“HERRAMIENTA SINGLE SIGN-ON PARA OPTIMIZAR EL ACCESO A LOS SERVICIOS WEB EN UNA UNIVERSIDAD DEL DEPARTAMENTO DE LAMBAYEQUE”

Karol Melissa Arbaiza Godos

HERRAMIENTA SINGLE SIGN-ON PARA OPTIMIZAR EL ACCESO A LOS SERVICIOS WEB EN UNA UNIVERSIDAD DEL DEPARTAMENTO DE LAMBAYEQUE

RESUMEN

Este estudio, tuvo como objetivo, realizar una investigación de una herramienta de 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 del Departamento de Lambayeque 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.

ABSTRACT

The objective of this article is to carry out an investigation of a Single Sign On solution, with the purpose of optimizing the Users authentication process for access to web services at University of Lambayeque; facing the current problem generated by providing authentication for each of the multiple applications and web services provided to the university community.

PALABRAS CLAVES

SSO, Autenticación, Certificados Digitales, Cifrado, SSL.

KEY WORDS

Single Sign On, Authentication, Digital Certificates, Encryption, Secure Sockets Layer

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.

En la actualidad, la Universidad del Departamento de Lambayeque (a la cual la nombraremos en adelante como UDPL) 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.

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 UDPL, 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 embargo, 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.

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 quefueronadministrados por la institución y que al mismo tiempo les permitiera escalar en algún futuro a tecnologías quefueronmanejadas 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. Específicamente 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 presento 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 existió un control eficiente de la identidad.

La propuesta de solución del proyecto tuvo 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 dio 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.

Ante los problemas tecnológicos actuales que enfrentaba la UDPL 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 deseó implementar una solución de herramienta de tipo Single Sign – On y así se:

- ✓ Mejoró considerablemente los tiempos de acceso a los diferentes servicios web, dependiendo el requerimiento del usuario (alumno, docente y administrativo).

- ✓ Mejoró el servicio al usuario (alumno, docente y administrativo), evitando la incomodad de recordar diferentes contraseñas de acceso para cada aplicación.
- ✓ Evitó redundancia de datos en su información.
- ✓ Optimizó el Recurso Humano de la Oficina General de Sistemas Informáticos Administrativos de la UDPL; Asignando al personal técnico que actualmente se destina a la labor de gestión de contraseñas, en proyectos de mayor envergadura para la universidad.

Todo ello se resume en el objetivo de haber optimizado el proceso de autenticación de los usuarios en la UDPL para acceso a los servicios web, mediante la implementación de SSO (single sign-on).

METODOLOGÍA

Esta investigación es descriptiva, teniendo como población a los 15 743 usuarios de la comunidad universitaria (universo) que accedan a los servicios web de la UDPL y como muestra (un grupo de 30 alumnos de la Escuela Profesional de Ingeniería Agrícola) se tuvo en consideración a usuarios que tenían acceso a más de un servicio web de la UDPL, tales como estudiantes que se encontraban cursando el tercer ciclo de una escuela profesional; así como también sus respectivos docentes.

En cuando al desarrollo de su metodología se analizó las credenciales que fueron 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, se incorporó infraestructura replicada con el fin de manejar la contingencia y redundancia en tiempo real (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.

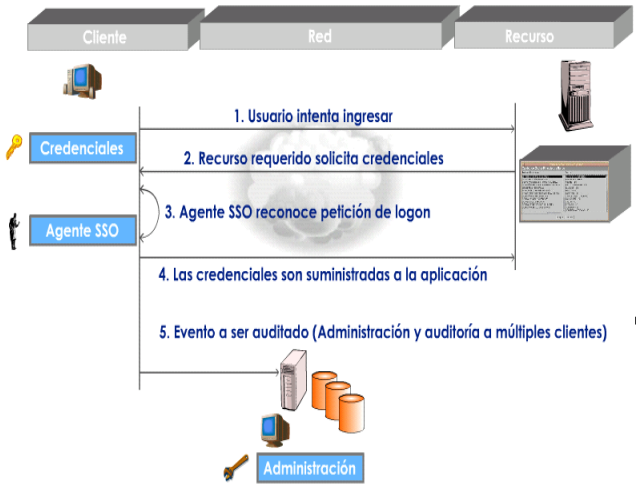


Figura 2: Arquitectura por administración centralizada con almacenamiento local de credenciales

(Elaboración del Autor)

Seguidamente las credenciales fueron 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.), se ingresa la información y se accede en el momento de ingreso, para esto de 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, esto pasa 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. Al final el servidor resulta ser una aplicación independiente que cuenta con un administrador diferente, ahora se cuenta con información que es almacenada en bases de datos comerciales o en directorios de manera encriptada.

