UNIVERSIDAD NACIONAL
“PEDRO RUIZ GALLO”
ESCUELA DE POSGRADO

MAESTRÍA EN INGENIERÍA DE SISTEMAS

“IMPLEMENTACIÓN SSO (SINGLE SIGN-ON) PARA OPTIMIZAR EL ACCESO A LOS SERVICIOS WEB EN LA UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO”

TESIS

PRESENTADA PARA OBTENER EL GRADO ACADÉMICO DE MAESTRO EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN GERENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN Y GESTIÓN DEL SOFTWARE

AUTOR:

ING. KARINA ARACELI MINO PÉREZ

ASESOR:

MG. ROBERT EDGAR PUICAN GUTIÉRREZ

LAMBAYEQUE – PERÚ

2017

Implementación SSO (Single Sign-On) para optimizar el acceso a los servicios web en la Universidad Nacional Pedro Ruiz Gallo.

Ing. Karina Araceli Mino Pérez
AUTOR

Mg. Robert Edgar Puican Gutiérrez
ASESOR

Presentada a la Escuela de Posgrado de la Universidad Nacional Pedro Ruiz Gallo para optar el Grado de: MAESTRO EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN GERENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN Y GESTIÓN DEL SOFTWARE

APROBADO POR:

Mg. Ernesto Karlo Celi Arévalo
PRESIDENTE DEL JURADO

Mg. Edward Ronald Haro Maldonado
SECRETARIO DEL JURADO

Mg. Pedro Fiestas Rodríguez
VOCAL DEL JURADO

DEDICATORIA

A mis padres Laura Rosa y Edgardo, ejemplos de dedicación y superación constante, que me permiten cristalizar el logro de mis objetivos.

A mi hijo Rodrigo Nicolás, motor y motivo en mi vida, que me impulsa cada día a seguir adelante.

AGRADECIMIENTOS

A la Universidad Nacional Pedro Ruiz Gallo, por permitirme desarrollar la presente Tesis de Investigación.

A mi asesor Ing. Mg. Robert Edgar Puican Gutiérrez, por todo el apoyo brindado en la realización de la tesis.

A todas las personas que de una u otra manera me apoyaron en la culminación de la misma.

TABLA DE CONTENIDOS

ANEXOS

RESUMEN

La presente investigación, tiene como objetivo de estudio, realizar una investigación de una solución Single Sign On, con el propósito de optimizar el proceso de autenticación de los usuarios para el acceso a los servicios web en la Universidad Nacional Pedro Ruiz Gallo (UNPRG); frente al problema actual que genera el brindar una autenticación por cada una de las múltiples aplicaciones y servicios web que brinda a la comunidad universitaria.

El presente documento se organiza en tres capítulos, los cuales se detallan a continuación:

En el Capítulo I, se presenta el análisis del objeto de estudio, considerando los antecedentes del problema, planteamiento del problema, formulación del problema, justificación e importancia del estudio, los objetivos, la hipótesis, las variables, diseño de contrastación de la hipótesis y población y muestra.

En el Capítulo II, se indica el marco teórico propuesto para el entendimiento de la investigación, describiendo los conceptos de Single Sign-On (SSO), características, clasificación y arquitectura; así como también Secure Sockets Layer – SSL, certificados digitales y algoritmos de criptografía.

Finalmente, en el Capítulo III, se define el desarrollo de la propuesta Single Sign On en la Universidad Nacional Pedro Ruiz Gallo; presentando una ddescripción de la situación actual, en el proceso de autenticación para el acceso a los servicios web que brinda la UNPRG; el análisis de mecanismos de solución Single Sign On y el Desarrollo de Propuesta SSO - UNPRG.

ABSTRACT

The purpose of this research is to investigate a Single Sign On solution, with the purpose of optimizing the Users authentication process for access to web services at Pedro Ruiz Gallo National University (UNPRG); facing the current problem generated by providing authentication for each of the multiple applications and web services provided to the university community.

The present document is organized in three chapters, which are detailed as follows:

Chapter I, presents the study object analysis, considering the problem antecedents, approach to the problem, problem formulation, justification and Importance of the study, objectives, hypotheses, variables, hypothesis testing design and population and sample.

In the Chapter II, is indicated the theoretical frame proposed for the understanding of the investigation, describing the concepts of Single Sign-On (SSO), characteristics, classification and architecture; as well as also Secure Sockets Layer - SSL, digital certificates and algorithms of cryptography.

Finally, Chapter III defines the development of Single Sign On proposal at the Pedro Ruiz Gallo National University; presenting a description of the current situation, in the authentication process for access to web services provided by the UNPRG; the analysis of Single Sign On solution mechanisms and the SSO - UNPRG Proposal Development.

INTRODUCCIÓN

Hoy en día los servicios web, se han convertido en una tecnología fundamental para el intercambio de datos, mediante aplicaciones web desarrolladas en diferentes lenguajes de programación.

Así mismo, existen diferentes aplicaciones web ya desarrolladas, tanto en software libre como propietarias, que las instituciones optan por su implementación.

Para obtener acceso a estas diferentes aplicaciones, es necesario una autenticación, en su mayoría por medio de un nombre de usuario (username) y su contraseña (password). Como resultado, el usuario llega a poseer tantas cuentas de autenticación, como aplicaciones a las cuales tenga que acceder; generando malestar al usuario en recordar las múltiples cuentas de acceso, existiendo la posibilidad de olvidar alguna de ellas.

A finales de la década del 90 se trató de buscar la solución de este problema y surge el término Gestión de Acceso a Web (Web Access Management), que constituye una subcategoría de lo que se conoce como Gestión de Identidad (Identity Management). La Gestión de Identidad es un sistema integrado de políticas y procesos organizacionales que pretende facilitar y controlar el acceso a sistemas de información e instalaciones.

Al surgimiento de la Gestión de Acceso a Web esta era conocida como Single Sign On (SSO) y era simple en sus capacidades pero resolvía la principal necesidad de la época, cómo compartir la información del usuario a través de diferentes dominios sin tener que obligar al mismo a identificarse más de una vez. Actualmente se han desarrollado varios métodos de autenticación entre los que se encuentran Central Authentication Service (CAS), Shibboleth, Security Assertion Markup Language (SAML), OpenID, y OAuth (este último utilizado en las populares redes sociales Facebook y Twitter).

CAPITULO I: ANÁLISIS DEL OBJETO DE ESTUDIO

1.1 ANTECEDENTES DEL PROBLEMA

A nivel Internacional encontramos los siguientes antecedentes:

De acuerdo a Cevallos Teneda (2016), Las diferentes aplicaciones y sistemas web ofrecen múltiples servicios a los usuarios, por lo tanto los proveedores de estos servicios están forzados a formar colaboraciones temporales o fijas, para brindar dichos beneficios con tan solo un clic. La gestión de la identidad hace referencia al conjunto de políticas, procesos y tecnologías que permiten establecer cuentas de usuario y reglas relacionadas a la administración de la información y recursos digitales dentro de la organización. Esto requiere que los participantes de la identidad federada establezcan relaciones de confianza entre sí y por lo tanto permitir el intercambio de servicios o el consumo entre los socios de forma segura y confiable. Al aprovechar una arquitectura de gestión de identidades se puede establecer, ejecutar, actualizar o disolver las relaciones de confianza que requiere la colaboración institucional, lo que reduce en gran medida los costos de configuración y evita errores en los dominios individuales de la organización. El objetivo es brindar a la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, un enfoque orientado a la gestión eficaz de manejo de usuarios en las diferentes plataformas usadas dentro del ámbito académico, para acceder a servicios como cuentas de correo, plataformas educativas, repositorios virtuales, equipos informáticos, entre otros.

Cano Moreno (2014), A medida que los sistemas informáticos proliferan para soportar los procesos del negocio, tanto los usuarios, como administradores de sistemas se enfrentan a una tarea complicada para completar las funciones laborales. Los usuarios típicamente se tienen que autenticar en múltiples sistemas, necesitando una pantalla de autenticación por cada uno de los sistemas, esto podría involucrar usuarios y contraseñas distintas, mientras que los administradores de sistemas se enfrentan a la tarea de estar administrando las cuentas de los usuarios en cada uno de estos sistemas, y de estarlos coordinando para que la información sea consistente e integra de acuerdo a las políticas de seguridad de la organización. El Centro de Cálculo e Investigación Educativa se estaba enfrentando a esta

problemática, por lo que se detectó la oportunidad de mejora en la implementación de un sistema que permita la unificación de usuarios de los distintos aplicativos informáticos que son administrados por la institución y que al mismo tiempo les permitiera escalar en algún futuro a tecnologías que son manejadas a través de internet, como lo es, el sistema de inicio de sesión de Google. El proyecto consistió en la implementación de un sistema de autenticación único (SSO) que le permite a los usuarios iniciar sesión en un sistema centralizador y que es independiente de la aplicación. De esta forma se hizo transparente la comunicación entre los sistemas informáticos que el usuario utiliza para realizar las labores diarias.

González Díaz (2010), En la Universidad Tecnológica de Bolívar, no existe un suficiente nivel de integración entre los sistemas de información. Algunos sistemas no están diseñados para la operación actual. En consecuencia no cubren todos los procesos haciéndose necesario el trabajo manual. Baja inducción de los empleados a los cargos, que ocasionan tasas de error altas por desconocimiento del proceso o del manejo del sistema.

En nuestro país, podemos mencionar como antecedentes dos investigaciones, basadas en la problemática de las entidades del estado peruano: SUNAT y el Banco de la Nación.

Bringas Masgo (2011), En el contexto de mejorar la estructura y funcionamiento del estado se convierte en una necesidad para mantener la competitividad del estado peruano. Estas mejoras significativas se han logrado a través de una serie de reformas en los procesos de negocio de las instituciones del estado basándose en un uso intensivo de las TIC's.

En este marco, es el que se plantea establecer las bases para una mejor integración de los servicios de las entidades del sector público y privado. Especificamente se aborda como principal objetivo el tema de la autenticación de personas jurídicas a través del servicio autenticación de la cuenta SUNAT Operaciones en Línea (clave SOL).

Castro Velarde & Guzmán Salgado (2010), La dificultad que se presenta para desarrollar estrategias eficientes relacionadas a la administración de control de accesos internos y externos de usuarios a los recursos informáticos, al acceso personalizado de los mismos, el manejo de la información confidencial, así como al cumplimento adecuado de las normas regulatorias requieren de un estricto control interno y de un alto nivel de seguridad por lo que no existe un control eficiente de la identidad.

La propuesta de solución del proyecto tiene como objetivo implantar un sistema donde los usuarios realicen por única vez el procedimiento de identificación y autenticación para el acceso a los diferentes servicios brindados dentro de la infraestructura informática. El mecanismo habitual para lograr esta funcionalidad es que el procedimiento de identificación y autenticación dé como resultado un conjunto de credenciales que pueden ser posteriormente utilizadas para demostrar la identidad de los usuarios en el acceso a los diferentes servicios, sin necesidad de volver a proporcionar la información de autenticación.

1.2 PLANTEAMIENTO DEL PROBLEMA

En la actualidad, la Universidad Nacional Pedro Ruiz Gallo (a la cual la nombraremos en adelante como UNPRG) brinda múltiples servicios web para sus diferentes usuarios de la comunidad universitaria (docentes, estudiantes y administrativos), tales como el sistema para la gestión de la información académica de la Oficina General de Asuntos Académicos, el sistema de Actas Virtuales, el correo electrónico institucional, El Aula virtual, etc.; todas ellas direccionadas desde su portal web www.unprg.edu.pe.

Los servicios mencionados, fueron implementados en diferentes plataformas tecnológicas de las cuales podemos mencionar como lenguajes de Programación a Php y Java, así como gestores de Base de Datos MySql y Oracle.

Todos estos servicios web disponibles en el campus de la UNPRG, utilizan diferentes formularios de acceso, ya sea para ingresar únicamente a partes restringidas para realizar labores administrativas dentro del sitio, o a un espacio

personal con información específica donde el usuario va hacer uso del servicio como tal, y que tiene su perfil de usuario previamente establecido.

Sin embrago, ninguno de estos servicios web, cuentan con una sincronización de credenciales de acceso por medio de una sola interfaz, que permitan que se alimenten de información el uno del otro; haciendo que cada una posea su propia información de usuario y contraseña almacenada independientemente en sus respectivas base de datos, trayendo como consecuencia redundancia de datos y generando inconformidad entre los usuarios al contar con diferentes contraseñas que necesita recordar para un mismo usuario.

1.3 FORMULACION DEL PROBLEMA

¿El acceso a los servicios web, mediante la implementación de SSO (single sign-on), optimizará el proceso de autenticación de los usuarios en la UNPRG?

1.4 JUSTIFICACION E IMPORTANCIA DEL ESTUDIO

Ante los problemas actuales tecnológicos que enfrenta la UNPRG y al no contar con una solución que permita reducir estas dificultades, a través de una sola credencial de acceso para sus diferentes servicios web que brinda a la comunidad universitaria; se desea implementar una solución de tipo Single Sign – On y así lograr:

- ✓ Mejorar considerablemente los tiempos de acceso a los diferentes servicios web, dependiendo el requerimiento del usuario (alumno, docente y administrativo).
- ✓ Mejorar el servicio al usuario (alumno, docente y administrativo), evitando la incomodad de recordar diferentes contraseñas de acceso para cada aplicación.
- ✓ Evitar redundancia de datos en su información.
- ✓ Optimizar el Recurso Humano de la Oficina General de Sistemas Informáticos Administrativos de la UNPRG; Asignando al personal técnico

que actualmente se destina a la labor de gestión de contraseñas, en proyectos de mayor envergadura para la universidad.

Por ello, se considera de gran importancia el desarrollo del presente proyecto.

1.5 OBJETIVOS

1.5.1 Objetivo General

Optimizar el proceso de autenticación de los usuarios en la UNPRG para acceso a los servicios web, mediante la implementación de SSO (single sign-on)

1.5.2 Objetivos Específicos

1. Analizar la situación actual, en el proceso de autenticación para el acceso a los servicios web que brinda la UNPRG.
2. Analizar los Mecanismos de Solución Single Sign On.
3. Seleccionar el mecanismo de Single Sign-On para los servicios Web.
4. Desarrollar la Propuesta SSO - UNPRG.
5. Analizar e Interpretar de Resultados del proceso de autenticación con SSO y sin SSO.

1.6 HIPOTESIS

La Implementación de una solución Single Sign-On, optimizará el proceso de autenticación a los usuarios de la UNPRG, para el acceso a los servicios web.

1.7 VARIABLES.

VARIABLES	INDICADORES	SUB INDICADORES	ÍNDICES	TÉCNICAS
Dependiente Optimizar en el acceso a los servicios web de la UNPRG	Reducción de tiempo de acceso a los servicios web.	Tiempo de acceso	I1:Cantidad de tiempo que utiliza el usuario al acceder a los servicios web sin SSO I2: Cantidad de tiempo que utiliza el usuario al acceder a los servicios web con SSO	Monitoreo
Independiente Implementar de una solución Single Sign - On en la UNPRG.				

1.8 DISEÑO DE CONTRASTACIÓN DE LA HIPOTESIS

La Contrastación de la Hipótesis, se realizará mediante un diseño de un método descriptivo correlacional.

1.9 POBLACION Y MUESTRA

1.9.1 POBLACION:

La población está compuesta por los usuarios de la comunidad universitaria (universo) que accedan a los servicios web de la UNPRG.

1.9.2 MUESTRA:

Se tendrá en consideración a usuarios que tengan acceso a más de un servicio web de la UNPRG, tales como estudiantes que se encuentren cursando el tercer ciclo de una escuela profesional; así como también sus respectivos docentes.

CAPITULO II: MARCO TEÓRICO

2.1 SINGLE SIGN-ON (SSO)

Para comprender la definición de SSO, citamos a los siguientes autores:

Rouse (2010), Single Sign-On (SSO) es una sesión de usuario / autenticación proceso que permite a un usuario que introduzca un nombre y una contraseña para acceder a múltiples aplicaciones.

Para Chicano Tejada (2014), Las herramientas de sistemas de punto único de autenticación o Single Sign On (SSO) facilitan que los usuarios de los sistemas de información realicen solo una vez el procedimiento de identificación y autenticación para acceder a los distintos servicios que facilitan dichos sistemas. Es decir, los procedimientos SSO habilitan al usuario para acceder a todos los servicios del sistema con solo una autenticación.

Martín Echeverría (2014) "…todas las aplicaciones dirigen la identificación de los usuarios al SSO, que dependiendo del recurso al que desea el usuario acceder, exigirá un tipo de identificación más o menos fuerte,..".

Podemos concluir que SSO, es un procedimiento de autenticación Única, que permite al usuario acceder a múltiples sistemas, aplicaciones o servicios web de diferentes plataformas de desarrollo, mediante una única solicitud de acceso; teniendo como objetivo la transferencia de la funcionabilidad de cada uno de sus mecanismos de seguridad.

2.1.1 CARACTERÍSTICAS SSO

Para Edelman (2014), el sistema Single Sign-On (SSO) o español Inicio de Sesión Único, es una solución de administración de contraseñas efectiva y fácil de implementar que aumenta la seguridad tanto de la computadora del usuario

como de las aplicaciones de la empresa, mientras reduce al mismo tiempo los costos relacionados con la administración de las contraseñas e incrementa la productividad y la satisfacción del usuario.

Las principales características del SSO son:

- Multiplataforma:

  Este tipo de solución Single Sign – On facilita las tareas de acceso a los recursos de red desde distintas plataformas (combinación de hardware y software usada para ejecutar aplicaciones; en su forma más simple consiste únicamente de un sistema operativo, una arquitectura, o una combinación de ambos).

- Transparencia:

  Realiza el acceso a los recursos de los sistemas de una forma clara para el usuario debido a la automatización del inicio de sesión único.

- Facilidad de uso:

  Da la facilidad debido a que el usuario se autentica una sola vez y el sistema le permite tener acceso a los recursos para los cuales está autorizado en la empresa. Así se evita los retrasos producidos por las interrupciones por la solicitud de usuario y contraseña para el acceso a diferentes recursos o aplicaciones empleadas por el personal de la empresa.

