizó su normalidad, cuyos resultados se observan en la tabla 2-4, donde utilizando el algoritmo de la prueba Kolmogorov-Smirnov para muestras grandes (mayores a 30) con un nivel de significancia asintótica de 0,00 se evidencia que los datos no tienen una distribución normal.

Tabla 2-4: Prueba de normalidad para el indicador "Tiempo de respuesta"

		Tiempo de respuesta
N		10512
Parámetros normales[a,b]	Media	78346,1399
	Desviación estándar	187548,6662
Máximas diferencias extremas	Absoluta	,338
	Positivo	,326
	Negativo	-,338
Estadístico de prueba		,338
Sig. asintótica (bilateral)		,000[c]

Realizado por: David Rodríguez. 2019

Con este resultado obtenido se procedió a realizar un análisis estadístico inferencial no paramétrico para muestras independiente utilizando el algoritmo de la prueba de U de Mann-Whitney donde se obtiene un nivel de significancia de 0,00 con lo que se comprueba que existe

una diferencia significativa en el tiempo de respuesta entre las dos plataformas CAS y WSO2 como se observa en la tabla 3-4.

Tabla 3-4: Prueba de normalidad de muestras independientes (tiempo de respuesta)

	Hipótesis nula	Prueba	Sig.	Decisión
1	La distribución de Tiempo de respuesta es la misma entre las categorías de Plataforma SSO.	Prueba U de Mann-Whitney para muestras independientes	,000	Rechace la hipótesis nula.

Realizado por: David Rodríguez. 2019

Al existir una diferencia significativa entre las dos plataformas analizadas en el presente trabajo de investigación se procede a comparar las medias estadísticas de cada conjunto de datos cuyo resultado se puede observar en el gráfico 1-4 donde se concluye que la plataforma CAS es la mejor opción debido a que utiliza menor cantidad (11989,26 milisegundos) en promedio para ejecutar la misma tarea.

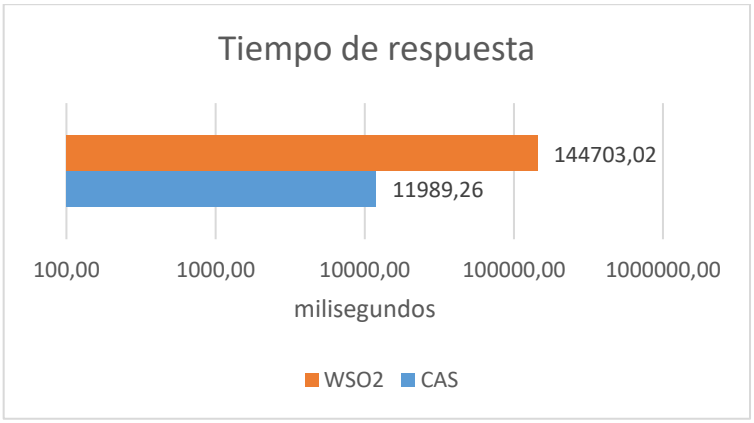

Gráfico 1-4: Variación del tiempo de respuesta entre SSO CAS y WSO2

Realizado por: David Rodríguez. 2019

4.1.2 Consumo de recurso (CPU)

A continuación, se procederá a realizar el análisis del consumo de recurso (CPU), una vez procesados de los datos de las pruebas realizadas, en la tabla 4-4 se observan los resultados estadísticos descriptivos del conjunto de datos correspondientes al indicador.

Tabla 4-4: Estadisticos descriptivos del consumo de CPU.

	Plataforma SSO			Estadístico	Error estándar
Consumo de CPU	CAS	Media		52,8411	3,04061
		95% de intervalo de confianza para la media	Límite inferior	46,8381	
			Límite superior	58,8441	
		Media recortada al 5%		53,5997	
		Mediana		81,2500	
		Varianza		1553,214	
		Desviación estándar		39,41084	
		Mínimo		,00	
		Máximo		92,60	
		Rango		92,60	
		Rango intercuartil		85,70	
		Asimetría		-,443	,187
		Curtosis		-1,711	,373
	WSO2	Media		35,6708	2,37337
		95% de intervalo de confianza para la media	Límite inferior	30,9852	
			Límite superior	40,3565	
		Media recortada al 5%		35,2997	
		Mediana		29,8500	
		Varianza		946,323	
		Desviación estándar		30,76236	
		Mínimo		,20	
		Máximo		78,60	
		Rango		78,40	
		Rango intercuartil		66,93	
		Asimetría		,178	,187
		Curtosis		-1,714	,373

Realizado por: David Rodríguez. 2019

4.1.2.1 Normalidad del consumo de recurso (CPU)

La comprobación de la normalidad del indicador "Consumo de recurso (CPU)" se realizó en el software estadístico SPSS, una vez configurado las variables se procedió agregar los datos recopilados y se analizó la normalidad de los mismo, cuyos resultados se observan en la tabla 5-4, donde utilizando el algoritmo de la prueba de Kolmogorov-Smirnov con un nivel de significancia asintótica de 0,00, se prueba que los datos no tienen una distribución normal.

Tabla 5-4: Prueba de normalidad de consumo de recurso (CPU)

		Consumo de CPU
N		336
Parámetros normales[a,b]	Media	44,2560
	Desviación estándar	36,33128
Máximas diferencias extremas	Absoluta	,177
	Positivo	,177
	Negativo	-,176
Estadístico de prueba		,177
Sig. asintótica (bilateral)		,000[c]

Realizado por: David Rodríguez. 2019

Con este resultado se procede a realizar un análisis estadístico inferencial no paramétrico para muestras independientes utilizando el algoritmo de la prueba de U de Mann-Whitney se obtiene un nivel de significancia de 0,00 con lo que se afirma que existe una diferencia significativa en el consumo de recurso RAM entre las dos plataformas CAS y WSO2 como se observa en la tabla 6-4.

Tabla 6-4: Prueba de normalidad de muestras independientes (CPU)

	Hipótesis nula	Prueba	Sig.	Decisión
1	La distribución de Consumo de CPU es la misma entre las categorías de Plataforma SSO.	Prueba U de Mann-Whitney para muestras independientes	,000	Rechace la hipótesis nula.

Realizado por: David Rodríguez. 2019

Al existir una diferencia significativa entre las dos plataformas, se procede a comparar las medias estadísticas de cada conjunto de datos cuyo resultado se puede observar en la Gráfico 2-4 donde se concluye que la plataforma WSO2 es mejor al utilizar una menor cantidad (35,7%) porcentual de CPU para ejecutar la misma tarea.

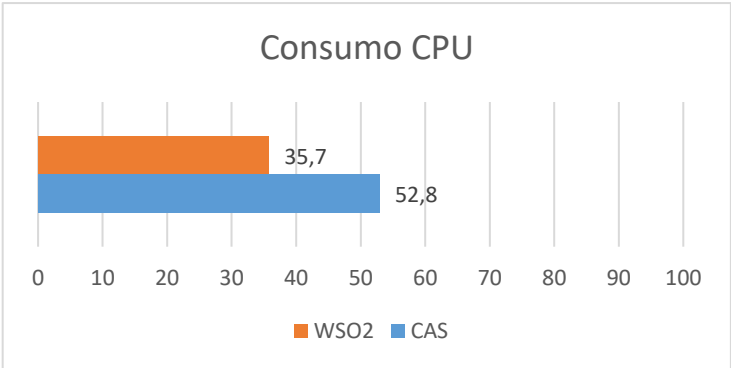

Gráfico 2-4: Variación del consumo de CPU entre SSO CAS y WSO2

Realizado por: David Rodríguez. 2019

4.1.3 Consumo de recurso (RAM)

A continuación, se procederá a realizar el análisis del consumo de recurso (RAM), que en este caso el objetivo de esta variable es de minimizar la cantidad porcentual utilizada para ejecutar la tarea, una vez procesados los datos de las pruebas realizadas, en la tabla 7-4 se observan los resultados estadísticos del conjunto de datos correspondientes al indicador.

Tabla 7-4: Estadísticos descriptivos del consumo de RAM.

	Plataforma SSO			Estadístico	Error estándar
Consumo de RAM	CAS	Media		1255397,500	5014,78508
		95% de intervalo de confianza para la media	Límite inferior	1245496,955	
			Límite superior	1265298,045	
		Media recortada al 5%		1260132,984	
		Mediana		1273502,000	
		Varianza		4224875654	
		Desviación estándar		64999,04349	
		Mínimo		1,10E+6	
		Máximo		1,32E+6	
		Rango		220216,00	
		Rango intercuartil		90969,00	
		Asimetría		-1,024	,187
		Curtosis		,258	,373
	WSO2	Media		1330427,286	734,51136
		95% de intervalo de confianza para la media	Límite inferior	1328977,161	
			Límite superior	1331877,410	
		Media recortada al 5%		1331007,931	
		Mediana		1332470,000	
		Varianza		90637166,62	
		Desviación estándar		9520,35538	
		Mínimo		1,30E+6	
		Máximo		1,35E+6	
		Rango		51708,00	
		Rango intercuartil		14111,00	
		Asimetría		-,910	,187
		Curtosis		,751	,373

Realizado por: David Rodríguez. 2019

4.1.3.1 Normalidad del consumo de recurso (RAM)

La comprobación de la normalidad del indicador "Consumo de recurso (RAM)" se realizó en el software estadístico SPSS, una vez configurado las variables se procedió agregar los datos recopilados, y se analizó la normalidad, cuyos resultados se observan en la tabla 8-4, aplicando el algoritmo de la prueba Kolmogorov-Smirnov para muestras grandes con un nivel de significancia asintótica de 0,00 se comprueba que los datos no tienen una distribución normal.

Tabla 8-4: Prueba de normalidad de consumo de recurso (RAM)

		Consumo de RAM
N		336
Parámetros normales[a,b]	Media	1292912,393
	Desviación estándar	59689,89553
Máximas diferencias extremas	Absoluta	,263
	Positivo	,186
	Negativo	-,263
Estadístico de prueba		,263
Sig. asintótica (bilateral)		,000[c]

Realizado por: David Rodríguez. 2019

Con este resultado obtenido se procede a realizar un análisis estadístico inferencial no paramétrico para muestras independientes utilizando el algoritmo de la prueba de U de Mann-Whitnev se obtiene un nivel de significancia de 0,00 con lo que se verifica que existe una diferencia significativa en el consumo de recurso RAM entre las plataformas CAS y WSO2 con se observa en la tabla 9-4.

Tabla 9-4: Prueba de normalidad de muestras independientes (RAM)

	Hipótesis nula	Prueba	Sig.	Decisión
1	La distribución de Consumo de RAM es la misma entre las categorías de Plataforma SSO.	Prueba U de Mann-Whitney para muestras independientes	,000	Rechace la hipótesis nula.

Realizado por: David Rodríguez. 2019

Al existir una diferencia significativa entre las dos plataformas analizadas en el presente trabajo de investigación, procede a comparar las medias estadísticas de cada conjunto de datos cuyo resultado se puede observar en el gráfico 3-4 donde se concluye que la plataforma CAS es mejor al utilizar una menor cantidad (87,19%) porcentual de RAM para ejecutar la misma tarea.

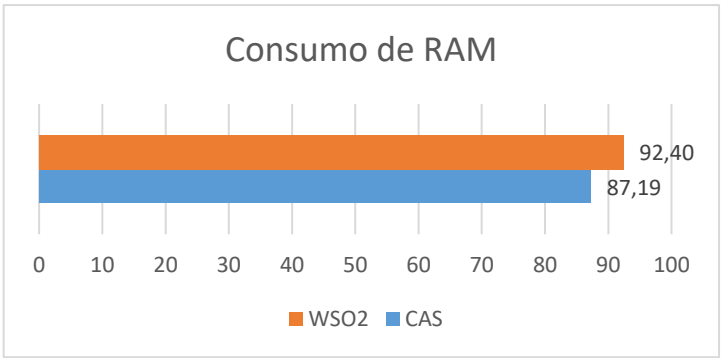

Gráfico 3-4: Variación del consumo de RAM entre SSO CAS y WSO2

Realizado por: David Rodríguez. 2019

4.1.4 Capacidad

Se realizó la prueba de carga extrema en los sistemas de autenticación para determinar su punto máximo de funcionamiento. Utilizando un total de 1200 peticiones concurrentes con cada plataforma. Se obtuvo el porcentaje de error de la ejecución de la tarea.

Tabla 10-4: Tabla comparativa de peticiones concurrentes.

Descripción	Error %
CAS	45,04
WSO2	81,17

Realizado por: David Rodríguez. 2019

En el gráfico 3-4 se observa la diferencia porcentual del error de carga obtenido de las pruebas realizadas donde se concluye que existe un menor nivel de afectación con sistema de autenticación CAS en comparación con el sistema de autenticación WSO2.

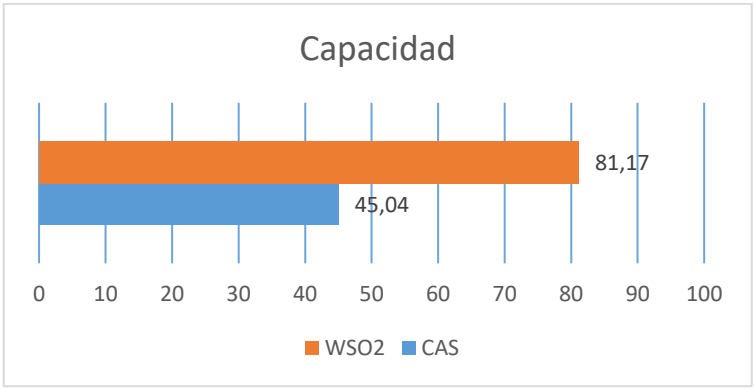

Gráfico 4-4: Variación porcentual de error de carga

Realizado por: David Rodríguez. 2019

4.2 Análisis de interpretación

De los resultados obtenidos y utilizando el método de NAIADE de análisis multicriterio, se estableció la Matriz de Impacto como se observa en la tabla 11-4.

Tabla 11-4: Matriz de impacto

Dimensiones y Variables	Unidad de medida	Tipo	Objetivo	CAS	WSO2
Tiempo de respuesta	Milisegundos	Cuantitativa	Minimizar	11989,26	144703,02

Consumo de recurso (CPU)	Porcentaje	Cuantitativa	Minimizar	52,80	35,70
Consumo de recurso (RAM)	Porcentaje	Cuantitativa	Minimizar	87,19	92,40
Capacidad	Porcentaje	Cuantitativa	Minimizar	45,04	81,17

Realizado por: David Rodríguez. 2019

4.3 Comprobación de la hipótesis

Para comprobar si se acepta la hipótesis, los resultados obtenidos se ingresaron en el software NAIADE de Análisis Multicriterio, según la matriz de impacto establecida en la tabla 11-4 como se observa en el gráfico 5-4.

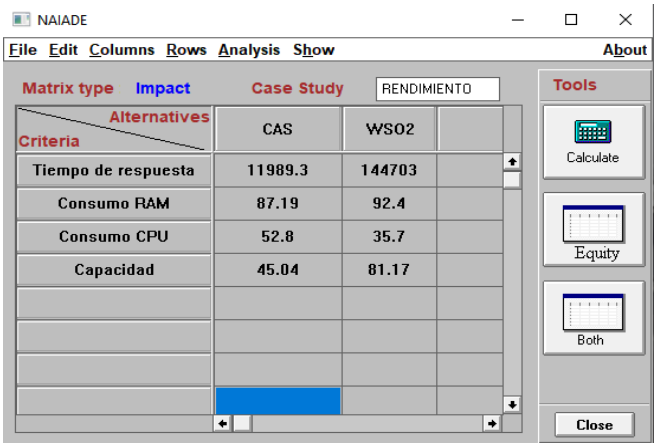

Gráfico 5-4: Matriz de impacto en NAIADE

Realizado por: David Rodríguez. 2019

Con un alfa (α) de 0,5; se obtiene un ranking Φ+ de 0.92 que selecciona al sistema de autenticación SSO CAS como mejor que el sistema de autenticación WSO2, se puede observar el resultado de la matriz de impacto en el gráfico 6-4.

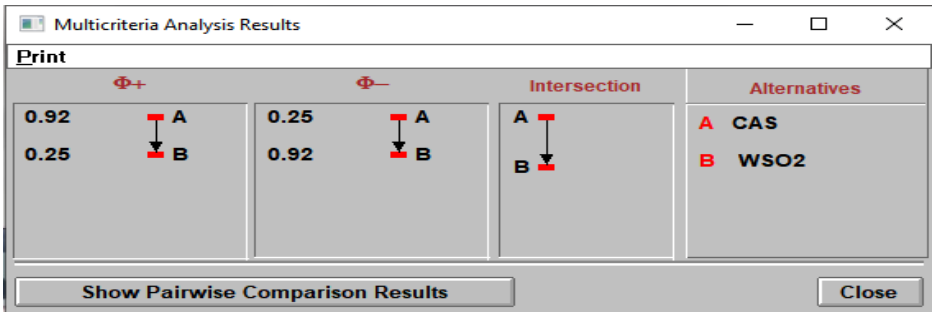

Gráfico 6-4: Resultado de la Matriz de Impacto
Realizado por: David Rodríguez. 2019

El resultado concuerda con la hipótesis del estudio "Los sistemas de autenticación (SSO) CAS y WSO2 IDENTITY SERVER presentan una diferencia significativa en cuanto al rendimiento del proceso de autenticación de usuarios para los aplicativos de AGROCALIDAD (Agencia de regulación y control fito y zoosanitario)", y se aceptada la hipótesis alternativa.

Se puede analizar cada criterio que ofrece el software, observándose gráficamente en el gráfico 7-4.

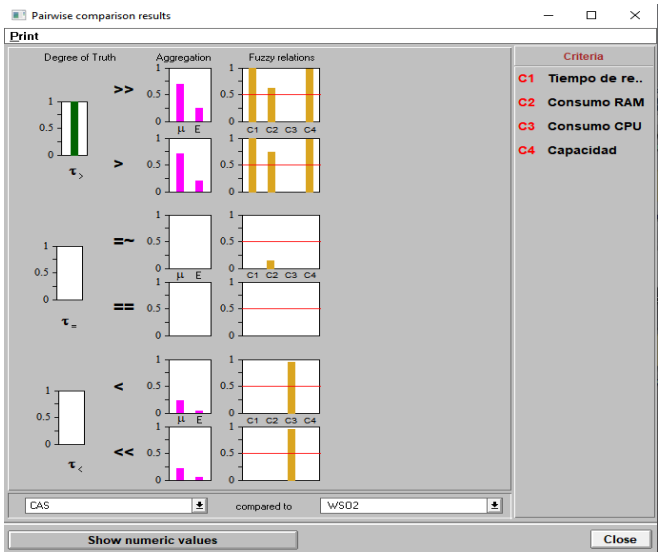

Gráfico 7-4: Comparación de pares CAS y WSO2
Realizado por: David Rodríguez. 2019

Las barras de violeta denotan un cambio significativo en los valores de los criterios que son las barras de color café.

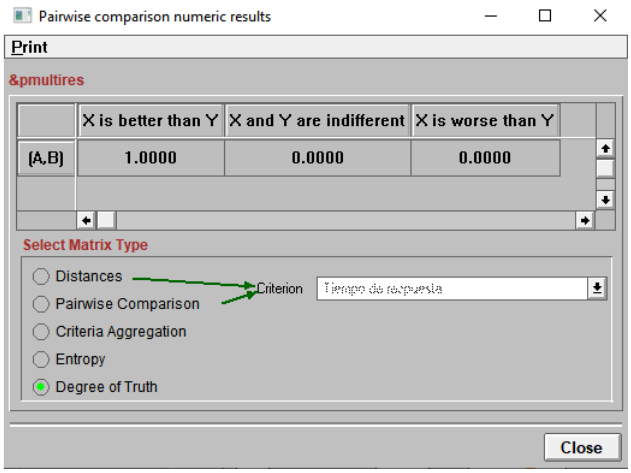

Gráfico 8-4: Grados de confianza
Realizado por: David Rodríguez. 2019

Se puede observar el grado de confianza de 1 (Ver gráfico 8-4) en sistema de autenticación SSO CAS que el sistema de autenticación WSO2, la misma que se denota con la barra de color verde.

CAPÍTULO V

5 PROPUESTA

5.1 Título de la propuesta

Manual de buenas prácticas del sistema de autenticación único (SSO).

5.2 Introducción

En la actualidad el no contar con un sistema de autenticación aumenta el número de ataques que se producen por internet, como medida para mitigar los ataques informáticos es utilizar el sistema de autenticación de usuarios único el cual nos permite una administración de cuentas, evitar el proceso repetitivo de loguearse para acceder a las diferentes aplicaciones, el servicio validad al usuario final si identidad para todas las aplicaciones a las que tiene derecho y elimina otras solicitudes cuando se cambia de aplicación durante la misma sesión.

Con el manual de buenas prácticas de los sistemas de autenticación único, se describe los pasos para su implementación con la finalidad de reducir los tiempos de instalación.

5.3 Objetivo

Elaborar un manual de buenas prácticas para la implementación del sistema de autenticación único.

5.4 Fundamento de la propuesta

El estudio del tiempo de respuesta, consumo de recursos y capacidad de los sistemas de autenticación único, su implementación de forma adecuada y eficiente fomentara la investigación de temas relacionados.

5.5 SSO sistema de autenticación único

En esta investigación se ha realizado una evaluación del rendimiento de los sistemas de autenticación CAS y WSO2 Identity server con la finalidad de elegir un sistema para mejorar el acceso a las diferentes plataformas.

Al momento de implementar un sistema de autenticación único, de acuerdo con el análisis realizado en el presente estudio de investigación se concluyó que el mejor sistema de autenticación de usuarios en CAS. Se recomienda realizar la instalación del sistema de autenticación único CAS, considerando las actividades descritas en el presente manual, al obviar ciertos procedimientos se puede poner en riesgo el acceso a las aplicaciones y el funcionamiento erróneo del sistema de autenticación.

5.6 Modelo lógico de la infraestructura de análisis

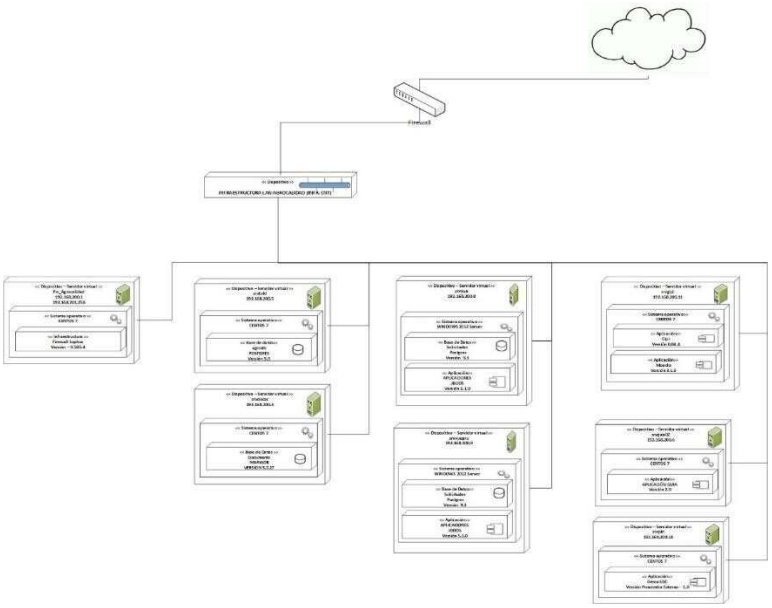

Gráfico 1-5: Infraestructura de servidores
Realizado por: David Rodríguez. 2019

Se presenta la distribución de los servidores y su conexión lógica, la cual se utilizó como referencia para realizar el análisis del rendimiento de los sistemas de autenticación SSO.

