Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

IMPLEMENTACIÓN DE LA PLATAFORMA DE AUTENTICACIÓN ÚNICA PARA SISTEMAS DE LA FACULTAD DE ARQUITECTURA, UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

Marco Antonio Zecaida Mijangos
Asesorado por el Ing. David Estuardo Morales Ajcot

Guatemala, enero de 2019

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

IMPLEMENTACIÓN DE LA PLATAFORMA DE AUTENTICACIÓN ÚNICA PARA SISTEMAS DE LA FACULTAD DE ARQUITECTURA, UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

MARCO ANTONIO ZECAIDA MIJANGOS
ASESORADO POR EL ING. DAVID ESTUARDO MORALES AJCOT

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN CIENCIAS Y SISTEMAS

GUATEMALA, ENERO DEL 2019

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Pedro Antonio Aguilar Polanco
VOCAL I	Ing. José Francisco Gómez Rivera
VOCAL II	Ing. Mario Renato Escobedo Martínez
VOCAL III	Ing. José Milton de León Bran
VOCAL IV	Br. Luis Diego Aguilar Ralón
VOCAL V	Br. Christian Daniel Estrada Santizo
SECRETARIA	Inga. Lesbia Magalí Herrera López

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Angel Roberto Sic García (a.i.)
EXAMINADORA	Inga. Floriza Felipa Ávila Pesquera
EXAMINADOR	Ing. Marlon Antonio Pérez Türk
EXAMINADOR	Ing. Sergio Leonel Gómez Bravo
SECRETARIA	Inga. Lesbia Magalí Herrera López

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

IMPLEMENTACIÓN DE LA PLATAFORMA DE AUTENTICACIÓN ÚNICA PARA SISTEMAS DE LA FACULTAD DE ARQUITECTURA, UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería en Ciencias y Sistemas, con fecha 22 de agosto de 2017.

Marco Antonio Zecaida Mijangos

Guatemala, 10 de Octubre de 2018

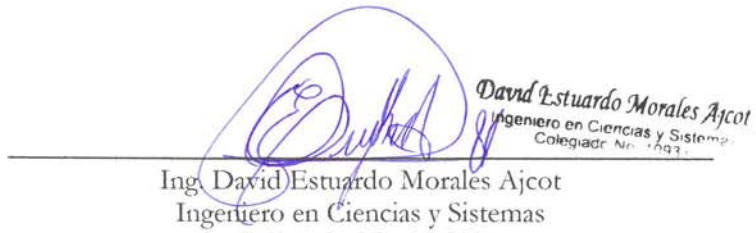
Inga. Christa del Rosario Classon de Pinto
Directora de la Unidad de EPS
Facultad de Ingeniería
Universidad de San Carlos de Guatemala

Ingeniera Christa del Rosario Classon de Pinto:

Hago de su conocimiento que he supervisado y doy por finalizado el desarrollo del Informe final del trabajo de EPS titulado **"IMPLEMENTACIÓN DE LA PLATAFORMA DE AUTENTICACIÓN ÚNICA PARA SISTEMAS DE LA FACULTAD DE ARQUITECTURA, UNIVERSIDAD DE SAN CARLOS DE GUATEMALA"**, el cual estuvo a cargo del estudiante de la carrera de Ingeniería en Ciencias y Sistemas **Marco Antonio Zecaida Mijangos**, identificado con el CUI **2325183510101** y con el de registro académico **200412604**, desarrollado en la unidad de informática y control académico de la facultad de arquitectura de la Universidad de San Carlos de Guatemala, durante el periodo de tiempo de 22 de agosto de 2017 al 22 de febrero de 2018.

Agradeciendo la atención a la presente y quedando a sus órdenes para cualquier información adicional.

Atentamente,



Ing. David Estuardo Morales Ajcot
Ingeniero en Ciencias y Sistemas
Colegiado No. 10,933
Teléfono: 5018-4010

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÍA

UNIDAD DE EPS

Guatemala, 12 de octubre de 2018.
REF.EPS.DOC.814.10.2018.