- Gestión sencilla:

  El uso de la solución de tipo Single Sign-On (SSO) sincroniza las contraseñas e información de los usuarios. Esto implica la reducción de la gestión de los recursos por parte de los administradores.

- Control de acceso:

  Este tipo de solución Single Sign-On no afecta porque solo implica cambiar los mecanismos de autenticación del cliente y/o servidor, pero no modifica los permisos de los recursos.

- Seguridad:

  La seguridad en este tipo de solución Single Sign-On depende de la arquitectura utilizada, pero en todos los casos la información viaja cifrada por la red (SSL, certificados...)

2.1.2 CLASIFICACIÓN SSO

Para Roebuck (2011), la clasificación el sistema Single Sign-On se basa en simple y complejo.

- Simple:

  Se puede diferenciar entre las empresas el sistema SSO es único (esté o no clusterizado), y otorga acceso a los usuarios de un único dominio de seguridad.

- Complejo:

  En este caso se encuentra una arquitectura propia de sistemas federados, entre los que existe algún mecanismo de interrelación o confianza. Para la arquitectura de autenticación centralizada, el usuario es identificado a través de un elemento (Token o certificado) que es el que intercambia con las entidades de autenticación. En el caso del mecanismo de autenticación múltiple, 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 servidora.

2.1.3 TIPOS DE HERRAMIENTAS SSO

Existente cinco principales tipos de SSO, conocidas también como reduced sign on systems, que es su traducción significa sistemas de autenticación reducida.

Chicano Tejada (2014), nos define los cinco tipos de herramientas SSO:

- Enterprise single sign-on (E-SSO) o Legacy Single Sign-On: estas herramientas utilizan una autenticación primaria para completar automáticamente las aplicaciones secundarias con el mismo usuario y contraseña.

- Web single sign-on (Web-SSO) o Web access management (Web-AM) : solo funciona en aplicaciones y recursos web y utilizan cookies para reconocer a aquellos usuarios que han accedido exitosamente y su estado de autenticación.

- Kerberos: protocolo que externaliza la autenticación de los usuarios a través del servidor Kerberos.

- OpenID: herramienta que compila la identidad en una dirección url, que puede ser verificada posteriormente por cualquier aplicación o servidor para conocer la identidad y los privilegios del usuario que pretende acceder a ellos.

- Identidad federada es una herramienta mediante la cual se evitan sutenticaciones redundantes para identificar a los usuarios en aplicaciones web.

2.1.4 ARQUITECTURA SSO

Caballero y Cano Martínez (2003), señalan con respecto a la arquitectura del sistema Single sign-On que existen diferentes tipos y que cada una de ellas posee características que la hace más apropiada para las diferentes empresas. La decisión de escoger una u otra arquitectura depende básicamente de los recursos informáticos y/o económicos disponibles, y las decisiones de diseño definidas por el equipo del proyecto de la empresa.

Del mismo modo Caballero y Cano Martínez, establecen que as diferentes arquitecturas Single Sign-On están compuestas por tres elementos básicos:

- Interfase: Es la forma en que el sistema Single Sign-On interactúa con una determinada aplicaciones y con el usuario.
- Administración: Es el mecanismo que permite configurar, mantener y monitorear el proceso del sistema Single Sign-On.
- Credenciales: Cada aplicación solicita información confidencial como nombre de usuario, contraseña, etc., y que en conjunto recibe el nombre de credenciales. Las credenciales deben guardadas de manera protegida para que sea únicamente el agente Single Sign-On quien logre acceder a ellas.

Así mismo Caballero y Cano Martínez, nos describen a continuación las arquitecturas usadas para la implementación del sistema Single SignOn:

2.1.4.1 Password vault

Se trata de la configuración más básica para implementar SSO utilizando credenciales. En este caso los tres elementos de la arquitectura se encuentran ubicados en el cliente y, por lo tanto, es justamente allí desde donde se accede a las aplicaciones, para lo cual se deben previamente almacenar las credenciales correspondientes, para que puedan ser suministradas a las aplicaciones cuando sea necesario, como se ilustra en la figura 1.

Figura 1: Arquitectura Password vault

(Caballero & Cano Martínez, 2003)

2.1.4.1.1 Características

- Las credenciales son almacenadas en un servidor central, quien entrega un certificado al cliente correspondiente, y las credenciales necesarias a la respectiva aplicación, en el momento de hacer el ingreso.
- Incorpora infraestructura replicada con el fin de manejar la contingencia y redundancia en tiempo real.
- Ofrece alta disponibilidad mediante software.

2.1.4.1.2 Ventajas

- Permite a los usuarios el acceso a las aplicaciones desde cualquier estación.
- Ofrece administración centralizada.
- Su infraestructura duplicada permite implementar alta disponibilidad y redundancia.

- Tanto el hardware como el software se encuentran debidamente especificados para enfrentar una situación de contingencia.

2.1.4.1.3 Desventajas

- La alta disponibilidad y redundancia que ofrece se basa en su infraestructura replicada, lo cual la hace costosa a nivel de hardware y software, como a nivel de administración y control de la misma.
- La información entre el cliente SSO y el servidor no viaja cifrada.

2.1.4.2 Administración centralizada con almacenamiento local de credenciales

Con el propósito de solucionar los principales inconvenientes que presenta la arquitectura Password Vault, surge la Administración centralizada con almacenamiento local de credenciales, ofreciendo un mecanismo para controlar y supervisar el proceso de ingreso, y eliminando la necesidad de configurar el SSO en cada uno de los clientes. La arquitectura en mención se ilustra en la figura 2.

Figura 2: Arquitectura por administración centralizada con almacenamiento local de credenciales

(Caballero & Cano Martínez, 2003)

2.1.4.2.1 Características

- Incluye un servidor central que permite realizar labores de administración.
- El software cliente es autónomo durante el proceso de autenticación, debido a que durante este proceso, la labor de administración se restringe a realizar monitoreo de los clientes.
- Las credenciales permanecen en el cliente.

2.1.4.2.2 Ventajas

- Control centralizado de la configuración y monitoreo del software del cliente.

- Las labores de administración tienen un bajo grado de complejidad.

2.1.4.2.3 Desventajas

- El hecho de almacenar las credenciales en el cliente hace que se deban tomar medidas de control de acceso y confidencialidad de la información.
- Una vez el cliente se ha conectado, el administrador del SSO sólo puede monitorear la conexión y no podría efectuar acciones de desconexión o cambio de configuración de la misma.
- La información entre el cliente SSO y el servidor no viaja cifrada.

2.1.4.3 Administración y almacenamiento de credenciales centralizados

La arquitectura SSO con administración y almacenamiento centralizado de credenciales (Figura 3) pretende solucionar los principales inconvenientes encontrados en la arquitectura que almacena las credenciales localmente, la cual ya ha sido presentada en el literal B.

Figura 3: Arquitectura por Administración y almacenamiento de credenciales centralizados

(Caballero & Cano Martínez, 2003)

2.1.4.3.1 Características

- Las credenciales son migradas a un servidor central, quien entrega las credenciales al cliente correspondiente en el momento de hacer el ingreso.
- El administrador determina la frecuencia con que se descargan las credenciales del servidor (Por sesión, por login, etc.).

2.1.4.3.2 Ventajas

- Permite a los usuarios el acceso a las aplicaciones desde cualquier estación, previa autenticación del mismo.

- Ofrece administración centralizada de credenciales disminuyendo posible manipulación de la misma en el cliente.

2.1.4.3.3 Desventajas

- Se crea un único punto de falla, convirtiendo al SSO en un gateway para todos los recursos de la organización, ya que el servidor debe ser contactado cada vez que se realice un ingreso. El acceso a todas las aplicaciones de la organización depende del servidor central.
- La configuración carece de redundancia, recuperación entre fallas y respaldo.
- La información entre el cliente SSO y el servidor no viaja cifrada.

2.1.4.4 Arquitectura SSO totalmente distribuida

La arquitectura SSO totalmente distribuida (mostrada en la figura 4) se caracteriza principalmente por separar el servidor de la base de datos, lo cual la hace completamente modular. Esta arquitectura soluciona los problemas encontrados en las arquitecturas anteriormente presentadas y adicionalmente ofrece múltiples ventajas.

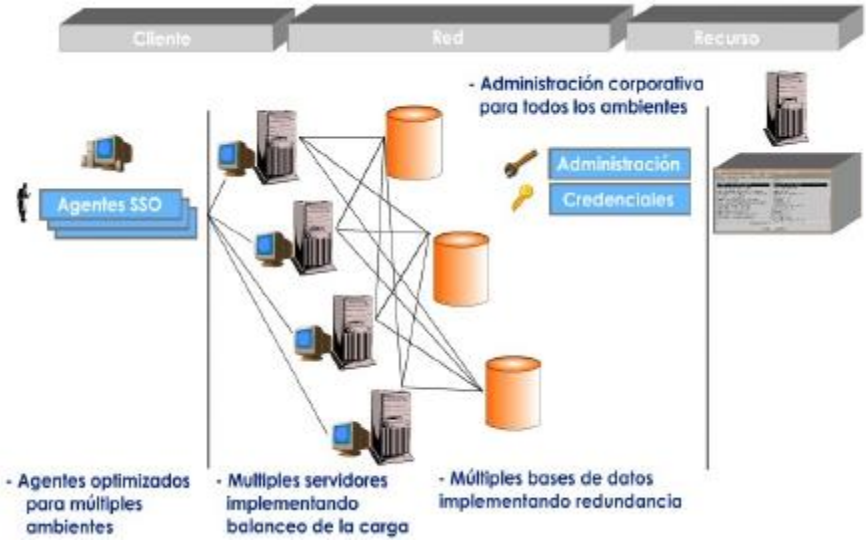


Figura 4: Arquitectura SSO totalmente distribuida

(Caballero & Cano Martínez, 2003)

2.1.4.4.1 Características

- La información se accede en el momento de ingreso.
- Cuenta con SSOs avanzados que utilizan bases de datos escalables que soportan redundancia (i.e. SQL Server u Oracle).
- Las bases de datos se encuentran sincronizadas con el fin de lograr redundancia y respaldo.
- El proceso de ingreso ha sido migrado a un recurso de red. Siempre y cuando el agente SSO pueda establecer conexión IP a un servidor SSO, las credenciales podrán ser solicitadas (y almacenadas en memoria caché para realizar offline logon) y el ingreso podrá ser realizado.
- El servidor resulta ser una aplicación independiente que cuenta con un administrador diferente.
- La información es almacenada en bases de datos comerciales o en directorios de manera encriptada.

Sin embargo, la información entre el cliente SSO y el servidor no viaja cifrada.

2.1.4.4.2 Ventajas

- Los agentes SSO se encuentran optimizados para múltiples ambientes (Terminal Server, Web, Win32).
- Contiene múltiples servidores implementando balanceo de la carga para aumentar la disponibilidad y la atención de los requerimientos de autenticación.
- El hecho de contar con múltiples servidores adicionalmente hace que se disminuya la latencia (ver glosario) de la red.
- Contiene múltiples bases de datos sincronizadas, implementando redundancia.
- Permite realizar funciones de administración corporativa para todos los ambientes.

2.1.4.4.3 Desventajas

- Solución altamente costosa por el ambiente distribuido requerido.
- Demorada implementación técnica por interacción entre múltiples sistemas operacionales.
- Soporte y administración complejos por la consideración anterior.

2.1.4.5 Administración y almacenamiento de credenciales centralizados garantizando alta disponibilidad y redundancia

La arquitectura SSO con administración y almacenamiento centralizado de credenciales garantizando alta disponibilidad y redundancia (Figura 5) es una adaptación de la arquitectura

presentada en C, incorporando algunas de las ventajas de la arquitectura totalmente distribuida, presentada en D.

Figura 5: Arquitectura po administración y almacenamiento de credenciales centralizados garantizando alta disponibilidad y redundancia

(Caballero & Cano Martínez, 2003)

2.1.4.5.1 Características

- Las credenciales son almacenadas en un servidor central, quien entrega un certificado al cliente correspondiente, y las credenciales necesarias a la respectiva aplicación, en el momento de hacer el ingreso.
- Incorpora infraestructura replicada con el fin de manejar la contingencia y redundancia en tiempo real.
- Ofrece alta disponibilidad mediante software.

2.1.4.5.2 Ventajas

- Permite a los usuarios el acceso a las aplicaciones desde cualquier estación.
- Ofrece administración centralizada.
- Su infraestructura duplicada permite implementar alta disponibilidad y redundancia.
- Tanto el hardware como el software se encuentran debidamente especificados para enfrentar una situación de contingencia.

2.1.4.5.3 Desventajas

- La alta disponibilidad y redundancia que ofrece se basa en su infraestructura replicada, lo cual la hace costosa a nivel de hardware y software, como a nivel de administración y control de la misma.
- La información entre el cliente SSO y el servidor no viaja cifrada.

2.2 SECURE SOCKETS LAYER – SSL

Secure Sockets Layer - SSL, que en su traducción significa Capa de Puertos Seguros; es un protocolo cifrado que proporciona comunicación segura en una red de comunicaciones de internet.

El protocolo SSL fue diseñado originalmente por Netscape. En 1996 se presenta la versión SSL 3.0 el cual recibió opiniones públicas y empresariales.

Su uso, es muy frecuente en las aplicaciones en las que se requiere la utilización de datos sensibles y se trabaja en los navegadores web bajo las siglas https. Es utilizado por la mayoría de bancos y en comercio electrónico.

González Manzano y Fuentes García-Romero de Tejada (2014) nos indica que, Este protocolo se caracteriza por soportar comprensión (aunque es opcional), hacer uso de certificados X.509 v3 y proporcionar los servicios de seguridad de autenticación en servidor (obligatoria), autenticación en cliente (opcional), integridad, confidencialidad y no repudio del cliente (opcional).

Del mismo modo González Manzano y Fuentes García-Romero de Tejada (2014), para comprender con simplicidad y de forma general en que consiste SSL, el funcionamiento del protocolo, nos presenta y explica la siguiente figura:

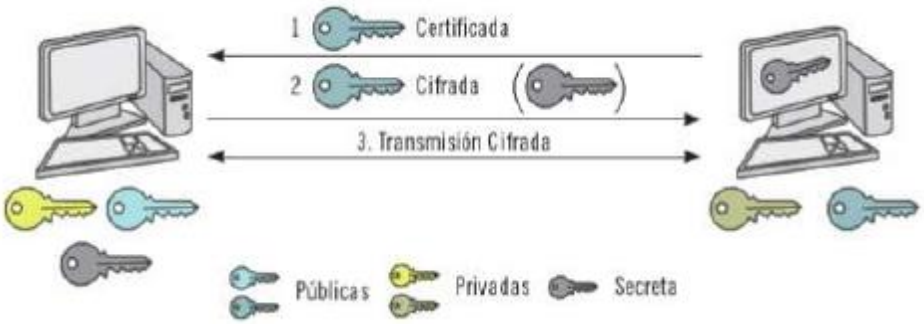


Figura 6: Funcionamiento genérico de SSL
(González Manzano & Fuentes García-Romero de Tejada, 2014)

Cada extremo de la comunicación posee un par de claves (junto con el certificado asociado y considerando que en el cliente es opcional). Suponiendo que un cliente A quiere establecer comunicación con un servidor B, 1) B envía su clave pública certificada a A. Posteriormente A, tras crear una clave secreta, 2) se la envía a B y finalmente, 3) la transmisión de información puede comenzar, considerando que la información se transmitirá cifrada mediante la clave secreta intercambiada.

Así mismo; González Manzano y Fuentes García-Romero de Tejada (2014), nos describe brevemente, los sub protocolos que conforma el SSL:

- Protocolo de saturación. Se ejecuta antes de transmitir los datos de la aplicación. En este protocolo el cliente y el servidor acuerdan los algoritmos que usarán para cifrar y aplicar control de integridad sobre los datos que intercambien. Para ello, el cliente ofrece las opciones disponibles y el servidor se autentica frente al cliente (enviándole su certificado de clave pública). Opcionalmente, también el cliente se puede autenticar.

- Protocolo de Registro. Este protocolo utiliza los algoritmos definidos por el de saturación para cifrar y aplicar el control de integridad sobre los datos. También comprime los datos, haciendo que la transmisión sea más ligera.

- Protocolo de Cambio de Especificación de Cifrado. Se emplea para que una de las partes anuncie a la otra que quiere cambiar la manera de cifrar la información. Solo consiste en un mensaje, que una parte envía a otra en el momento oportuno. De hecho, el protocolo de saturación siempre finaliza con ese mensaje. De esta manera, los acuerdos de ese protocolo empiezan a utilizarse.

- Protocolo de Aviso. Este protocolo tiene como función avisar a cualquiera de los participantes de algún tipo de incidencia ocurrida. Puede ser debida a un error fatal o una advertencia. Si el nivel es fatal (por ejemplo, si no hay acuerdo en el protocolo de saturación) la conexión SSL asociada se finaliza. Entre las advertencias se pueden destacar la recepción de un certificado expirado o el hecho de que una de las entidades no desee mandar más mensaje en una determinada conexión.

2.3 CERTIFICADOS DIGITALES

Un certificado digital, es un método estándar de verificación de la autenticidad de un servidor, un cliente o una aplicación.

Para garantizar la máxima seguridad de un certificado digital, existen entidades de reconocimiento internacional que proporcionan un certificado.

Hernández Encinas (2016) nos dice que, un certificado digital permite a su poseedor probar ante terceros que posee una clave criptográfica; es decir, se trata de la versión digital de un certificado ordinario en el que se garantiza que la clave pública y el resto de información contenida en el mismo pertenecen al usuario que se especifique en dicho certificado. La validez de dicha información está garantizada por una entidad reconocida (local, nacional o internacional), a modo de notario electrónico, denominada autoridad de certificación o AC.

El estándar más usado en los certificados digitales es el X.509 v3 y contiene la información que detallamos a continuación:

- Versión del certificado.
- Número de serie (Identificación del certificado).
- Identificador del algoritmo de firma digital.
- Emisor del certificado.
- Identificación del usuario del certificado.
- Tipo de criptosistema de clave pública que emplea el usuario.
- Clave pública y privada del usuario.
- Periodo de validez del certificado.
- Firma digital de la autoridad que avala el certificado.

A continuación, se muestra una la figura 7, donde se muestra la información de un certificado digital.