5.7 Descripción de la propuesta

Tomando como punto de partida el análisis realizado sobre el rendimiento de los sistemas de autenticación, a continuación, se describe el procedimiento que se debe seguir para la instalación y configuración de un sistema SSO.

Se consideran las siguientes fases:

- Fase 1 - Pasos previos a la instalación.
- Fase 2 - Instalación de sistema de autenticación CAS
- Fase 3 - Verificar funcionamiento del sistema de autenticación CAS.
- Fase 4 - Configurar el sistema de autenticación CAS en la aplicación.
- Fase 5 - Pruebas del sistema de autenticación CAS en la aplicación.

5.7.1 Fase 1 - Pasos previos a la instalación.

Para el análisis del rendimiento de los sistemas de autenticación SSO se trabajó con el sistema operativo Linux CentOS 7, el cual ofrece compatibilidad con los componentes a instalar y tiene un amplio soporte de repositorios.

La versión de JDK que se debe tener instalada es JDK 8, la versión con la que se realizó la implementación es jdk1.8.0_151, a continuación, se muestra su instalación.

- Abrir una terminal y seguir los comandos descritos para descargar el jdk1.8.0_151.

```
# cd /opt/

# wget --no-cookies --no-check-certificate --header "Cookie:
gpw_e24=http%3A%2F%2Fwww.oracle.com%2F; oraclelicense=accept-securebackup-
cookie" "https://download.oracle.com/otn-pub/java/jdk/8u151-
b09/42970487e3af4f5aa5bca3f542482c60/jdk-8u151-linux-x64.tar.gz"
```

- Crear la carpeta (java) en la cual se va a instalar el JDK.

```
# mkdir -p /usr/local/java/
```

- Dar permisos al JDK descargado con el siguiente comando.

```
# chmod a+x jdk-8u151-linux-x64.tar.gz
```

- Copiar el JDK descargado en la siguiente ruta en /usr/local/java y posterior ubicarse en la ruta que se copió el JDK con los siguientes comandos.

```
# cp -r jdk-8u151-linux-x64.tar.gz /usr/local/java/

# cd /usr/local/java/
```

- Descomprimir el JDK con el siguiente comando.

```
# tar xzf jdk-8u151-linux-x64.tar.gz
```

- Actualizar rutas del JDK instalado en el sistema operativo con los siguientes comandos.

```
# sudo update-alternatives --install "/usr/bin/java" "java" "/usr/local/java/jdk1.8.0_151/bin/java" 1

# sudo update-alternatives --install "/usr/bin/javac" "javac" "/usr/local/java/jdk1.8.0_151/bin/javac" 1

# sudo update-alternatives --install "/usr/bin/javaws" "javaws" "/usr/local/java/jdk1.8.0_151/bin/javaws" 1

# sudo update-alternatives --set java /usr/local/java/jdk1.8.0_151/bin/java

# sudo update-alternatives --set javac /usr/local/java/jdk1.8.0_151/bin/javac

# sudo update-alternatives --set javaws /usr/local/java/jdk1.8.0_151/bin/javaws
```

- Actualizar la versión JAVA como predeterminada en el sistema con el siguiente comando.

```
# update-alternatives --config java
```

- Actualiza las variables de entorno del sistema, para lo cual crear un archivo ejecutable y añadir la siguiente configuración.

```
# cd /etc/profile.d/

# nano java.sh
```

Agregar el siguiente código:

```
JAVA_HOME=/usr/local/java/jdk1.8.0_151

PATH=$PATH:$HOME/bin:$JAVA_HOME/bin

export JAVA_HOME

export PATH
```

Guardar y salir

- Cambiar los permisos de archivo creado anteriormente, para que se pueda ejecutar con el siguiente comando.

```
# chmod +x java.sh
```

- Actualizar las variables de entorno, para que el sistema tome como predeterminado el JDK instalado sin tener que reiniciar el sistema operativo, con el siguiente comando.

```
# source /etc/profile.d/java.sh
```

- Para verificar la versión de JAVA y JDK instalados, se utiliza el siguiente comando **java -versión**, nos muestra la versión de JAVA y JDK,

Gráfico 2-5: Versión de java
Realizado por: David Rodríguez. 2019

Se trabajó con un servidor apache-tomcat, el cual se lo coloco en /opt/apache-tomcat, se accederá por los puertos 8080 y 8443 (https).

La conexión segura (https) se configurará utilizando el certificado que disponga la institución, en el análisis se empleó un certificado autofirmado. Seguidamente se presenta la instalación y configuración de apache-tomcat, la versión de apache-tomcat con la cual se trabajó en el análisis es 9.0.20.

- Descargar Apache Tomcat de la URL presentada a continuación:

```
http://tomcat.apache.org/download-90.cgi

Core: tar.gz(pgp,md5)
```

- Descomprimir y copiar apache-tomcat en la siguiente ruta /opt
- Abrir una terminal y ubicar la ruta en la cual se descomprimió apache-tomcat y moverse a la carpeta bin, con los siguientes comandos.

```
# cd /opt/apache-tomcat-9.0.20/bin/
```

- Iniciar el servicio tomcat

```
# ./shutdown.sh //Detener Servicio Tomcat

# ./startup.sh   //Iniciar servicio Tomcat
```

- Configurar el menú de administración Tomcat, para acceder utilizando los roles de administrador, como se indica en las siguientes lineas de comando.

```
# cd /opt/apache-tomcat-9.0.20/conf/

#  vi tomcat-users.xml
```

Descomentar el siguiente código y agregar los roles de administrador.

```
<role rolename="tomcat"/>

 <role rolename="role1"/>

 <user username="tomcat" password="tomcat" roles="tomcat"/>

 <user username="both" password="tomcat" roles="tomcat,role1"/>

 <user username="role1" password="tomcat" roles="role1"/>

 <role rolename="manager-gui,admin-gui"/>    //Ingresar estas lineas

 <user username="tomcat" password="s3cret" roles="manager-gui,admin-gui"/>
```

Guardar y salir

- Configuración de variables de entorno en Tomcat

```
# /opt/apache-tomcat-9.0.20/bin

#vi catalina.sh
```

Agregar la siguientes lineas al inicio del archivo:

```
#!/bin/sh

JAVA_HOME=/usr/local/java/jdk1.8.0_151

PATH=$PATH:$HOME/bin:$JAVA_HOME/bin

export JAVA_HOME
```

export PATH

Guardar y salir

- Reiniciar el servicio tomcat, para lo cual ubicar la carpeta bin y ejecutar los siguientes comandos.

```
# ./shutdown.sh  //Detener servicio Tomcat

# ./startup.sh   //Iniciar servicio Tomcat
```

- Revisar el servicio tomcat en el navegador, para lo cual ingresar la IP y el puerto 8080 del servidor en el cual se instaló tomcat, como se muestra a continuación.

```
http://IPdelServidor:8080
```

Gráfico 3-5: Interfaz web de tomcat.
Realizado por: David Rodríguez. 2019

Al visitar la página, se observa la documentación de tomcat, lo instalado correctamente, caso contrario realice los pasos anteriores hasta que esta prueba sea ejecutada correctamente.

- Una vez instalado tomcat correctamente se instala el certificado para habilitar el puerto 8443 (https).

  Se empleo un certificado autofirmado, se detalla los pasos para crear e instalar:

- Generar certificado con el siguiente comando.

```
# openssl genrsa -out /etc/pki/tls/private/sp.key 1024
```

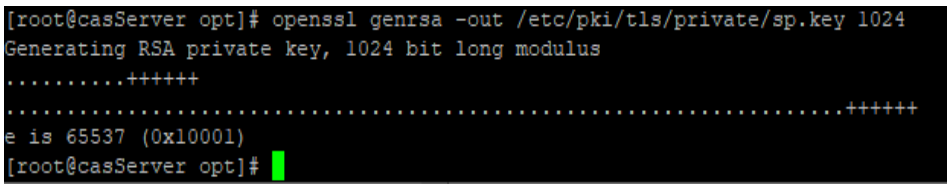

Gráfico 4-5: Generating RSA private key
Realizado por: David Rodríguez. 2019

- Crear archivo crt y pem

```
# openssl req -new -x509 -days 3650 -key /etc/pki/tls/private/sp.key -out /etc/pki/tls/certs/sp.crt
```

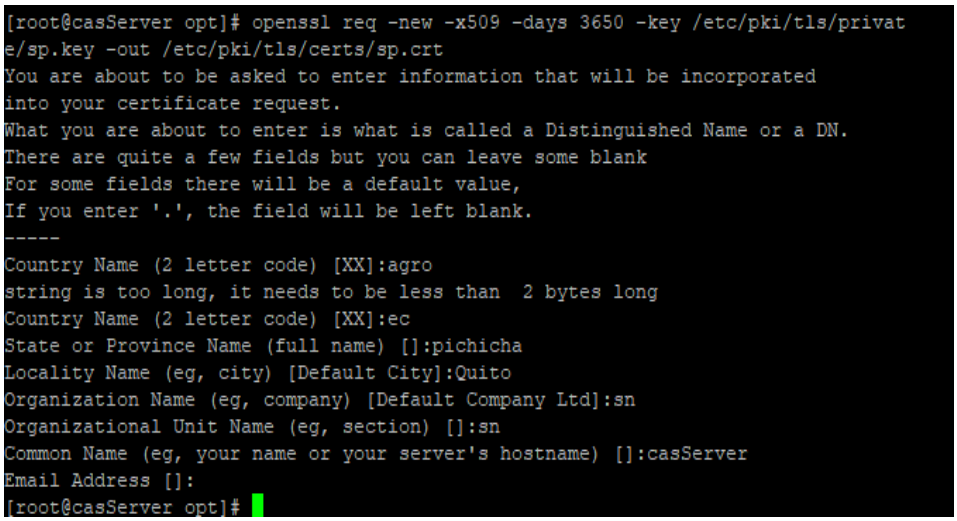

Gráfico 5-5: Crear certificado sp.crt
Realizado por: David Rodríguez. 2019

```
# openssl req -new -x509 -days 3650 -keyout /etc/pki/tls/certs/sp.pem
```

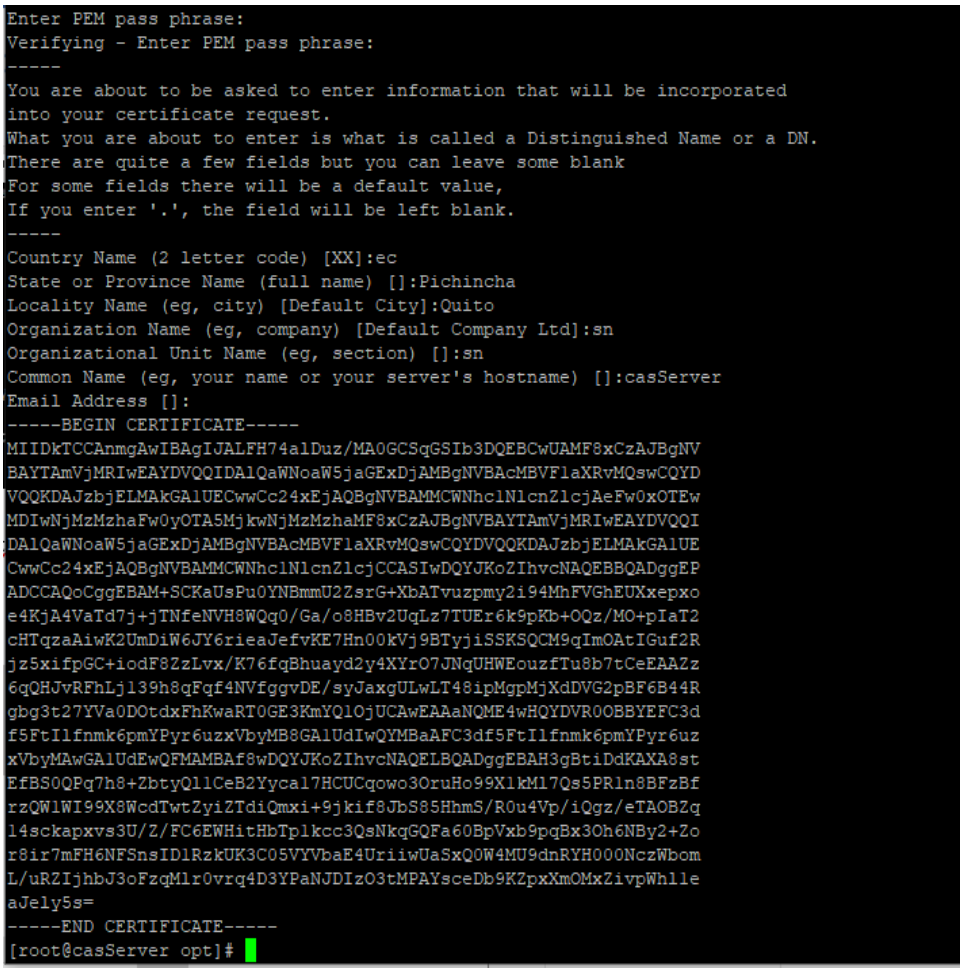

Gráfico 6-5: Certificado sp.pem
Realizado por: David Rodríguez. 2019

JAVA_HOME/bin/keytool -genkey -alias tomcat -keyalg RSA -keystore /usr/local/java/jdk1.8.0_151/bin/keystore

keytool -importkeystore -srckeystore /usr/local/java/jdk1.8.0_151/bin/keystore -destkeystore /usr/local/java/jdk1.8.0_151/bin/keystore -deststoretype pkcs12

- Actualizar la configuración en el archivo apache-tomcat-9.0.20/conf/server.xml de tomcat

Redireccionar peticiones al puerto 8443 con la siguiente configuración.

```
<Connector port="8080" protocol="HTTP/1.1"
           connectionTimeout="20000"
           redirectPort="8443" />
```

Gráfico 7-5: Configurar conector tomcat.
Realizado por: David Rodríguez. 2019

- Configurar la ruta del certificado

  Aquí se puede elegir la ruta del certificado, en nuestro caso vamos a indicar la ruta del certificado autofirmado, la institución debe indicar la ruta de su certificado.

```
<!-- Define a SSL Coyote HTTP/1.1 Connector on port 8443
-->
<Connector
           protocol="org.apache.coyote.http11.Http11NioProtocol"
           port="8443" maxThreads="200"
           scheme="https" secure="true" SSLEnabled="true"
           keystoreFile="/usr/local/java/jdk1.8.0_151/bin/keystore"
           keystorePass="changeit"
           enableLookups="false"
           disableUploadTimeout="true"
           clientAuth="false" sslProtocol="TLS"/>
```

Gráfico 8-5: Configuración de certificado.
Realizado por: David Rodríguez. 2019

- Crear el servicio de tomcat, mediante este servicio se puede iniciar y parar tomcat utilizando systemctl.

```
# sudo useradd -s /bin/false -g daemon -d /opt/apache-tomcat-9.0.20 tomcat

# sudo chgrp -R daemon /opt/apache-tomcat-9.0.20

# sudo nano /etc/systemd/system/tomcat.service
```

Agregar la siguiente configuración:

[Unit]
Description=Apache Tomcat Web Application Container
After=network.target syslog.target
[Service]
Type=forking
Environment=JAVA_HOME=/usr/local/java//jdk1.8.0_151
Environment=CATALINA_PID=/opt/apache-tomcat-9.0.20/temp/tomcat.pid
Environment=CATALINA_HOME=/opt/apache-tomcat-9.0.20
Environment=CATALINA_BASE=/opt/apache-tomcat-9.0.20
Environment='CATALINA_OPTS=-Xms1G -Xmx1G -Djava.net.preferIPv4Stack=true'
Environment='JAVA_OPTS=-Djava.awt.headless=true -Djava.security.egd=file:/dev/./urandom'
ExecStart=/opt/apache-tomcat-9.0.20/bin/startup.sh

ExecStop=/opt/apache-tomcat-9.0.20/bin/shutdown.sh
User=daemon
Group=daemon
UMask=0007
RestartSec=10
Restart=always
[Install]
WantedBy=multi-user.target
Guardar y salir

- Agregar el grupo y usuario al servicio tomcat creado, se agrega a un grupo y usuario propio del sistema operativo.

```
# chown -R daemon:daemon tomcat
```

- Inicializar el servicio tomcat.

```
# systemctl enable tomcat-systemd.service

# systemctl start tomcat-systemd.service

# systemctl daemon-reload
```

5.7.2 Fase 2 - Instalar el sistema de autenticación SSO CAS

El sistema de autenticación que SSO CAS que se utilizó en el análisis es la versión 4.0 el cual se describe en la instalación y configuración.

A continuación, se muestra los pasos a seguir:

- Abrir una terminal, crear una carpeta llamada (cas) acceder a la carpeta y se descarga CAS mediante los siguientes comandos:

```
# mkdir /opt/cas

# cd /opt/cas

# wget http://downloads.jasig.org/cas/cas-server-4.0-release.zip
```

- Descomprimir el archivo CAS descargado, para lo cual utilizar el siguiente comando.

```
# unzip cas-server-4.0-release.zip
```

- Renombrar la carpeta descomprimida y acceder a la misma, utilizando los siguientes comandos.

```
# mv cas-server-4.0 cas

# cd cas
```

- Copiar el archivo cas.war a la carpeta webapps de tomcat, mediante el siguiente comando.

```
# cp modules/cas.war /opt/apache-tomcat-9.0.20/webapps
```

- Reiniciar el servicio tomcat, para que desplegar el archivo cas.war.

```
# systemctl restart  tomcat
```

- Configuración de los usuarios

  En este punto se configura los usuarios, para el acceso a la aplicación.

```
# nano /opt/apache-tomcat-9.0.20/webapps/cas/WEB-INF/deployerConfigContext.xml
```

Agregar la siguiente configuración para la conexión a la base de datos.

```
<!-- Authentication method start    -->

<bean id="dataSource"
  class="com.mchange.v2.c3p0.ComboPooledDataSource"
  p:driverClass="com.mysql.jdbc.Driver"
  p:jdbcUrl="jdbc:mysql://192.168.1.4:3306/lportal"
  p:user="root"
  p:password="lalX"#df&rtr6"/>



<!-- Authentication method end  p:passwordEncoder-ref="passwordEncoder"-->
<bean id="passwordEncoder"
      class="org.jasig.cas.authentication.handler.DefaultPasswordEncoder"
      c:encodingAlgorithm="MD5"
      p:characterEncoding="UTF-8" />

<bean id="SearchModeSearchDatabaseAuthenticationHandler"
      class="org.jasig.cas.adaptors.jdbc.SearchModeSearchDatabaseAuthenticationHandler"
      p:dataSource-ref="dataSource"

      p:tableUsers="user_"
      p:fieldUser="screenname"
      p:fieldPassword="password_" />

    <!-- Required for proxy ticket mechanism -->
    <bean id="proxyPrincipalResolver"
          class="org.jasig.cas.authentication.principal.BasicPrincipalResolver" />
```

Gráfico 9-5: Configuración de usuarios.
Realizado por: David Rodríguez. 2019

5.7.3 Fase 3 - Verificar funcionamiento del sistema de autenticación CAS

Una vez realizado los pasos anteriores, se verifica el funcionamiento del sistema de autenticación CAS, para lo cual abrir el navegador WEB, ingresar la siguiente URL:

```
http://IP-SERVER:8080/cas/login
https://IP-SERVER:8080/cas/login
```

Al visitar la url anterior observa el login de sistema de autenticación CAS, como se muestra en el gráfico 2-5 y gráfico 2-6, se instalado correctamente, caso contrario realice los pasos anteriores hasta que esta prueba sea ejecutada correctamente.

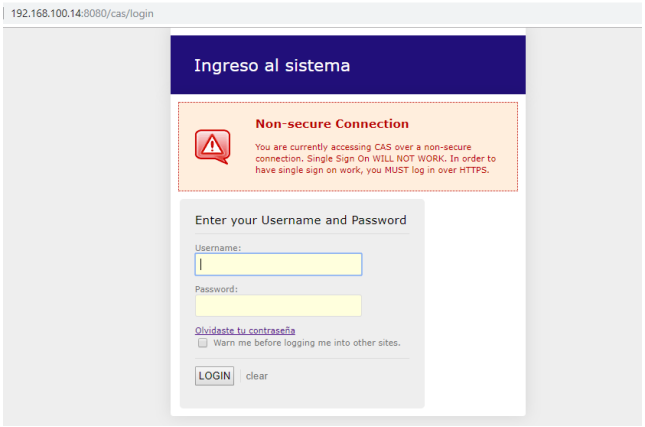

Gráfico 10-5: Test login CAS
Realizado por: David Rodríguez. 2019

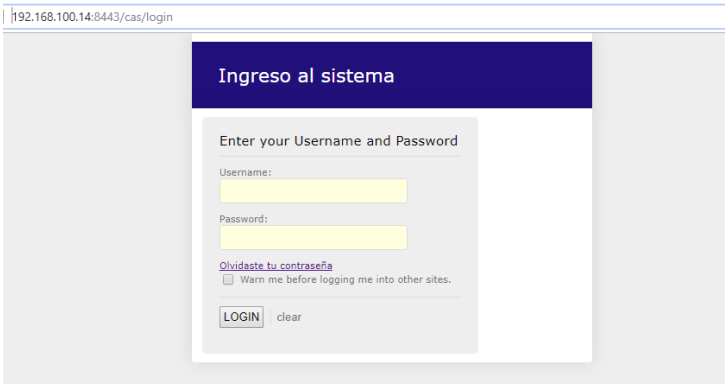

Gráfico 11-5: Test SSL en sistema de autenticación CAS
Realizado por: David Rodríguez. 2019

5.7.4 Fase 4 - Configurar el sistema de autenticación CAS en la aplicación

Para realizar la comunicación entre el sistema SSO y la aplicación se instala un cliente CAS en la aplicación, esta permite la comunicación de del sistema de autenticación CAS y la aplicación.