Inga. Christa Classon de Pinto
Directora Unidad de EPS
Facultad de Ingeniería
Presente

Estimada Ingeniera Classon de Pinto:

Por este medio atentamente le informo que como Supervisora de la Práctica del Ejercicio Profesional Supervisado, (E.P.S) del estudiante universitario de la Carrera de Ingeniería en Ciencias y Sistemas, **Marco Antonio Zecaida Mijangos, Registro Académico 200412604 y CUI 2325 18351 0101** procedí a revisar el informe final, cuyo título es **IMPLEMENTACIÓN DE LA PLATAFORMA DE AUTENTICACIÓN ÚNICA PARA SISTEMAS DE LA FACULTAD DE ARQUITECTURA, UNIVERSIDAD DE SAN CARLOS DE GUATEMALA..**

En tal virtud, **LO DOY POR APROBADO**, solicitándole darle el trámite respectivo.

Sin otro particular, me es grato suscribirme.

Atentamente,

"Id y Enseñad a Todos"

Universidad de San Carlos de Guatemala
Inga. Floriza Ávila Pesquera de Medinilla
ASESORA - SUPERVISORA DE EPS
Unidad de Prácticas de Ingeniería y EPS
Facultad de Ingeniería

Inga. Floriza Felipa Ávila Pesquera de Medinilla
Supervisora de EPS
Área de Ingeniería en Ciencias y Sistemas

FFAPdM/RA

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÍA

UNIDAD DE EPS

Guatemala, 12 de octubre de 2018.
REF.EPS.D.395.10.2018.

Ing. Marlon Antonio Pérez Turk
Director Escuela de Ingeniería Ciencias y Sistemas
Facultad de Ingeniería
Presente

Estimado Ingeniero Pérez Türk:

Por este medio atentamente le envío el informe final correspondiente a la práctica del Ejercicio Profesional Supervisado, (E.P.S) titulado **IMPLEMENTACIÓN DE LA PLATAFORMA DE AUTENTICACIÓN ÚNICA PARA SISTEMAS DE LA FACULTAD DE ARQUITECTURA, UNIVERSIDAD DE SAN CARLOS DE GUATEMALA.,** que fue desarrollado por el estudiante universitario **Marco Antonio Zecaida Mijangos, Registro Académico 200412604 y CUI 2325 18351 0101** quien fue debidamente asesorado por el Ing. David Estuardo Morales Ajcor y supervisado por la Inga. Floriza Felipa Ávila Pesquera de Medinilla.

Por lo que habiendo cumplido con los objetivos y requisitos de ley del referido trabajo y existiendo la aprobación del mismo por parte del Asesor y la Supervisora de EPS, en mi calidad de Director apruebo su contenido solicitándole darle el trámite respectivo.

Sin otro particular, me es grato suscribirme.

Atentamente,
"Id y Enseñad a Todos"

Inga. Christa Classon de Pinto
Directora Unidad de EPS

Universidad de San Carlos de Guatemala
DIRECCIÓN
Unidad de Prácticas de Ingeniería y EPS
Facultad de Ingeniería

CCsP/ra

Universidad San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, 24 de octubre de 2018

Ingeniero
Marlon Antonio Pérez Türk
Director de la Escuela de Ingeniería
En Ciencias y Sistemas

Respetable Ingeniero Pérez:

Por este medio hago de su conocimiento que he revisado el trabajo de graduación-EPS del estudiante **MARCO ANTONIO ZECAIDA MIJANGOS** carné **200412604** y **CUI 2325 18351 0101,** titulado: **"IMPLEMENTACIÓN DE LA PLATAFORMA DE AUTENTICACIÓN ÚNICA PARA SISTEMAS DE LA FACULTAD DE ARQUITECTURA, UNIVERSIDAD DE SAN CARLOS DE GUATEMALA"** y a mi criterio el mismo cumple con los objetivos propuestos para su desarrollo, según el protocolo.