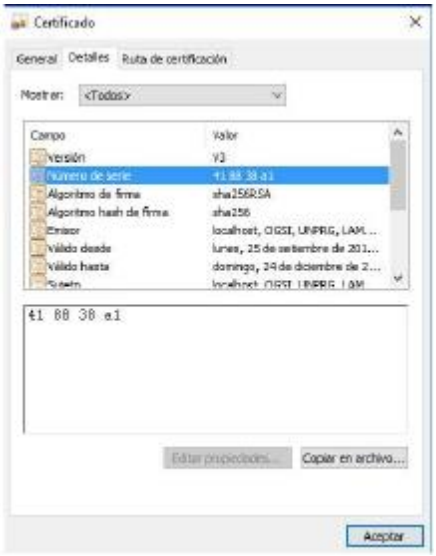


Figura 7: Información de un Certificado Digital

(Propia)

Para la obtención de un certificado, mediante una autoridad de certificación (AC), se realiza el siguiente proceso:

1ro. El usuario solicita a la AC (vía internet) la expedición de un certificado.

2do. La AC, solicita al usuario sus respectivos datos personales, comprobando la autenticidad de los datos por la AC.

3ro. La AC requiere al navegador del usuario que genere la clave pública y la clave privada para el usuario respectivo.

4to. La AC genera un fichero electrónico con los datos de los campos respectivos al tipo de certificado solicitado por el usuario.

5to. La AC firma digitalmente el resumen del contenido del fichero que se ha generado, añadiendo esta firma al mismo fichero, dando como resultado el certificado digital del usuario.

En el Perú, el Registro de Identificación y Estado Civil (RENIEC), es la entidad de Certificación Nacional, que cumple con las funciones de registro y verificación.

Así mismo la autoridad supervisora de la AC en Perú, es el Instituto Nacional de Defensa de la Competencia y de la Propiedad Intelectual (INDECOPI), aprobado en el Reglamento de Firmas y Certificados Digitales mediante Decreto Supremos 019-2002-JUS y ratificado por el Decreto Supremo 004-2007-PCM.

2.4 ALGORITMOS DE CRIPTOGRAFIA

Para Páez Rivadeneira (2015), El mecanismo más básico es el denominado criptosistema o algoritmo de encriptación, que define dos transformaciones:

- La Encriptación: conversión el texto en claro (plaintext) en el texto cifrado o criptograma (ciphertext) mediante el empleo de la denominada clave de encriptación: y
- La Desencriptación: proceso inverso que se emplea la llamada clave de desencriptación.

El objetivo de los algoritmos de encriptación es asegurar el servicio de confidencialidad, pues para poder desencriptar la información transferida, es necesario del conocimiento de la clave de desencriptación por parte del receptor.

Así mismo Páez Rivadeneira (2015) distingue dos tipo de claves que pueden utilizarse para el cifrado (así como para la firma digital y autenticación):

- Claves Simétricas: siguen un modelo antiguo en que el emisor y el receptor comparten algún tipo de patrón. Por lo tanto, el mismo patrón lo utilizan el emisor para cifrar el mensaje y el receptor para descrifrarlo. El riesgo que implican estas claves, es que deberá buscar un método de transporte seguro para utilizarlo cuando comparta su clave secreta con las personas con las que desea comunicarse.
- Claves Asimétricas: se crea una pareja de claves. La pareja de claves está compuesta de una clave pública y una clave privada, que son distintas entre sí. La clave privada contiene una parte mayor de patrón cifrado secreto de la clave pública.

Para su mejor entendimiento, a continuación se muestran las Figuras 8 y 9:

Figura 8: Cifrado de claves simétricas

(Recuperado de https://www.ibm.com/support/knowledgecenter/es/)

Figura 9: Cifrado de claves asimétricas

(Recuperado de https://www.ibm.com/support/knowledgecenter/es/)

Para efectos de esta investigación es importante saber el tipo de cifrado que se utiliza en el protocolo SSL y para ello Páez Rivadeneira (2015), nos afirma que el protocolo SSL, utiliza tanto el cifrado de claves públicas como el cifrado de claves simétricas. El cifrado de claves públicas se utiliza para el protocolo de conexión TCP/IP. Durante el protocolo de conexión, la clave maestra se pasa del cliente al servidor. El cliente y el servidor crean sus propias claves de sesión utilizando la clave maestra. Las claves de sesión se utilizan para cifrar y descifrar los datos del resto de la sesión.

2.4.1 Cifrado Simétrico o de Secreto Compartido

Para Baca Urbina (2016), el cifrado simétrico se divide en cifrado por bloques y cifrado de flujo. En el cifrado por bloques, como su nombre lo indica, se cifran y descifran bloques de bits al mismo tiempo. Las operaciones que se hacen a los bits en varias ocasiones, llamadas rondas, son sustituciones,

permutaciones, rotaciones y operaciones lógicas. Ejemplos de cifradores simétricos son: ADES, DES y TDES. El TDES es el mismo DES original, pero debido a que los criptólogos encontraron cierta deficiencias, se determinó hacer tres veces las rondas de operaciones que se hacen con el DES, porl lo que el TDES significa triple DES.

Por otro lado, el cifrado de flujo de cifra y descifra bit por bit (ejemplos de estos cifradores son: RC4 y A5/1, respectivamente)

2.4.2 Cifrado Asimétrico o de Clave Pública

Para Hernández Encinas (2016), La criptografía de clave pública no se basa tanto en operaciones lógicas como lo hacen los cifradores en flujo y en bloque, sino que lo hace en operaciones matemáticas que están relacionadas con determinados problemas, supuestamente difíciles de resolver. Por este motivo, los mensajes suelen ser números con los que llevar a cabo operaciones y no tanto colecciones de bits, aunque tal consideración depende del criptosistema de que se trate.

Es importante mencionar a: Diffie-Hellman, RSA (Rivert – Shamir - Adelman), DSA(Digital Signature Algorithm), ElGamal, Criptografía de curva elíptica, Criptosistema de Merkle-Hellman, Goldwasser-Micali, Goldwasser-Micali-Rivest, Cifrado extremo a Extremo, como algunos algoritmos y tecnologías de claves asimétricas. Y si hablamos de algunos protocolos que usan los algoritmos mencionados anteriormente, tenemos a: DSS ("Digital Signature Standard") con el algoritmo DSA ("Digital Signature Algorithm"), PGP, GPG, una implementación de OpenPGP, SSH, SSL y TLS

Dentro de los algoritmos más usados, Páez Rivadeneira (2015) cita a:

- RSA (Rivert – Shamir - Adelman)

  Este algoritmo fue inventado por R. Rivest, A. Shamir y L. Adleman (de sus iniciales proviene e; nombre del algoritmo) en el Massachusetts Institute of Technology (MIT). RSA emplea ventajas proporcionadas

por las propiedades de los números primos cuando se aplican sobre ellos operaciones matemáticas. La robustez del algoritmo se basa en la facilidad para encontrar dos números primos grandes frente a la enorme dificultad que presenta la factorización de su producto. Aunque el avance tecnológico hace que cada vez sea más rápido un posible ataque por fuerza bruta, el simple hecho de aumentar la longitud de las claves empleadas supone un incremento en la carga computacional lo suficientemente grande para que este tipo de ataque sea inviable. Sin embargo, se ha de notar que, aunque el hecho de aumentar la longitud de las claves RSA no supone ninguna dificultad tecnológica, las leyes de exportación de criptografía de EEUU imponen un límite de dicha longitud.

- DSA(Digital Signature Algorithm)

  Un algoritmo muy extendido es el Digital Signature Algorithm (DSA) definido en el Digital Signature Standard (DSS), el cual fue propuesto por el U.S. National Institute of Standards and Technology (NIST). Este algoritmo se basa en la función exponencial discreta en un campo de elementos finito, la cual tiene la característica de ser difícilmente reversible (logaritmo discreto).

  Para aplicaciones únicamente de autenticación e integridad, no firma, se puede añadir una clave simétrica a la generación de resumen. De esta manera no es necesario encriptar, esta clave ya demuestra que el usuario es auténtico y el resumen propiamente demuestra la integridad del texto. El problema es utilizar una clave simétrica y, por lo tanto, se debe transmitir por un canal seguro, el sistema utilizado actualmente es el de claves de sesión encriptadas mediante la clave privada del emisor.

CAPITULO III: DESARROLLO DE SINGLE SIGN ON EN LA UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

3.1 DESCRIPCIÓN DE LA SITUACIÓN ACTUAL, EN EL PROCESO DE AUTENTICACIÓN PARA EL ACCESO A LOS SERVICIOS WEB QUE BRINDA LA UNPRG.

3.1.1 La Universidad

La Universidad Nacional Pedro Ruiz Gallo (UNPRG), es una comunidad académica integrada por docentes, estudiantes y graduados que brinda formación profesional humanística, científica y tecnológica con clara conciencia de nuestra región y del país como realidad multicultural, adopta el concepto de educación como derecho fundamental y servicio público esencial.(Estatuto,2015,p.6)

Basándonos en su estatuto del año 2015, la organización académica de la UNPRG, comprende dos niveles: pregrado y posgrado; para efectos de esta investigación, nos enmarcaremos en el nivel de pregrado; se sustenta en un régimen académico por facultades, las cuales cuenta con 14 facultades las que se listan a continuación:

1 Facultad de Ciencias Físicas y Matemáticas
2 Facultad de Ciencias Económicas, Administrativas y Contables
3 Facultad de Ingeniería Zootecnia
4 Facultad de la Facultad de Agronomía
5 Facultad de Ingeniería Mecánica y Eléctrica
6 Facultad de Ciencias Biológicas
7 Facultad de Enfermería
8 Facultad de Ciencias Históricos Sociales y Educación
9 Facultad de Medicina Veterinaria
10 Facultad de Ingeniería Civil, Sistemas y Arquitectura
11 Facultad de Derecho y Ciencias Políticas
12 Facultad de Ingeniería Química e Industrias Alimentarias
13 Facultad de Medicina Humana
14 Facultad de Ingeniería Agrícola

Así mismo, uno de sus regímenes para poder cumplir con sus funciones, es el régimen Administrativo, por ello cuenta con personal administrativo distribuidos entre sus diferentes oficinas y facultades.

3.1.2 Los Usuarios y Servicios

Podemos definir a un usuario, como la persona quien habitualmente utiliza algún tipo de objeto o un servicio en algún lugar determinado.

Por ello, en la UNPRG, podemos definir claramente como usuarios a: los Docentes, Alumnos y Administrativos, que utilizan los diferentes servicios que ofrece la universidad.

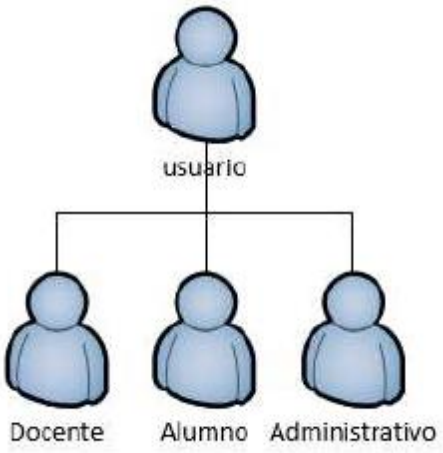


Figura 10: Tipos de Usuarios UNPRG
(Elaboración del Autor)

Según los reportes obtenidos de la Oficina General de Recursos Humanos (Docentes Nombrados y Personal Administrativo Nombrado, Servicios Personales y CAS), y de la Oficina General de Asuntos Académicos (Alumnos matriculados en el ciclo académico 2017-I), la UNPRG cuenta con las siguientes cantidades de usuarios:

N°	Facultad	Abrev.	Total
1	Facultad de Ciencias Económicas, Administrativas y Contables	FACEAC	93
2	Facultad de Ciencias Físicas y Matemáticas	FACFYM	134
3	Facultad de Ciencias Históricos Sociales y Educación	FACHSE	82
4	Facultad de la Facultad de Agronomía	FAG	38
5	Facultad de Ciencias Biológicas	FCCBB	44
6	Facultad de Derecho y Ciencias Políticas	FDCP	27
7	Facultad de Enfermería	FE	34
8	Facultad de Ingeniería Agrícola	FIA	25
9	Facultad de Ingeniería Civil, Sistemas y Arquitectura	FICSA	83
10	Facultad de Ingeniería Mecánica y Eléctrica	FIME	26
11	Facultad de Ingeniería Química e Industrias Alimentarias	FIQIA	37
12	Facultad de Ingeniería Zootecnia	FIZ	18
13	Facultad de Medicina Humana	FMH	67
14	Facultad de Medicina Veterinaria	FMV	24
	T O T A L		732

N°	Escuela Profesional	Total Esc.	Facultad	Total Fac.
1	Administración	639		
2	Contabilidad	598	FACEAC	
3	Economía	634		
4	Comercio Negocios Internacionales	610		2,481
5	Ingeniería en Computación e Informática	555		
6	Estadística	459		
7	Física	173	FACFyM	
8	Matemáticas	331		
9	Ingeniería Electrónica	528		2,046
10	Educación	1,134		
11	Sociología	207		
12	Ciencias de la Comunicación	219		
13	Arqueología	147		
14	Psicología	248	FACHSE	2,236

CANTIDAD DE DOCENTE NOMBRADOS POR FACULTAD

35

CANTIDAD DE ALUMNOS MATRICULADOS EN EL CICLO 2017-I

15	Arte	281		
16	Agronomía	492	FAG	492
17	Ciencias Biológicas	548	FCCBB	548
18	Derecho	636	FDCP	887
19	Ciencias Políticas	251		
20	Enfermería	296	FE	296
21	Ingeniería Agrícola	569	FIA	569
22	Arquitectura	549	FICSA	1,898
23	Ingeniería Civil	778		
24	Ingeniería de Sistemas	571		
25	Ingeniería Mecánica y Eléctrica	606	FIME	606
26	Ingeniería Química	416	FIQIA	861
27	Ingeniería de Industrias Alimentarias	445		
28	Ingeniería Zootecnia	384	FIZ	384
29	Medicina Humana	371	FMH	371
30	Medicina Veterinaria	524	FMV	524
	TOTAL	14,199	TOTAL	14,199

CANTIDAD DE ADMINISTRATIVOS SEGÚN SU CONDICION

CONDICION	Total
Nombrados	382
Servicios Personales	221
Contrato Administrativo de Servicios	209
TOTAL DE USUARIO	812

RESUMEN DE USUARIOS

Tipo de Usuarios	Total
Docente (Nombrados)	732
Alumno (Matriculados 2017-I)	14,199
Administrativo (Nombrado, SP y CAS)	812
TOTAL DE USUARIO	15,743

Hoy en día la Universidad Nacional Pedro Ruiz Gallo, cuenta con seis (06) aplicación o servicios web, que ofrece a su comunidad universitaria, las cuales se detallan a continuación, considerando el acceso por sus diferentes usuarios :

RELACION DE APLICACIONES/SERVICIOS WEB Y SU ACCESO SEGÚN USUARIO

N°	Aplicaciones/Servicios Web	Acceso según tipo de Usuario		
		Docente	Alumno	Administrativo
1	Correo Institucional: <usuario>@unprg.edu.pe	X	X	X
2	Sistema Académico (Actas Virtuales)	X	X	X
3	Biblioteca On-Line	X	X	X
4	Administración Portal Web			X
5	Administración Libro de Reclamaciones			X
6	Administración de Pagos Admisión			X

N°	Aplicaciones/Servicios Web	Tipo de Usuarios		
		Docente	Alumno	Administrativo
1	Aula Virtual	X	X	
2	Blog de Docentes	X		
3	Bolsa de Trabajo		X	

Así mismo, se encuentran en proceso de implementación las siguientes

Para acceder a las mencionadas aplicaciones o servicios web, se realiza mediante el Portal web, observando que en cada una de ellas es necesario el ingreso de su usuario y contraseña para su autenticación, tal y como se observa a continuación.