Se describe los pasos a continuación:

- Abrir una terminal acceder al directorio opt y descargar phpCAS, una vez descargado se procede a descomprimir el archivo, como se muestra a continuación.

```
# cd /opt

# wget https://github.com/apereo/phpCAS/archive/1.3.6.tar.gz

# tar xvzf 1.3.6.tar.gz
```

- Copiar los archivos descargados en la siguiente ruta /var/www/html/agrodbcas

```
#cp phpCAS-1.3.6/Source/* /var/www/html/agrodbcas/
```

- Configurar el siguiente archivo, para que permita interactuar con el sistema de autenticaion CAS.

```
# cd /var/www/html/agrodbcas/

# nano config.php
```

Agregar la siguiente configuración:

//indicar la ruta del archivo index de la aplicación

```
$phpcas_path = '/var/www/html/agrodbcas/index.php';
```

//indicar la IP del servidor de autenticación CAS

```
$cas_host = '192.168.1.6:8443/cas';
```

// Context of the CAS Server

```
$cas_context = '';
```

// Port of your CAS server. Normally for a https server it's 443

```
$cas_port = 443;
```

// Path to the ca chain that issued the cas server certificate

```
$cas_server_ca_cert_path = '/path/to/cachain.pem';
```

Guardar y salir

- Agregar la configuración en el archivo de inicio (index.php) de sistema GUIA, para que redireccione las peticiones de login al servicio de autenticacion CAS.

```
# cd /var/www/html/agrodbcas

# nano index.php
```

```
<?php
include_once('CAS.php');
require_once 'config.php';
phpCAS::setDebug();
// initialize phpCAS
phpCAS::client(CAS_VERSION_2_0, $cas_host, $cas_port, $cas_context);
// no SSL vlidation for the CAS server
phpCAS::setNoCasServerValidation();
phpCAS::forceAuthentication();
//
if (isset($_REQUEST['logout'])) {
        //phpCAS::logoutWithUrl("index.php");
        phpCAS::logout();
//      header('Location: salir.php');
}
```

Gráfico 12-5: Configurar CAS en aplicación.
Realizado por: David Rodríguez. 2019

Guardar y salir

5.7.5 Fase 5 - Pruebas del sistema de autenticación CAS en la aplicación

Una vez realizada las configuraciones descritas anteriormente realizar las pruebas de acceso a la aplicación.

- Ingresar la URL del servidor WEB https://IP-SERVER-WEB/agrodbcas/ y nos redirecciona al servidor de autenticación SSO CAS como observamos en el gráfico 7-5.

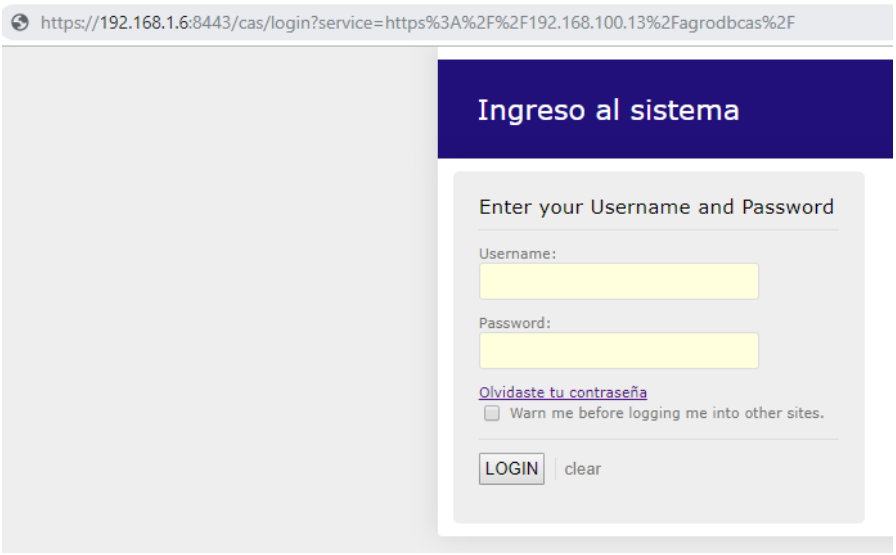

Gráfico 13-5: Login aplicación WEB
Realizado por: David Rodríguez. 2019

- Registrar las credenciales y nos retorna a la URL del servidor WEB como se muestra en el gráfico 8-5.

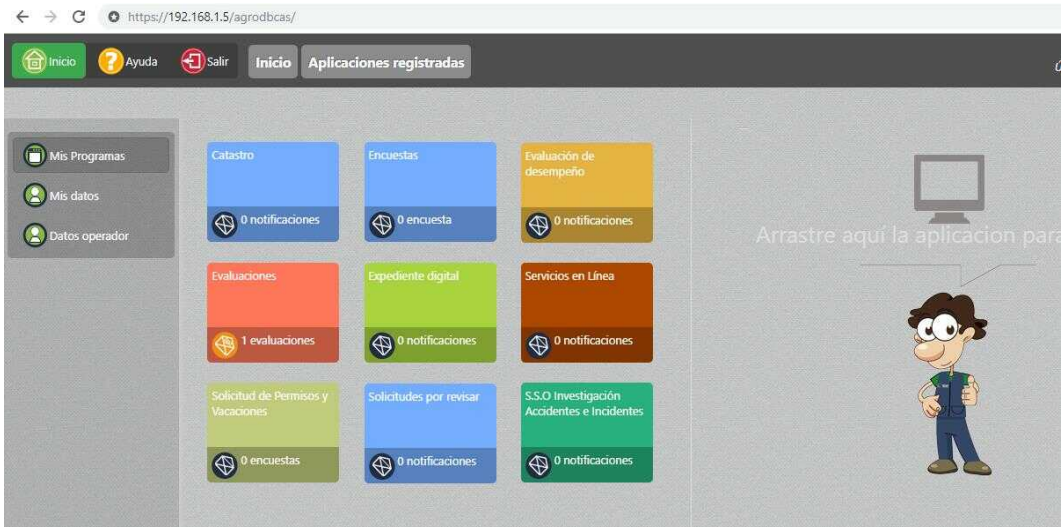

Gráfico 14-5: Página principal de la aplicación WEB
Realizado por: David Rodríguez. 2019

- Si las credenciales son incorrectas se mantienen en el servidor de autenticación como se muestra en el gráfico 9-5.

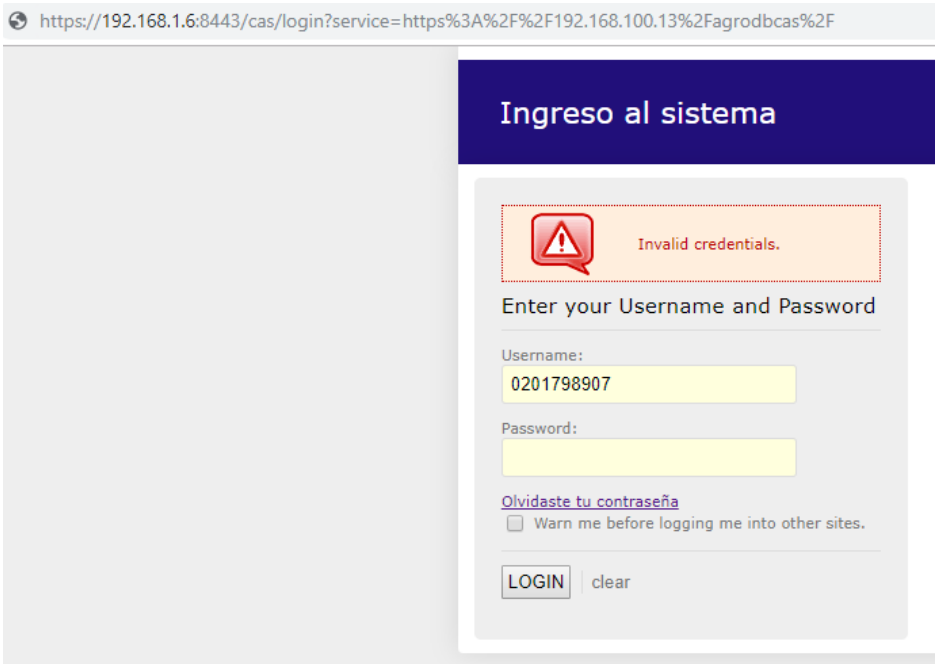

Gráfico 15-5: Login fallido
Realizado por: David Rodríguez. 2019

CONCLUSIONES

Una vez culminado las actividades del presente proyecto de investigación se ha obtenido las siguientes conclusiones:

- Luego de la instalación y configuración de los sistemas de autenticación SSO CAS y WSO2 Identity server se determinó que tienen una documentación clara y que está constantemente actualiza por su comunidad así también admiten integrar múltiples servidores de base de datos o directorios activos como MySQL y LDPA.

- Los servidores del ambiente de producción de AGROCALIDAD, permitió diseñar los escenarios para los experimentos a través de un plan de pruebas que permitió realizar el plan de pruebas bajo las mismas condiciones de manera controlada para cada plataforma CAS y WSO2 y evitar sesgos en la recopilación de datos.

- Luego de análisis se obtuvo los siguientes resultados: Para el "Tiempo de Respuesta" existe una diferencia de 132.713,76 (milisegundos) en promedio a favor de CAS, para el "Consumo recurso CPU" existe una diferencia porcentual 17,1 % a favor de WSO2, en cuanto al "Consumo recurso RAM" existe una diferencia porcentual de 5,21 % a favor de CAS y para el indicador de "Capacidad" existe una diferencia porcentual de 36,13 % a favor de CAS. Finalmente aplicando el análisis multicriterio con el método de NAIADE se obtiene un ranking positivo de 0,92 a favor del sistema de autenticación CAS, por lo cual se acepta la hipótesis alternativa y se rechaza la nula.

- La elaboración del manual de buenas prácticas de los sistemas de autenticación único SSO de plataformas Open Source, sistematiza los pasos necesarios para la implementación, los mismos que están verificados a la fecha de culminación del presente trabajo, el cual constituye una herramienta para los administradores de seguridad de la información de una organización que requiera de la implantación de estas plataformas.

RECOMENDACIONES

- Mantener actualizado la versión de sistemas de autenticación único para evitar vulnerabilidades en la seguridad de la información.

- Evaluar el sistema de autenticación periódicamente en ambientes controlados con el fin de detectar posibles fallos de seguridad en el mismo o su configuración. Mediante el cual se garantice su utilización.

- Diseñar planes de contingencia en el caso de sufrir ataques de denegación de servicios que permitan mitigar los mismo, garantizando de esta manera la información y manteniendo siempre el servicio hacia sus usuarios.

- Capacitar a los usuarios de los sistemas sobre la correcta creación de sus credenciales para el acceso a los sistemas, garantizado el acceso a la información mediante el uso de claves fuertes.

- Como trabajo futuro se propone evaluar las características que no se consideraron en esta investigación, como el análisis del cifrado de información en el tráfico de la red, también la utilización de directorios activos LDPA en otros servicios.

BIBLIOGRAFÍA

Agencia de regulación y control fito y zoosanitario. (2019). Obtenido de http://www.agrocalidad.gob.ec/

Anithadevi, M. S. (03 de 2015). *sciencedirect.* Obtenido de https://doi.org/10.1016/j.procs.2015.03.228

Baldeón, G. M. (2012). *Repositorio Institucional de la Universidad de las Fuerzas Armadas ESPE*. Obtenido de http://repositorio.espe.edu.ec/handle/21000/6026

Carrada, R. (2014). Algoritmos criptograficos de cifrado. Obtenido de https://issuu.com/danielricardocarradapena/docs/algoritmos_criptografis_de_cifrado

chakray. (2019). Obtenido de https://www.chakray.com/es/que-es-el-single-sign-on-sso-definicion-caracteristicas-y-ventajas/2/

Chakray.com. (2019). *slideshare.net.* Obtenido de https://es.slideshare.net/wso2.org/implementacin-de-autenticacin-federada-con-wso2-identity-server-51

Chovis. (2016). *Diferencia DES y AES.* Obtenido de http://chovis.hol.es/aprendamos/que-es/diferencia-entre-des-y-aes-algoritmos-de-encriptacion/

conectasoftware.com. (2019). Obtenido de https://conectasoftware.com/ciberseguridad/hackers-crackers-no-galletas-definiendo-tipos-intrusos

Consumoteca. (12 de 08 de 2009). *consumoteca.com/telecomunicaciones/internet/loguearse*. Obtenido de https://www.consumoteca.com/telecomunicaciones/internet/loguearse/

criptored.upm.es. (20 de 01 de 2003). Obtenido de http://www.criptored.upm.es/guiateoria/gt_m163a.htm Acceso: 20 de enero del 2003.

David Lozano, D. G. (02 de 06 de 2017). *https://patents.google.com.* Obtenido de https://patents.google.com/patent/WO2013186070A1/en?q=oauth&oq=oauth

docs.moodle.org. (17 de 04 de 2017). Obtenido de https://docs.moodle.org/all/es/Autenticaci%C3%B3n_por_servidor_CAS_(SSO)

Foundation, A. S. (2019). *Apache JMeter*. Obtenido de http://jmeter.apache.org/index.html

fwptt. (2018). Obtenido de http://fwptt.sourceforge.net/

George A. Gellert, J. F. (2017). *Clinical impact and value of workstation single sign-on.* Obtenido de https://doi.org/10.1016/j.ijmedinf.2017.02.008

Gómez, A. (2011). *Mecanismos de Gestión de Acceso a sistemas Web en Intranets.* Santa Clara. Obtenido de http://dspace.uclv.edu.cu/bitstream/handle/123456789/4679/Alberto%20G%C3%B3mez%20Quesada.pdf?sequence=1&isAllowed=y

Gómez, Á. (2018). *TIPOS DE ATAQUES E INTRUSOS EN LAS REDES INFORMATICAS.* Obtenido de http://www.edisa.com/wp-content/uploads/2014/08/Ponencia_-_Tipos_de_ataques_y_de_intrusos_en_las_redes_informaticas.pdf

Hernandez, S. (14 de 11 de 2010). *intrusos informaticos.* Obtenido de http://ser05m.obolog.es/intrusos-informaticos-991855

Hitha Reddy, V. R. (2012). Obtenido de A Survey on Single Sign-On Techniques: https://doi.org/10.1016/j.protcy.2012.05.019

IBM. (2018). *IBM*. Obtenido de https://www.ibm.com/mx-es/analytics/spss-statistics-software

ISO. (2019). *iso25000*. Obtenido de https://iso25000.com/index.php/normas-iso-25000/iso-25010

Itzcoatl, S. M. (11 de 2010). *revista.seguridad.unam.mx.* Obtenido de https://revista.seguridad.unam.mx/numero-17/criptograf%C3%AD-y-criptoan%C3%A1lisis-la-dial%C3%A9ctica-de-la-seguridad

legislacion Informática. (11 de Febrero de 2016). Obtenido de http://legislacion7.blogspot.com/2016/02/ecuador-estadisticas-de-delitos.html

linux, u. &. (2019). Obtenido de UNIX: https://www.unix.com/man-page/centos/1/top/

Luz, S. d. (2010). Obtenido de Criptografía : Algoritmos de cifrado de clave simétrica: https://www.redeszone.net/2010/11/04/criptografia-algoritmos-de-cifrado-de-clave-simetrica/

Martín, J. i. (2019). Obtenido de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/28021/6/nacho_martinTFM0114memoria.pdf

Microsoft. (Octubre de 2016). *MSDN*. Obtenido de MSDN: https://msdn.microsoft.com/es-es/library/dn263062.aspx

microsoft.com. (2006). Obtenido de http://msdn.microsoft.com/en-us/library/aa745042%28v=bts.10%29.aspx

Oliva Mateos, A. (2016). *APLICACIÓN DE SEGURIDAD EN SERVICIOS WEB XML PARA DISPOSITIVOS MÓVILES MEDIANTE LA IMPLEMENTACIÓN DE UN PERFIL*.

OpenID. (2018). *OpenID.net*. Obtenido de http://openid.net/what-is-openid/

Pereira, B., Ayaach, F., Quintero, H., & Granadillo, I. (2019). *idecame.uaeh.edu.mx.* Obtenido de http://cidecame.uaeh.edu.mx/lcc/mapa/PROYECTO/libro22/metricas.pdf

Red IRIS. (2008). Obtenido de https://www.rediris.es/cert/doc/unixsec/node14.html

Sanchez, J. (2019). Obtenido de https://jordisan.net/proyectos/Autent_y_auth-J_Sanchez.pdf

Sanz, O. S. (19 de octubre de 2016). *En mi local funciona*. Recuperado el 18 de mayo de 2018, de http://enmilocalfunciona.io/desarrollando-con-la-plataforma-wso2-introduccion/

Sara Arancibi, E. C. (2019). Obtenido de diiuchile: http://www.dii.uchile.cl/~ceges/publicaciones/ceges48.pdf

Seguridad America. (2018). Obtenido de https://www.seguridadamerica.com/iam-single-sign-on-sso/

Seguridad de la Información. (2016). *https://www.segu-info.com.ar*. Obtenido de https://www.segu-info.com.ar/ataques/tipos.htm

Servicio Ecuatoriano de Normalizacion. (2003). *normalizacion.gob.ec.* Obtenido de http://www.normalizacion.gob.ec/wpcontent/uploads/downloads/2016/05/nte_inen_iso_iec_27001.pdf

Softevolution. (6 de Febrero de 2018). Obtenido de http://www.softevolution.es/paginas-web/las-cookies-las-paginas-web-una-forma-almacenar-informacion/

Surya, N. A. (2015). Obtenido de Single Sign on Mechanism Using Attribute Based Encryption in Distributed Computer Networks: https://doi.org/10.1016/j.procs.2015.03.228

Teravainen, T. (2019). Obtenido de http://searchsecurity.techtarget.com/definition/single-sign-on

Trilla, M. (2019). *studies.ac.upc.edu.* Obtenido de http://studies.ac.upc.edu/FIB/CASO/seminaris/1q0304/T7.ppt

UCO. (2010). Obtenido de https://www.uco.es/servicios/informatica/sistemas/doc_ccc/fed_SSO/Requisitos_SSO.html

UNICON. (2019). *CAS*. Obtenido de https://www.unicon.net/opensource/cas

universidadviu.es. (06 de 12 de 2017). Obtenido de https://www.universidadviu.es/que-es-un-sniffer/

Urban. (06 de 2015). *todas las tribus urbanas.blogspot.com.* Obtenido de https://todas-las-tribus-urbanas.blogspot.com/2015/06/piratas-informaticos.html

Vargas, F. M. (2016). *Sistema Integrado de Autenticacion.* Cartagena, Colombia. Obtenido de http://biblioteca.unitecnologica.edu.co/notas/tesis/0069824.pdf

vcd.cl. (20 de 01 de 2003). Obtenido de http://www.vcd.cl/tombrad/pcasual/ayuda5.html

WSO. (2019). Obtenido de https://docs.wso2.com/display/IS530/WSO2+Identity+Server+Documentation

WSO2. (2018). *WSO2 The Open Source*. Recuperado el 14 de 05 de 2018, de https://wso2.com/

WSO2. (2019). Obtenido de https://wso2.com: https://wso2.com/library/articles/2017/08/what-is-wso2-identity-server/

ANEXOS

ANEXO A: Instalar y configurar servicio de autenticación SSO CAS.

Para la instalación del servicio de autenticación (SSO) CAS se han definido los siguientes pasos:

Una vez ingresado en la consola de CentOS 7, se procede con la ejecución de los siguientes comandos:

Loguearse como root

su –

Descargar e instalar de Java

```
# cd /opt/

# wget --no-cookies --no-check-certificate --header "Cookie:
gpw_e24=http%3A%2F%2Fwww.oracle.com%2F; oraclelicense=accept-securebackup-cookie"
"https://download.oracle.com/otn-pub/java/jdk/8u151-
b09/42970487e3af4f5aa5bca3f542482c60/jdk-8u151-linux-x64.tar.gz"
```

Creamos la carpeta java

```
# mkdir -p /usr/local/java/
```

Damos permisos al archivo

```
# chmod a+x jdk-8u151-linux-x64.tar.gz

# cp -r jdk-8u151-linux-x64.tar.gz /usr/local/java/

# cd /usr/local/java/

# tar xzf jdk-8u151-linux-x64.tar.gz

# sudo update-alternatives --install "/usr/bin/java" "java" "/usr/local/java/jdk1.8.0_151/bin/java"
1
# sudo update-alternatives --install "/usr/bin/javac" "javac"
"/usr/local/java/jdk1.8.0_151/bin/javac" 1
```

```
# sudo update-alternatives --install "/usr/bin/javaws" "javaws"
"/usr/local/java/jdk1.8.0_151/bin/javaws" 1

# sudo update-alternatives --set java /usr/local/java/jdk1.8.0_151/bin/java

# sudo update-alternatives --set javac /usr/local/java/jdk1.8.0_151/bin/javac

# sudo update-alternatives --set javaws /usr/local/java/jdk1.8.0_151/bin/javaws
```

Actualizar la versión JAVA como predeterminada en el sistema

```
# update-alternatives --config java
```

Actualiza el PATH del sistema

```
# cd /etc/profile.d/

# nano java.sh
```

Agregamos el siguiente código:

```
JAVA_HOME=/usr/local/java/jdk1.8.0_151

PATH=$PATH: $HOME/bin:$JAVA_HOME/bin

export JAVA_HOME

export PATH
```

Guardar y salir

```
# chmod +x java.sh
```

Recargar y actualizar el PATH

```
# source /etc/profile.d/java.sh
```

Verificamos:

```
[root@casServer opt]# java -version
java version "1.8.0_151"
Java(TM) SE Runtime Environment (build 1.8.0_151-b12)
Java HotSpot(TM) 64-Bit Server VM (build 25.151-b12, mixed mode)
[root@casServer opt]#
```

Gráfico 1: Test login CAS

Realizado por: David Rodríguez. 2019

Instalación de Tomcat

Descargar Apache Tomcat

```
http://tomcat.apache.org/download-90.cgi

Core:

tar.gz(pgp,md5)
```

Descomprimir apache-tomcat-9.0.20

```
Copiar el archivo a /opt
```

Revisar el servicio con el siguiente comando como usuario root

```
# cd /opt/apache-tomcat-9.0.20/bin/

# ls

# ./shutdown.sh  //Detener Servicio Tomcat

# ./startup.sh   //Iniciar servicio Tomcat
```

Configurar el menú de administración Tomcat

```
# cd /opt/apache-tomcat-9.0.20/conf/

# ls

# vi tomcat-users.xml

<role rolename="tomcat"/>

  <role rolename="role1"/>

  <user username="tomcat" password="tomcat" roles="tomcat"/>

  <user username="both" password="tomcat" roles="tomcat,role1"/>

  <user username="role1" password="tomcat" roles="role1"/>
```

```
  <role rolename="manager-gui,admin-gui"/>    //Ingresar estas lineas

  <user username="tomcat" password="s3cret" roles="manager-gui,admin-gui"/>

# ./shutdown.sh  //Detener Servicio Tomcat

# ./startup.sh   //Iniciar servicio Tomcat
```

Revisar ingresando a esta dirección

```
http://IPdelServidor:8080
```

Configuración de variables de entorno en Tomcat

```
# /opt/apache-tomcat-9.0.20/bin

#vi catalina.sh

#!/bin/sh

JAVA_HOME=/usr/local/java/jdk1.8.0_151

PATH=$PATH:$HOME/bin:$JAVA_HOME/bin

export JAVA_HOME

export PATH
```