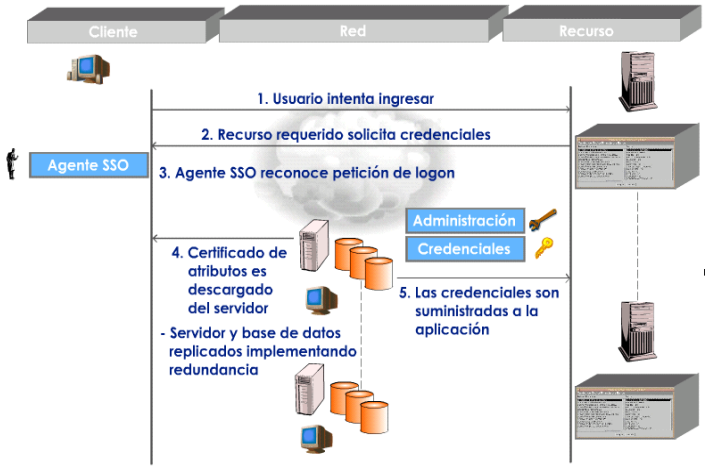


Figura 5: Arquitectura po administración y almacenamiento de credenciales centralizados garantizando alta disponibilidad y redundancia

(Caballero & Cano Martínez, 2003)

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.

Al finalizar 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.

Como técnica de recolección de datos se realizó el monitoreo, observación de campo, mediante instalación de cronómetros digitales en el computador de cada alumno, el cual media el tiempo de carga por cada página de lo logueo hacia el ingreso del sistema, aquí se tuvo como indicador la Reducción de tiempo de acceso a los servicios web, como sub indicador al Tiempo de acceso.

El desarrollo de este estudio fue apoyado con herramientas de medición de carga como google page speed, gt metrix y la Enterprise single sign-on (E-SSO) o Legacy Single Sign-On; esta herramienta utiliza una autenticación primaria para completar automáticamente las aplicaciones secundarias con el mismo usuario y contraseña.

RESULTADOS

La Universidad del Departamento de Lambayeque (UDPL), 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 UDPL, 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*

Es importante 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 UDPL, podemos definir claramente como usuarios a: los Docentes, Alumnos y Administrativos, que utilizan los diferentes servicios que ofrece la universidad.

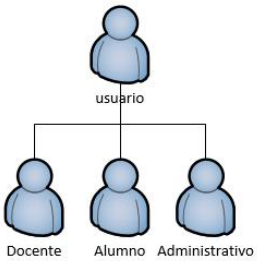


Figura 1: Tipos de Usuarios UDPL
(Elaboración del Autor)

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 UDPL cuenta con las siguientes cantidades de usuarios que se detalla a continuación:

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

La UDPL, 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	Adminis-trativo
1	Correo Institucional: <usuario>@UDPL.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

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 UDPL

N°	Aplicaciones/Servicios Web	Lenguaje de Programación	Gestor de Base de Datos
1	Correo Institucional: <usuario>@UDPL.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 UDPL.

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 UDPL; 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 UDPL.

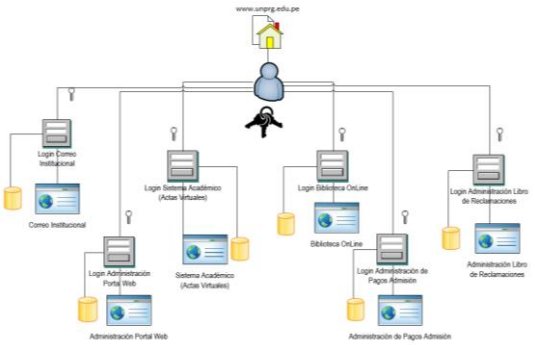


Figura 2: Proceso actual de autenticación para el acceso a los servicios web que brinda la UDPL (Elaboración del Autor)

Para el análisis e interpretación de los resultados, se identifica la variable dependiente "Optimizar el acceso a los servicios web de la UDPL" 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.

Índices:

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.*

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
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 UDPL; 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.

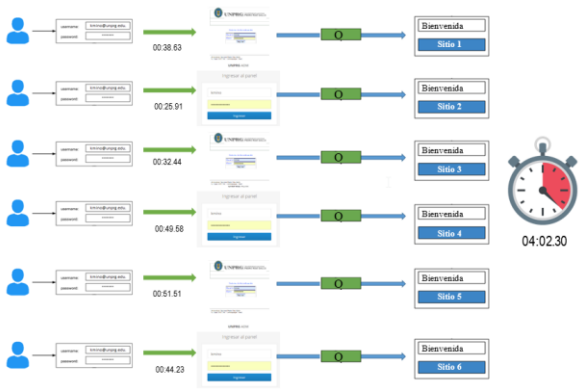


Figura 3: Diagrama de Análisis del Índice I1 para Prueba 1.
(Elaboración del Autor)

Análisis de Resultados Índice I2

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

Al igual que en el análisis de I1, Calculamos el tiempo promedio de acceso a todas las aplicaciones o servicios web de la UDPL; 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.