Aplicaciones/servicios web:

PORTAL WEB

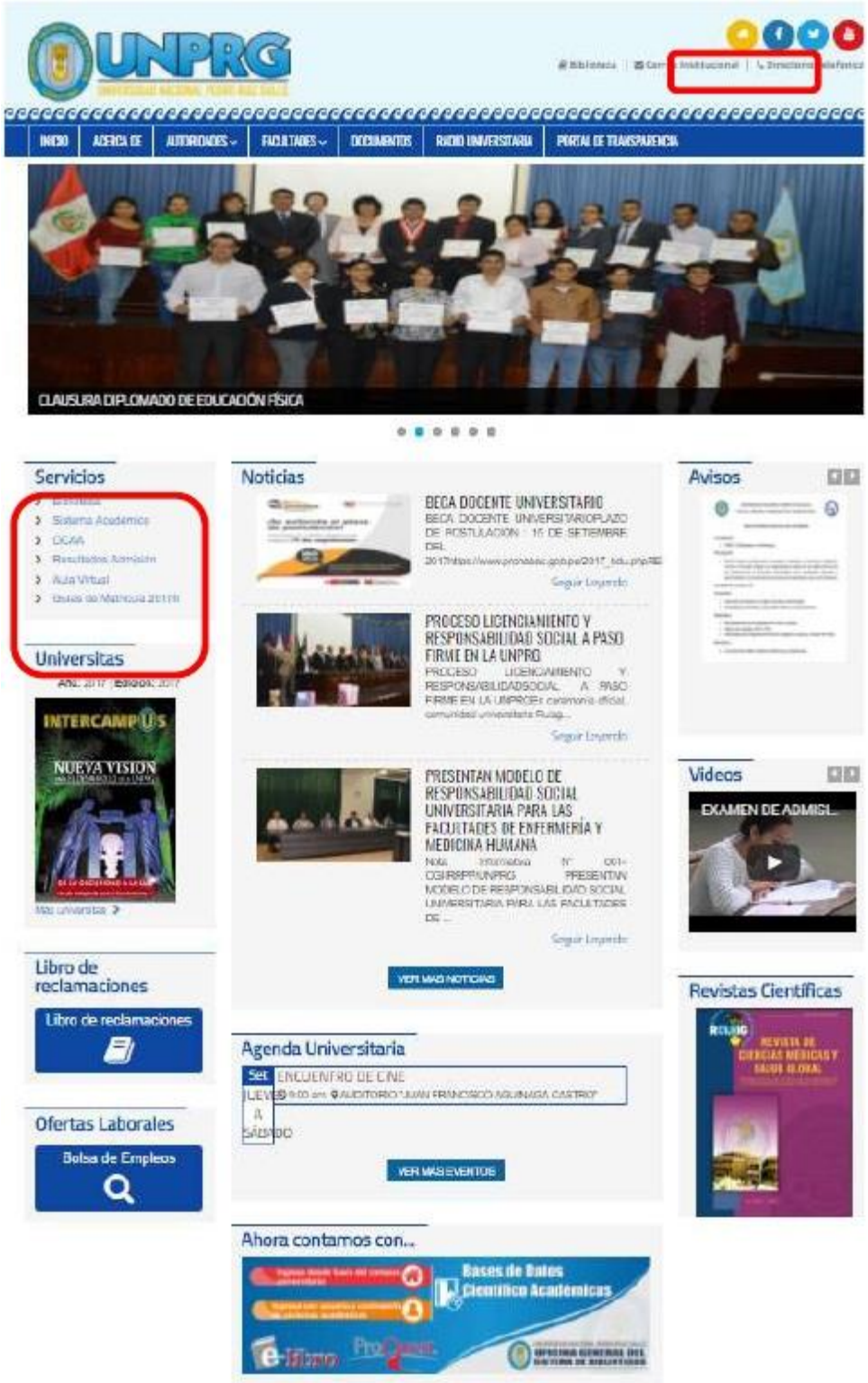


Figura 11: Portal web UNPRG

(Recuperado de http://www.unprg.edu.pe)

CORREO INSTITUCIONAL (correo.unprg.edu.pe)

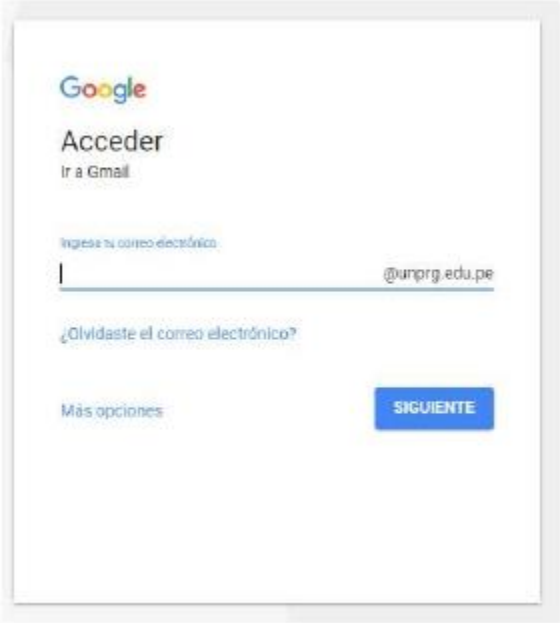


Figura 12: Ingreso de cuenta
(Recuperado de http:/correo.unprg.edu.pe)

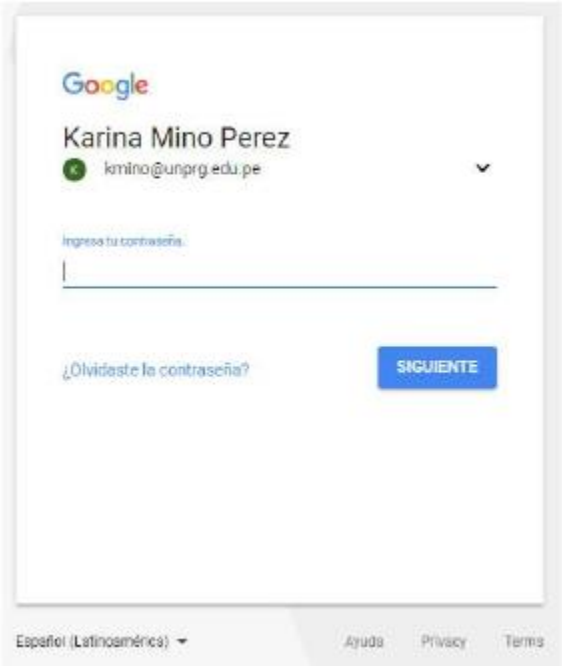


Figura 13: Ingreso de contraseña
(Recuperado de http:/correo.unprg.edu.pe)

SISTEMA ACADEMICO

Figura 14: Ingreso del Sistema Académico
(Recuperado de http://aplicaciones.unprg.edu.pe:8181/ModuloAutenticacion/)

BIBLIOTECA ON LINE

Figura 15: Ingreso a Biblioteca On Line
(Recuperado de http://www.unprg.edu.pe/univ/biblioteca/logm/login.php)

LIBRO DE RECLAMACIONES

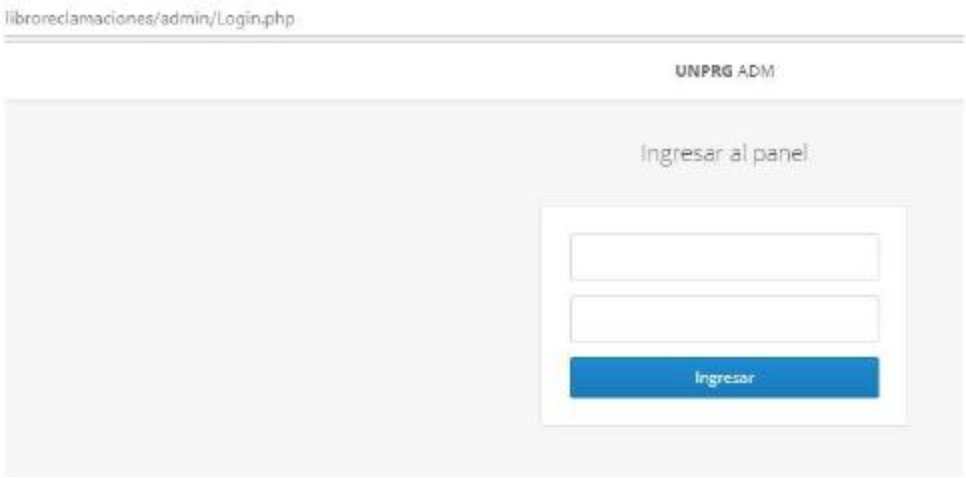


Figura 16: Ingreso al Libro de Reclamaciones
(Recuperado de http://www.unprg.edu.pe/univ/portal/libroreclamaciones/admin/Login.php)

ADMINISTRACION PORTAL WEB

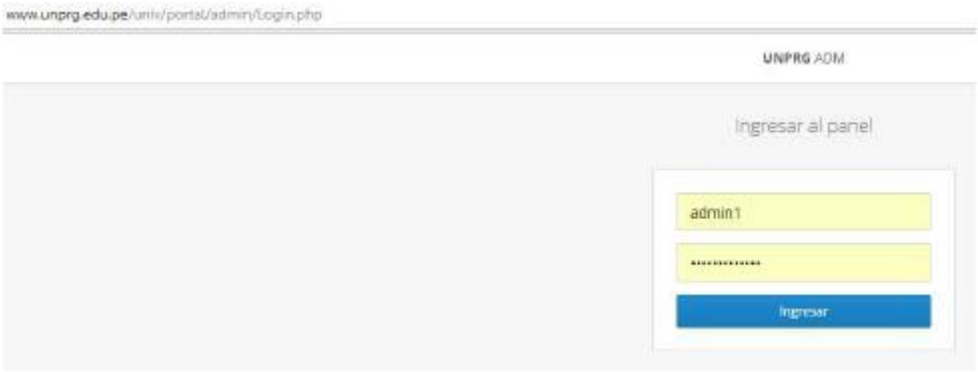


Figura 17: Ingreso a la Administración Portal Web
(Recuperado de http://www.unprg.edu.pe/univ/portal/admin/Login.php)

ADMINISTRACION DE PAGOS ADMISION

Figura 18: Ingreso a la Administración de Pagos Admisión
(Recuperado de http://www.unprg.edu.pe/inscripciones/ImportarPago/)

Así mismo, se observa que en sus aplicaciones web, no existe un estándar en su plataforma de desarrollo; consecuencia de ello es la existencia de islas de información.

A continuación se presenta el siguiente cuadro de análisis :

PLATAFORMA DE DESARROLLO DE APLICACIONES O SERVICIOS WEB UNPRG

N°	Aplicaciones/Servicios Web	Lenguaje de Programación	Gestor de Base de Datos
1	Correo Institucional: <usuario>@unprg.edu.pe	Servicio de Google	Servicio de Google
2	Sistema Académico (Actas Virtuales)	Java 1.7	Oracle 12C
3	Biblioteca On-Line	Servicio de E-Libro Servicio de ProQuest	Servicio de E-Libro Servicio de ProQuest
4	Administración Portal Web	Php 5.3	MySql
5	Administración Libro de Reclamaciones	Php 5.3	MySql
6	Administración de Pagos Admisión	Php 5.3	MySql

Como podemos analizar, en la actualidad existen un promedio de 15,743 usuarios que acceden a todas o una de las 6 aplicaciones o servicios web que brinda la UNPRG.

Para que el usuario pueda acceder a estas aplicaciones, es necesario la autenticación del mismo, es decir debe ingresar su usuario y contraseña para validar su acceso.

Al conocer la independencia que existe entre estas aplicaciones, observamos que cada una de ellas maneja su propio módulo de autenticación, generando tantos usuarios y contraseñas como aplicaciones existan en la UNPRG; que en algunos casos puede ser los mismos datos de acceso, así como en otros totalmente diferente, teniendo como consecuencia una redundancia de datos.

Todo esto, conlleva a una serie de incomodidades a los usuarios por lo que deben de recordar sus datos de acceso (usuario y contraseña) en cada una de las diferentes aplicaciones a las cuales desean ingresar; incentivando a la vez la realización de malas prácticas de seguridad en las aplicaciones web, tales como: contraseñas inseguras, anotación en cualquier medio de sus usuarios y contraseñas, reutilización de contraseñas, entre otras.

En resumen, se representa mediante un diagrama, el proceso actual de autenticación para el acceso a los servicios web que brinda la UNPRG.

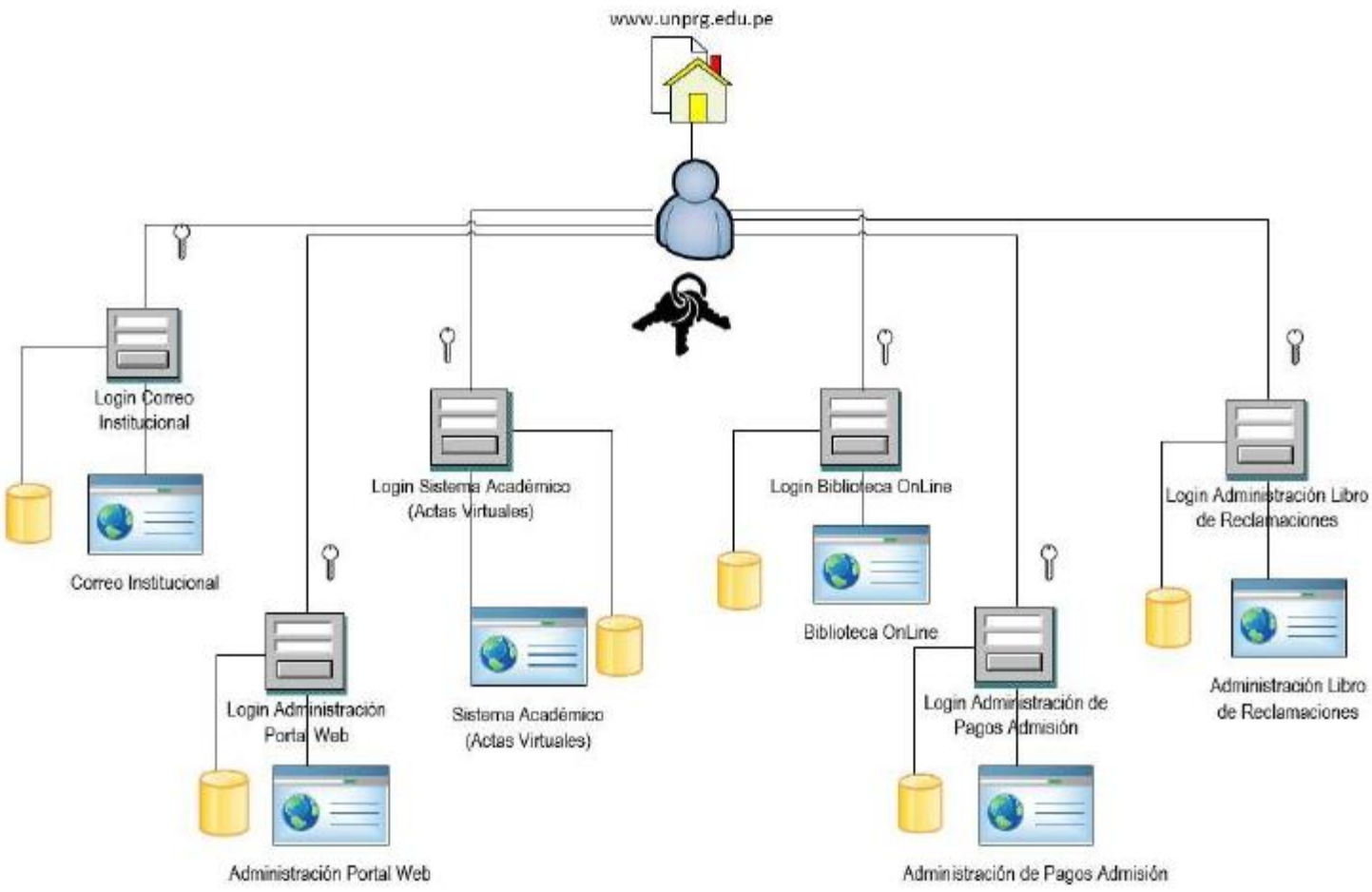


Figura 18: Proceso actual de autenticación para el acceso a los servicios web que brinda la UNPRG

(Elaboración del Autor)

3.2 ANÁLISIS DE MECANISMOS DE SOLUCIÓN SINGLE SIGN ON.

Para dar solución al problema descrito en esta investigación, se analiza las diversas soluciones de implementación y protocolos de desarrollado para iniciar y terminar una sesión de usuario conectado (protocolo de sesión), que mejor se adapte a los requerimientos de los servicios web que brinda la Universidad Nacional Pedro Ruiz Gallo a su comunidad universitaria.

.

A continuación presentamos una lista de implementaciones en SSO para su análisis y comparación.

SSO PROPIETARIAS – SOFTWARE COMERCIAL

Nº	Nombre del Producto	Proyecto / Proveedor	Licencia	Descripción
1	Bitium	Bitium	Propietario	Solución de gestión de acceso y identidad basada en la nube empresarial con inicio de sesión único, integración de directorios activos y opciones de autenticación de dos factores
2	AuthStack	Buckhill Ltd	Propietario	Una plataforma de software de acceso único y una plataforma de software de inicio de sesión único. Disponible en el mercado AWS.
3	Ubuntu Single Sign On	Canonical Ltd.	Propietario	SSO basado en OpenID para los servicios de Launchpad y Ubuntu
4	OpenAthens	Eduserv	Propietario	Identidad y soluciones de gestión de acceso a IdPs y SPs que permiten la gestión de acceso a recursos basados en la web. Instalación local, servicio totalmente alojado o opciones de integración ADFS / LDAP , equipo de soporte dedicado. Mantiene la Federación OpenAthens . SAML 1.1, SAML 2.0, SSO, auto-registro, compatibilidad con Shibboleth, API.
5	Facebook connect	Facebook	Propietario	Facebook SSO a terceros habilitado por Facebook
6	IceWall SSO	Hewlett-Packard	Propietario	Solución Web y de Single Sign-On Federada

Nº	Nombre del Producto	Proyecto / Proveedor	Licencia	Descripción
7	IBM Tivoli Access Manager	IBM	Propietario	Web, empresa y SSO federada. IBM Tivoli Identity Manager proporciona una plataforma de gestión de identidades.
8	JanrainFederate SSO	Janrain	Propietario	Usuario social y convencional SSO
9	LoginRadius	LoginRadius Inc.	Propietario	Gestión de Identidad y Acceso de Cliente basada en la nube con registro de usuario, inicio de sesión social , SSO federado (SAML 1.1, Saml 2.0, Oauth2, JWT, Multipass, etc.) e inicio de sesión único Web .
10	Active Directory Federation Services	Microsoft	Propietario	Sistema de reclamaciones y federación de aplicaciones
11	Microsoft account	Microsoft	Propietario	Servicio web de inicio de sesión único de Microsoft
12	NetIQ Access Manager	NetIQ	Propietario	Gestión de acceso, federación y plataforma de control de acceso basada en riesgo
13	SecureLogin	NetIQ	Propietario	Enterprise Single-Sign-On
14	Numina Application Framework	Numina Solutions	Propietario	Sistema de inicio de sesión único para Windows (OpenID RP & OP, SAML IdP y propietario)
15	OneLogin	OneLogin Inc.	Propietario	Gestión de identidad y acceso basada en la nube con inicio de sesión único (SSO) e integración de directorios activos
16	Oracle Identity Management	Oracle Corporation	Propietario	Gestión de Identidad y Acceso Suite de productos de Oracle
17	Acces: One	Pirean	Propietario	Workforce con base en la nube, gestión de identidad y acceso de los ciudadanos y los consumidores con registro de usuarios, inicio de sesión social, SSO federado (SAML, OAuth2, OpenID Connect, JWT, etc.) y Web single sign on. Incluye servicios de Gestión de Identidad, Gobernabilidad y Gestión de Identidad Móvil / SSO.

Nº	Nombre del Producto	Proyecto / Proveedor	Licencia	Descripción
18	PortalGuard	PistolStar, Inc.	Propietario	Paquete de autenticación integrada todo en uno: SSO, 2FA, SSPR y más de 120 funciones
19	myOneLogin	VMware	Propietario	Inicio de sesión único de Cloud
20	CA SSO (anteriormente CA Siteminder)	CA Technologies	Software comercial	Web, empresa y SSO federada. CA SSO proporciona una plataforma de gestión de identidades.
21	Enterprise SSO, Web Access Manager	Evidian	Software comercial	Enterprise SSO, Web SSO, Federación de Identidad. Evidian proporciona una plataforma global de gestión de identidades con Identity Governance and Administration.
22	OpenAM	ForgeRock	Software comercial	Gestión de acceso, derechos y plataforma de servidor de federación
23	Xpress Sign-On	ILANTUS Technologies	Software Comercial	Software de inicio de sesión único en los modos On-Premise y Private Cloud. Soporta SSO a cualquier aplicación, incluyendo Web Single Sign-On, SSO federado así como clientes gruesos (pendiente de patente). Soporte para administración de contraseñas, gestión del ciclo de vida de los usuarios y gestión del acceso. Mobile Identity Management / SSO / Gestión de Contraseñas.