Crear un servicio de tomcat

```
# sudo useradd -s /bin/false -g daemon -d /opt/apache-tomcat-9.0.20 tomcat

# sudo chgrp -R daemon /opt/apache-tomcat-9.0.20

# sudo nano /etc/systemd/system/tomcat.service
```

Agregar la siguiente configuración

```
 [Unit]

Description=Apache Tomcat Web Application Container

After=network.target syslog.target
```

```
[Service]

Type=forking

Environment=JAVA_HOME=/usr/local/java//jdk1.8.0_151

Environment=CATALINA_PID=/opt/apache-tomcat-9.0.20/temp/tomcat.pid

Environment=CATALINA_HOME=/opt/apache-tomcat-9.0.20

Environment=CATALINA_BASE=/opt/apache-tomcat-9.0.20

Environment='CATALINA_OPTS=-Xms1G -Xmx1G -Djava.net.preferIPv4Stack=true'

Environment='JAVA_OPTS=-Djava.awt.headless=true -
Djava.security.egd=file:/dev/./urandom'

ExecStart=/opt/apache-tomcat-9.0.20/bin/startup.sh

ExecStop=/opt/apache-tomcat-9.0.20/bin/shutdown.sh

User=daemon

Group=daemon



UMask=0007

RestartSec=10

Restart=always



[Install]

WantedBy=multi-user.target
```

Guardar y salir

```
# chown -R daemon:daemon tomcat
```

Inicializamos el servicio

```
# systemctl enable tomcat-systemd.service

# systemctl start tomcat-systemd.service

# systemctl daemon-reload
```

Instalar CAS 4.0

```
# mkdir /opt/cas

# cd /opt/cas

# wget http://downloads.jasig.org/cas/cas-server-4.0-release.zip

# unzip cas-server-4.0-release.zip

# mv cas-server-4.0 cas

# cd cas

# cp modules/cas.war /opt/apache-tomcat-9.0.20/webapps
```

Restart tomcat

```
# systemctl restart  tomcat
```

Test CAS Server login page

```
http://IP-SERVER:8080/cas/login
```

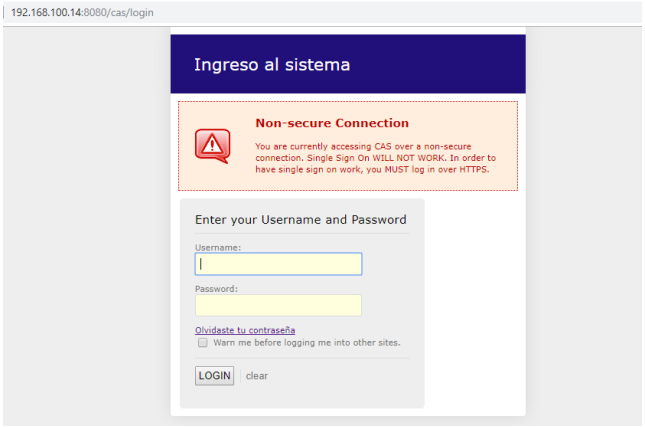

Gráfico 2: Test login CAS
Realizado por: David Rodríguez. 2019

Configurar SSL con certificado autofirmado

```
# openssl genrsa -out /etc/pki/tls/private/sp.key 1024
```

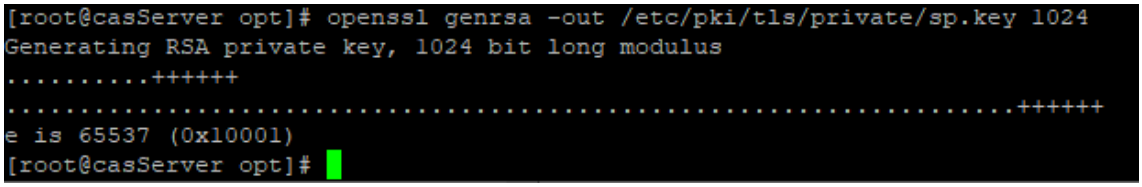

Gráfico 3: Generating RSA private key
Realizado por: David Rodríguez. 2019

openssl req -new -x509 -days 3650 -key /etc/pki/tls/private/sp.key -out /etc/pki/tls/certs/sp.crt

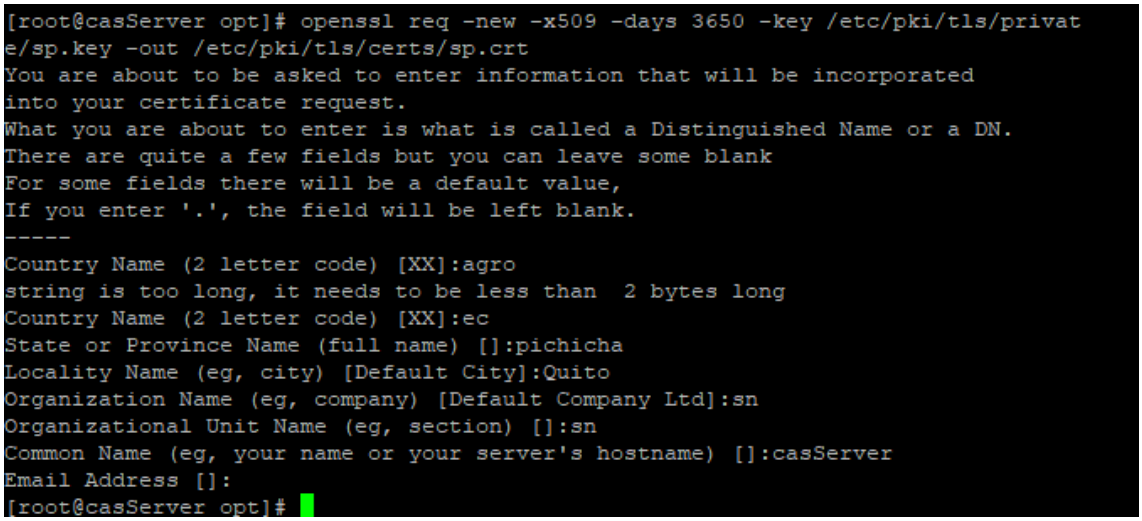

Gráfico 4: Crear certificado sp.crt
Realizado por: David Rodríguez. 2019

openssl req -new -x509 -days 3650 -keyout /etc/pki/tls/certs/sp.pem

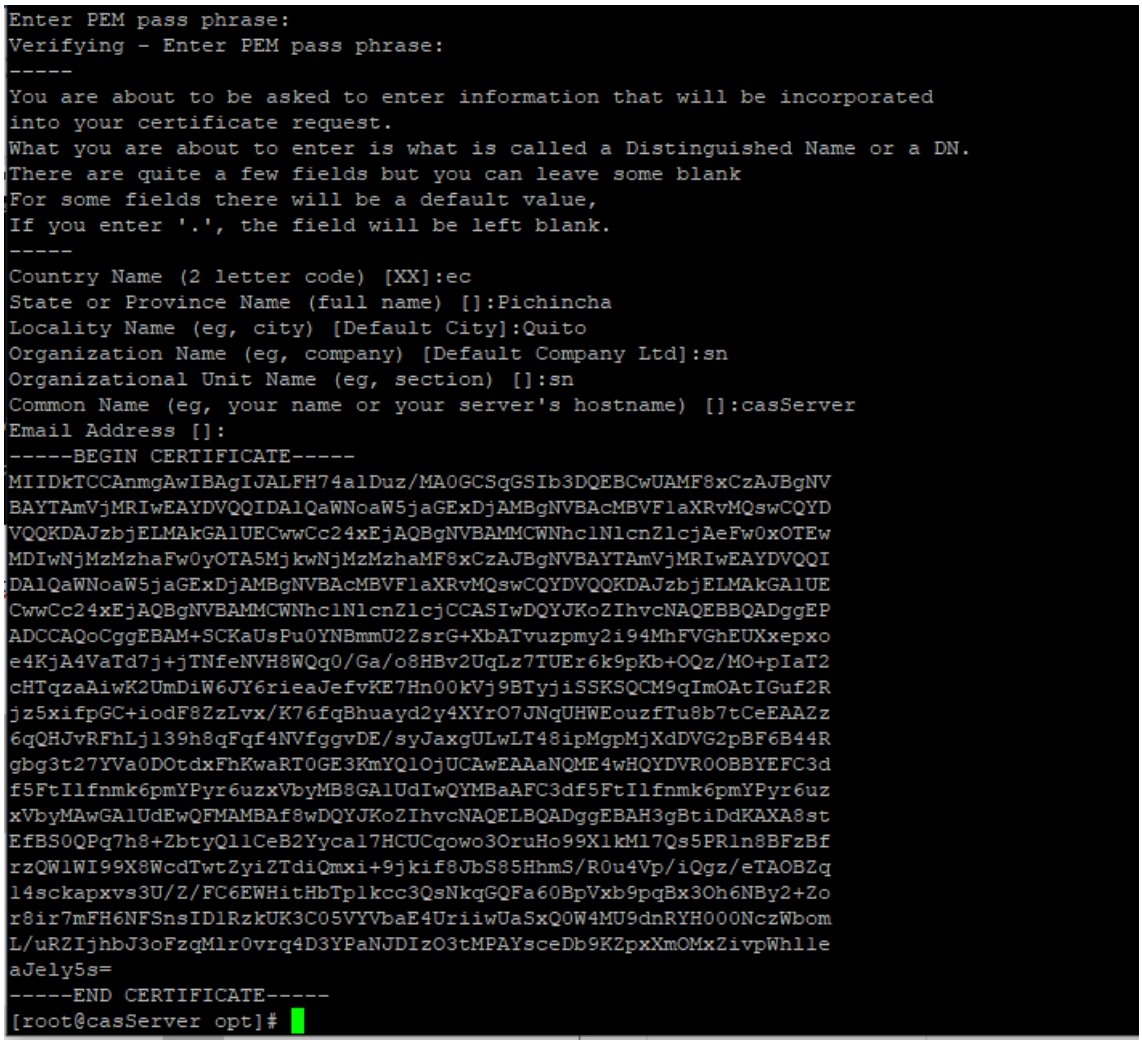

Gráfico 5: Crear certificado sp.pem
Realizado por: David Rodríguez. 2019

JAVA_HOME/bin/keytool -genkey -alias tomcat -keyalg RSA -keystore /usr/local/java/jdk1.8.0_151/bin/keystore

keytool -importkeystore -srckeystore /usr/local/java/jdk1.8.0_151/bin/keystore -destkeystore /usr/local/java/jdk1.8.0_151/bin/keystore -deststoretype pkcs12

Actualizar configuración en el archivo apache-tomcat-9.0.20/conf/server.xml de tomcat

Redireccionar peticiones al puerto 8443

```
<Connector port="8080" protocol="HTTP/1.1"
           connectionTimeout="20000"
           redirectPort="8443" />
```

Configurar la ruta del certificado

```
<!-- Define a SSL Coyote HTTP/1.1 Connector on port 8443
-->
<Connector
           protocol="org.apache.coyote.http11.Http11NioProtocol"
           port="8443" maxThreads="200"
           scheme="https" secure="true" SSLEnabled="true"
           keystoreFile="/usr/local/java/jdk1.8.0_151/bin/keystore"
           keystorePass="changeit"
           enableLookups="false"
           disableUploadTimeout="true"
           clientAuth="false" sslProtocol="TLS"/>
```

Reiniciar el servicio de tomcat

```
# systemctl restart tomcat
```

Test CAS Server login page

```
https://IP-SERVER:8443/cas/login
```

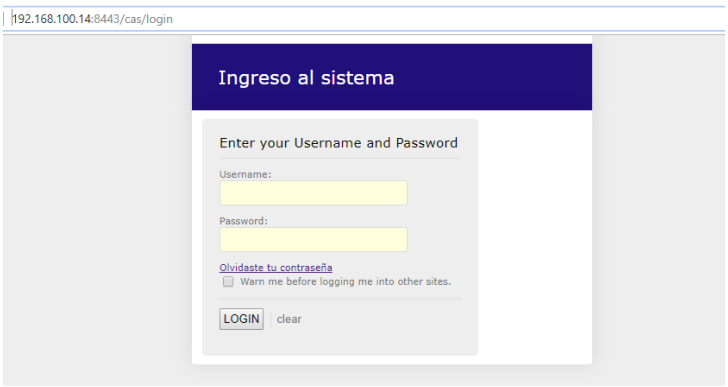

Gráfico 6: Test SSL en sistema de autenticación CAS
Realizado por: David Rodríguez. 2019

ANEXO B: Instalar y configurar sistema de autenticación CAS en el servidor web GUIA.

Para configurar el servicio de autenticación (SSO) CAS 4.0 en el servidor web CAS se han definido los siguientes pasos:

Una vez ingresado en la consola de CentOS 7, se procede con la ejecución de los siguientes comandos:

Loguearse como root

su –

Descargar phpCAS

```
# cd /opt

# wget https://github.com/apereo/phpCAS/archive/1.3.6.tar.gz

# tar xvzf 1.3.6.tar.gz

#cp phpCAS-1.3.6/Source/* /var/www/html/agrodbcas/
```

Agregamos en archivo de configuración en el agrodbcas

```
# cd /var/www/html/agrodbcas/

# nano config.php
```

Agregamos la siguiente configuración

```
<?php

/**

 * The purpose of this central config file is configuring all examples

 * in one place with minimal work for your working environment

 * Just configure all the items in this config according to your environment

 * and rename the file to config.php

 *
```

```
 * PHP Version 5

 *

 * @file     config.php

 * @category Authentication

 * @package  PhpCAS

 * @author   Joachim Fritschi <jfritschi@freenet.de>

 * @author   Adam Franco <afranco@middlebury.edu>

 * @license  http://www.apache.org/licenses/LICENSE-2.0  Apache License 2.0

 * @link     https://wiki.jasig.org/display/CASC/phpCAS

 */

$phpcas_path = '/var/www/html/agrodbcas/index.php';

///////////////////////////////////////

// Basic Config of the phpCAS client //

///////////////////////////////////////

// Full Hostname of your CAS Server

$cas_host = '192.168.1.6:8443/cas';

// Context of the CAS Server

$cas_context = '';



// Port of your CAS server. Normally for a https server it's 443

$cas_port = 443;

// Path to the ca chain that issued the cas server certificate
```

```
$cas_server_ca_cert_path = '/path/to/cachain.pem';

////////////////////////////////////////

// Advanced Config for special purposes //

////////////////////////////////////////



// The "real" hosts of clustered cas server that send SAML logout messages

// Assumes the cas server is load balanced across multiple hosts

$cas_real_hosts = array('cas-real-1.example.com', 'cas-real-2.example.com');



// Client config for cookie hardening

$client_domain = '127.0.0.1';

$client_path = 'phpcas';

$client_secure = true;

$client_httpOnly = true;

$client_lifetime = 1;

// Database config for PGT Storage

$db = 'pgsql:host=localhost;dbname=phpcas';

//$db = 'mysql:host=localhost;dbname=phpcas';

$db_user = 'phpcasuser';

$db_password = 'mysupersecretpass';

$db_table = 'phpcastabel';

$driver_options = '';
```

```
//////////////////////////////////////////

// End Configuration -- Don't edit below //

//////////////////////////////////////////

// Generating the URLS for the local cas example services for proxy testing

if (isset($_SERVER['HTTPS']) && $_SERVER['HTTPS'] == 'on') {

    $curbase = 'https://' . $_SERVER['SERVER_NAME'];

} else {

    $curbase = 'http://' . $_SERVER['SERVER_NAME'];

}

if ($_SERVER['SERVER_PORT'] != 80 && $_SERVER['SERVER_PORT'] != 443) {

    $curbase .= ':' . $_SERVER['SERVER_PORT'];

}

$curdir = dirname($_SERVER['REQUEST_URI']) . "/";

// CAS client nodes for rebroadcasting pgtIou/pgtId and logoutRequest

$rebroadcast_node_1 = 'http://cas-client-1.example.com';

$rebroadcast_node_2 = 'http://cas-client-2.example.com';

// access to a single service

$serviceUrl = $curbase . $curdir . 'index.php';

// access to a second service

$serviceUrl2 = $curbase . $curdir . 'example_service_that_proxies.php';

$pgtBase = preg_quote(preg_replace('/^http:/', 'https:', $curbase . $curdir), '/');

$pgtUrlRegexp = '/^' . $pgtBase . '.*$/';
```

```
$cas_url = 'https://' . $cas_host;

if ($cas_port != '443') {

    $cas_url = $cas_url . ':' . $cas_port;

}

$cas_url = $cas_url . $cas_context;

// Set the session-name to be unique to the current script so that the client script

// doesn't share its session with a proxied script.

// This is just useful when running the example code, but not normally.

session_name(

    'session_for:'

    . preg_replace('/[^a-z0-9-]/i', '_', basename($_SERVER['SCRIPT_NAME']))

);

// Set an UTF-8 encoding header for internation characters (User attributes)

header('Content-Type: text/html; charset=utf-8');

?>
```

Guardar y salir

Agregamos la siguiente configuración en index.php de sistema GUIA

```
# cd /var/www/html/agrodbcas

# nano index.php
```

```php
<?php
include_once('CAS.php');
require_once 'config.php';
phpCAS::setDebug();
// initialize phpCAS
phpCAS::client(CAS_VERSION_2_0, $cas_host, $cas_port, $cas_context);
// no SSL vlidation for the CAS server
phpCAS::setNoCasServerValidation();
phpCAS::forceAuthentication();
//
if (isset($_REQUEST['logout'])) {
        //phpCAS::logoutWithUrl("index.php");
        phpCAS::logout();
//      header('Location: salir.php');
}
```

Ingresamos en la URL del servidor WEB https://192.168.1.5/agrodbcas/ y nos redirecciona al servidor de autenticación SSO CAS como observamos en el gráfico 7.

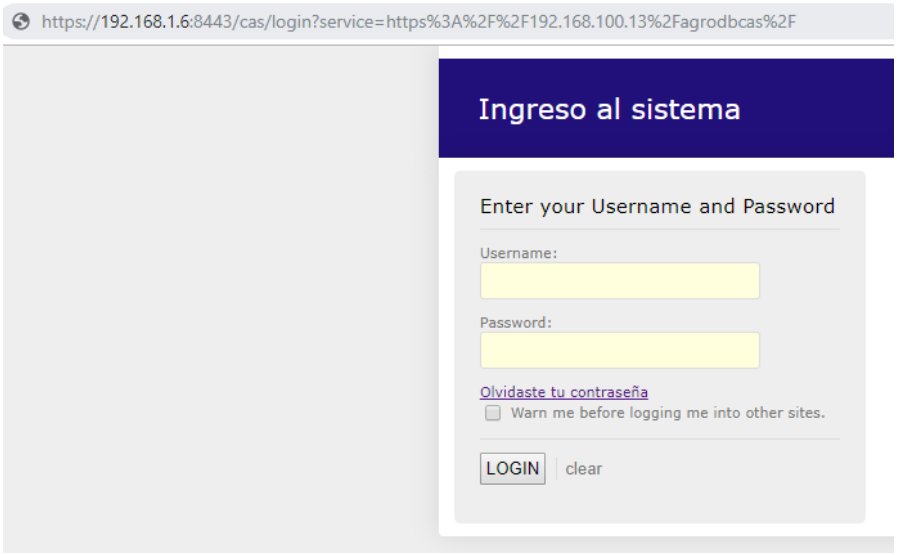

Gráfico 7: Login sistema web GUIA
Realizado por: David Rodríguez. 2019

ANEXO C: Instalación y configuración de WSO2 identity server.