Al agradecer su atención a la presente, aprovecho la oportunidad para suscribirme,

Atentamente,

Ing. Carlos Alfredo Azurdia
Coordinador de Privados
y Revisión de Trabajos de Graduación

ESCUELA DE INGENIERÍA EN CIENCIAS Y SISTEMAS

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÌA
ESCUELA DE INGENIERÍA EN
CIENCIAS Y SISTEMAS
TEL: 24188000 Ext. 1534

El Director de la Escuela de Ingeniería en Ciencias y Sistemas de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del asesor con el visto bueno del revisor y del Licenciado en Letras, del trabajo de graduación, ***"IMPLEMENTACIÓN DE LA PLATAFORMA DE AUTENTICACIÓN ÚNICA PARA SISTEMAS DE LA FACULTAD DE ARQUITECTURA, UNIVERSIDAD DE SAN CARLOS DE GUATEMALA"*** *realizado por el estudiante, MARCO ANTONIO ZECAIDA MIJANGOS, aprueba el presente trabajo y solicita la autorización del mismo.*

"ID Y ENSEÑAD A TODOS"

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION DE INGENIERIA EN CIENCIAS Y SISTEMAS

Ing. Marlon Antonio Pérez Türk
Director
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, 23 de enero de 2019

Universidad de San Carlos
De Guatemala

Facultad de Ingeniería
Decanato

Ref. DTG.19.2019

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería en Ciencias y Sistemas del trabajo de graduación titulado: **"IMPLEMENTACIÓN DE LA PLATAFORMA DE AUTENTICACIÓN ÚNICA PARA SISTEMAS DE LA FACULTAD DE ARQUITECTURA, UNIVERSIDAD DE SAN CARLOS DE GUATEMALA"** presentado por el estudiante universitario: **Marco Antonio Zecaida Mijangos** y después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, se autoriza la impresión del mismo.

IMPRÍMASE.

Ing. Pedro Antonio Aguilar Polanco
Decano

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANO
FACULTAD DE INGENIERIA

Guatemala, Enero de 2019

/echm

ACTO QUE DEDICO A:

Dios Por estar en lo pequeño y en lo grande, en cada paso que di desde el principio hasta el final. Por ser la luz que iluminó mí camino en los momentos difíciles y por permitirme terminar el día de hoy un ciclo importante en mi vida.

Mis padres Por el apoyo que me brindaron desde el primer día de escuela. Por siempre velar por mí desde un aspecto integral. Porque siempre han sido el apoyo que necesito en las buenas y en las malas.

Mi hermana Por llenar de alegría mi vida, por ser esa hada colocha y divertida que Dios me regaló.

Mi abuelita Por ser siempre la persona que en silencio me apoyó y sufrió conmigo. Porque en los momentos difíciles su cariño y amor han sido de fortaleza.

Mis amigos Porque junto a ellos pase momentos muy felices y también de muchos sacrificios. Porque me demostraron: que en los momentos difíciles una sonrisa puede cambiar tu día y que en la adversidad se moldean las buenas amistades.

AGRADECIMIENTOS A:

Universidad de San Carlos de Guatemala	Por ser mi casa de estudios a la cual me llena de orgullo pertenecer por su prestigio y porque me ha enseñado a luchar por mis sueños.
Facultad de Ingeniería	Por ser la facultad que me mostró las maravillas que existen a nivel profesional y me enseñó a explorar mis capacidades.
Facultad de Arquitectura	Por facilitarme las herramientas que me permitieron llevar a cabo mi trabajo de graduación.
Compañeros y amigos de Centro de Cálculo e Investigación Educativa	Por ser maestros y amigos, por ser apoyo importante en la última parte de la carrera.
Ing. David Estuardo Morales Ajcot	Por su respaldo y acompañamiento en el desarrollo de mi trabajo de graduación, por ser guía, ejemplo y buen amigo.
Rosita Azucena del Cid	Por su cariño y apoyo en mi carrera, por escucharme y alentarme.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES VII
LISTA DE SÍMBOLOS IX
GLOSARIO XI
RESUMEN XV
OBJETIVOS XVII
INTRODUCCIÓN XIX