Nº	Nombre del Producto	Proyecto / Proveedor	Licencia	Descripción
1	CoSign single sign on	Universidad de Michigan	Académico	SSO para la Universidad de Michigan

SSO ACADEMICO

Nº	Nombre del Producto	Proyecto / Proveedor	Licencia	Descripción
1	Shibboleth	Shibboleth	Free & Open Source (Apache 2.0)	Control de acceso de código abierto basado en SAML
2	Keycloak	Red Hat	Open source	SSO federado (LDAP y Active Directory), protocolos estándar (OpenID Connect, OAuth 2.0 y SAML 2.0) para Web, agrupación y inicio de sesión único
3	CAS / Central Authentication Service	Apereo	Open source	Implementación de servidor / cliente SSO de protocolo abierto y de código abierto con soporte para protocolos CAS, SAML1, SAML2, OAuth2, SCIM, OpenID Connect y WS-Fed tanto como proveedor de identidad como proveedor de servicios con otras funciones auxiliares que tratan con el consentimiento del usuario, acceso gestión, suplantación, condiciones de uso, etc. Licenciado bajo Apache 2.0.
4	IBM Identity Mapping	IBM	Software libre	Funciona con Kerberos (por ejemplo, Active Directory) y otros mecanismos de autenticación para asignar identidades diferentes y por lo tanto permitir el inicio de sesión único a todas las plataformas de servidor IBM (Windows, Linux, PowerLinux, IBM i, i5 / OS, OS / 400, AIX) nombre difiere.
5	Accounts & SSO	Nokia , Intel	Software libre	Implementación de cliente con plugins para varios servicios / protocolos
6	ORY Hydra	ORY GmbH	Software libre	Implementación de servidores OAuth 2.0 y OpenID Connect que se conecta a cualquier infraestructura de autenticación existente. Licenciado bajo Apache 2.0
7	ZXID	ZXID	Software libre	Referencia Implementación de la seguridad TAS3

Por otro lado, es importante el análisis de los protocolo de sesión que se detallan en el siguiente cuadro:

Protocolo	Propósito	Última versión / estado	Ventajas	Desventaja
OpenID	Autenticación (federada)	2.0 (de 2007)	Single-sign-on sin depender de ningún proveedor específico (federado).	Protocolo complejo y antiguo; potenciales problemas de seguridad, privacidad, usabilidad. Pocos incentivos para ser consumidor.
OAuth	Autorización	2.0 (en borrador, pero muy utilizada)	Muy utilizado en servidores de Internet.	Dependencia de un servidor para la autenticación (delegada).
OpenID OAuth Hybrid Protocol	Autenticación (federada) + autorización; interfaz única	Borrador (pero adoptado por grandes proveedores)	Una única interfaz para autenticación (OpenID) + autorización (OAuth).	Depende de que los servidores implementen ambos protocolos.
Facebook Connect	Autenticación (delegada) + autorización + funciones red social	Abandonado en favor de OAuth 2.0	Parte de una amplia base de usuarios y datos personales.	Muy ligado a un único proveedor. Problemas de privacidad.
OpenID Connect	Autenticación (federada) a partir de OAuth	Propuesta (sobre OAuth 2.0)	Las mismas ventajas que OpenID con una implementación más sencilla; aprovecha las implementaciones de OAuth 2.0.	Similares a OpenID; pocos incentivos para ser consumidor.
CAS		3.5.2		

Después de analizar y comparar las diversas soluciones de implementación SSO y protocolos de sesión, basándonos en la situación actual de la UNPRG explicado en el ítem 3.1 del presente capitulo, se determinó que la solución que cubre la mayoría de los requerimientos de los servicios web ofrecidos por la UNPRG es Central Authentication Service (CAS).

3.3 DESARROLLO DE PROPUESTA SSO - UNPRG.

El objetivo de la propuesta Central Authentication Service (CAS), es dar solución a la problemática en el proceso de autenticación para el acceso a los servicios web que brinda la UNPRG; proponiendo una solución con un método centralizados de autenticación conocido como Single Sign-On; representado en la figura 19.

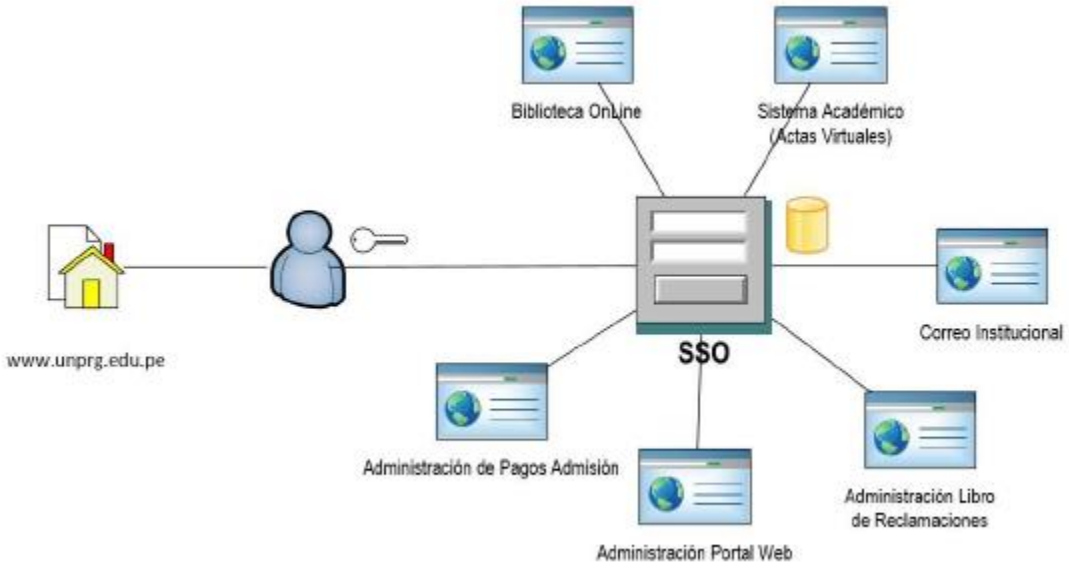


Figura 19: Proceso de autenticación para el acceso a los servicios web que brinda la UNPRG – SSO CAS
(Elaboración del Autor)

3.3.1 Diseño del proceso basados en la propuesta SSO CAS - UNPRG

El proceso de autenticación basado en SSO – CAS UNPRG, se describe mediante el diagrama de secuencia.

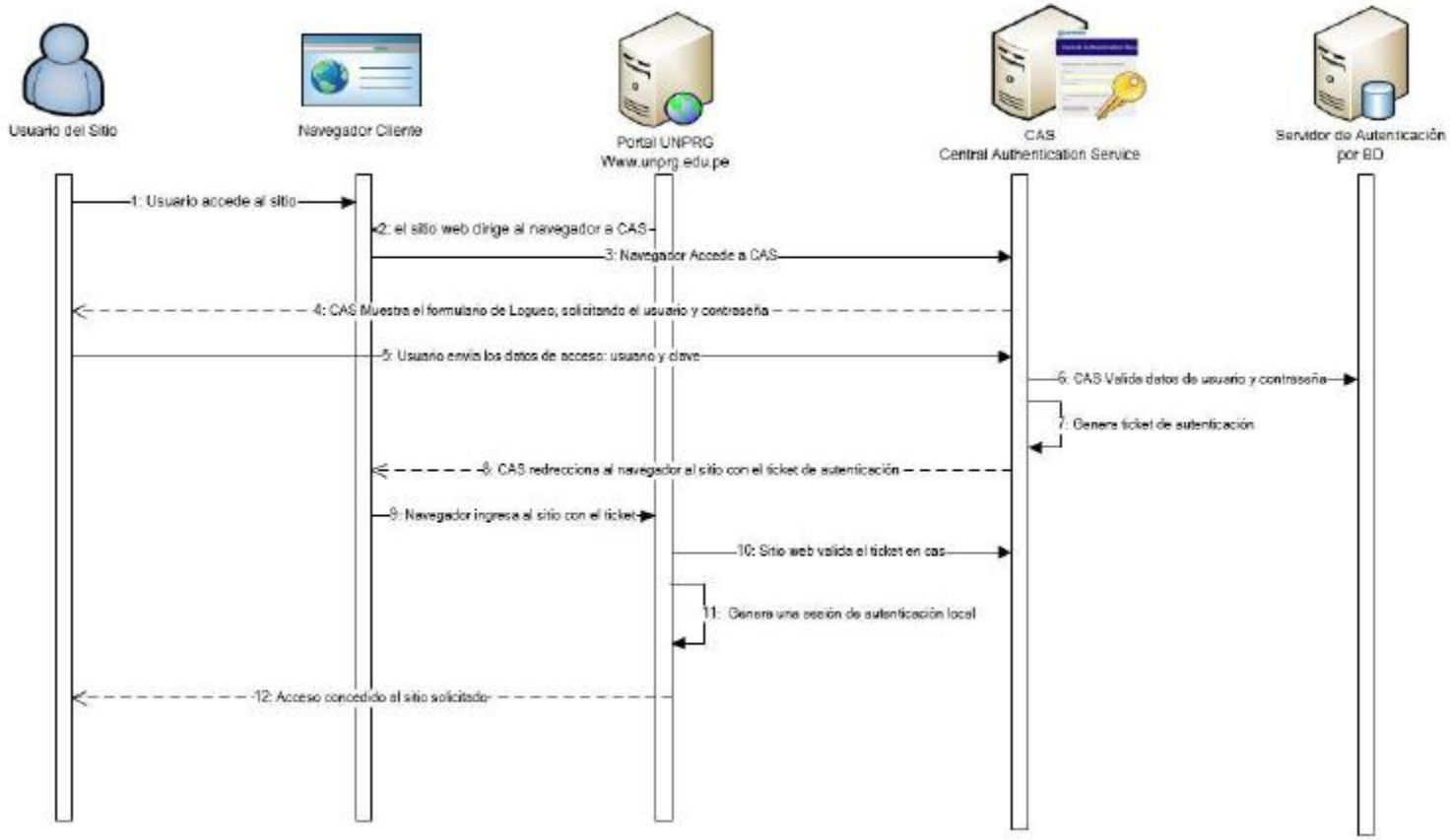


Figura 20: Diagrama de Secuencia del Proceso de autenticación para el acceso a los servicios web que brinda la UNPRG – SSO CAS (Elaboración del Autor)

3.4 ANÁLISIS E INTERPRETACIÓN DE RESULTADOS.

Para el análisis, se toma como punto de referencia la variable dependiente "Optimizar el acceso a los servicios web de la UNPRG" en base al indicador "Reducción de tiempo de acceso a los servicios web", efectuando una comparación entre los índices I1 e I2. Así mismo se considera dentro de la muestra establecida, a un grupo de 30 alumnos de la Escuela Profesional de Ingeniería Agrícola del curso de Computación Básica.

INDICES :

- I1 : Cantidad de tiempo que utiliza el usuario al acceder a los servicios web sin SSO.
- I2: Cantidad de tiempo que utiliza el usuario al acceder a los servicios web con SSO.

3.4.1 Análisis de Resultados Índice I1

APLICACIÓN	Correo Institucional (mm:ss.00)	Actas Virtuales (mm:ss.00)	Biblioteca On Line (mm:ss.00)	Administración Portal Web (mm:ss.00)	Administración Libro Reclamaciones (mm:ss.00)	Administración Pagos de Admisión (mm:ss.00)
Prueba 1	00:38.63	00:25.91	00:32.44	00:49.58	00:51.51	00:44.23
Prueba 2	00:32.99	00:27.36	00.37.30	00:51.23	00:52.36	00:44.18
Prueba 3	00:39.25	00:14.54	00:35.62	00:52.03	00:55.21	00:45.01
Prueba 4	00:33.96	00:30.25	00:33.98	00:54.33	00:54.86	00:45.03
Prueba 5	00:37.36	00:19.63	00:34.02	00:50.22	00:54.36	00:45.89
Prueba 6	00:39.52	00:18.94	00:31.26	00:51.66	00:55.23	00:43.99
Prueba 7	00:33.90	00:19.01	00:33.05	00:52.00	00:53.69	00:43.89
Prueba 8	00:36.12	00:21.65	00:33.62	00:53.11	00:54.36	00:44.22
Prueba 9	00:39.12	00:22.03	00:34.25	00:53.58	00:56.01	00:44.35
Prueba 10	00:41.12	00:23.00	00:35.22	00:54.12	00:54.91	00:44.36
Prueba 11	00:40.25	00:20.06	00:33.96	00:51.66	00:52.94	00:45.02
Prueba 12	00:39.65	00:21.03	00:35.20	00:52.87	00:51.93	00:44.56
Prueba 13	00:38.52	00:22.33	00:33.22	00:54.88	00:54.69	00:45.22
Prueba 14	00:36.25	00:21.05	00:36.11	00:52.33	00:54.91	00:46.01
Prueba 15	00:39.66	00:19.15	00:35.66	00:53.66	00:55.89	00:45.13
Prueba 16	00:40.15	00:19.56	00:34.67	00:53.19	00:53.21	00:45.16
Prueba 17	00:41.52	00:21.36	00:36.14	00:51.26	00:54.33	00:45.55
Prueba 18	00:42.03	00:25.23	00:34.22	00:48.97	00:58.36	00:44.36
Prueba 19	00:44.25	00:26.01	00:36.01	00:49.55	00:57.01	00:44.63
Prueba 20	00:43.22	00:24.03	00:35.46	00:49.63	00:57.36	00:44.72

APLICACIÓN	Correo Institucional (mm:ss.00)	Actas Virtuales (mm:ss.00)	Biblioteca On Line (mm:ss.00)	Administración Portal Web (mm:ss.00)	Administración Libro Reclamaciones (mm:ss.00)	Administración Pagos de Admisión (mm:ss.00)
Prueba 21	00:42.11	00:23.99	00:34.52	00:51.51	00:56.49	00:45.22
Prueba 22	00:45.13	00:22.03	00:36.01	00:53.23	00:55.23	00:45.89
Prueba 23	00:45.44	00:19.57	00:35.24	00:54.82	00:57.89	00:47.02
Prueba 24	00:42.10	00:18.78	00:34.21	00:52.19	00:57.69	00:46.23
Prueba 25	00:38.09	00:26.02	00:34.77	00:54.32	00:56.32	00:45.26
Prueba 26	00:39.29	00:23.68	00:33.66	00:51.48	00:57.69	00:45.38
Prueba 27	00:38.64	00:24.13	00:35.22	00:52.36	00:58.63	00:45.63
Prueba 28	00:39.55	00:17.99	00:38.11	00:52.84	00:56.66	00:45.74
Prueba 29	00:40.21	00:17.58	00:37.88	00:52.30	00:57.22	00:45.57
Prueba 30	00:44.77	00:18.59	00:36.23	00:56.01	00:57.13	00:45.19
Tiempo Promedio en Autenticarse	00:39.76	00:21.82	00:33.67	00:52.36	00:55.47	00:45.09
Tiempo de Cambio de Pagina	-	00:02.00	00:02.00	00:02.00	00:02.00	00:02.00

Calculamos el tiempo promedios de acceso a todas las aplicaciones o servicios web de la UNPRG; Así mismo se considera el tiempo que genera el cambiar de una página en la que se encuentra el módulo de autenticación de cada aplicación o servicio web.

Tiempo:	Total de Tiempo (mm:ss.00)
Promedio en Autenticarse (A)	04:08.16
De Cambio de Pagina (B)	00:10.00
Tiempo Total Promedio en Autenticarse en Todas las aplicaciones (A+B)	04:18.16

Por tanto, tenemos como resultado para I1 = 04: 18.16 expresados en mm:ss.00.

Figura 21: Diagrama de Análisis del Índice I1 para Prueba 1.
(Elaboración del Autor)

APLICACIÓN	ACCESO VIA SSO	Correo Institucional	Actas Virtuales	Biblioteca On Line	Administración Portal Web	Administración Libro Reclamaciones	Administración Pagos de Admisión
Prueba 1	00:40.38	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00
Prueba 2	00:41.62	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00
Prueba 3	00:40.28	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00
Prueba 4	00:42.07	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00
Prueba 5	00:40.25	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00
Prueba 6	00:40.10	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00
Prueba 7	00:39.26	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00
Prueba 8	00:40.51	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00
Prueba 9	00:41.56	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00
Prueba 10	00:42.12	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00
Prueba 11	00:40.65	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00
Prueba 12	00:40.87	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00
Prueba 13	00:41.48	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00
Prueba 14	00:41.11	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00
Prueba 15	00:41.53	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00
Prueba 16	00:40.99	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00
Prueba 17	00:41.69	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00
Prueba 18	00:42.20	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00
Prueba 19	00:42.91	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00
Prueba 20	00:42.40	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00
Prueba 21	00:42.31	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00
Prueba 22	00:42.92	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00
Prueba 23	00:43.33	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00
Prueba 24	00:41.87	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00
Prueba 25	00:42.46	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00
Prueba 26	00:41.86	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00
Prueba 27	00:42.44	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00
Prueba 28	00:41.82	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00
Prueba 29	00:41.79	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00
Prueba 30	00:42.99	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00
Tiempo Promedio en Autenticarse	00:41.59	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00
Tiempo de Cambio de Pagina	-	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00	00:00.00

3.4.2 Análisis de Resultados Índice I2

Al igual que en el análisis de I1, Calculamos el tiempo promedios de acceso a todas las aplicaciones o servicios web de la UNPRG; Así mismo se considera el tiempo 00:00.00, porque solo existe una página dónde encontraremos el módulo de autenticación.