Para la instalación del servicio de autenticación WSO2 IDENTITY SERVER se han definido los siguientes pasos:

Una vez ingresado en la consola de CentOS 7, se procede con la ejecución de los siguientes comandos:

Loguearse como root

su –

Descargar e instalar de Java

```
# cd /opt/

# wget --no-cookies --no-check-certificate --header "Cookie:
gpw_e24=http%3A%2F%2Fwww.oracle.com%2F; oraclelicense=accept-securebackup-cookie"
"https://download.oracle.com/otn-pub/java/jdk/8u151-
b09/42970487e3af4f5aa5bca3f542482c60/jdk-8u151-linux-x64.tar.gz"
```

Creamos la carpeta java

```
# mkdir -p /usr/local/java/
```

Damos permisos al archivo

```
# chmod a+x jdk-8u151-linux-x64.tar.gz

# cp -r jdk-8u151-linux-x64.tar.gz /usr/local/java/

# cd /usr/local/java/

# tar xzf jdk-8u151-linux-x64.tar.gz

# sudo update-alternatives --install "/usr/bin/java" "java" "/usr/local/java/jdk1.8.0_151/bin/java"
1

# sudo update-alternatives --install "/usr/bin/javac" "javac"
"/usr/local/java/jdk1.8.0_151/bin/javac" 1
```

```
# sudo update-alternatives --install "/usr/bin/javaws" "javaws"
"/usr/local/java/jdk1.8.0_151/bin/javaws" 1

# sudo update-alternatives --set java /usr/local/java/jdk1.8.0_151/bin/java

# sudo update-alternatives --set javac /usr/local/java/jdk1.8.0_151/bin/javac

# sudo update-alternatives --set javaws /usr/local/java/jdk1.8.0_151/bin/javaws
```

Actualizar la versión JAVA como predeterminada en el sistema

```
# update-alternatives --config java
```

Actualiza el PATH del sistema

```
# cd /etc/profile.d/

# nano java.sh
```

Agregamos el siguiente código:

```
JAVA_HOME=/usr/local/java/jdk1.8.0_151

PATH=$PATH: $HOME/bin:$JAVA_HOME/bin

export JAVA_HOME

export PATH
```

Guardar y salir

```
# chmod +x java.sh
```

Recargar y actualizar el PATH

```
# source /etc/profile.d/java.sh
```

Descargar e instalar WSO2 Identity server

Descargar el binario

https://wso2.com/identity-and-access-management/

Copiamos a /opt

```
# cd /opt           t

# unzip wso2is-5.3.0.zip

# chown a+x wso2is-5.3.0
```

Inicializar el servicio

```
# cd /opt/wso2is-5.3.0/bin

# ./wso2server.sh
```

Accedemos pro medio del navegador web

https://192.168.1.7:9443/carbon

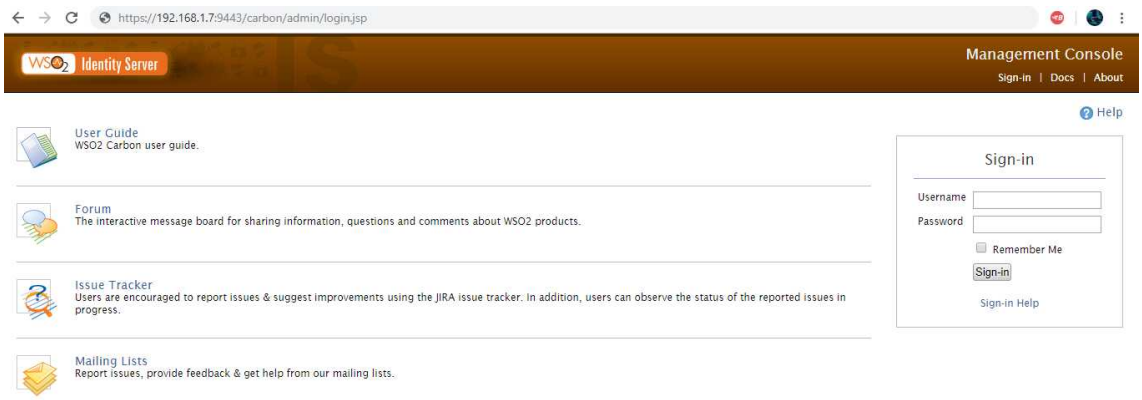

Gráfico 8: Login sistema WSO2 Identity server
Realizado por: David Rodríguez. 2019

Acedemos con las credenciales:

Username: admin

Password: admin

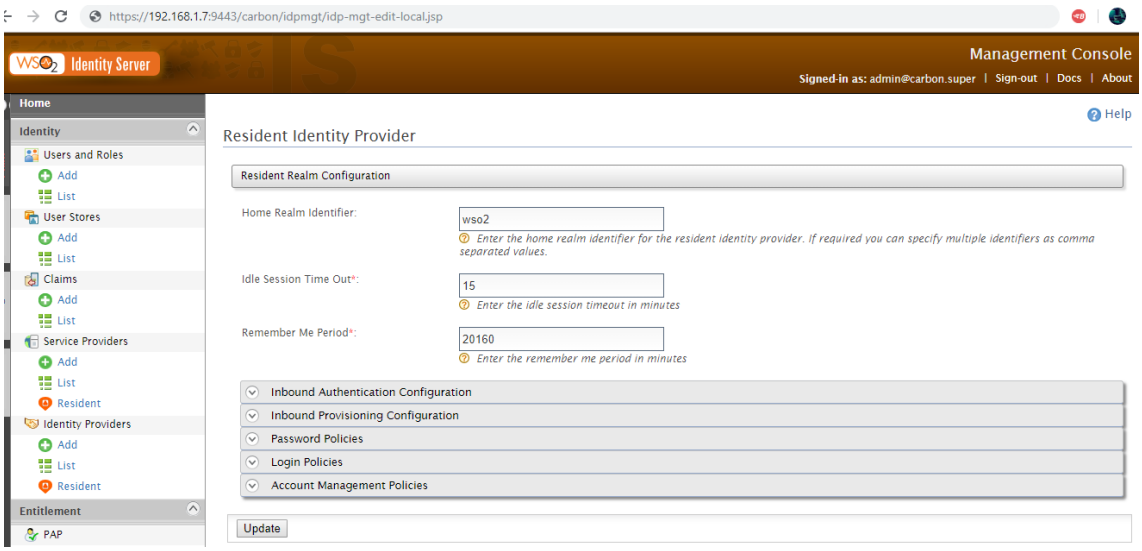

Gráfico 9: Interfaz wso2 Identity server
Realizado por: David Rodríguez. 2019

Agregar proveedor de servicios en SAML SSO

Issuer:simplesaml

Assertion Consumer URL: http://192.168.1.5/simplesaml/module.php/saml/sp/saml2-acs.php/wso2-saml

Enable Single Logout: True

SLO Response URL: http:// 192.168.1.5/simplesamlphp/www/module.php/saml/sp/saml2-logout.php/wso2-saml

Keep the defaults for the rest.

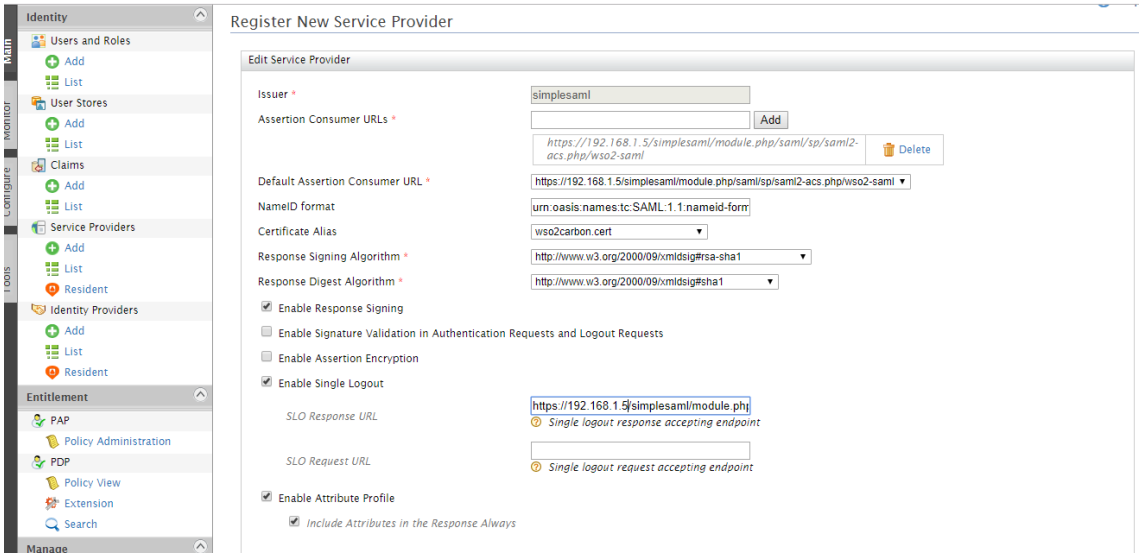

Gráfico 10: Configurar proveedor de servicios WSO2
Realizado por: David Rodríguez. 2019

Configurar proveedor de identidad

Seleccionar Resident en Proveedores de identidad

Configurar SSO webde SAML2

Registrar https://192.168.1.7:9443/samlsso

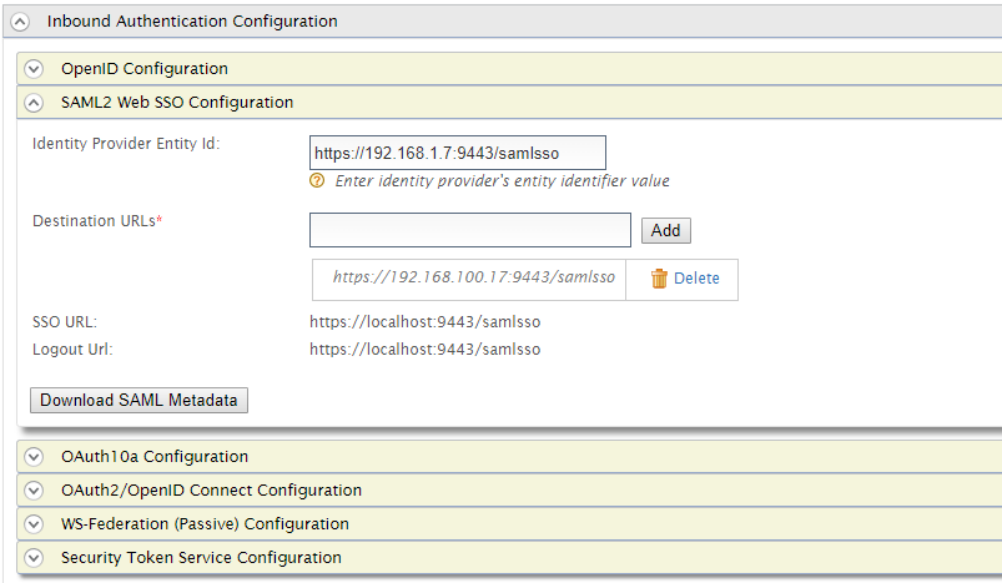

Gráfico 11: Configurar proveedor de servicios WSO2
Realizado por: David Rodríguez. 2019

ANEXO D: Instalar y configurar WSO2 en server web GUIA.

Para la instalación y configuración de WSO2 en el servidor web GUIA se han definido los siguientes pasos:

Una vez ingresado en la consola de CentOS 7, se procede con la ejecución de los siguientes comandos:

Loguearse como root

su –

Instalar extensiones requeridas de PHP

```
# yum install php-cli

# yum install php-common

# yum install php-curl

# yum install php-pear

# yum install php-mcryp
```

Instalar simplesamlphp en servidor web GUIA

```
# sudo mkdir /var/simplesamlphp/

# cd /var/simplesamlphp/

# wget https://github.com/simplesamlphp/simplesamlphp/releases/download/simplesamlphp-1.11.0/simplesamlphp-1.11.0.tar.gz

# tar xvf simplesamlphp-1.11.0.tar.gz

# mv simplesamlphp-1.11.0 simplesamlphp

# cd simplesamlphp

# cp -r metadata-templates/*.php metadata/

# cp -r config-templates/*.php config
```

Configurar simplesamlphp en HTTP

```
# cd /var/www/html

# ln -s /var/simplesamlphp/simplesamlphp/www simplesaml

# cd /var/simplesamlphp/simplesamlphp

# nano config/authsources.php
```

Agregar la siguiente configuración

```
'wso2-sp' => array(

'saml:SP',

'entityID' => 'simplesaml',

'idp' => 'https://192.168.1.7:9443/saml',

'discoURL' => NULL,

),
```

Guardar y salir

Agregar los metadatos del proveedor de identidad

```
# cd /var/simplesamlphp/simplesamlphp

# nano metadata/saml20-idp-remote.php
```

Agregar la siguiente configuración

```
$metadata[‘https://192.168.1.7:9443/samlsso’] = array(
      ‘name’ => array(

      ‘en’ => ‘WSO2 IS’,

      ‘no’ => ‘WSO2 IS’,

),

      ‘description’ => ‘Login with WSO2 IS SAML2 IdP.’,
```

```
    'SingleSignOnService' => 'https://192.168.1.7:9443',
    'SingleLogoutService' => 'https://192.168.1.7:9443',
    'certFingerprint'     => '6bf8e136eb36d4a56ea05c7ae4b9a45b63bf975d'
);
```

ANEXO E: Datos obtenidos de las pruebas realizadas para el indicador tiempo de respuesta.

Tiempo de respuesta CAS

Tiempo de respuesta CAS										
Datos 1	**Datos 2**	**Datos 3**	**Datos 4**	**Datos 5**	**Datos 6**	**Datos 7**	**Datos 8**	**Datos 9**	**Datos 10**	**Datos 11**
4544	4544	4544	4544	4544	4544	4544	4544	4544	26	29284
4544	4544	4544	4544	4544	4544	4544	4544	4544	17977	29307
4544	4544	4544	4544	4544	4544	4544	4544	4544	23094	1936
4544	4544	4544	4544	4544	4544	4544	4544	4544	51975	2150
4544	4544	4544	4544	4544	4544	4544	4544	4544	47842	3160
4544	4544	4544	4544	4544	4544	4544	4544	4544	99	2369
4544	4544	4544	4544	4544	4544	4544	4544	4544	75	17399
4544	4544	4544	4544	4544	4544	4544	4544	4544	172	2925
4544	4544	4544	4544	4544	4544	4544	4544	4544	25	2886
4544	4544	4544	4544	4544	4544	4544	4544	4544	44035	26273
4544	4544	4544	4544	4544	4544	4544	4544	4544	48224	14489
4544	4544	4544	4544	4544	4544	4544	4544	4544	49323	25838
4544	4544	4544	4544	4544	4544	4544	4544	4544	22622	2848
4544	4544	4544	4544	4544	4544	4544	4544	4544	50623	13256
4544	4544	4544	4544	4544	4544	4544	4544	4544	201	17562
4544	4544	4544	4544	4544	4544	4544	4544	4544	105	13254
4544	4544	4544	4544	4544	4544	4544	4544	4544	69682	17940
4544	4544	4544	4544	4544	4544	4544	4544	4544	49359	16650
4544	4544	4544	4544	4544	4544	4544	4544	4544	46548	3101
4544	4544	4544	4544	4544	4544	4544	4544	4544	21149	3496
4544	4544	4544	4544	4544	4544	4544	4544	4544	45155	3733
4544	4544	4544	4544	4544	4544	4544	4544	4544	46572	2843
4544	4544	4544	4544	4544	4544	4544	4544	4544	88	3108
4544	4544	4544	4544	4544	4544	4544	4544	4544	26281	18536
4544	4544	4544	4544	4544	4544	4544	4544	4544	72	18359
4544	4544	4544	4544	4544	4544	4544	4544	4544	20033	18928
4544	4544	4544	4544	4544	4544	4544	4544	4544	24694	18809
4544	4544	4544	4544	4544	4544	4544	4544	4544	186	18829
4544	4544	4544	4544	4544	4544	4544	4544	4544	128	18811
4544	4544	4544	4544	4544	4544	4544	4544	4544	67	16301
4544	4544	4544	4544	4544	4544	4544	4544	4544	23	13838
4544	4544	4544	4544	4544	4544	4544	4544	4544	70	17742
4544	4544	4544	4544	4544	4544	4544	4544	4544	61427	17972
4544	4544	4544	4544	4544	4544	4544	4544	4544	25	18484
4544	4544	4544	4544	4544	4544	4544	4544	4544	55998	65667
4544	4544	4544	4544	4544	4544	4544	4544	4544	50526	57781
4544	4544	4544	4544	4544	4544	4544	4544	4544	58899	63769
4544	4544	4544	4544	4544	4544	4544	4544	4544	59282	18832
4544	4544	4544	4544	4544	4544	4544	4544	4544	58853	14127

4544	4544	4544	4544	4544	4544	4544	4544	4544	62431	4704
4544	4544	4544	4544	4544	4544	4544	4544	4544	63517	18975
4544	4544	4544	4544	4544	4544	4544	4544	4544	29075	19059
4544	4544	4544	4544	4544	4544	4544	4544	4544	30549	17189
4544	4544	4544	4544	4544	4544	4544	4544	4544	59265	19483
4544	4544	4544	4544	4544	4544	4544	4544	4544	54930	4383
4544	4544	4544	4544	4544	4544	4544	4544	4544	46113	4404
4544	4544	4544	4544	4544	4544	4544	4544	4544	19584	49812
4544	4544	4544	4544	4544	4544	4544	4544	4544	20344	143956
4544	4544	4544	4544	4544	4544	4544	4544	4544	66393	14678
4544	4544	4544	4544	4544	4544	4544	4544	4544	50431	65596
4544	4544	4544	4544	4544	4544	4544	4544	4544	48208	4471
4544	4544	4544	4544	4544	4544	4544	4544	4544	151	3548
4544	4544	4544	4544	4544	4544	4544	4544	4544	53792	4741
4544	4544	4544	4544	4544	4544	4544	4544	4544	172	3251
4544	4544	4544	4544	4544	4544	4544	4544	4544	49846	73086
4544	4544	4544	4544	4544	4544	4544	4544	4544	49987	74795
4544	4544	4544	4544	4544	4544	4544	4544	4544	56534	41468
4544	4544	4544	4544	4544	4544	4544	4544	4544	143	150852
4544	4544	4544	4544	4544	4544	4544	4544	4544	136	48512
4544	4544	4544	4544	4544	4544	4544	4544	4544	55453	148366
4544	4544	4544	4544	4544	4544	4544	4544	4544	352	74925
4544	4544	4544	4544	4544	4544	4544	4544	4544	58550	16064
4544	4544	4544	4544	4544	4544	4544	4544	4544	95	16292
4544	4544	4544	4544	4544	4544	4544	4544	4544	54105	16175
4544	4544	4544	4544	4544	4544	4544	4544	4544	326	3019
4544	4544	4544	4544	4544	4544	4544	4544	4544	67893	4551
4544	4544	4544	4544	4544	4544	4544	4544	4544	63	5618
4544	4544	4544	4544	4544	4544	4544	4544	4544	53505	5789
4544	4544	4544	4544	4544	4544	4544	4544	4544	49450	3499
4544	4544	4544	4544	4544	4544	4544	4544	4544	56266	5809
4544	4544	4544	4544	4544	4544	4544	4544	4544	28593	3045
4544	4544	4544	4544	4544	4544	4544	4544	4544	52383	4436
4544	4544	4544	4544	4544	4544	4544	4544	4544	23253	7066
4544	4544	4544	4544	4544	4544	4544	4544	4544	55952	4606
4544	4544	4544	4544	4544	4544	4544	4544	4544	55215	3132
4544	4544	4544	4544	4544	4544	4544	4544	4544	21721	4451
4544	4544	4544	4544	4544	4544	4544	4544	4544	24294	3919
4544	4544	4544	4544	4544	4544	4544	4544	4544	52791	4893
4544	4544	4544	4544	4544	4544	4544	4544	4544	21371	4214
4544	4544	4544	4544	4544	4544	4544	4544	4544	22370	16641
4544	4544	4544	4544	4544	4544	4544	4544	4544	22381	3269
4544	4544	4544	4544	4544	4544	4544	4544	4544	17838	20653
4544	4544	4544	4544	4544	4544	4544	4544	4544	21853	4724

4544	4544	4544	4544	4544	4544	4544	4544	2804	24922	5200
4544	4544	4544	4544	4544	4544	4544	4544	3440	22649	5562
4544	4544	4544	4544	4544	4544	4544	4544	3434	18417	17308
4544	4544	4544	4544	4544	4544	4544	4544	3584	20563	5408
4544	4544	4544	4544	4544	4544	4544	4544	3835	20369	4956
4544	4544	4544	4544	4544	4544	4544	4544	3883	55452	4648
4544	4544	4544	4544	4544	4544	4544	4544	3789	53250	3416
4544	4544	4544	4544	4544	4544	4544	4544	3749	62130	4568
4544	4544	4544	4544	4544	4544	4544	4544	3864	53375	3724
4544	4544	4544	4544	4544	4544	4544	4544	4180	24396	50110
4544	4544	4544	4544	4544	4544	4544	4544	4908	1062	136764
4544	4544	4544	4544	4544	4544	4544	4544	5205	1042	51869
4544	4544	4544	4544	4544	4544	4544	4544	5561	1356	143834
4544	4544	4544	4544	4544	4544	4544	4544	6236	1489	4424
4544	4544	4544	4544	4544	4544	4544	4544	6353	61612	3859
4544	4544	4544	4544	4544	4544	4544	4544	6785	1205	4446
4544	4544	4544	4544	4544	4544	4544	4544	6738	54457	4986
4544	4544	4544	4544	4544	4544	4544	4544	7067	55340	71075
4544	4544	4544	4544	4544	4544	4544	4544	6971	159	64416
4544	4544	4544	4544	4544	4544	4544	4544	8233	1110	69898
4544	4544	4544	4544	4544	4544	4544	4544	10946	212	36636
4544	4544	4544	4544	4544	4544	4544	4544	12843	1633	2154
4544	4544	4544	4544	4544	4544	4544	4544	14311	1145	148382
4544	4544	4544	4544	4544	4544	4544	4544	18008	56918	2220
4544	4544	4544	4544	4544	4544	4544	4544	17777	257	69354
4544	4544	4544	4544	4544	4544	4544	4544	17933	211	47870
4544	4544	4544	4544	4544	4544	4544	4544	22557	56462	146251
4544	4544	4544	4544	4544	4544	4544	4544	23298	131	42480
4544	4544	4544	4544	4544	4544	4544	4544	23782	1114	137090
4544	4544	4544	4544	4544	4544	4544	4544	27212	194	20650
4544	4544	4544	4544	4544	4544	4544	4544	28745	136	5674
4544	4544	4544	4544	4544	4544	4544	4544	29712	129	15887
4544	4544	4544	4544	4544	4544	4544	4544	29605	74	11456
4544	4544	4544	4544	4544	4544	4544	4544	29916	26934	2911
4544	4544	4544	4544	4544	4544	4544	4544	30203	1375	2510
4544	4544	4544	4544	4544	4544	4544	4544	31897	59542	2138
4544	4544	4544	4544	4544	4544	4544	4544	33467	55981	3460
4544	4544	4544	4544	4544	4544	4544	4544	35087	133	5651
4544	4544	4544	4544	4544	4544	4544	4544	37585	1274	72326
4544	4544	4544	4544	4544	4544	4544	4544	38262	1503	4819
4544	4544	4544	4544	4544	4544	4544	4544	38840	1568	3675
4544	4544	4544	4544	4544	4544	4544	4544	41012	117	3104
4544	4544	4544	4544	4544	4544	4544	4544	41224	138	5820
4544	4544	4544	4544	4544	4544	4544	4544	41196	144	5723

4544	4544	4544	4544	4544	4544	4544	4544	42285	1486	4662
4544	4544	4544	4544	4544	4544	4544	4544	42833	1395	3157
4544	4544	4544	4544	4544	4544	4544	4544	42673	55425	3237
4544	4544	4544	4544	4544	4544	4544	4544	43178	24272	2877
4544	4544	4544	4544	4544	4544	4544	4544	43727	25645	3071
4544	4544	4544	4544	4544	4544	4544	4544	43204	57018	3853
4544	4544	4544	4544	4544	4544	4544	4544	43639	60003	2214
4544	4544	4544	4544	4544	4544	4544	4544	43611	23427	4140
4544	4544	4544	4544	4544	4544	4544	4544	43893	59449	12061
4544	4544	4544	4544	4544	4544	4544	4544	43931	56221	18320
4544	4544	4544	4544	4544	4544	4544	4544	44487	52621	4850
4544	4544	4544	4544	4544	4544	4544	4544	44478	24496	22726
4544	4544	4544	4544	4544	4544	4544	4544	45499	99	3319
4544	4544	4544	4544	4544	4544	4544	4544	48307	107	3210
4544	4544	4544	4544	4544	4544	4544	4544	48542	22225	3264
4544	4544	4544	4544	4544	4544	4544	4544	47355	19387	2530
4544	4544	4544	4544	4544	4544	4544	4544	48958	60126	3781
4544	4544	4544	4544	4544	4544	4544	4544	52179	53157	2900
4544	4544	4544	4544	4544	4544	4544	4544	52400	1464	2580
4544	4544	4544	4544	4544	4544	4544	4544	53000	1058	3664
4544	4544	4544	4544	4544	4544	4544	4544	53410	793	2745
4544	4544	4544	4544	4544	4544	4544	4544	53887	109	4106
4544	4544	4544	4544	4544	4544	4544	4544	53749	106	2124
4544	4544	4544	4544	4544	4544	4544	4544	53813	110	2335
4544	4544	4544	4544	4544	4544	4544	4544	54796	850	4253
4544	4544	4544	4544	4544	4544	4544	4544	55424	980	2731
4544	4544	4544	4544	4544	4544	4544	4544	56117	56725	74198
4544	4544	4544	4544	4544	4544	4544	4544	55541	83	8276
4544	4544	4544	4544	4544	4544	4544	4544	56677	779	2616
4544	4544	4544	4544	4544	4544	4544	4544	55625	694	3450
4544	4544	4544	4544	4544	4544	4544	4544	57601	74	41016
4544	4544	4544	4544	4544	4544	4544	4544	58325	101	144249
4544	4544	4544	4544	4544	4544	4544	4544	58795	200	35690
4544	4544	4544	4544	4544	4544	4544	4544	57922	24665	145550
4544	4544	4544	4544	4544	4544	4544	4544	58980	24407	7350
4544	4544	4544	4544	4544	4544	4544	4544	59361	59963	36049
4544	4544	4544	4544	4544	4544	4544	4544	58708	59640	145312
4544	4544	4544	4544	4544	4544	4544	4544	58795	54350	46837
4544	4544	4544	4544	4544	4544	4544	4544	55482	378	147292
4544	4544	4544	4544	4544	4544	4544	4544	58633	336	43233
4544	4544	4544	4544	4544	4544	4544	4544	59072	78	140638
4544	4544	4544	4544	4544	4544	4544	4544	59107	113	39448
4544	4544	4544	4544	4544	4544	4544	4544	58380	20896	141183
4544	4544	4544	4544	4544	4544	4544	4544	56844	58639	67835