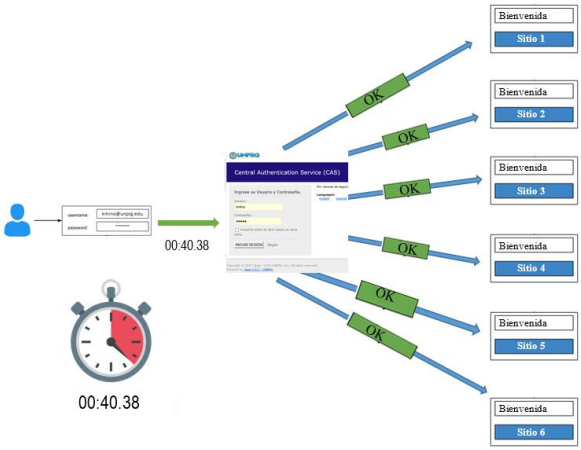


Figura 4: Diagrama de Análisis del Índice I2 para Prueba 1.

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**

DISCUSIONES

Roberto Crespo (2015), en su Estudio y Análisis de Factibilidad de la solución tipo Single Sign On para pequeñas empresas, tiene como objetivo Agilizar considerablemente los tiempos de acceso a varias aplicaciones por parte del usuario final, e implementa una solución de tipo Single Sign On, en PYMES de Guayaquil que cuenten con un portafolio de software y manejo de claves de acceso para cada una de ellas.

Su propuesta metodológica de su estudio se basó en la recolección de datos y diseñó una encuesta para el personal del área que maneja las cuentas de acceso a las diferentes aplicaciones. Así mismo su Población y muestra se detalla en el siguiente cuadro.

Sectores	Población	Muestra
Público y Privado	900	110
TOTAL	**900**	**110**

Elaboración: Marisol Alvarado
Fuente: Datos de la Investigación

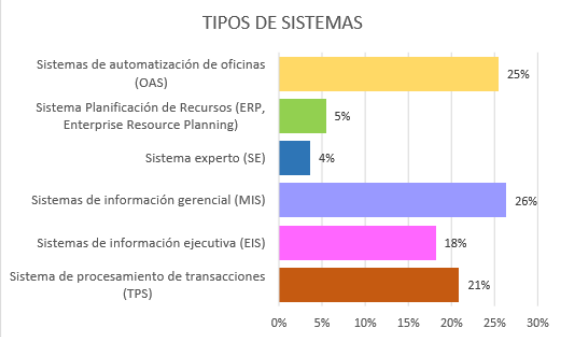
Se aplicaron las encuestas a las empresas que se muestran en el cuadro siguiente:

EMPRESAS CON MULTIPLES SISTEMAS DE INFORMACION	PROVINCIA
Armada del Ecuador	GUAYAS
Bassa CIA. Ltda.	GUAYAS

Elaboración: Marisol Alvarado
Fuente: Datos de la Investigación

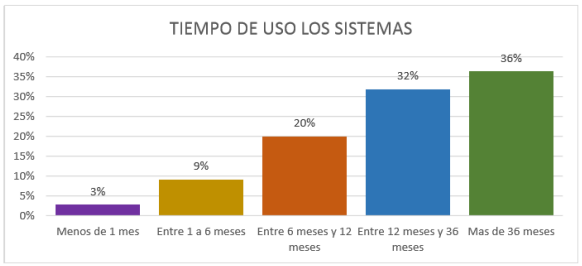
A continuación, Crespo, nos muestra su interpretación y análisis de resultados considerando la situación de los usuarios que utilizan los diferentes sistemas de información en su empresa.