Tiempo:	Total de Tiempo (mm:ss.00)
Promedio en Autenticarse (A)	00:41.59
De Cambio de Pagina (B)	00:00.00
Tiempo Total Promedio en Autenticarse en Todas las aplicaciones (A+B)	00:41.59

Por tanto, tenemos como resultado para I2 = 00: 41.59 expresados en mm:ss.00.

Después de realizar los cálculos respectivos basados en los índices I1 e I2, analizamos que existe una reducción del 83.89 % del tiempo con la implementación de la solución SSO.

Comparación de Tiempos	Tiempo	%
I1: Sin SSO	04:18.16	100.00
I2: Con SSO	00:41.59	16.11
Reducción de Tiempo Promedio		83.89

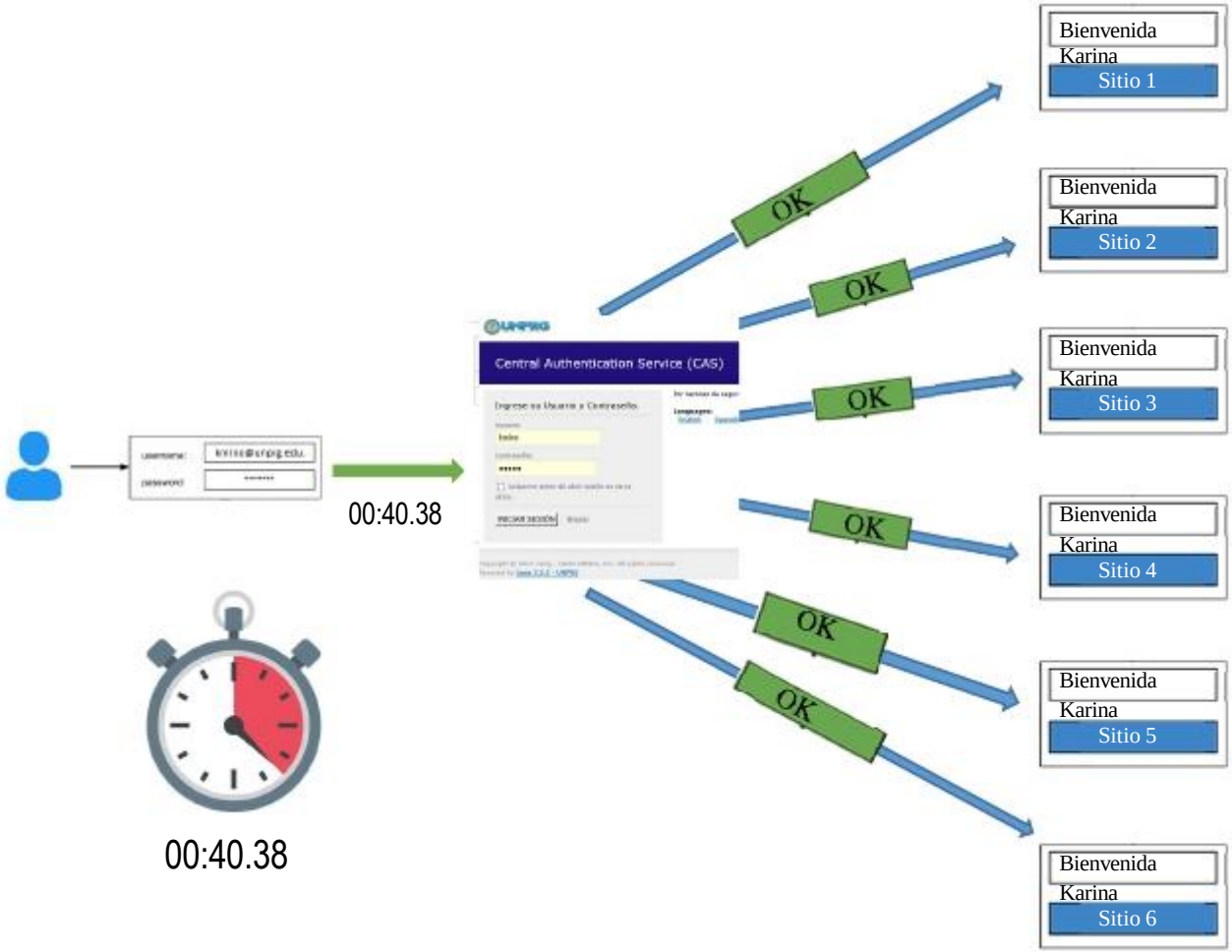


Figura 22: Diagrama de Análisis del Índice I2 para Prueba 1.
(Elaboración del Autor)

CONCLUSIONES

- La situación actual, en el proceso de autenticación para el acceso a los servicios web que brinda la UNPRG, es engorroso para el usuario final, ya que tiene que usar diferentes usuarios e interfaces de autenticación, generando redundancia de datos.
- Después de haber realizado un estudio comparativo entre los diferentes mecanismos SSO, web SSO es el mecanismo que cubre los requerimientos de sus aplicaciones web en la UNPRG.
- El mecanismo CAS, es el que cubre los mayores protocoles de comunicación para la integración de las aplicaciones en la UNPRG.
- Es factible la implementación de la propuesta desarrollada, basada en apache tomcat, conectada a la BD Oracle e integrada con un puente para la ejecución de sus aplicaciones desarrolladas en php.
- La Implementación de una solución Single Sign-On, optimizó el proceso de autenticación a los usuarios de la UNPRG, para el acceso a los servicios web.

RECOMENDACIONES

Se recomienda a la UNPRG, la adquisición de certificados por autoridades de certificación ya sea de reconocimiento nacional o internación para mejor la seguridad de sus aplicaciones.

Así mismo, se recomienda la creación de políticas de creación de usuarios y contraseñas; así como también normar el procedimiento del mismo.

Para los profesionales en desarrollo de aplicaciones o público en general que busque soluciones de autenticación única, se les recomienda seguir profundizándose en las demás soluciones de Single Sign On muy interesantes, pero que no se aplicaron a la universidad por no cubrir sus requerimientos.

REFERENCIAS BIBLIOGRÁFICAS

1. Alvarado Aguirre, M. D. (2015). Estudio y Análisis de Factibilidad de la Solución Tipo Single Sign-On. Tesis, Guayaquil - Ecuador.

2. Bringas Masgo, I. E. (2011). Admistración de Identidades Federadas de Personas Jurídicas en la Superintendencia Nacional de Administración Tributaria. Tesis, Lima - Perú.

3. Caballero, I., & Cano Martínez, J. (2003). Consideraciones para Implementar una Arquitectura Single Sign-On. Obtenido de http://www.criptored.upm.es/guiateoria/gt_m142j.htm.

4. Cano Moreno, J. L. (2014). Implementación del Sistema Centralizado de Autenticación y Autorización. Tesis, Guatemala.

5. Castro Velarde, K. E., & Guzmán Salgado, J. d. (2010). Implantación del Sistema de administración de accesos e identidads en el proceso de control de accesos en el Banco de la Nación. Tesis, Lima - Perú.

6. Cevallos Teneda, A. (2016). Sistema de Federaciones de Identidades para la Facultad de Ingeniería en Sistemas, Electrónica e Industrial usando Software de Código Abierto. Proyecto de Investigación, Ambato - Ecuador. Recuperado el 10 de 03 de 2017

7. Chicano Tejada, E. (2014). Gestión de servicios en el sistema informático. Madrid, España: IC.

8. González Díaz, S. (2010). Implementación de un sistema unificado de autenticación de usuarios aplicado a los diferentes servicios de la Universidad Tecnológica de Bolívar. Tesis, Cartagena. Recuperado el 10 de 03 de 2010

9. Roebuck, K. (2011). Single Sign-on (SSO) (Emereo ed.). Emereo.

10. González, M. L., & Fuentes, G. D. T. J. M. (2014). Sistemas seguros de acceso y transmisión de datos (MF0489_3). Madrid, ESPAÑA: IC Editorial. Retrieved from http://www.ebrary.com

11. Hernández, E. L. (2016). La criptografía. Madrid, ESPAÑA: Editorial CSIC Consejo Superior de Investigaciones Científicas. Retrieved from http://www.ebrary.com

12. Páez, R. J. J. (2015). Derecho y TICS. Quito, EC: Corporación de Estudios y Publicaciones. Retrieved from http://www.ebrary.com

13. Baca, U. G. (2016). Introducción a la seguridad informática. Distrito Federal, MÉXICO: Grupo Editorial Patria. Retrieved from http://www.ebrary.com

ANEXOS

A. ANEXO: INSTALACION DE JAVA 64 BITS

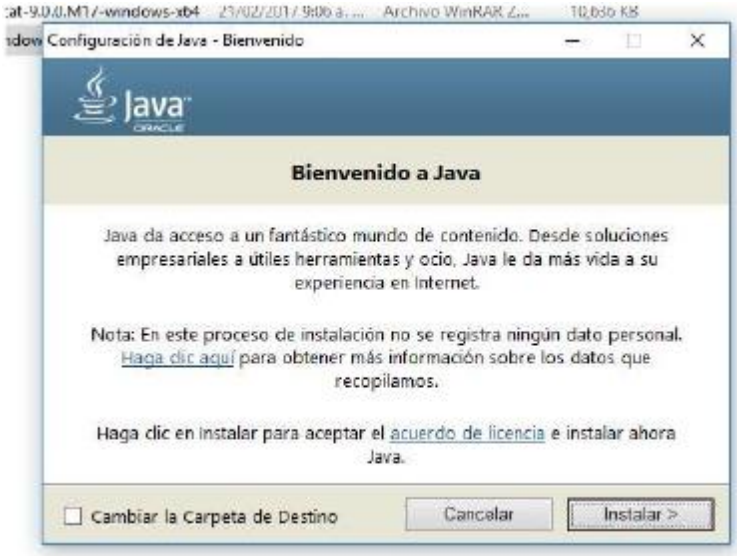


Figura A-1: Iniciando Instalación Java jre-8u144-windows-x64

Figura A-2: Progreso de Instalación Java jre-8u144-windows-x64

Figura A-3: Finalizando Instalación Java jre-8u144-windows-x64

B. ANEXO: CONFIGURACION DEL JAVA_HOME

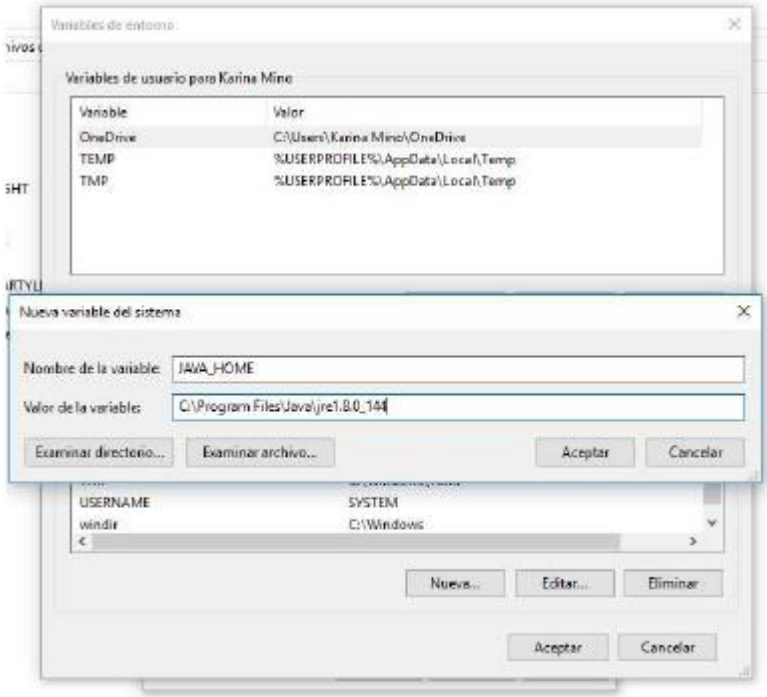


Figura B-1: Configuración de Variable de Entorno.

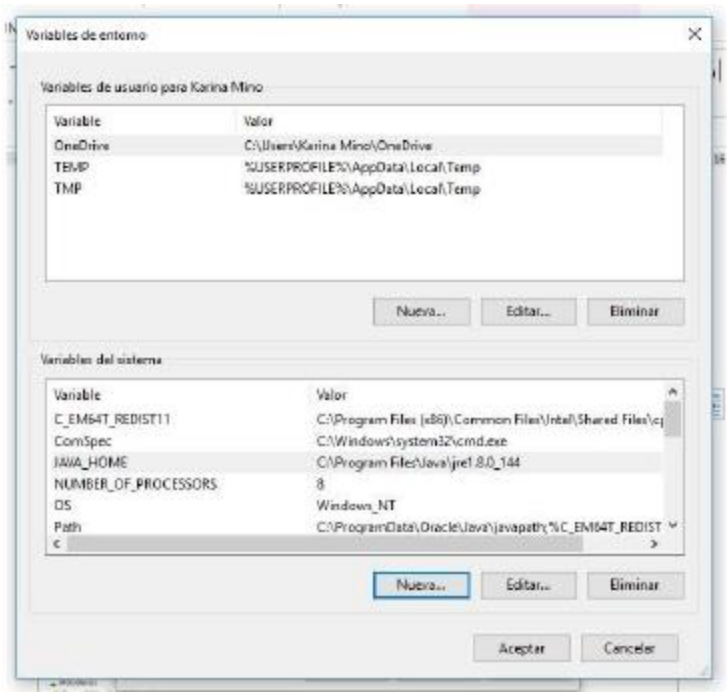


Figura B-2: Variable de Entorno JAVA_HOME creada.

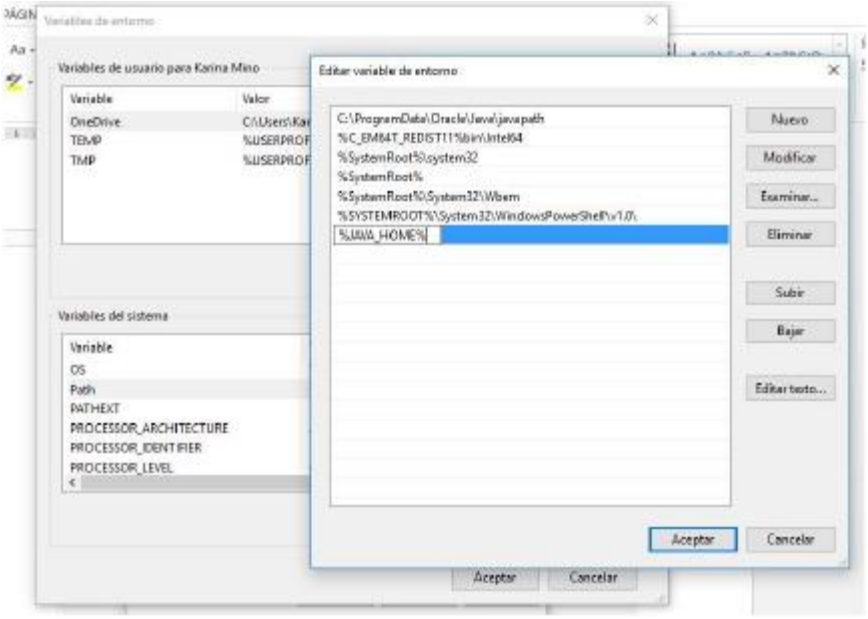


Figura B-3: Configuración del PATH del JAVA_HOME

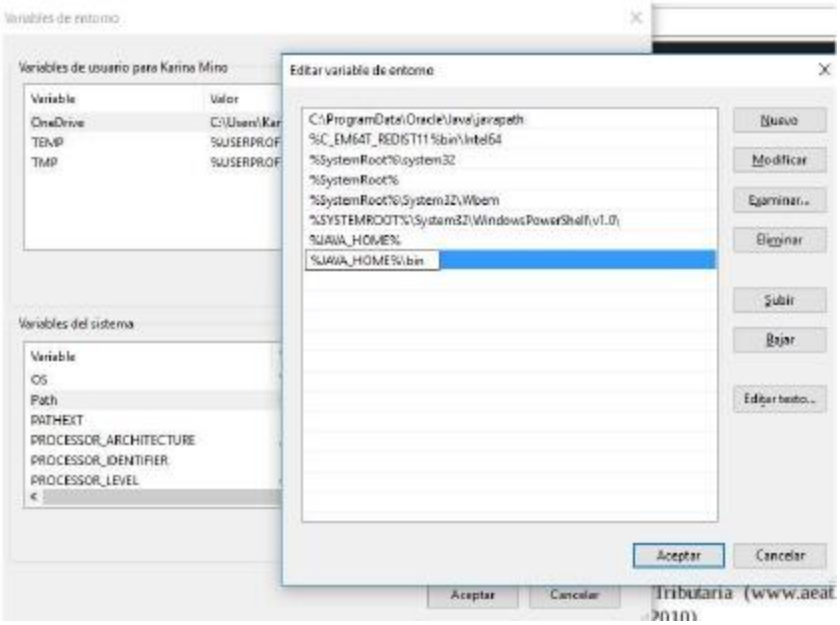


Figura B-4: Configuración del PATH del JAVA_HOME\bin

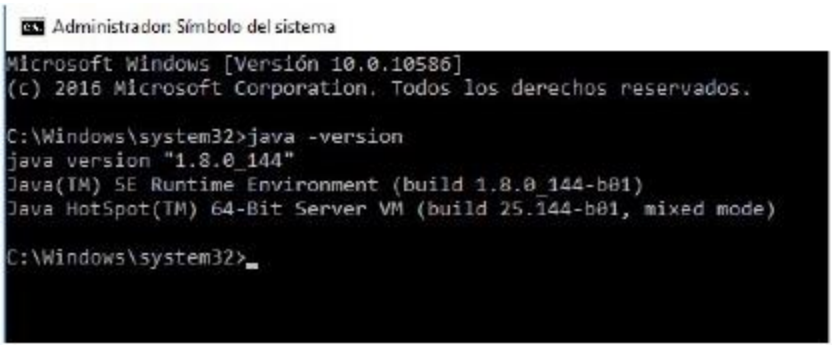
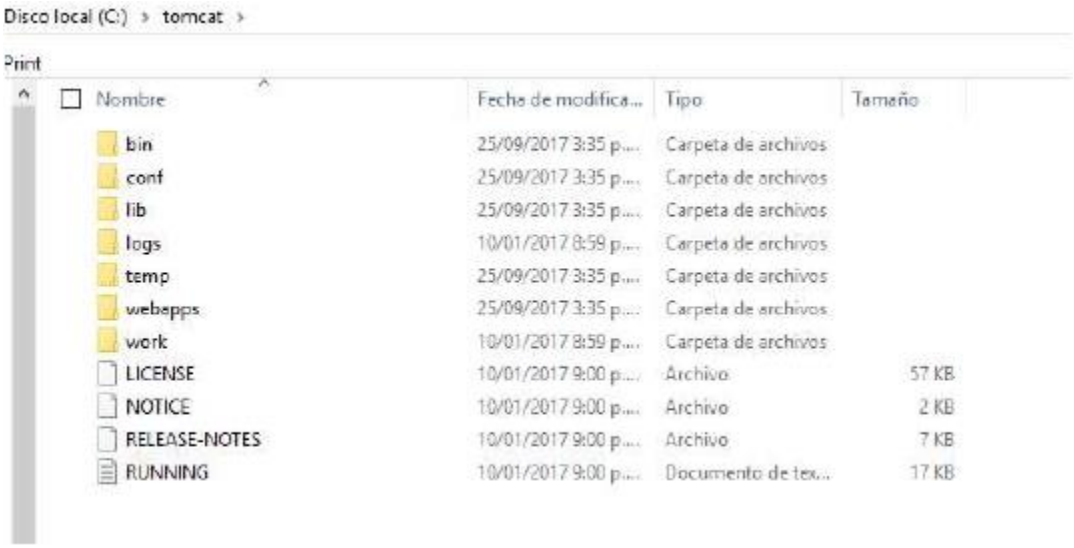


Figura B-5: Verificación de la versión del Java instalado.