4544	4544	4544	4544	4544	4544	4544	4544	58452	60809	52533
4544	4544	4544	4544	4544	4544	4544	4544	59310	65251	2332
4544	4544	4544	4544	4544	4544	4544	4544	58672	200	146586
4544	4544	4544	4544	4544	4544	4544	4544	58742	20249	4050
4544	4544	4544	4544	4544	4544	4544	4544	59538	53097	4052
4544	4544	4544	4544	4544	4544	4544	4544	60087	127	35741
4544	4544	4544	4544	4544	4544	4544	4544	59007	88	141475
4544	4544	4544	4544	4544	4544	4544	4544	58478	52808	5590
4544	4544	4544	4544	4544	4544	4544	4544	58888	38	3243
4544	4544	4544	4544	4544	4544	4544	4544	60680	50543	5953
4544	4544	4544	4544	4544	4544	4544	4544	59779	69942	5977
4544	4544	4544	4544	4544	4544	4544	4544	60294	59832	6132
4544	4544	4544	4544	4544	4544	4544	4544	60940	60439	3754
4544	4544	4544	4544	4544	4544	4544	4544	60215	24575	2517
4544	4544	4544	4544	4544	4544	4544	4544	61105	59840	6141
4544	4544	4544	4544	4544	4544	4544	4544	61542	63291	3759
4544	4544	4544	4544	4544	4544	4544	4544	60126	60754	13856
4544	4544	4544	4544	4544	4544	4544	4544	62420	490	19451
4544	4544	4544	4544	4544	4544	4544	4544	61354	124	39364
4544	4544	4544	4544	4544	4544	4544	4544	62545	21654	151384
4544	4544	4544	4544	4544	4544	4544	4544	61345	63607	74658
4544	4544	4544	4544	4544	4544	4544	4544	59111	56815	23134
4544	4544	4544	4544	4544	4544	4544	4544	61626	24474	18545
4544	4544	4544	4544	4544	4544	4544	4544	62376	58864	14276
4544	4544	4544	4544	4544	4544	4544	4544	62018	62784	3828
4544	4544	4544	4544	4544	4544	4544	4544	62709	26521	4146
4544	4544	4544	4544	4544	4544	4544	4544	61327	55869	2571
4544	4544	4544	4544	4544	4544	4544	4544	60422	58441	2772
4544	4544	4544	4544	4544	4544	4544	4544	60395	57202	2479
4544	4544	4544	4544	4544	4544	4544	4544	62368	66028	3050
4544	4544	4544	4544	4544	4544	4544	4544	61617	62093	3342
4544	4544	4544	4544	4544	4544	4544	4544	61217	60622	7993
4544	4544	4544	4544	4544	4544	4544	4544	60905	64418	2920
4544	4544	4544	4544	4544	4544	4544	4544	62895	64142	3482
4544	4544	4544	4544	4544	4544	4544	4544	64297	59321	14190
4544	4544	4544	4544	4544	4544	4544	4544	62135	55489	20439
4544	4544	4544	4544	4544	4544	4544	4544	62830	59666	7810
4544	4544	4544	4544	4544	4544	4544	4544	63931	65406	2572
4544	4544	4544	4544	4544	4544	4544	4544	62950	63704	7634
4544	4544	4544	4544	4544	4544	4544	4544	63122	61350	3294
4544	4544	4544	4544	4544	4544	4544	4544	60867	62152	4594
4544	4544	4544	4544	4544	4544	4544	4544	62383	61587	3020
4544	4544	4544	4544	4544	4544	4544	4544	64207	62515	20120
4544	4544	4544	4544	4544	4544	4544	4544	61159	59524	20802

4544	4544	4544	4544	4544	4544	4544	4544	63710	588	20808
4544	4544	4544	4544	4544	4544	4544	4544	63941	992	14707
4544	4544	4544	4544	4544	4544	4544	4544	63064	558	13981
4544	4544	4544	4544	4544	4544	4544	4544	63608	69597	14709
4544	4544	4544	4544	4544	4544	4544	4544	61148	197	20793
4544	4544	4544	4544	4544	4544	4544	4544	63259	133	3809
4544	4544	4544	4544	4544	4544	4544	4544	62764	129	20590
4544	4544	4544	4544	4544	4544	4544	4544	63432	56955	18281
4544	4544	4544	4544	4544	4544	4544	4544	64272	52925	21694
4544	4544	4544	4544	4544	4544	4544	4544	64079	56655	73156
4544	4544	4544	4544	4544	4544	4544	4544	61681	80749	2914
4544	4544	4544	4544	4544	4544	4544	4544	62721	24418	6694
4544	4544	4544	4544	4544	4544	4544	4544	63506	25237	3058
4544	4544	4544	4544	4544	4544	4544	4544	63208	25611	2980
4544	4544	4544	4544	4544	4544	4544	4544	61584	23686	6182
4544	4544	4544	4544	4544	4544	4544	4544	62985	23794	3584
4544	4544	4544	4544	4544	4544	4544	4544	62551	58352	3383
4544	4544	4544	4544	4544	4544	4544	4544	62390	62282	3234
4544	4544	4544	4544	4544	4544	4544	4544	63894	588	3596
4544	4544	4544	4544	4544	4544	4544	4544	63476	671	7757
4544	4544	4544	4544	4544	4544	4544	4544	64217	575	2670
4544	4544	4544	4544	4544	4544	4544	4544	62105	270	3722
4544	4544	4544	4544	4544	4544	4544	4544	66302	150	3364
4544	4544	4544	4544	4544	4544	4544	4544	65055	157	21636
4544	4544	4544	4544	4544	4544	4544	4544	63274	925	6955
4544	4544	4544	4544	4544	4544	4544	4544	62921	83	2976
4544	4544	4544	4544	4544	4544	4544	4544	62742	59515	9114
4544	4544	4544	4544	4544	4544	4544	4544	65043	1017	4385
4544	4544	4544	4544	4544	4544	4544	4544	63166	385	2749
4544	4544	4544	4544	4544	4544	4544	4544	63653	59923	18913
4544	4544	4544	4544	4544	4544	4544	4544	63019	59561	3737
4544	4544	4544	4544	4544	4544	4544	4544	66231	60057	13702
4544	4544	4544	4544	4544	4544	4544	4544	64163	65830	70432
4544	4544	4544	4544	4544	4544	4544	4544	65474	63338	37087
4544	4544	4544	4544	4544	4544	4544	4544	64138	68168	46011
4544	4544	4544	4544	4544	4544	4544	4544	65183	26935	144634
4544	4544	4544	4544	4544	4544	4544	4544	64378	66434	140055
4544	4544	4544	4544	4544	4544	4544	4544	66355	69223	3993
4544	4544	4544	4544	4544	4544	4544	4544	65189	63194	5687
4544	4544	4544	4544	4544	4544	4544	4544	66146	62850	4773
4544	4544	4544	4544	4544	4544	4544	4544	65181	61474	30204
4544	4544	4544	4544	4544	4544	4544	4544	65627	62409	
4544	4544	4544	4544	4544	4544	4544	4544	65332	63391	
4544	4544	4544	4544	4544	4544	4544	4544	65737	64818	

4544	4544	4544	4544	4544	4544	4544	4544	66454	61130	
4544	4544	4544	4544	4544	4544	4544	4544	67367	63232	
4544	4544	4544	4544	4544	4544	4544	4544	63952	60776	
4544	4544	4544	4544	4544	4544	4544	4544	64078	25196	
4544	4544	4544	4544	4544	4544	4544	4544	67136	62764	
4544	4544	4544	4544	4544	4544	4544	4544	65377	61079	
4544	4544	4544	4544	4544	4544	4544	4544	66774	66314	
4544	4544	4544	4544	4544	4544	4544	4544	64464	60102	
4544	4544	4544	4544	4544	4544	4544	4544	68189	60947	
4544	4544	4544	4544	4544	4544	4544	4544	65976	62533	
4544	4544	4544	4544	4544	4544	4544	4544	68783	37422	
4544	4544	4544	4544	4544	4544	4544	4544	64434	26067	
4544	4544	4544	4544	4544	4544	4544	4544	66618	62253	
4544	4544	4544	4544	4544	4544	4544	4544	65041	60920	
4544	4544	4544	4544	4544	4544	4544	4544	69240	69462	
4544	4544	4544	4544	4544	4544	4544	4544	66232	65433	
4544	4544	4544	4544	4544	4544	4544	4544	66107	67588	
4544	4544	4544	4544	4544	4544	4544	4544	67247	26537	
4544	4544	4544	4544	4544	4544	4544	4544	66775	26118	
4544	4544	4544	4544	4544	4544	4544	4544	67626	29651	
4544	4544	4544	4544	4544	4544	4544	4544	66998	27789	
4544	4544	4544	4544	4544	4544	4544	4544	67159	24911	
4544	4544	4544	4544	4544	4544	4544	4544	67531	36243	
4544	4544	4544	4544	4544	4544	4544	4544	68802	29725	
4544	4544	4544	4544	4544	4544	4544	4544	65147	20483	
4544	4544	4544	4544	4544	4544	4544	4544	65603	1825	
4544	4544	4544	4544	4544	4544	4544	4544	65712	312	
4544	4544	4544	4544	4544	4544	4544	4544	68979	2098	
4544	4544	4544	4544	4544	4544	4544	4544	66154	21787	
4544	4544	4544	4544	4544	4544	4544	4544	66800	74372	
4544	4544	4544	4544	4544	4544	4544	4544	68620	1329	
4544	4544	4544	4544	4544	4544	4544	4544	68403	71298	
4544	4544	4544	4544	4544	4544	4544	4544	66258	1753	
4544	4544	4544	4544	4544	4544	4544	4544	65321	1228	
4544	4544	4544	4544	4544	4544	4544	4544	68852	352	
4544	4544	4544	4544	4544	4544	4544	4544	68856	1426	
4544	4544	4544	4544	4544	4544	4544	4544	68156	67167	
4544	4544	4544	4544	4544	4544	4544	4544	68630	1802	
4544	4544	4544	4544	4544	4544	4544	4544	65794	64837	
4544	4544	4544	4544	4544	4544	4544	4544	66648	467	
4544	4544	4544	4544	4544	4544	4544	4544	66762	1641	
4544	4544	4544	4544	4544	4544	4544	4544	66177	572	
4544	4544	4544	4544	4544	4544	4544	4544	65838	1218	
4544	4544	4544	4544	4544	4544	4544	4544	68663	603	

4544	4544	4544	4544	4544	4544	4544	4544	68367	427	
4544	4544	4544	4544	4544	4544	4544	4544	66601	1852	
4544	4544	4544	4544	4544	4544	4544	4544	68361	320	
4544	4544	4544	4544	4544	4544	4544	4544	71589	163	
4544	4544	4544	4544	4544	4544	4544	4544	66716	1969	
4544	4544	4544	4544	4544	4544	4544	4544	68935	1851	
4544	4544	4544	4544	4544	4544	4544	4544	68242	1067	
4544	4544	4544	4544	4544	4544	4544	4544	69813	2150	
4544	4544	4544	4544	4544	4544	4544	4544	67925	73021	
4544	4544	4544	4544	4544	4544	4544	4544	67682	69531	
4544	4544	4544	4544	4544	4544	4544	4544	67570	162	
4544	4544	4544	4544	4544	4544	4544	4544	68682	131	
4544	4544	4544	4544	4544	4544	4544	4544	70689	72270	
4544	4544	4544	4544	4544	4544	4544	4544	69557	61911	
4544	4544	4544	4544	4544	4544	4544	4544	70065	374	
4544	4544	4544	4544	4544	4544	4544	4544	68663	289	
4544	4544	4544	4544	4544	4544	4544	4544	70846	21727	
4544	4544	4544	4544	4544	4544	4544	4544	70129	26095	
4544	4544	4544	4544	4544	4544	4544	4544	68393	64323	
4544	4544	4544	4544	4544	4544	4544	4544	71034	24804	
4544	4544	4544	4544	4544	4544	4544	4544	70984	72187	
4544	4544	4544	4544	4544	4544	4544	4544	70615	71140	
4544	4544	4544	4544	4544	4544	4544	4544	72556	74660	
4544	4544	4544	4544	4544	4544	4544	4544	71059	66249	
4544	4544	4544	4544	4544	4544	4544	4544	72635	61965	
4544	4544	4544	4544	4544	4544	4544	4544	70742	64109	
4544	4544	4544	4544	4544	4544	4544	4544	70012	72608	
4544	4544	4544	4544	4544	4544	4544	4544	68955	60005	
4544	4544	4544	4544	4544	4544	4544	4544	70851	24658	
4544	4544	4544	4544	4544	4544	4544	4544	72571	66736	
4544	4544	4544	4544	4544	4544	4544	4544	71545	30620	
4544	4544	4544	4544	4544	4544	4544	4544	69099	24891	
4544	4544	4544	4544	4544	4544	4544	4544	71860	913	
4544	4544	4544	4544	4544	4544	4544	4544	70726	23592	
4544	4544	4544	4544	4544	4544	4544	4544	71365	69758	
4544	4544	4544	4544	4544	4544	4544	4544	69723	23265	
4544	4544	4544	4544	4544	4544	4544	4544	74402	918	
4544	4544	4544	4544	4544	4544	4544	4544	71742	62013	
4544	4544	4544	4544	4544	4544	4544	4544	72921	16077	
4544	4544	4544	4544	4544	4544	4544	4544	72351	22238	
4544	4544	4544	4544	4544	4544	4544	4544	74508	234	
4544	4544	4544	4544	4544	4544	4544	4544	74873	961	
4544	4544	4544	4544	4544	4544	4544	4544	73202	64058	
4544	4544	4544	4544	4544	4544	4544	4544	72028	18571	

4544	4544	4544	4544	4544	4544	4544	4544	74420	69560	
4544	4544	4544	4544	4544	4544	4544	4544	74812	24010	
4544	4544	4544	4544	4544	4544	4544	4544	74127	23193	
4544	4544	4544	4544	4544	4544	4544	4544	73738	65795	
4544	4544	4544	4544	4544	4544	4544	4544	73160	63308	
4544	4544	4544	4544	4544	4544	4544	4544	70610	64043	
4544	4544	4544	4544	4544	4544	4544	4544	66215	69172	
4544	4544	4544	4544	4544	4544	4544	4544	74182	23148	
4544	4544	4544	4544	4544	4544	4544	4544	73733	70530	
4544	4544	4544	4544	4544	4544	4544	4544	65620	62709	
4544	4544	4544	4544	4544	4544	4544	4544	72739	23968	
4544	4544	4544	4544	4544	4544	4544	4544	73089	47081	
4544	4544	4544	4544	4544	4544	4544	4544	74093	140491	
4544	4544	4544	4544	4544	4544	4544	4544	72654	24447	
4544	4544	4544	4544	4544	4544	4544	4544	72515	414	
4544	4544	4544	4544	4544	4544	4544	4544	73740	469	
4544	4544	4544	4544	4544	4544	4544	4544	72437	27969	
4544	4544	4544	4544	4544	4544	4544	4544	73911	965	
4544	4544	4544	4544	4544	4544	4544	4544	74798	770	
4544	4544	4544	4544	4544	4544	4544	4544	72561	900	
4544	4544	4544	4544	4544	4544	4544	4544	70362	1266	
4544	4544	4544	4544	4544	4544	4544	4544	74160	21152	
4544	4544	4544	4544	4544	4544	4544	4544	72844	1189	
4544	4544	4544	4544	4544	4544	4544	4544	73473	155	
4544	4544	4544	4544	4544	4544	4544	4544	73233	25708	
4544	4544	4544	4544	4544	4544	4544	4544	68826	68099	
4544	4544	4544	4544	4544	4544	4544	4544	73808	70425	
4544	4544	4544	4544	4544	4544	4544	4544	74355	61240	
4544	4544	4544	4544	4544	4544	4544	4544	76506	60926	
4544	4544	4544	4544	4544	4544	4544	4544	76365	63547	
4544	4544	4544	4544	4544	4544	4544	4544	77888	950	
4544	4544	4544	4544	4544	4544	4544	4544	74777	916	
4544	4544	4544	4544	4544	4544	4544	4544	45695	1511	
4544	4544	4544	4544	4544	4544	4544	4544	57493	370	
4544	4544	4544	4544	4544	4544	4544	4544	56877	1897	
4544	4544	4544	4544	4544	4544	4544	4544	79679	460	
4544	4544	4544	4544	4544	4544	4544	4544	71926	419	
4544	4544	4544	4544	4544	4544	4544	4544	68823	1859	
4544	4544	4544	4544	4544	4544	4544	4544	80463	1735	
4544	4544	4544	4544	4544	4544	4544	4544	82127	1925	
4544	4544	4544	4544	4544	4544	4544	4544	80041	800	
4544	4544	4544	4544	4544	4544	4544	4544	79514	47988	
4544	4544	4544	4544	4544	4544	4544	4544	82799	136582	
4544	4544	4544	4544	4544	4544	4544	4544	49595	59615	

4544	4544	4544	4544	4544	4544	4544	4544	72231	238	
4544	4544	4544	4544	4544	4544	4544	4544	82797	403	
4544	4544	4544	4544	4544	4544	4544	4544	14745	330	
4544	4544	4544	4544	4544	4544	4544	4544	74531	69399	
4544	4544	4544	4544	4544	4544	4544	4544	71776	401	
4544	4544	4544	4544	4544	4544	4544	4544	14291	410	
4544	4544	4544	4544	4544	4544	4544	4544	80915	276	
4544	4544	4544	4544	4544	4544	4544	4544	81617	65873	
4544	4544	4544	4544	4544	4544	4544	4544	69223	1446	
4544	4544	4544	4544	4544	4544	4544	4544	79212	67421	
4544	4544	4544	4544	4544	4544	4544	4544	182	591	
4544	4544	4544	4544	4544	4544	4544	4544	168	64711	
4544	4544	4544	4544	4544	4544	4544	4544	80	68531	
4544	4544	4544	4544	4544	4544	4544	4544	67	73929	
4544	4544	4544	4544	4544	4544	4544	4544	69890	474	
4544	4544	4544	4544	4544	4544	4544	4544	72454	1836	
4544	4544	4544	4544	4544	4544	4544	4544	49879	66967	
4544	4544	4544	4544	4544	4544	4544	4544	47474	68497	
4544	4544	4544	4544	4544	4544	4544	4544	17627	66112	
4544	4544	4544	4544	4544	4544	4544	4544	17896	274	
4544	4544	4544	4544	4544	4544	4544	4544	182	67443	
4544	4544	4544	4544	4544	4544	4544	4544	172	47642	
4544	4544	4544	4544	4544	4544	4544	4544	51	133349	
4544	4544	4544	4544	4544	4544	4544	4544	44	70466	
4544	4544	4544	4544	4544	4544	4544	4544	48386	69923	
4544	4544	4544	4544	4544	4544	4544	4544	61359	77904	
4544	4544	4544	4544	4544	4544	4544	4544	19841	67414	
4544	4544	4544	4544	4544	4544	4544	4544	75	59047	
4544	4544	4544	4544	4544	4544	4544	4544	34	70941	
4544	4544	4544	4544	4544	4544	4544	4544	22277	58543	
4544	4544	4544	4544	4544	4544	4544	4544	108	40618	
4544	4544	4544	4544	4544	4544	4544	4544	38	138404	
4544	4544	4544	4544	4544	4544	4544	4544	76909	68266	
4544	4544	4544	4544	4544	4544	4544	4544	49465	64792	
4544	4544	4544	4544	4544	4544	4544	4544	15901	61029	
4544	4544	4544	4544	4544	4544	4544	4544	18062	70778	
4544	4544	4544	4544	4544	4544	4544	4544	16850	466	
4544	4544	4544	4544	4544	4544	4544	4544	139	60836	
4544	4544	4544	4544	4544	4544	4544	4544	91	69730	
4544	4544	4544	4544	4544	4544	4544	4544	57236	66001	
4544	4544	4544	4544	4544	4544	4544	4544	178	27164	
4544	4544	4544	4544	4544	4544	4544	4544	218	19261	
4544	4544	4544	4544	4544	4544	4544	4544	77	16166	
4544	4544	4544	4544	4544	4544	4544	4544	109	14278	

4544	4544	4544	4544	4544	4544	4544	4544	51098	21537	
4544	4544	4544	4544	4544	4544	4544	4544	17369	20221	
4544	4544	4544	4544	4544	4544	4544	4544	60974	21559	
4544	4544	4544	4544	4544	4544	4544	4544	168	22916	
4544	4544	4544	4544	4544	4544	4544	4544	74	27025	
4544	4544	4544	4544	4544	4544	4544	4544	44600	23475	
4544	4544	4544	4544	4544	4544	4544	4544	17617	23487	
4544	4544	4544	4544	4544	4544	4544	4544	81166	23079	
4544	4544	4544	4544	4544	4544	4544	4544	80389	10375	
4544	4544	4544	4544	4544	4544	4544	4544	72566	27145	
4544	4544	4544	4544	4544	4544	4544	4544	65263	25594	
4544	4544	4544	4544	4544	4544	4544	4544	48579	43790	
4544	4544	4544	4544	4544	4544	4544	4544	19568	133042	
4544	4544	4544	4544	4544	4544	4544	4544	56172	24830	
4544	4544	4544	4544	4544	4544	4544	4544	65121	19510	
4544	4544	4544	4544	4544	4544	4544	4544	65179	26174	
4544	4544	4544	4544	4544	4544	4544	4544	206	18722	
4544	4544	4544	4544	4544	4544	4544	4544	73	39196	
4544	4544	4544	4544	4544	4544	4544	4544	55797	141735	
4544	4544	4544	4544	4544	4544	4544	4544	34967	68133	
4544	4544	4544	4544	4544	4544	4544	4544	62310	66790	
4544	4544	4544	4544	4544	4544	4544	4544	601	24007	
4544	4544	4544	4544	4544	4544	4544	4544	236	18056	
4544	4544	4544	4544	4544	4544	4544	4544	13425	24125	
4544	4544	4544	4544	4544	4544	4544	4544	72651	63666	
4544	4544	4544	4544	4544	4544	4544	4544	55169	19193	
4544	4544	4544	4544	4544	4544	4544	4544	52679	65882	
4544	4544	4544	4544	4544	4544	4544	4544	62769	19353	
4544	4544	4544	4544	4544	4544	4544	4544	151	26105	
4544	4544	4544	4544	4544	4544	4544	4544	55	64659	
4544	4544	4544	4544	4544	4544	4544	4544	53583	65238	
4544	4544	4544	4544	4544	4544	4544	4544	21250	17670	
4544	4544	4544	4544	4544	4544	4544	4544	44981	22971	
4544	4544	4544	4544	4544	4544	4544	4544	42622	22226	
4544	4544	4544	4544	4544	4544	4544	4544	14566	17622	
4544	4544	4544	4544	4544	4544	4544	4544	13534	19229	
4544	4544	4544	4544	4544	4544	4544	4544	172	18152	
4544	4544	4544	4544	4544	4544	4544	4544	163	22708	
4544	4544	4544	4544	4544	4544	4544	4544	68	15957	
4544	4544	4544	4544	4544	4544	4544	4544	148	15861	
4544	4544	4544	4544	4544	4544	4544	4544	24	15087	
4544	4544	4544	4544	4544	4544	4544	4544	34	24398	
4544	4544	4544	4544	4544	4544	4544	4544	45424	69344	
4544	4544	4544	4544	4544	4544	4544	4544	51114	16045	