1. FASE DE INVESTIGACIÓN 1
1.1. Antecedentes de la empresa 1
1.1.1. Reseña histórica 2
1.1.2. Misión 2
1.1.3. Visión 3
1.1.4. Servicios que realiza 3
1.2. Descripción de las necesidades 3
1.2.1. Por parte del personal de informática de Control Académico 4
1.2.1.1. Reducir el uso de credenciales distintas para un mismo individuo 4
1.2.1.2. Recuperación de contraseña 4
1.2.1.3. Promover el correo institucional 4
1.2.2. Por parte del usuario final 5
1.2.2.1. Integrar la autenticación de los sistemas 5
1.3. Priorización de las necesidades 5

2. FASE TÉCNICO PROFESIONAL 7
2.1. Descripción del proyecto 7
2.1.1. Funcionamiento de la plataforma 7
2.1.1.1. Funciones para el usuario final 8
2.1.1.2. Funciones para el usuario administrador de la plataforma 11
2.1.1.3. Funciones para el arquitecto de software 15
2.2. Investigación preliminar para la solución del proyecto 17
2.2.1. Conocimientos básicos sobre sistemas de autenticación única 17
2.2.1.1. Autenticación 17
2.2.1.2. Autorización 18
2.2.2. Herramientas a utilizar 18
2.2.2.1. Servidor SSO OpenAM 19
2.2.2.2. OpenAM Web Policy Agents 19
2.2.2.3. Servidor LDAP OpenDJ 20
2.2.2.4. Talend Open Studio Integration for data Integration 20
2.2.2.5. HAProxy 21
2.3. Presentación de la solución al proyecto 21
2.3.1. Arquitectura de la plataforma 21
2.3.1.1. Servidores LDAP 22
2.3.1.1.1. Replicación de la información 23
2.3.1.2. Servidores de autenticación 23
2.3.1.3. Proxy 23
2.3.1.3.1. Balanceo de carga 23
2.3.1.4. Sistemas externos 24

2.3.1.5. Usuario 24
2.3.2. Desarrollo de la solución 24
2.3.2.1. Configuración inicial de los servidores 25
2.3.2.1.1. Configuración genérica de los servidores 26
2.3.2.1.2. Servidores con protocolo LDAP 26
2.3.2.1.3. Instalación de servidores SSO 26
2.3.2.1.4. Instalación Haproxy 27
2.3.2.2. Proceso de Extracción, Transformación y Carga (ETL) 27
2.3.2.2.1. Definición inicial 28
2.3.2.2.2. Extracción de la información 28
2.3.2.2.3. Puesta en marcha 29
2.3.2.3. Configuración de la herramienta OpenAM 30
2.3.2.3.1. Instalación y configuración inicial de la herramienta 30
2.3.2.3.2. Modificación y personalización de la interfaz 31
2.3.2.3.3. Configuración del proxy 31
2.3.2.4. Integración de sistemas 32

2.3.2.4.1. Integración sistema de docentes.....32
2.3.2.4.2. Integración de G Suite al SSO.....32
2.3.2.5. Interfaz de cambio de contraseña 33
2.3.2.6. Puesta en producción de la plataforma de autenticación 33
2.3.3. Funcionamiento de la interfaz de autenticación 34
2.4. Costos del proyecto.....36
2.4.1. Cálculo de costos en recurso humano 36
2.4.2. Cálculo de costos en equipo 37
2.4.3. Cálculo total de costos 38
2.5. Beneficios del proyecto 38
2.5.1. Beneficios para el usuario final.....39
2.5.2. Beneficios del administrador de la plataforma.....39
2.5.3. Beneficio del arquitecto 40

3. FASE DE ENSEÑANZA Y APRENDIZAJE.....41
3.1. Capacitación 41
3.1.1. Carga de usuarios 41
3.1.2. Configuraciones habituales al sistema 42
3.1.3. Configuraciones de integración 42
3.2. Material elaborado.....42
3.2.1. Manual de usuario.....42
3.2.2. Manual técnico 43