C. ANEXO: CONFIGURACION DE APACHE TOMCAT

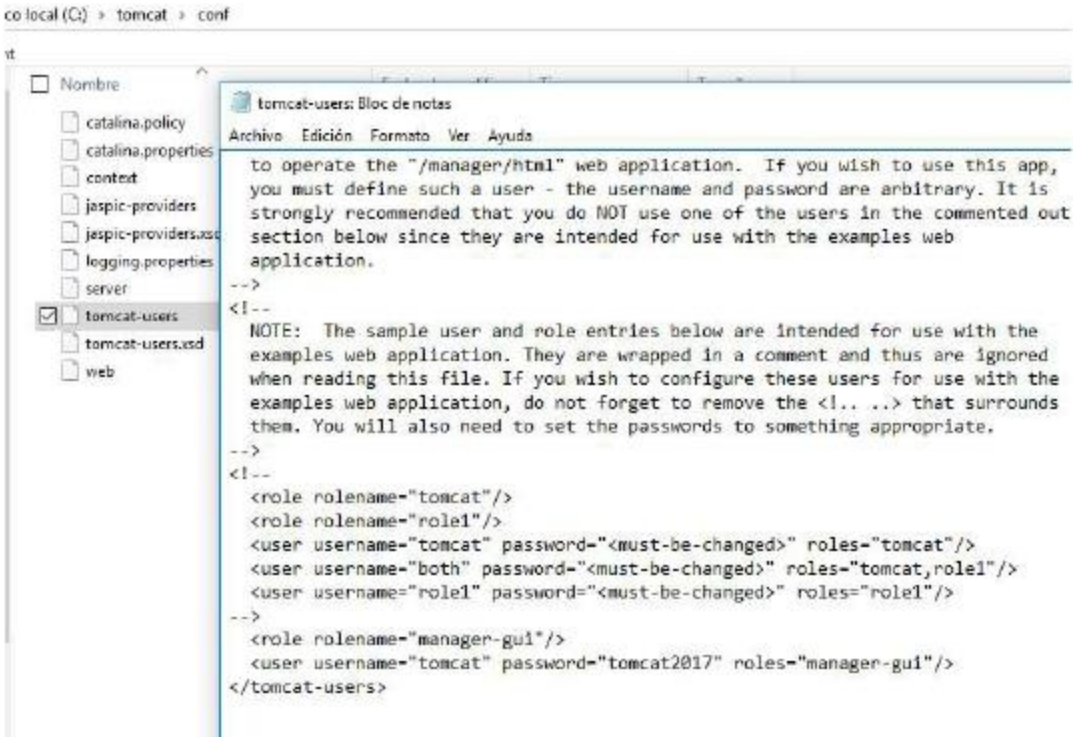


Disco local (C:) › tomcat ›

Print

Nombre	Fecha de modifica...	Tipo	Tamaño
bin	25/09/2017 3:35 p...	Carpeta de archivos	
conf	25/09/2017 3:35 p...	Carpeta de archivos	
lib	25/09/2017 3:35 p...	Carpeta de archivos	
logs	10/01/2017 8:59 p...	Carpeta de archivos	
temp	25/09/2017 3:35 p...	Carpeta de archivos	
webapps	25/09/2017 3:35 p...	Carpeta de archivos	
work	10/01/2017 8:59 p...	Carpeta de archivos	
LICENSE	10/01/2017 9:00 p...	Archivo	57 KB
NOTICE	10/01/2017 9:00 p...	Archivo	2 KB
RELEASE-NOTES	10/01/2017 9:00 p...	Archivo	7 KB
RUNNING	10/01/2017 9:00 p...	Documento de tex...	17 KB

Figura C-1: Desplegando APACHE TOMCAT.



co local (C:) › tomcat › conf

Nombre

catalina.policy
catalina.properties
context
jaspic-providers
jaspic-providers.xsd
logging.properties
server
tomcat-users
tomcat-users.xsd
web

tomcat-users: Bloc de notas

Archivo Edición Formato Ver Ayuda

```
  to operate the "/manager/html" web application.  If you wish to use this app,
  you must define such a user - the username and password are arbitrary. It is
  strongly recommended that you do NOT use one of the users in the commented out
  section below since they are intended for use with the examples web
  application.
-->
<!--
  NOTE:  The sample user and role entries below are intended for use with the
  examples web application. They are wrapped in a comment and thus are ignored
  when reading this file. If you wish to configure these users for use with the
  examples web application, do not forget to remove the <!.. ..> that surrounds
  them. You will also need to set the passwords to something appropriate.
-->
<!--
  <role rolename="tomcat"/>
  <role rolename="role1"/>
  <user username="tomcat" password="<must-be-changed>" roles="tomcat"/>
  <user username="both" password="<must-be-changed>" roles="tomcat,role1"/>
  <user username="role1" password="<must-be-changed>" roles="role1"/>
-->
  <role rolename="manager-gui"/>
  <user username="tomcat" password="tomcat2017" roles="manager-gui"/>
</tomcat-users>
```

Figura C-2: Configuración DEL USUARIO TOMCAT

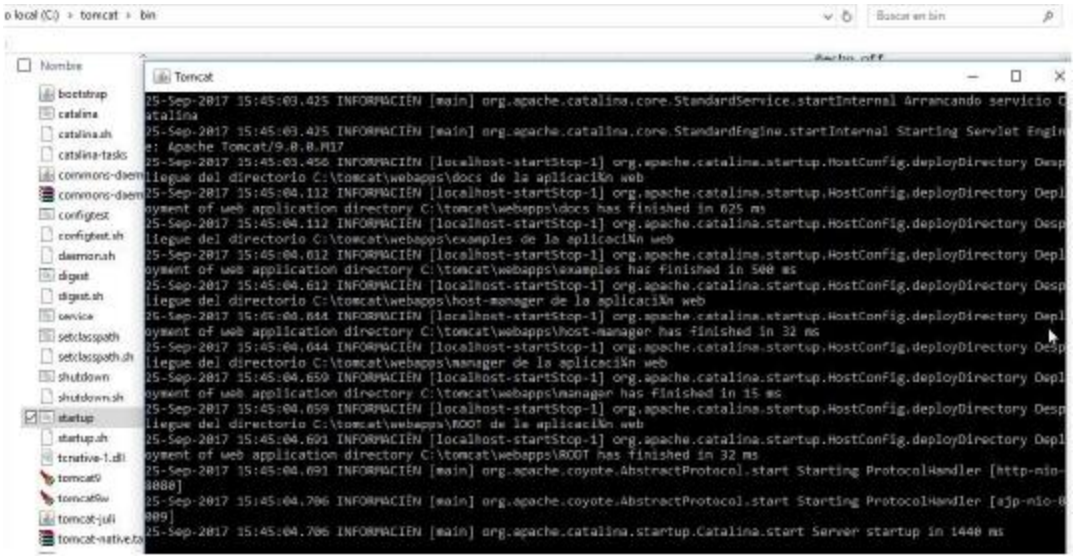


Figura C-3: Ejecutando TOMCAT

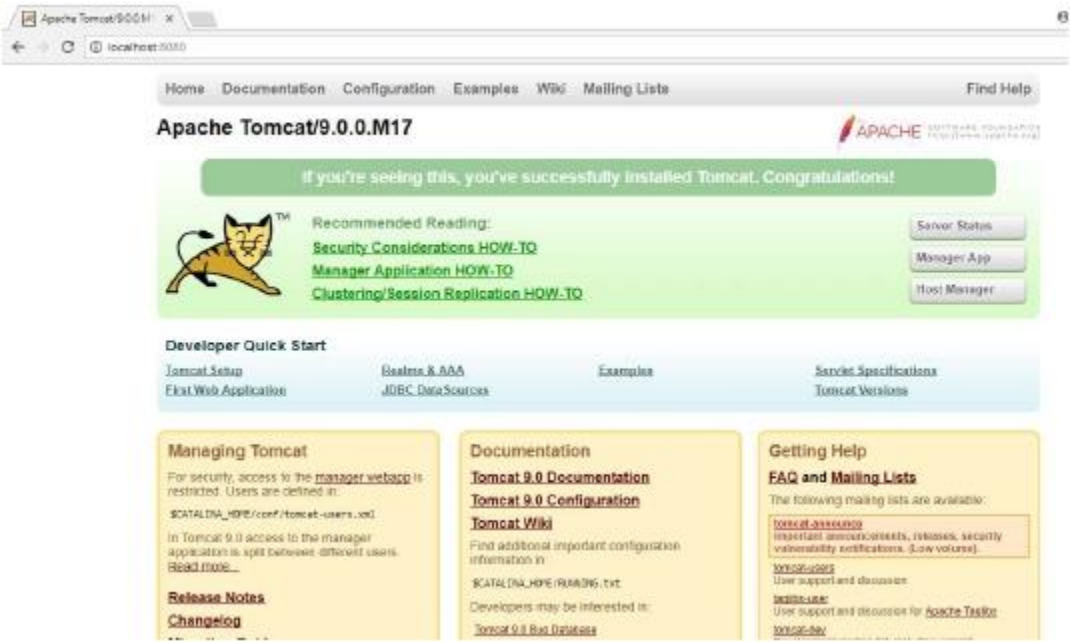


Figura C-4: Accediendo al Gestor de aplicaciones web - Apache Tomcat

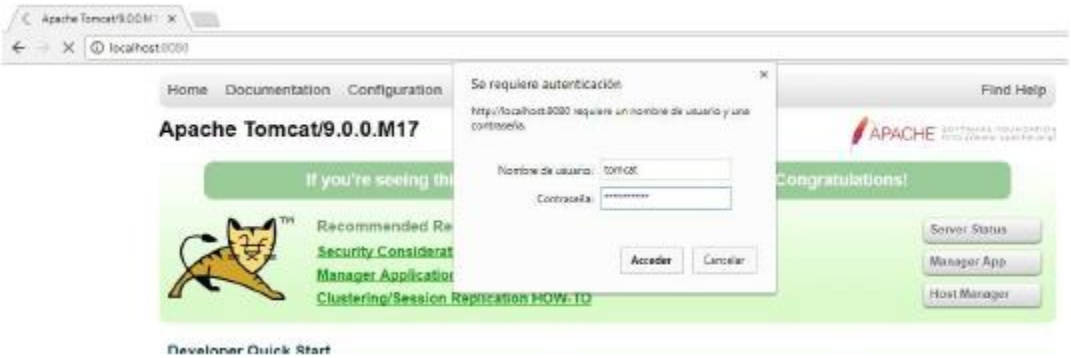


Figura C-5: Autenticación de usuario TOMCAT configurado.

Figura C-6: Gestor de Aplicaciones Web de TOMCAT.

D. ANEXO: INSTALANDO PROTOCOLO SEGURO SOBRE TOMCAT - SSL

Figura D-1: Accediendo a carpeta bin del java (keytool.)

Figura D-2: Generando clave SSL

Figura D-3: Generando clave SSL

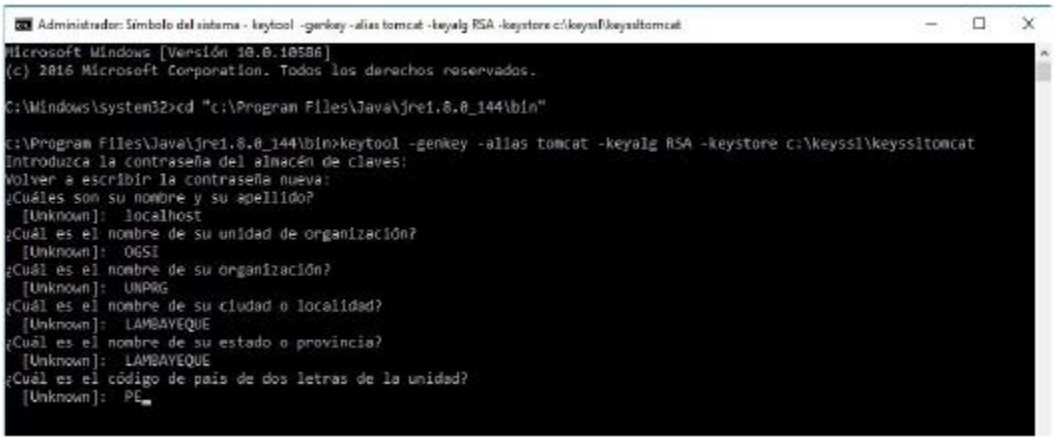


Figura D-4: Ingreso de datos solicitados de clave SSL

```
Administrador: Símbolo del sistema - keytool -genkey -alias tomcat -keyalg RSA -keystore c:\keyssl\keyssltomcat
Microsoft Windows [Versión 10.0.10586]
(c) 2016 Microsoft Corporation. Todos los derechos reservados.

C:\Windows\system32>cd "c:\Program Files\Java\jre1.8.0_144\bin"

c:\Program Files\Java\jre1.8.0_144\bin>keytool -genkey -alias tomcat -keyalg RSA -keystore c:\keyssl\keyssltomcat
Introduzca la contraseña del almacén de claves:
Volver a escribir la contraseña nueva:
¿Cuáles son su nombre y su apellido?
  [Unknown]:  localhost
¿Cuál es el nombre de su unidad de organización?
  [Unknown]:  OGSI
¿Cuál es el nombre de su organización?
  [Unknown]:  UNPRG
¿Cuál es el nombre de su ciudad o localidad?
  [Unknown]:  LAMBAYEQUE
¿Cuál es el nombre de su estado o provincia?
  [Unknown]:  LAMBAYEQUE
¿Cuál es el código de país de dos letras de la unidad?
  [Unknown]:  PE
¿Es correcto CN=localhost, OU=OGSI, O=UNPRG, L=LAMBAYEQUE, ST=LAMBAYEQUE, C=PE?
  [no]:  SI
```

Figura D-5: Confirmación de datos solicitados de clave SSL.

```
Administrador: Símbolo del sistema - keytool -genkey -alias tomcat -keyalg RSA -keystore c:\keyssl\keyssltomcat
Microsoft Windows [Versión 10.0.10586]
(c) 2016 Microsoft Corporation. Todos los derechos reservados.

C:\Windows\system32>cd "c:\Program Files\Java\jre1.8.0_144\bin"

c:\Program Files\Java\jre1.8.0_144\bin>keytool -genkey -alias tomcat -keyalg RSA -keystore c:\keyssl\keyssltomcat
Introduzca la contraseña del almacén de claves:
Volver a escribir la contraseña nueva:
¿Cuáles son su nombre y su apellido?
  [Unknown]:  localhost
¿Cuál es el nombre de su unidad de organización?
  [Unknown]:  OGSI
¿Cuál es el nombre de su organización?
  [Unknown]:  UNPRG
¿Cuál es el nombre de su ciudad o localidad?
  [Unknown]:  LAMBAYEQUE
¿Cuál es el nombre de su estado o provincia?
  [Unknown]:  LAMBAYEQUE
¿Cuál es el código de país de dos letras de la unidad?
  [Unknown]:  PE
¿Es correcto CN=localhost, OU=OGSI, O=UNPRG, L=LAMBAYEQUE, ST=LAMBAYEQUE, C=PE?
  [no]:  SI

Introduzca la contraseña de clave para <tomcat>
        (INTRO si es la misma contraseña que la del almacén de claves):
```

Figura D-6: Ingreso de contraseña para clave tomcat.

```
Administrador: Símbolo del sistema - keytool -genkey -alias tomcat -keyalg RSA -keystore c:\keyssl\keyssltomcat
Microsoft Windows [Versión 10.0.10586]
(c) 2016 Microsoft Corporation. Todos los derechos reservados.

C:\Windows\system32>cd "c:\Program Files\Java\jre1.8.0_144\bin"

c:\Program Files\Java\jre1.8.0_144\bin>keytool -genkey -alias tomcat -keyalg RSA -keystore c:\keyssl\keyssltomcat
Introduzca la contraseña del almacén de claves:
Volver a escribir la contraseña nueva:
¿Cuáles son su nombre y su apellido?
  [Unknown]:  localhost
¿Cuál es el nombre de su unidad de organización?
  [Unknown]:  OGSI
¿Cuál es el nombre de su organización?
  [Unknown]:  UNPRG
¿Cuál es el nombre de su ciudad o localidad?
  [Unknown]:  LAMBAYEQUE
¿Cuál es el nombre de su estado o provincia?
  [Unknown]:  LAMBAYEQUE
¿Cuál es el código de país de dos letras de la unidad?
  [Unknown]:  PE
¿Es correcto CN=localhost, OU=OGSI, O=UNPRG, L=LAMBAYEQUE, ST=LAMBAYEQUE, C=PE?
  [no]:  SI

Introduzca la contraseña de clave para <tomcat>
        (INTRO si es la misma contraseña que la del almacén de claves):
Volver a escribir la contraseña nueva:
```

Figura D-7: Ingreso de confirmación de contraseña para clave tomcat.

```
Administrador: Símbolo del sistema
Microsoft Windows [Versión 10.0.10586]
(c) 2016 Microsoft Corporation. Todos los derechos reservados.

C:\Windows\system32>cd "c:\Program Files\Java\jre1.8.0_144\bin"

c:\Program Files\Java\jre1.8.0_144\bin>keytool -genkey -alias tomcat -keyalg RSA -keystore c:\keyssl\keyssltomcat
Introduzca la contraseña del almacén de claves:
Volver a escribir la contraseña nueva:
¿Cuáles son su nombre y su apellido?
  [Unknown]:  localhost
¿Cuál es el nombre de su unidad de organización?
  [Unknown]:  OGSI
¿Cuál es el nombre de su organización?
  [Unknown]:  UNPRG
¿Cuál es el nombre de su ciudad o localidad?
  [Unknown]:  LAMBAYEQUE
¿Cuál es el nombre de su estado o provincia?
  [Unknown]:  LAMBAYEQUE
¿Cuál es el código de país de dos letras de la unidad?
  [Unknown]:  PE
¿Es correcto CN=localhost, OU=OGSI, O=UNPRG, L=LAMBAYEQUE, ST=LAMBAYEQUE, C=PE?
  [no]:  SI

Introduzca la contraseña de clave para <tomcat>
        (INTRO si es la misma contraseña que la del almacén de claves):
Volver a escribir la contraseña nueva:

c:\Program Files\Java\jre1.8.0_144\bin>
```

Figura D-8: Clave SSL creada.

```
c:\Program Files\Java\jre1.8.0_144\bin>keytool -list -keystore c:\keyssl\keyssltomcat
```

Figura D-9: Comprobando la creación del key

```
c:\Program Files\Java\jre1.8.0_144\bin>keytool -list -keystore c:\keyssl\keyssltomcat
Introduzca la contraseña del almacén de claves:
```

Figura D-10: Ingreso de contraseña del almacén de claves.

```
c:\Program Files\Java\jre1.8.0_144\bin>keytool -list -keystore c:\keyssl\keyssltomcat
Introduzca la contraseña del almacén de claves:

Tipo de Almacén de Claves: JKS
Proveedor de Almacén de Claves: SUN

Su almacén de claves contiene 1 entrada

tomcat, 25/09/2017, PrivateKeyEntry,
Huella Digital de Certificado (SHA1): 0F:35:85:3A:F5:09:C9:AD:CF:E0:2C:22:29:64:AF:3A:24:C6:36:C6

c:\Program Files\Java\jre1.8.0_144\bin>
```

Figura D-11: Visualización de la clave creada.