4544	4544	4544	4544	4544	4544	4544	4544	22895	71124	
4544	4544	4544	4544	4544	4544	4544	4544	61	65024	
4544	4544	4544	4544	4544	4544	4544	4544	34	63956	
4544	4544	4544	4544	4544	4544	4544	4544	56943	64782	
4544	4544	4544	4544	4544	4544	4544	4544	50442	2138	
4544	4544	4544	4544	4544	4544	4544	4544	39899	70874	
4544	4544	4544	4544	4544	4544	4544	4544	60221	62185	
4544	4544	4544	4544	4544	4544	4544	4544	51933	73895	
4544	4544	4544	4544	4544	4544	4544	4544	25755	71200	
4544	4544	4544	4544	4544	4544	4544	4544	20153	1935	
4544	4544	4544	4544	4544	4544	4544	4544	20112	66376	
4544	4544	4544	4544	4544	4544	4544	4544	60644	18404	
4544	4544	4544	4544	4544	4544	4544	4544	45384	16765	
4544	4544	4544	4544	4544	4544	4544	4544	51791	72782	
4544	4544	4544	4544	4544	4544	4544	4544	186	18773	
4544	4544	4544	4544	4544	4544	4544	4544	49498	23956	
4544	4544	4544	4544	4544	4544	4544	4544	49709	19203	
4544	4544	4544	4544	4544	4544	4544	4544	113	23943	
4544	4544	4544	4544	4544	4544	4544	4544	221	27286	
4544	4544	4544	4544	4544	4544	4544	4544	146	24758	
4544	4544	4544	4544	4544	4544	4544	4544	24	27102	

Realizado por: David Rodríguez. 2019

Tiempo de respuesta WSO2

Tiempo de respuesta WSO2										
Datos 1	**Datos 2**	**Datos 3**	**Datos 4**	**Datos 5**	**Datos 6**	**Datos 7**	**Datos 8**	**Datos 9**	**Datos 10**	**Datos 11**
146098	329395	24864	56	83319	367354	153	482	397136	852	110121
35733	26102	27057	29	59223	363880	75	168	23013	36553	255
150648	537	523572	110864	778805	20857	486184	339212	413640	1749	116
3232	1066	26753	52	80340	323	34627	21721	42569	655	120670
3694	1408	519324	26	772397	364529	36	58	61087	1493	99577
20817	1039	25924	156633	75110	929773	37866	23	341	866	105484
3072	969	4315	71	774187	363686	43171	21759	785	13608	801257
3272	563	352	40	72126	916774	56429	542191	40600	425	36011
28654	1429	34809	110594	782089	20507	36540	695818	38152	11026	1061867
4995	581	17025	185	22143	20458	18798	21532	27299	1616	28411
10533	83814	126866	134547	21003	139966	110800	35914	157	54	240946
93939	26816	25779	136689	249178	477104	190099	61	535867	12852	43007
32059	26202	29974	186	786778	296	177	37	22587	13112	883354
440897	35872	519350	190622	250274	372533	154	21247	33516	980	59033
283306	456	524790	659193	252328	373490	376	210	89	877	1055934
30177	26652	982	192860	86038	19115	53	21298	413	12249	65
26792	65114	667	198159	770241	246	57	68653	37473	1281	435
23303	1241	930	189721	58307	289	163	874792	122175	350	423

12867	376	25504	192	307933	429	246	159	41961	463	98826
17658	39550	24432	157990	283453	373747	248	688487	508854	12892	98786
415997	480094	603	659058	783835	357770	109	60	22731	892	99974
405	272	125371	260	136251	143683	69	174	65810	54	241502
91169	51273	671	207636	61453	927121	85	344914	65047	63062	1064846
27554	1317	155	201423	64416	369311	84	21137	156	12136	104020
26092	40220	24855	638	68487	15985	783	614183	51625	13061	127219
439	744	24234	197828	71367	830	39017	65	22604	13451	164
159	336579	523018	633	66747	1058	38178	19075	772	13130	133069
291	1057	23921	199927	788554	373289	254	75	76757	819	130383
384466	836	522267	548	72374	367540	37418	175	44740	13596	298
786	892	24930	588	788048	935226	82	268	23444	12358	45
68	596	1613	199	59850	13168	187	37	663469	12523	275
101	2404	21220	82	780207	926057	226060	203	719	13780	95055
319	105150	125976	21004	140723	144338	248	249	88	21	201
94968	25790	935	732	491	6992	69	85	45533	11166	878947
27891	1069	72986	192617	253820	10075	38005	145	121	935	22028
25442	1125	486	193044	92534	928485	186	844422	1080	13696	898847
19389	105837	346	354	86343	11076	91	141	35879	11841	904
29886	348484	27253	179	92439	76	208	72	343	11169	22203
357842	1491	524508	152358	253385	30	225674	88	807	11771	22261
30080	1192	24114	663255	256767	381831	225980	349825	108117	12135	96006
15895	76464	521456	58	88293	222	39551	27	1601	12597	888298
28404	1147	84758	199386	780850	11265	159	60	117	11188	986
26838	586	525887	199	64950	927875	34754	624793	213	11551	964
33447	105658	125308	21245	114232	142230	147588	37	879	236193	238802
90902	1143	24076	213160	782166	11568	38531	26	1977	8415	39490
7447	26702	5527	87	79937	67	226182	21304	22041	8868	918253
357049	25237	460	29	60830	35	283	21136	397673	14012	97060
32026	582	456	147111	773665	12168	41120	708995	34206	84207	814981
28936	851	777	192528	74872	11824	180	196	602342	10024	96340
7041	341970	71903	255	353586	12649	299	62	22075	456185	126282
35444	27254	6267	202849	66380	61	305	660	50823	519	1064501
32309	25633	1339	157609	774665	28	458	142	1225	8579	126348
252	37824	23676	661309	270904	12004	367	577	1133	85	128932
32573	38325	732	168815	780981	443345	81	53	33913	7859	125444
128	111457	129578	21004	136551	146415	150	129123	551	34	337287
93501	83290	23429	665500	80419	12952	102	418	21956	10489	735841
9288	25948	519332	202418	78478	12712	2640	592209	758752	74983	120
28648	51169	23771	212406	80247	940604	229822	352774	1300	711845	109
299420	485361	519009	214031	64801	384702	2337	68691	141	1941	289
293952	34092	1170	91	778630	198	229933	853122	1452	124188	120783
7468	846	23868	214638	175	12579	2004	234	141	172	912819
6347	1333	406	45	1245	447462	2150	696450	105	126510	92

31140	2766	21002	80	89401	13069	867	85	2504	48	43972
32719	83780	24307	40	82044	931427	919	24	143	19	1142614
264	1796	525992	85	788598	13249	38744	857307	2793	65874	764
613	12686	126131	22347	811	14608	148941	21071	64703	16574	79
93500	114000	20172	21004	120	142208	33512	115334	21376	229834	737
147	111965	515574	53	78296	945289	541208	211	90748	959375	94963
11679	42565	23685	184066	74650	13722	230948	203	92949	69556	895700
109	81123	531958	162	94182	12558	232348	373466	105920	201	35634
307	79260	23287	144383	80943	935409	98	594484	557693	43464	882489
72	24600	517681	55	76793	11390	41	74596	3098	671297	666
28402	85435	23989	323	61764	12583	35814	221	1885	56460	41006
10163	107270	910	328	788862	942158	96	86	40460	66486	551997
10220	100777	1863	197362	93758	405344	232392	21	69941	835126	107869
38005	60343	23418	669785	1718	192	79	22135	21441	83	47170
34599	1491	133317	190025	141098	13135	148234	718975	61540	89	171
92001	109968	23717	530	78080	143210	800	126588	42366	286	1079777
33016	83876	1126	157182	81301	380532	231533	282	21298	45936	65
12334	84925	23307	667012	83001	207	1153	206	2023	51145	48
6054	1563	432	232	630	12955	1297	599637	642233	829569	38000
36330	44412	1321	149520	78770	383076	235769	210	2061	68735	923185
37543	11274	22959	201483	358	261	43547	22750	2107	728638	107235
5128	108465	521396	222	73491	11856	1120	853478	503	222	822020
36605	42321	414493	163252	69681	938385	41632	702211	688645	49049	47846
112689	1586	841	675866	791434	383319	34977	717507	115096	755376	921806
26586	21006	23321	67	67371	12014	290	204	520961	32898	45806
32129	342922	131259	26	180	11647	145697	714405	161020	41206	286769
95226	109815	22938	136970	785998	146551	33217	77	2428	176	41009
43279	111305	521467	201593	75117	178	72	192	432733	818547	223
32053	1100	22910	668085	81691	386744	178	23296	83843	79	203
31395	1574	652	211260	786711	233	179	23583	1606	27	37254
13960	2505	557	202506	95520	11121	77	532444	412868	45465	1088902
35978	85644	7824	166431	788563	955450	75	256	110	17196	42071
35826	971	947	678250	235598	11942	899	189	1792	51297	895874
352	1596	418	327	781499	392550	212	23269	2414	675706	47139
34893	21002	22422	87	71531	198	47	23	4649	47885	886891
33324	1398	524141	41	81390	11605	39620	159	33137	282	50064
61	1335	133265	203962	212	11623	148213	21004	70386	310	238820
93084	111889	1083	134892	788656	140900	39150	150100	311	26	43407
30262	455	8014	204588	81417	12417	65	21386	2748	391	813612
39255	997	22304	196	776871	209	26	179	418233	75066	213
33173	1632	635	159830	76894	11824	34876	67	57473	342	43587
13652	754	22261	668134	81751	12026	531978	57	2225	54366	32696
342	86136	535513	205846	784830	398198	39132	714119	82102	653485	938271
41612	832	22399	169595	61979	198	44040	625848	2095	52929	44819

80	110197	520737	673221	69811	12002	31504	629055	2558	203	47056
44536	1776	9209	415	785066	523565	35033	618776	39369	50550	33631
42908	13274	22266	153385	65426	9614	37306	198	578515	86	946142
35272	568	129505	167604	141	393918	92	867356	339	34	203
72259	111484	22290	136664	781535	141263	238226	112	4910	279582	81
36709	1100	527747	675408	249147	12447	35564	367652	2209	48305	49497
41613	24338	22216	369	80284	172	1069193	749462	1473	529092	36692
35582	37226	22224	108	80031	13680	91	23328	32998	70530	1085616
43116	605	524054	32	84248	74	72	986	1193	69465	39782
308610	730	22097	166387	64086	29	239062	379129	84354	204	1061165
294759	36019	522214	673218	789607	404013	32913	1068	2645	71193	89
17998	21003	8959	163507	70135	13076	152	374939	170	730697	514
40288	25197	22054	163729	1481	12882	139	1115	5601	121	672
17517	4175	22042	682276	89639	424863	231	1037	2099	50	39892
34838	968	5191	182304	24603	173	26497	1065	27286	76025	32841
11173	109383	18146	45384	118	140483	148650	167	356	238209	247
91501	600	131051	686093	74127	62	246	311	76510	56735	903902
38964	12649	22202	339	75057	23	98	22947	128900	196	562
42444	25436	3162	154916	788105	404515	613	550874	2598	97598	49068
37119	88308	22199	179861	2272	965955	86	23422	54258	60863	904590
9211	493538	527279	295	2111	14609	818	160	3035	758878	39885
297459	1090	22424	97	1421	70	750	22998	1475	271	858101
38761	454	537307	33	87409	25	239632	67	3175	177	44193
21010	1178	444	229894	82214	15734	212	1084	495568	59	40275
40512	36352	10750	211259	791419	15145	27630	616581	61161	82066	1075074
16093	14507	11280	181262	38678	958467	506893	1012	487045	246	34423
40089	112287	11437	223	890	144455	121460	228	357	233275	265
92405	1436	129854	685712	90667	408050	241241	1144	5835	53175	815323
624	1078	11150	172126	782520	283	44259	604151	1661	748145	41403
13052	695	113017	186	75258	404288	241372	22987	44151	93409	45751
45555	2600	11639	78	791169	16358	241283	381160	21318	52443	835542
37142	719	700	70	75999	429153	293	22630	34220	760147	44852
43085	38995	331	223446	91055	407841	240953	150	1629	77533	615985
19626	15189	11735	191	787586	212	242147	22308	1460	81155	40588
16482	15345	12513	172550	74851	62	147	103	2264	100568	816025
906	935	11952	688653	793168	16747	40966	199	33776	50549	49702
627	1010	12525	176098	80688	963790	553785	22280	35018	448	908007
20041	114781	10493	137253	139102	140589	122122	90	67370	157	842
213	979	136368	687212	83435	35	1552	22762	1852	21163	35515
883	2408	13400	174141	84749	408161	1597	71	73576	1030893	1082730
905	635	12998	689835	278597	223	1700	21965	108162	610	257
35720	24878	11667	21298	798990	410032	1721	160	61200	657	260
114622	26911	13753	219875	73179	15906	1938	21425	40052	94156	57397
37477	25464	12240	175808	790624	436945	1662	78	34092	219	1087813

40679	1217	10396	694344	76239	410995	1741	705	1768	84	42969
594	25613	11683	208	785121	961592	34331	660	977	78718	908192
42763	547	10281	189873	81737	402700	510379	487	1320	838181	43729
15252	2090	8585	683830	78245	13912	35212	128	113931	271	836558
235	111960	7682	140490	133699	141991	171	174	65549	57	769
92132	36780	128986	154157	90289	197	491	162	587	68	48712
37703	73450	8528	690337	75159	416790	245809	104	1567	54869	1086973
259	36239	96534	210	204	420882	536	98	94537	586	54642
17625	14520	538922	66	224	15576	421	163	400	88009	825126
319197	25669	8431	220511	71850	970829	32042	66	384	63408	39023
524	731	8037	691077	793463	409455	432	121	1749	772332	920792
39997	15230	95669	187857	71541	974102	247307	53	687397	160	36987
41678	59898	162369	189	788776	14261	278	29	1253	21235	1093587
41092	25565	142907	164476	155	419083	520	21574	131221	769776	42347
22956	14724	137697	165096	87	970530	263556	21	641	84	825980
42930	116500	74378	135429	138297	143287	890	78	66352	404	105
93293	845	131315	145410	25090	11903	481682	21821	69815	414	47755
36251	1564	145	122614	19925	856	176	199	7770	94433	909893
35982	25625	189	284	264509	844	320	124	2286	759963	50512
464511	376	70	263	190	695	610837	22	60617	59157	899629
33315	41153	552	184735	20387	11337	197	375383	52225	95	32966
38160	15693	419	693026	19301	415159	293919	21583	2388	82244	1074910
659	15874	24	34429	22103	9487	293726	252	2793	756270	44239
1279	1181	83	689636	213	8800	95	96	8569	102	1059015
39196	14906	47	242580	23709	971259	68	25	421803	66888	40458
16671	358320	23913	125189	21398	78	513402	21165	9435	659655	834987
42815	12565	545929	24249	920	26178	159	26889	66409	21008	161
93625	115749	131034	137062	22588	141327	29	79	406469	401	38217
347	1662	130448	691218	23342	71	33	111	527723	21146	1104505
38871	14829	135717	149273	25230	252	202	20	2586	91217	53829
39764	514	108900	168243	23626	14590	297389	379328	1273	840789	1091820
37053	1088	113528	185544	804416	986937	517651	265	1652	75122	50519
1637	1528	24279	701661	26078	422771	220	628102	9133	762790	35249
306885	15928	552974	148636	327980	14454	210	21152	2370	85695	884909
1549	15019	295	691207	265	22905	518200	383639	3381	80054	206
757	25374	172	180206	29133	24332	517752	376302	34715	766634	38018
39215	738	262	144912	29764	995698	518339	877127	1292	81137	1098131
38902	728	30	705952	133582	22060	123929	122	540	248	964
93050	115607	136326	936	28188	145990	300588	664	1635	231521	37908
34329	18300	65	34423	28406	23965	605	284	3108	87886	829975
311865	83965	25456	700923	32756	444243	669	30	560	1057971	38718
39712	16966	79	26914	30149	71	298107	384874	37391	70809	954967
33744	13075	118034	29561	815417	34	652	639096	32715	55985	35109
37927	15986	119522	182	31828	25341	151	133	21474	59616	47632

311685	14084	132892	26	29836	77	520254	21294	507	60103	837896
321166	25270	100239	21400	26114	447654	107	59	3283	101788	35249
604	25107	126291	170106	36679	1003693	65	269	112188	94778	34128
611	15114	96735	233471	30652	42	26	21397	654	81863	122
1172	13151	102377	21413	138298	25765	150545	168	614	1016891	233
93856	114941	131588	100269	27812	142069	298200	484	67993	275944	73
1207	73010	139027	210	411375	463373	308	102	116729	82773	384
314877	877	131638	38800	30872	447182	422	628028	32536	882069	302
1074	17041	282	215	30285	25228	307910	372579	21166	72066	47706
793	14267	213	224112	33805	999248	93	21087	917	21170	1090609
740	15634	74643	172132	31962	264	25	633338	2084	847279	38660
397	472445	214	170614	816587	26119	308359	779	2715	1001	183
1607	44660	172832	120956	36400	432857	213	21116	32717	266	30844
40227	18742	141985	294	27190	47573	642025	381286	9533	117	836908
655	12799	305	159	37028	45026	210	912	37943	209	43509
300412	13204	336	352	138901	276	147547	21189	806	565	61
93287	117414	137245	102	31785	141897	303131	152858	53994	275597	835912
35752	14491	212	29	400483	44367	171	648581	544876	69241	34169
656	13946	109	21101	30078	45890	537179	908	33094	786924	53308
1349	1332	130	142	36915	440725	178	613824	60060	96293	34052
1199	811	101815	174814	31376	447086	316947	21112	1000	1255	409
471	14019	251	703759	34748	35642	537744	622144	1224	86	426
353818	1745	207	110923	36190	854	324372	632971	9228	121	247
527	13328	25930	708697	27060	50267	319392	493	286	94163	41177
41048	403	107649	154603	28000	48397	317853	69620	1330	669912	933661
1666	304	93	171543	35692	856	1361475	1291	411287	59904	53790
40610	14905	102	158397	145652	49732	147494	546378	804	99238	232137
94487	117346	132625	138642	32247	141429	72	55533	1612	277314	833948
354	15857	25330	185838	34577	985	92	71	885	63121	51840
316845	13919	75	696208	824675	54163	459	373769	137473	2015	933359
35549	98422	129363	149808	28764	54243	366	646283	1443	80958	41623
34460	14943	170864	129996	26245	56263	309060	649144	1862	86995	1064550
30424	37337	144216	695954	415841	58704	320015	294	569	79838	38373
670	26241	546327	120655	30054	56230	1359236	1408	1788	64832	828835
27260	15524	105166	229407	419885	62689	307262	89	9421	878193	44632
615	12957	425737	40114	39743	1302	414	642969	904	64542	913768
36290	27059	212	705633	32925	62066	308	878485	1048	87169	37574
311768	500765	94243	41057	5673	1423	21141	297	19701	84960	34137
11579	112843	19133	137025	18592	144477	147633	233	242324	527	288048
82952	36899	132897	123819	140061	1344	308032	882556	487	1811	925033
416	99883	130297	168531	38079	1363	310067	80	8647	58690	55611
1145	500004	1364	698608	36036	66993	540302	388975	509	394	905587
589	26557	248	174867	320953	74930	578	2582	161	2273	54501
277	92491	385	21328	32113	1489	446	2622	1734	21104	1096199

1029	108644	103735	147390	26434	73355	642044	882714	35144	2459	51799
546	744	1569	694378	397327	77859	441	3014	687264	87839	555022
373	155	245	155736	37141	81195	541659	21134	8787	355	43748
573	15396	120001	125606	49400	3039	318625	2769	402	272	35698
417	754	1533	701017	26115	2530	309755	649957	44700	94699	823595
139	116644	116898	47661	28417	141697	147669	130607	200160	490	230597
94933	195	94892	178547	139465	86338	309498	745655	960494	67923	36191
568	11659	95659	133608	27550	72885	313706	2767	10716	1031980	1099207
226	12150	192	182823	34438	2673	471	312	1480	86993	36391
283	14340	120544	654	30114	2773	629	434	12641	639733	846140
149	15125	96035	1254	316679	2828	832181	3218	12206	2304	27625
28154	12670	189	55	26281	88957	1106	21224	21664	85041	907977
25830	39763	400	1347	35689	3386	1168	235	439652	61787	60354
340306	29317	26550	781	41207	79590	1074	168	10044	850961	40194
9408	12520	95801	1354	32082	3753	983	709844	10110	83985	842624
325047	38904	131979	168686	36138	83645	590	3042	21736	172	29074
471	117967	574	329	39623	146415	126249	154920	182	277961	1203
208	16218	132591	119	139879	101910	21173	21134	693345	86950	833269
334328	27764	553	1402	248	4281	147	900788	634	97487	
541	497952	595	171583	27608	105605	581378	3026	122522	835314	
1576	12209	197	1738	35114	106813	222	652018	79133	506	
6278	18156	386	129850	31890	103223	656128	725544	11071	64980	
8016	9668	468	127652	391247	105472	191	3043	11401	675261	
324615	13064	479	1862	40377	109484	19004	3162	21822	273	
324143	517	139	155066	823576	3641	553944	21183	901623	99756	
367	154	175	2174	38575	5394	103	380242	697992	74867	
6231	18542	26944	134540	33338	3565	253	707316	391	73357	
6528	91419	316	365	552	145012	119797	57027	157	473	
94714	7742	21003	708066	141575	4429	80	21206	30500	82904	
7134	22302	348	1639	24951	3545	585880	392566	546908	102957	
324017	7421	375	883	391352	5722	318465	1446423	21639	102464	
6651	26810	666	133946	29129	5566	655864	382666	54753	93973	
24452	28020	486	75	622	109647	510	741939	83473	2837	
122020	31723	27817	179362	21061	109042	484	4503	952535	74519	
24440	69227	146293	709351	336624	102661	262	772668	81487	104512	
24985	503711	297	34137	271041	112018	676113	4205	11687	90848	
349199	12754	326	709982	21260	111568	221	850	429533	1035	
337504	7910	144564	229525	239	114990	588241	4068	12201	3346	
118598	120249	106879	139650	211	147240	148333	57805	180610	276728	
74918	5786	76	186306	138790	110175	332	451	11676	3406	
29543	5319	91182	706474	16455	3908	322394	715	479425	76967	
45067	40452	28156	236209	821006	113176	654251	77	71371	125	
44403	5665	28865	709126	19982	4047	162	205	79144	3465	
25920	310	3076	244270	3158	3847	208	293	42346	3731	