Tipos de Sistemas que utiliza el encuestado:



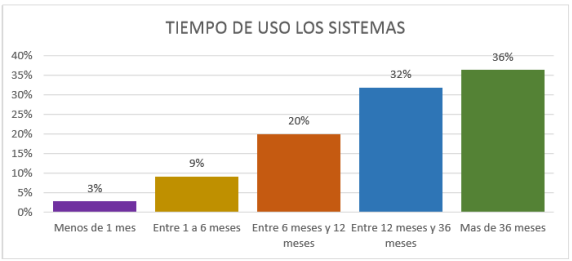
Elaboración: Marisol Alvarado
Fuente: Datos de la Investigación

Tiempo que lleva usando los sistemas de información el encuestado en la empresa



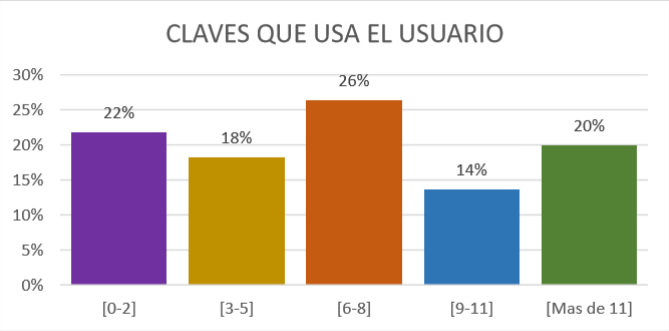
Elaboración: Marisol Alvarado
Fuente: Datos de la Investigación

Frecuencia de uso de los sistemas de información



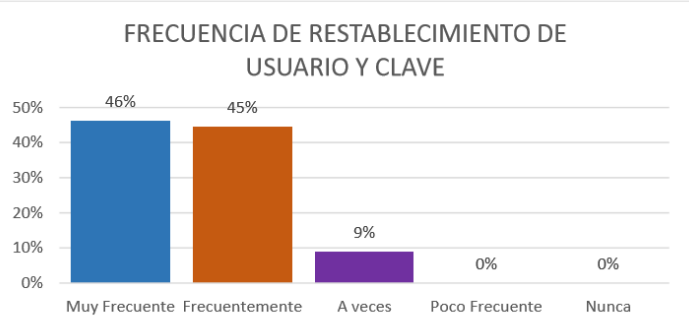
Elaboración: Marisol Alvarado
Fuente: Datos de la Investigación

Numero de claves que maneja el encuestado



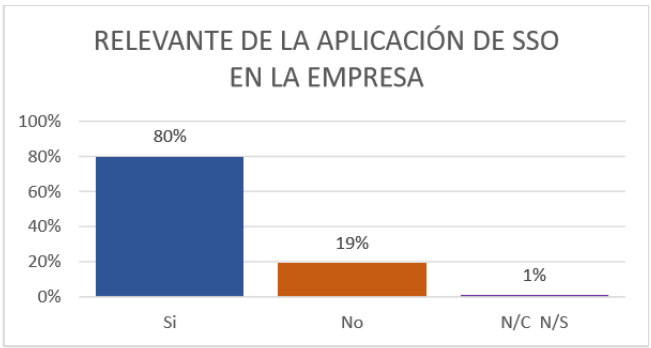
Elaboración: Marisol Alvarado
Fuente: Datos de la Investigación

Frecuencia de restablecer claves



Elaboración: Marisol Alvarado
Fuente: Datos de la Investigación

Considera el uso de una solución tipo Single Sign-On



Elaboración: Marisol Alvarado
Fuente: Datos de la Investigación

Crespo, basado en su estudio, nos muestra como resultados que la utilización de una solución Single Sign-On para las pequeñas y medianas empresas (PYMES), es muy beneficiosa al nivel tecnológico, operativo

y de costos. Por ello la implementación de la solución Single Sign-On adiciona algunos beneficios tales como:

Los resultados obtenidos de esta investigación, facilitarían en la toma de decisión sobre la utilización de una solución tipo Single Sign On para las pequeñas y medianas empresas (PYMES) teniendo en consideración el análisis de factibilidad que nos da como resultado que la solución Single Sign-On es bastante beneficiosa a nivel de tecnología, operatividad y costo. En este sentido la implementación de la solución tipo Single Sign-On sugiere algunos beneficios adicionales para las organizaciones como son: Disminución de la operatividad relacionada a la administración de contraseñas, control centralizado de autenticación para las aplicaciones corporativas, mayor comodidad y facilidad de uso de las aplicaciones corporativas para los usuarios finales, entre otras.

Al analizar las dos investigaciones en Single Sign-On nos damos cuenta que es una solución óptima para cualquier empresa u organización que cuente con diferentes aplicaciones y deseen optimizar tiempos de acceso a sus aplicaciones con un solo logueo; así mismo se incrementa el grado de satisfacción de los usuarios al tener el control de sus aplicaciones mediante un solo usuario y clave de acceso.

CONCLUSIONES

- La situación actual, en el proceso de autenticación para el acceso a los servicios web que brinda la UDPL, 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 UDPL.
- El mecanismo CAS, es el que cubre los mayores protocoles de comunicación para la integración de las aplicaciones en la UDPL.
- 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 UDPL, para el acceso a los servicios web.

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