E. ANEXO: CONFIGURAR HTTPS EN TOMCAT

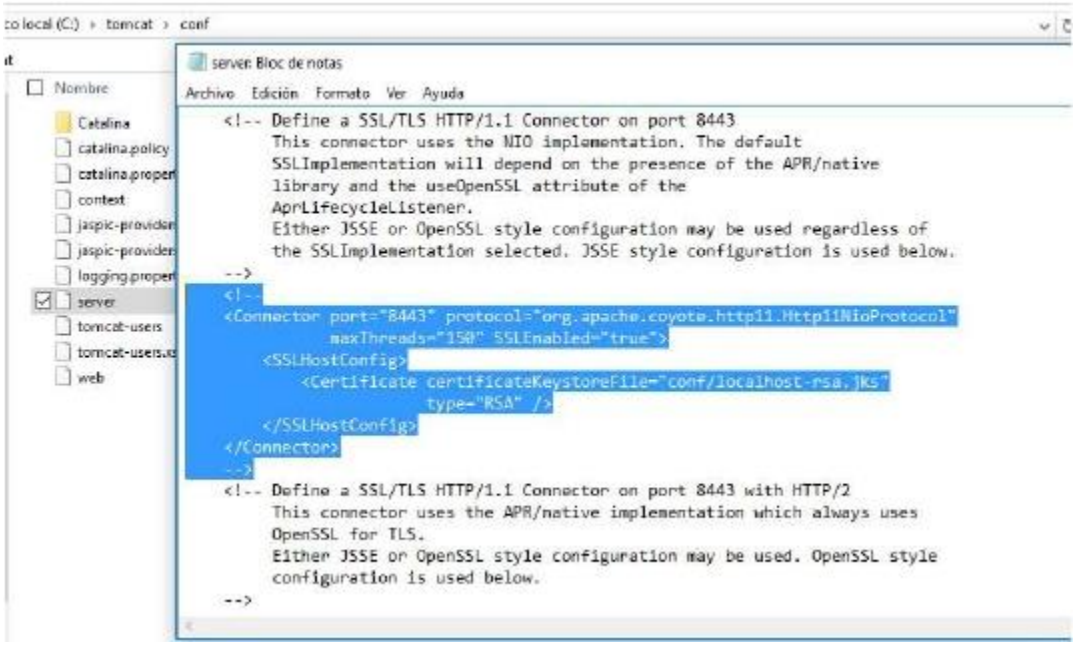


Figura E-1: Ubicación del archivo de configuración (tomcat/conf/server)

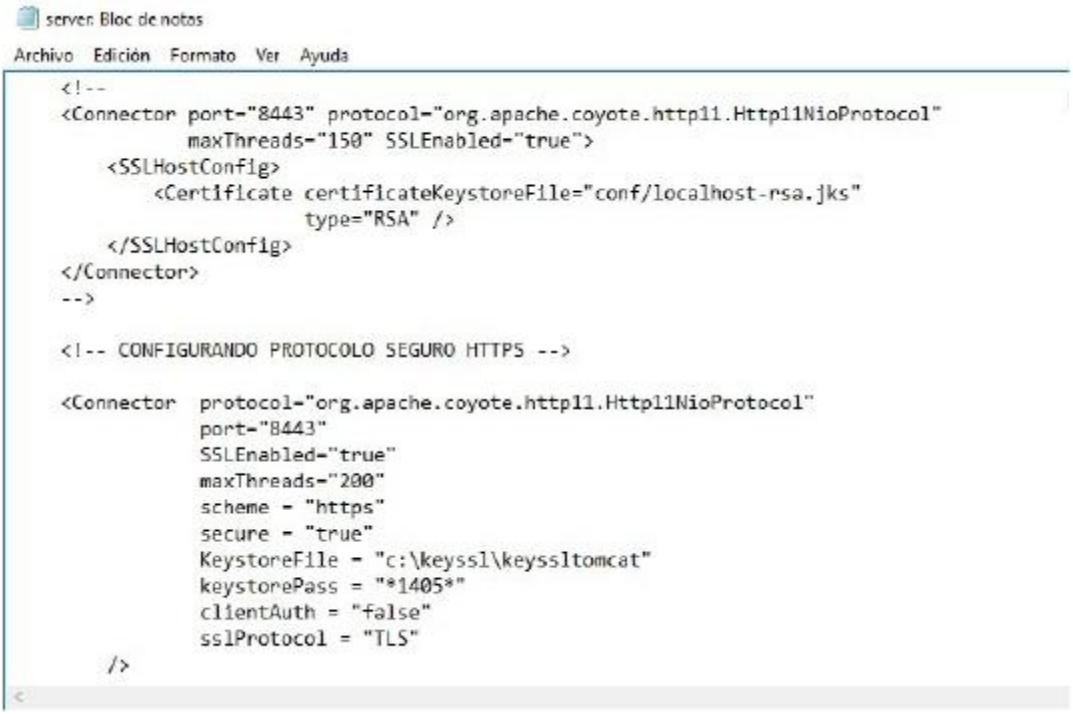


Figura E-2: Modificación de parámetros en Connector protocol.

F. ANEXO: VERIFICACION DEL FUNCIONAMIENTO DEL PROTOCOLO SEGURO HTTPS.

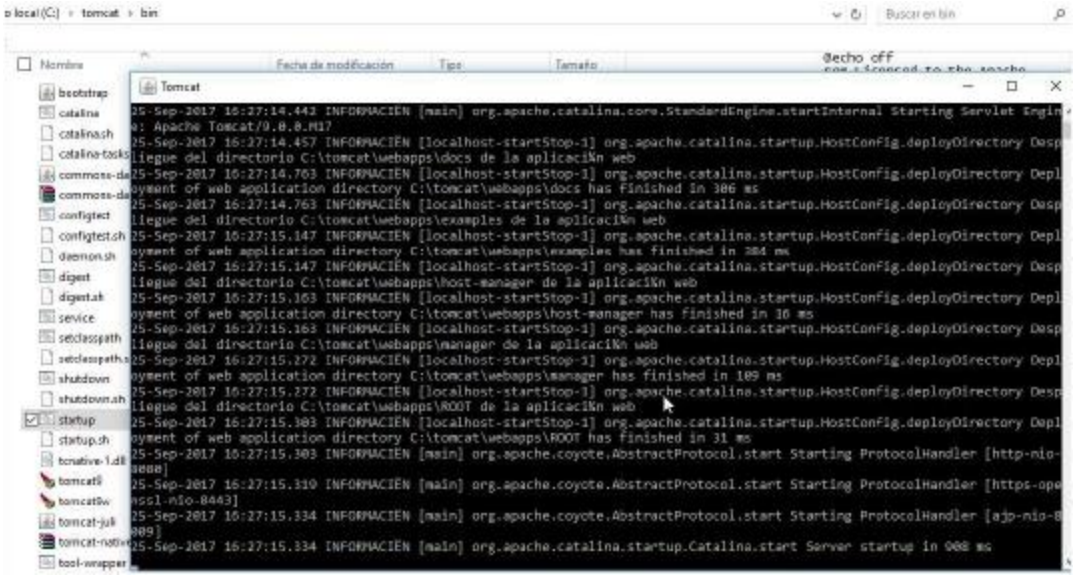


Figura F-1: Ejecución del tomcat.

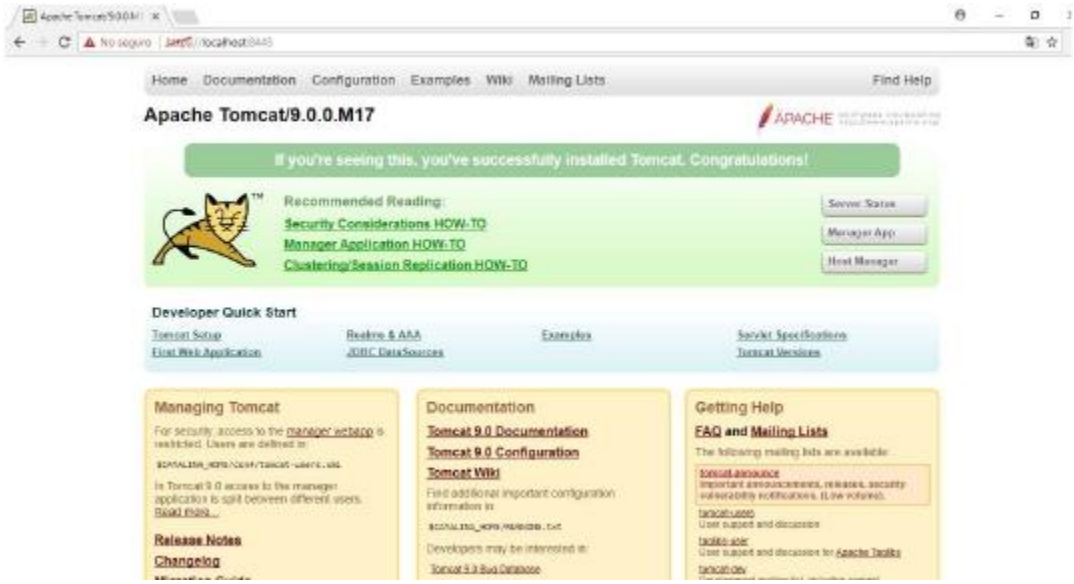


Figura F-2: Cargar navegador con https.

Figura F-3: Cargar Gestor de Aplicaciones con https.

G. ANEXO: CONFIGURANDO TOMCAT - CAS.

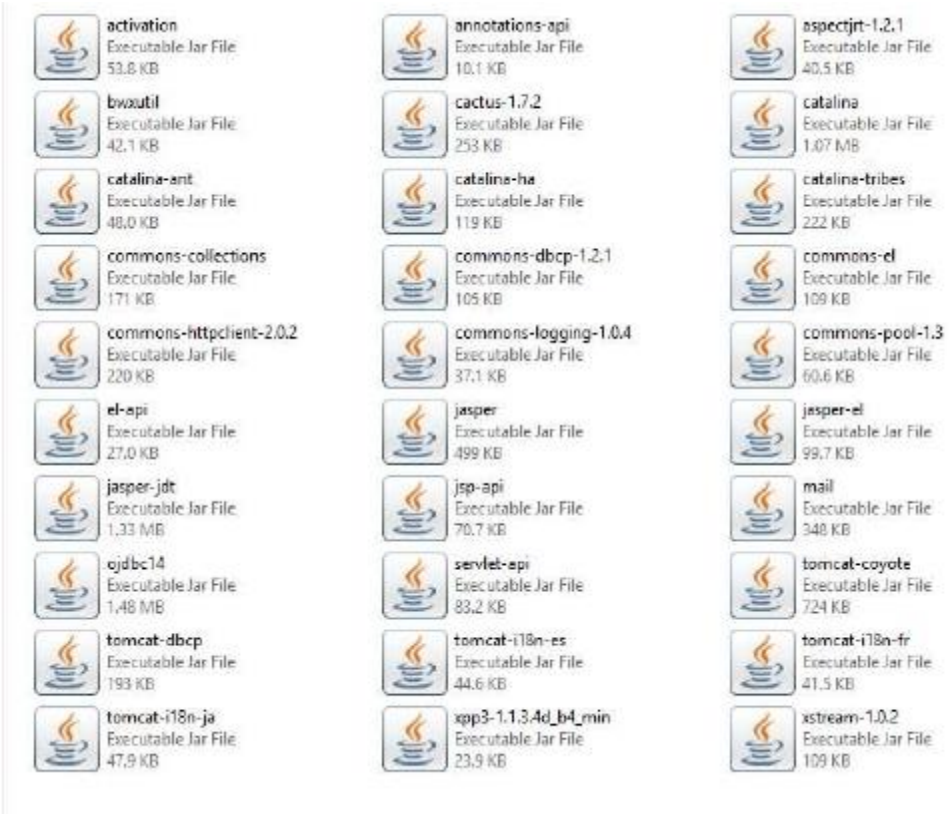


Figura G-1: Desplegando las librerías requeridas

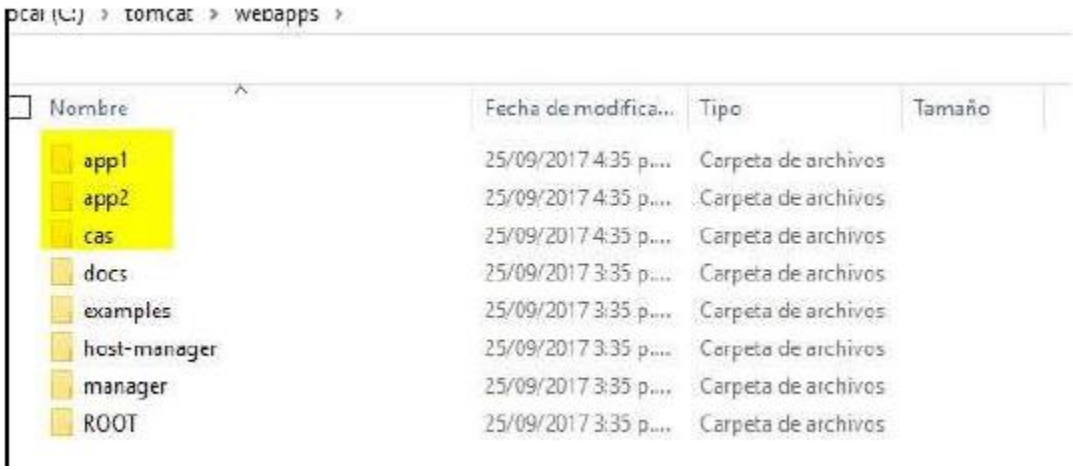


Figura G-2: Desplegando CAS y aplicaciones de pruebas

Figura G-3: Verificación que las aplicaciones de prueba estén inicializadas

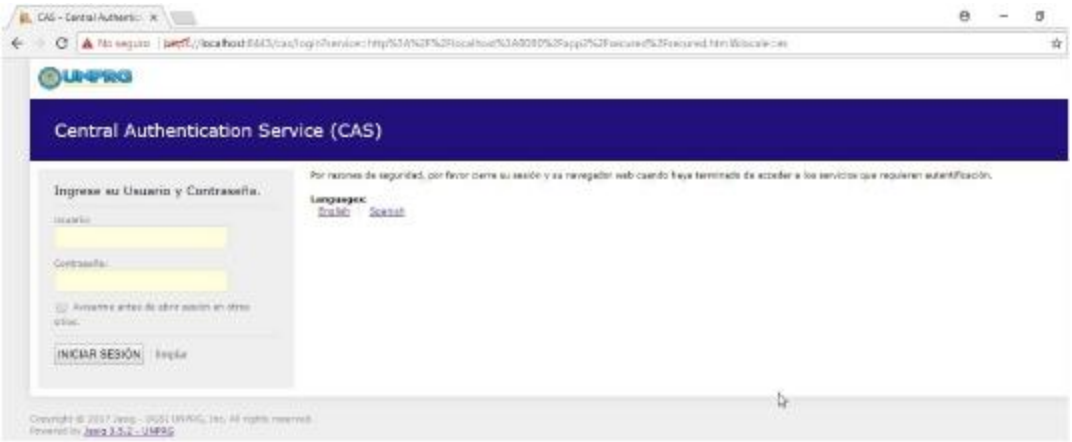


Figura G-4: Verificación de la ejecución correcta del CAS.

Figura G-5: Validando autenticación, con usuario kmino.

Figura G-5: Accediendo a dos de las aplicaciones de prueba.

Figura G-6: Accediendo a la aplicación de prueba Actas Virtuales.

Figura G-7: Accediendo a la aplicación de prueba BD on Line.