83812	30327	28219	60474	6338	4311	321167	4256	762514	110881	
88201	503234	547852	699855	3192	4166	183	650937	42553	709271	
98672	68229	532	125768	5901	117745	21374	21166	90892	80548	
472084	29750	742	192414	3689	4800	21110	652484	615066	3835	
96027	219	28369	715708	428138	4391	812809	21113	503444	75175	
472084	13223	90469	15883	3732	26233	150512	21135	284864	21017	
93135	284	32	135274	223	146285	21136	132372	31873	583	
97201	29163	3497	135133	402357	4445	657218	647384	12804	79447	
469605	28020	26957	172749	3151	4239	114	651549	1052	3761	
96371	381	29498	700762	822543	123179	219	464	31342	3793	
929	79240	392	40508	4003	3504	47	4314	12320	79061	
857	450	667	134979	346811	119611	659577	4240	457346	4520	
816	257	729	193156	2871	4334	21303	406	414765	3919	
435	142	570	21167	3388	4346	479135	4974	124377	97013	
625	3967	4116	706377	397315	3275	607187	623017	593395	67496	
6983	4083	29064	194552	4730	3468	21149	4133	79205	100610	
321660	128255	29117	21196	295980	4029	150212	5070	202566	4790	
86701	119510	134563	137229	143118	145047	313515	276	85968	237920	
289	28179	26877	131492	836820	3976	581737	5380	89798	5555	
204	30559	415	709091	329326	4168	144	21362	574864	97074	
344	3010	29225	39180	284773	2510	76	4749	78674	101369	
6890	3091	480	30309	852261	3470	442	4644	536	5797	
480	28817	298	712600	295262	138925	474	3849	85424	5569	
1231	63111	26910	39287	851967	1978	348	21597	10788	7189	
758	512230	29990	2683	285673	137327	141	389329	484548	6095	
1106	31715	29323	2554	854211	142151	674346	4817	113927	76842	
211	2245	28409	2649	300965	249	66	5189	69236	6103	
306338	2326	29330	130355	296835	130280	1393	889409	220	6027	
415	97666	133206	1277	139891	54080	225	54731	82779	237600	
203	290	546896	1998	859544	130452	593469	4223	91707	7832	
6895	76	21009	1431	290537	819	316048	3469	93039	5318	
25948	341	4690	174607	304250	873	317912	3924	923305	5877	
405	2312	111656	701819	344803	935	21369	887063	9594	93283	
24945	29127	142807	642	859685	954	605903	3117	92327	6314	
24091	65	552821	47592	308936	461918	318149	2257	969	5697	
32869	2495	29059	159216	31405	461388	447873	2459	85721	6809	
468939	29967	29913	704399	311140	150962	235	892406	820	7044	
72438	29288	110854	134087	859477	273	21490	2400	59181	5687	
73400	2036	29110	3713	377915	153851	1505	21174	55	5576	
95762	98040	133892	137306	361	144798	452000	60428	1981	235765	
24056	31292	5282	129208	299146	462995	667519	910788	482127	6880	
9155	31749	462	158401	299611	41157	610	21141	75575	69290	
62341	29913	30653	324	298824	460125	605050	1925	1455	791156	
91106	1918	5448	36009	450012	1019966	606256	378876	436127	111636	

847	27207	28398	138744	309245	155026	795	1272	22734	75749	
536	1800	215	707752	301860	48596	1126	983	217	782920	
335108	30766	29560	187122	312285	263	1168	213	11031	104506	
406	1759	5058	128268	864995	312	1299	129	8541	87187	
434	30323	29108	117793	347530	50372	1080	78	9663	780782	
1339	28563	28116	36160	857214	491051	48127	21164	23	5203	
431	321	228	138782	139980	150051	662971	629	10109	704	
104	80772	29690	173121	344083	50133	855	100	82426	5659	
335950	30138	551003	706994	852352	464961	336943	205	29581	98776	
1073	1519	28975	178772	344834	1012238	341	386561	618393	5215	
53720	234	29387	713088	850558	341	673124	175	64464	3609	
145	30878	28977	199210	337963	49402	63	21179	65574	5099	
8000	159	28608	133972	1085	488639	343451	189	601769	72404	
28817	1758	21003	177260	1105	48413	23	668378	86510	1106854	
32719	31119	107293	707925	287689	157805	189	382901	593456	3859	
454	29286	104407	118321	328844	159822	568020	240	720	96170	
7305	1724	28171	4791	858286	238	5812	897756	25256	97147	
9656	233	20963	138703	20034	146020	27251	59979	57	284025	
94452	1623	133026	133110	132507	480	53997	21219	551	104938	
356155	29212	29594	985	289393	448	475	409196	764	105582	
28526	1793	1322	185440	859134	24498	557	156	1380	1043375	
28735	29254	120909	371	299581	163344	678091	674421	1029	2359	
7941	30490	429	48032	857613	25138	190	114038	776	83800	
545	29708	120862	710542	19754	164035	344451	83	32351	1041472	
681	1978	552077	40587	1475	447	666543	475	39982	72643	
637	1785	476	43276	305106	640	343741	558	764540	784263	
206	1866	293	34113	1622	642	66	701	54308	73882	
254	32006	103835	719241	1838	560	838474	579	594673	1015931	
7686	119141	5703	130	1884	150188	25	1074	57	278671	
94834	34396	134072	6226	48841	27714	184	662	37354	410	
628	1921	6556	34879	2077	81	251	69463	22938	2045	
486	1965	7059	5864	312178	38	291	63	1080	71	
562	1899	483	6472	2736	167100	21115	22	51280	2670	
6582	29359	6747	37281	3168	275	528269	671223	784	916	
208	509959	198	719770	6224	32530	693227	90355	74060	912	
299	28778	6214	51831	6487	27479	343686	536252	183156	105541	
8171	91475	25990	705197	2870	27446	329250	667426	541068	76357	
7340	519921	559390	47649	4291	147	326832	194	266	114031	
7037	33018	27390	47927	4571	179	606477	667508	384	85643	
7288	116555	5971	114	6305	110092	340056	1237	192768	278049	
94684	31565	136064	46621	138762	28522	1788	669191	47684	114109	
328170	1976	5133	7196	1766	33	602807	69773	951	716998	
25191	1914	4614	36633	7315	52	599842	582259	678	293	
25180	1938	4843	725069	7837	26847	599068	385	273	46629	

47408	29076	4428	7153	386354	89	342087	22733	430180	874732	
7261	29065	24721	7760	206	117	342392	113705	58329	671	
29597	516166	554992	8341	10342	212	327295	22692	726	708	
25242	31067	4947	39294	12842	55	598857	710	470	635	
24991	2213	4985	226320	12360	29680	981	657	663	21891	
24532	31294	23510	47573	13102	32223	1136	113	103278	873438	
334104	122388	557271	135527	18965	147794	602663	1007	53	315	
95214	27717	139703	52103	140725	90	68	65	488144	21830	
45580	2271	23927	32067	878935	34	1271	672658	67009	76555	
351123	2295	556081	42216	20560	75	1328	151	804668	21758	
25719	2297	4485	5449	20573	30	915	81	493822	779625	
41896	2172	4314	6766	885733	32579	71	453	102573	105637	
23927	30652	22466	5846	21192	33924	603373	463	642482	77356	
476757	2246	555016	139651	880341	66	1769	399453	407	86622	
23800	358656	22275	5743	19887	44	1731	63729	67253	105910	
23503	67030	22177	5864	871019	31050	575307	391935	98362	81971	
23840	1905	561666	6715	22022	80	344315	387541	11716	216	
324977	96642	4862	21004	94	148461	1388762	922	24	264	
97045	30186	132815	55722	139511	31	1674	509591	876	285	
743	2269	22167	6675	21146	31151	586579	188	37374	84	
933	2032	21790	6278	879312	67	598640	361	695263	79	
776	415	560420	33152	22799	22	606501	344	296	80923	
8331	2220	21693	718454	875585	475806	598380	68	1098	1060	
28544	29111	564525	34449	75	488847	589277	29	11625	1073	
25497	31920	21593	724335	22577	1038947	2073	391977	506112	1160	
25128	167	563586	54823	886266	168	1999	680380	25126	1101	
25299	29915	105431	719171	23431	178105	2134	189	701297	1075	
930	18912	444	37122	23126	66	603879	79839	159551	190	
882	15701	403	24497	21064	15646	333354	26935	211163	21026	
99301	120394	133397	140288	160	149678	2250	41240	1657	85	
177	30836	112	35377	889756	179508	334073	82075	513158	177	
343	31788	109	6298	20409	365	21120	680442	509999	87808	
415	514436	107775	165909	877893	487561	603595	926362	776	87425	
248	28502	640	6490	70	484090	332200	327	472	109410	
9189	30748	77785	5688	360985	1044291	611519	162	89911	49245	
67721	34961	255	43730	31	438	325687	85	97051	98058	
774	2301	3066	7634	390268	43724	579670	437	1459	789318	
900	322	462	26755	206	178938	426	393784	45282	86841	
708	2234	141738	712215	377444	36604	148	75674	465084	401	
27830	378942	97938	40294	890093	34145	2741	73876	58	901995	
95735	235	132265	1617	144465	138367	1507	706	48964	83	
25984	313	93	26869	335567	210647	596333	78917	469	89338	
7817	74571	29	37060	882931	34590	336543	594941	788	564	
147	21002	111849	723775	369999	664	332479	83697	985	81047	

44478	201	161	31015	18821	32970	452695	162	9499	22839	
875	117	165	35903	879886	518980	580605	66	30805	90898	
588	26894	49	5973	254	999	598817	122164	466368	890157	
488	29354	29	51192	374489	215	578524	97079	65756	77268	
765	29404	101585	5218	884904	220	3636	567028	26429	802	
236	29194	125004	30600	371825	155	337134	96839	465692	914	
663	271	122201	5175	372168	98	1107	23431	25	365	
95537	118672	136028	279	266	146823	1497	61836	1068	1424	
436	69875	258	5386	879982	134	97	780	486	236	
6711	153	76	5851	370651	1146	3588	24143	2052	136	
374	2066	26	4599	883317	73	750	389041	59303	198	
1065	2298	105270	2913	484	1349	84	24130	932414	1185	
464	29099	118035	2389	356576	239	21197	191	11463	1041	
598	519298	576148	1986	188	114	504344	84	38043	92522	
612	33302	122	1747	381133	183661	3844	188	132517	104421	
23883	434	31	41328	890014	32721	3607	873	77404	23054	
56513	96	78044	36559	14589	33317	92474	307	598100	885997	
357462	323	571602	189883	14707	1527	3906	63673	231743	107122	
75558	124523	21001	1328	142578	147925	1276	64967	982	1539	
327790	30566	78143	716756	421085	635	615053	90	619	86419	
343380	713	240	209141	13433	34062	616484	262	1534	167	
6692	32738	99923	750939	80	150	328312	251	584	416	
28212	100	111418	238772	25	117	451299	143	105101	79	
857	161	282	222100	13280	97	4091	51863	550406	159	
714	26087	115813	769916	12876	132	4765	23690	10786	345	
2372	30418	116768	221995	13303	147	4935	62168	26389	31	
504	31110	282	770926	14274	31	332540	55604	146465	95097	
53329	514157	74994	224963	13028	495968	511	523525	55918	124096	
512	27806	89	234184	13858	35263	4411	226	238455	226	
84227	123857	21003	78	143945	123209	114632	160	10639	1802	
54515	3381	118122	83	12242	216767	4445	140	736	203	
24125	3075	64	54	223	155	236	139	10744	112311	
625	3054	116764	253338	380749	385	4795	408844	1042	111272	
797	3204	576521	245033	901595	78	4614	69291	47490	73545	
478	28990	171	771721	13414	215131	4851	1074	705706	764081	
469	29161	171	94	13596	217968	344028	433	10315	211	
480	31687	157	89	895751	39315	21108	24175	10733	342	
7852	31264	87	256686	14299	33251	508325	770652	394	87668	
10507	28759	70	778455	366157	47935	5150	24324	11067	96496	
592	28856	24	63598	891325	1043883	5056	531640	6030	1022181	
12429	123597	23872	140924	25972	144773	26979	65	27165	2049	
224	27020	136375	775405	43	30983	150334	250	234151	106174	
933	105028	114743	61200	12992	595	449	220	575	764932	
360350	425	102426	771758	61	276	418	219	42275	124	

770	32447	112355	79854	25	875	21114	247	667468	33	
350875	30405	273	60260	14203	245	6265	295	49968	121640	
7466	309	419	774124	14729	907	71	143	960056	800317	
322	27181	486	64470	13785	261	71	234	11377	115467	
597	30037	103575	81668	12844	109	4339	93	9867	120956	
841	60991	102898	70813	899271	112	4314	1406	10475	318	
83785	4050	119378	248390	14625	218583	4499	121	48003	97289	
415780	123877	90	101816	15016	138500	4427	44950	610291	2328	
402	560	286	71267	141807	36667	150550	193	103	112966	
850	3409	152	770784	381112	111	4644	257	43087	801605	
25004	29017	260	71046	77	33867	539	394687	44654	87802	
36824	27387	75	60438	13420	36818	56	127	12221	797534	
550	517448	735	61484	63	31630	3963	673117	10914	124861	
36043	517593	109092	770112	205	497736	697883	1062	36215	122058	
87694	27116	113625	71241	242	30255	3567	406004	96710	60365	
95932	531044	108613	78655	16073	296	21115	43749	11258	1060189	
56144	27791	234	783188	376415	133	335133	200	35265	116159	
458911	518091	124098	60810	904575	32	700353	115	33041	593	
328113	125013	111342	40238	345791	121674	172	473	57235	241776	
99912	26358	21004	777832	142283	348	114893	49608	232179	794	
55782	522562	188	267	176	344	58	106033	34110	912	
875	27243	189	150	19863	286	685	572782	1854	113275	
56698	28669	87	218638	121100	329	617297	188	35878	127920	
25638	76383	99	81864	20795	81	273	709	1075	874875	
25681	403	126	246	20492	93	699334	34	58250	98008	
924	27019	23	66123	361260	58	356011	82	11638	89803	
8544	29056	107405	228555	20603	81	268	680900	989	921	
41015	26955	115302	57920	373	38371	82	38	12382	995	
317835	26988	98603	767402	403	36377	700745	78	39007	92716	
66513	126103	109922	139773	366920	150557	1175	59715	841	239370	
98920	513860	133966	67393	139633	33201	56736	33	216	1069667	
440661	32050	123441	227	359133	31365	850	224	434685	26001	
732	31050	76	76705	21057	30673	1027	23561	2319	1080251	
377	25368	76	65946	187	127	613	57758	41865	1176	
8506	526876	144	777357	247	31	21220	22959	720690	1188	
25927	698	161	65975	362209	161	620063	58848	2041	1278	
904	394	468	60333	919163	220	690346	60343	11494	101856	
34727	25726	478	72345	366877	270	148	441929	12477	799077	
2444	517335	61	67223	197	119	71	40313	11439	57772	
616	26207	31	784160	19754	100	707934	35349	42267	117604	
1470	128312	130669	136840	924717	148	457	390	47247	236052	
99953	522647	126166	73646	141778	32324	46941	23478	42	1074570	

Realizado por: David Rodríguez. 2019

ANEXO F: Datos obtenidos de las pruebas realizadas para el indicador consumo de recurso (RAM - CPU).

Consumo Recurso (RAM - CPU)

CONSUMO DE RECURSOS			
CAS		WSO2	
CPU (%)	MEM (MB)	CPU (%)	MEM (MB)
5	1218516	67,50	1326012
0,3	1218620	66,1	1323916
13,8	1218624	53,4	1321604
49,4	1219312	70,2	1321020
87,6	1219960	66,7	1321656
87,5	1220708	72,4	1321880
89,7	1221304	68,2	1322652
84	1222208	68,9	1321964
84,7	1223396	38,7	1327444
86,6	1224148	0,7	1331932
89,6	1225124	30,1	1338624
88,9	1225612	71,8	1338896
81	1230352	78,2	1338028
86,4	1231400	76	1338028
87,1	1231944	67,6	1338356
83,8	1233016	40,8	1333096
81,7	1233868	77	1333292
86,5	1234580	75,5	1334032
90	1234880	75,8	1336100
82,2	1235192	77,1	1329644
87,5	1235628	70,1	1329568
86,4	1236336	71,7	1330152
86	1236896	72,8	1330492
88	1237560	76,9	1331668
86,3	1237624	77,1	1332792
20,9	1257212	78,4	1334064
81,5	1262320	70,2	1322776
91,8	1264832	77,3	1323300
90,5	1267440	71,1	1324404
84,1	1270608	74,8	1326020
83,9	1273088	72,7	1329476
80,6	1273420	75,6	1330364
90,3	1273584	71,4	1331216
92,6	1274040	0,8	1343276
87,2	1274296	0,3	1338308
84	1274820	0,4	1337568
18,1	1289356	0,2	1337864

40,8	1298396	0,2	1336576
88	1298572	2,1	1337424
88	1298444	0,2	1337044
86,1	1299212	0,9	1336040
89	1299520	2,8	1336544
78,7	1298768	1,9	1336120
80,6	1299712	2,4	1335688
86,1	1300412	7,3	1338540
81,7	1300924	6,9	1338924
84,4	1301020	4,8	1341340
82,3	1301184	4,1	1341756
84,9	1301712	2,8	1331988
5,7	1311096	11,2	1334456
48	1312368	9,7	1337388
86,4	1312004	11,1	1333664
87,3	1311828	11,6	1337500
88,8	1311460	0,7	1338156
63,6	1312212	3,2	1339992
86,4	1313476	5,1	1334976
86,9	1313412	0,8	1337440
84,7	1312752	1	1343200
88,8	1312496	1,1	1338252
84,8	1312644	1,1	1342588
69,4	1314568	1,1	1336832
87,1	1313880	1,4	1339204
76,1	1314024	1,1	1344732
85,6	1313952	1,1	1339748
92,2	1313820	1,4	1342196
89,7	1314208	0,7	1343892
82,4	1314100	1	1345508
67,1	1314248	1,4	1337264
70,8	1314296	0,7	1338988
91,2	1314596	0,7	1340700
86	1314444	1,1	1334128
89,2	1313968	3,5	1335776
60,4	1319620	8	1323204
81,7	1319972	1,3	1305404
86,1	1320056	2	1316180
84,7	1320656	40,5	1321776
82,1	1321132	14,1	1341800
91,5	1321228	1,2	1348812
82,5	1322292	2,6	1329912
91,7	1322296	2,6	1325572
85,6	1322528	10,6	1329132

88,3	1322952	7,1	1341540
83,8	1323552	0,8	1340364
13,7	1319584	3,8	1341460
33,4	1316984	3,1	1340724
89,1	1309560	11,9	1326432
85,4	1309156	23,9	1333856
88,2	1310304	19,5	1335992
86,2	1310456	11,5	1326836
83,6	1310504	15,2	1336652
84,8	1310816	7,1	1338048
92,2	1310628	10,9	1337196
85,2	1310484	17,3	1338964
84,2	1310232	23,5	1332256
83,7	1306008	31	1332248
66,7	1306448	21,8	1339592
57,1	1312260	9,8	1328148
91,4	1312456	26,8	1331788
82,9	1311396	32,6	1303924
79,4	1312868	44,3	1305640
87,3	1314228	60,1	1307792
81,5	1315088	65,2	1310392
80,5	1313140	48	1315612
86,5	1312424	33,3	1330464
89,9	1304244	18	1297104
80,3	1304296	30,8	1306164
88,4	1303696	11,5	1310612
83,9	1303620	1,8	1316316
86,4	1303696	2,9	1321080
51,5	1296432	10,6	1333724
8,2	1311820	59,4	1337064
61,3	1312924	31,6	1328276
83,5	1310632	43,3	1330876
50	1298380	50,5	1334032
5,9	1309736	45,3	1326044
14,2	1284856	30,3	1328292
22,3	1257272	16,1	1329836
5,8	1230472	68,2	1332752
0,7	1230412	29,6	1333016
0,3	1230400	0,7	1335876
0,7	1230268	51,9	1340292
0,7	1230244	69,7	1328724
0,3	1230236	66,2	1330928
0,7	1230228	69,1	1333244
0,3	1230216	60,8	1336508

0,7	1230208	73,5	1339180
0,3	1230200	13	1336060
0,3	1230192	22,6	1343976
0,7	1230184	75	1332848
0,3	1230032	72,8	1334912
0,7	1230088	76,5	1336052
0,7	1230000	76,5	1337924
2,7	1206216	57,4	1330824
0,3	1206184	1,1	1345264
0,7	1206160	0,4	1317944
0,7	1205960	58,7	1318832
0,7	1205944	78,6	1320012
0,7	1205936	72,8	1322112
0,7	1205928	72,5	1323260
0,3	1205920	15	1337256
0,3	1205796	73,8	1327332
0,7	1205788	77,5	1329260
0,3	1205780	73,9	1330548
0,3	1205636	76,6	1332684
0,3	1205628	73,5	1334176
0,3	1205620	42	1319828
0	1205612	71,7	1320604
0,3	1205604	72	1320964
0,3	1205596	61,6	1321800
0,3	1205588	73	1323340
0,7	1205580	43	1322236
5,9	1103376	65,3	1326724
0,7	1103376	19,6	1325176
0,7	1103368	12,2	1326160
1	1103360	17,8	1337740
0,7	1103352	67,9	1323476
0,7	1103344	12,3	1327560
0,3	1103336	6,3	1324160
0,7	1104656	7,7	1308332
0,3	1104640	50,9	1309296
7,1	1106476	76,4	1310084
7,1	1107452	25,3	1321440
0,7	1107444	76,1	1321800
0,3	1107436	76,6	1322160
0,7	1107428	77	1322184
0,7	1107420	75,4	1321932
0,7	1107412	75,7	1323024
3,7	1110584	52,8	1336788

Realizado por: David Rodríguez. 2019