CONCLUSIONES.....45
RECOMENDACIONES 47
BIBLIOGRAFÍA.....49

APÉNDICES 51

ÍNDICE DE ILUSTRACIONES

FIGURAS

1. CDU usuario final 8
2. CDU usuario administrador 11
3. CDU arquitecto de software 15
4. Arquitectura, plataforma de autenticación única 22
5. Flujo configuración de servidores 25
6. Modelo de extracción de datos 27
7. Flujo configuraciones herramienta OpenAM 30
8. Interfaz personalizada 31
9. Flujo integración sistema de docentes 32
10. Flujo integración con G Suite 33
11. Detalle del funcionamiento, plataforma de autenticación única 35

TABLAS

I. Autenticarse en sistema integrado 9
II. Interfaz de cambio de contraseña 10
III. Carga de datos servidor LDAP 12
IV. Actualización de ETL 13
V. Cambios en la configuración de la plataforma 14
VI. Integración de nuevos sistemas a la plataforma 16
VII. Costo recurso humano, desarrollo de SSO 37
VIII. Costo de equipo, desarrollo de SSO 38
IX. Costos totales, desarrollo de SSO 38

LISTA DE SÍMBOLOS

Símbolo	Significado
Q	Quetzales

GLOSARIO

Ambiente	Comprende hardware, software y configuraciones necesarias para hacer funcionar un sistema.
Ambiente de desarrollo	Es un marco de trabajo que es de preparación y comprende la etapa de elaboración del producto a construir.
Autenticación	Es la acción a través de la cual, un usuario por medio de sus credenciales valida que tenga acceso al sistema.
ETL	Extract, transform and load, en español significa extraer, transformar y cargar, es un proceso que consiste en cargar información de distintas fuentes, para luego transformarla y enviarla a una nueva fuente de datos.
ForgeRock	Es una empresa estadounidense que desarrolla software para la gestión de acceso e identidad.
Google	Es una de las empresas más cotizadas en el actual mundo tecnológico y se especializa en servicios y productos relacionados a internet, software y recursos electrónicos.

G Suite	Es un servicio de Google que proporciona grupos de cuentas de correo y aplicaciones asociadas a cada usuario, relacionado con un dominio personalizado por el cliente.
LDAP	Lightweight Directory Access Protocol, en español Protocolo Ligero/Simplificado de Acceso a Directorios, es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red.
LDAPv3	Es la versión del protocolo, LDAP que se encuentra en funciones en el año 2018.
Licencia Común de Desarrollo y Distribución (CDDL)	Licencia de código abierto y libre. Los ficheros de este tipo de licencia pueden ser combinados con licencias de otro tipo.
Open Identity Platform Community	Es una comunidad que se encarga de la distribución del software para administración de acceso e identidades con distribución de Licencia Común de Desarrollo y Distribución.

Servidor	Es una aplicación en ejecución (software) capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia.
SSO	Es un procedimiento de autenticación que habilita al usuario para acceder a varios sistemas con una sola instancia de identificación.
Sun Microsystems	Empresa informática dedicada a vender estaciones de trabajo, servidores, componentes informáticos, software y servicios informáticos adquiridas por Oracle Corporation en el año 2010.
Virtualización	Es una técnica que permite ejecutar y desplegar múltiples sistemas operativos en un mismo servidor físico.

RESUMEN

El presente informe describe la implementación de una plataforma de autenticación única, que permita al departamento de informática de la Facultad de Arquitectura, centralizar la autenticación de los sistemas que tiene a su cargo. Dicho desarrollo contempla la integración del sistema de docentes y el sistema de correo institucional que provee la herramienta G Suite de Google, como guía para la integración de nuevos sistemas.

Para la integración de usuarios al sistema, se crearon procesos que permitan realizar la carga de estos a través de la extracción y trasformación de datos de distintas fuentes.

La plataforma de autenticación única le brindará al usuario final una interfaz de autenticación amigable, que le permita consolidar las contraseñas de las aplicaciones que utiliza actualmente y que están integradas a dicha plataforma.

OBJETIVOS

General

Establecer las bases de una plataforma de autenticación única, en la que se puedan legitimar todos los usuarios que tienen acceso a los diferentes sistemas de la Facultad de Arquitectura.

Específicos

1. Facilitar una arquitectura informática, que permita balanceo de carga y que contemple el crecimiento de la misma.

2. Presentar al usuario un entorno amigable e intuitivo, en el que se le permita manejar mediante un solo usuario, la entrada a todos los sistemas que le brinda la Facultad de Arquitectura.

3. Proveer al usuario, seguridad en el proceso de autenticación y uso de los sistemas.

4. Integrar diferentes sistemas, a través, de una plataforma de autenticación única, brindando las herramientas para la escalabilidad de la plataforma, de forma que facilite la integración de los mismos.

INTRODUCCIÓN

A medida que la tecnología avanza, las instituciones educativas tienen en sus manos la oportunidad de progreso. La oportunidad de cambio, se ve limitada en ocasiones por la falta de recursos económicos para adquirir recurso humano y tecnológico. Es por esa razón, que la Facultad de Ingeniería en conjunto con la Escuela de Ciencias y Sistemas, desarrolla por medio del Ejercicio Profesional Supervisado (EPS), programas que brindan a las instituciones personal capacitado, para el desarrollo de herramientas tecnológicas según la necesidad de cada institución.

La Facultad de Arquitectura conociendo sus limitaciones hace uso de este tipo de proyectos, para la mejora integral de las distintas unidades que la conforman. Debido al creciente número de aplicaciones que tiene a su cargo la unidad de informática, planifica la implementación de una herramienta que integre cada una de ellas y les brinde a los usuarios una mejor experiencia en el uso de sus aplicaciones, para beneficio tanto de estudiantes, docentes como del personal administrativo. En virtud, de esta planificación surge la implementación de una plataforma de autenticación única.

A medida, que la unidad de informática ha crecido, se han desarrollado sistemas que automatizan la gran mayoría de los procesos, que dicha unidad tiene a su cargo. Derivado del aumento en la tecnología, los usuarios, que tienen diariamente que acceder a más de un sistema, se ven en la tediosa tarea de realizar varias veces una autenticación y memorizar más de una contraseña.

Como solución a esta necesidad, se plantea el desarrollo de una plataforma, que le permita a la unidad de informática, brindarle al usuario final un sistema de autenticación integrado, en el que pueda hacer un solo ingreso por medio de una única contraseña.

El presente proyecto, brindará las bases de dicha plataforma, siendo esta implementada, bajo un sistema de autenticación único (SSO), progresivo cuya finalidad será integrar el sistema orientado a docentes y al correo institucional, permitiendo la escalabilidad para que la unidad informática siga integrando más sistemas según sea su prioridad.

1. FASE DE INVESTIGACIÓN

Durante esta fase, se identificó un proyecto que calificara como Ejercicio Profesional Supervisado (EPS), tomando en cuenta características, como el tiempo estimado, conceptos evaluados en el desarrollo, técnicas a utilizar entre otros.

La Facultad de Arquitectura identificó, una problemática dentro de los procesos de ingreso a los sistemas que tienen a su cargo. Se planteó una solución a la medida sobre la base de los recursos disponibles. Dicho planteamiento, fue evaluado por la unidad de EPS quien, determinó que el proyecto era viable y cumplía con los requisitos necesarios para realizar un proyecto de seis meses.

1.1. Antecedentes de la empresa

"La Facultad de Arquitectura busca formar profesionales de alto nivel académico en el campo de la arquitectura, diseño gráfico y otras especialidades en ramas afines, orientadas a atender con calidad, eficiencia, eficacia y pertinencia, las demandas de la sociedad guatemalteca"[1].

La Unidad de Informática y Control Académico de la Facultad de Arquitectura, tiene a su cargo la administración de varias aplicaciones, algunas propias de control académico y otras para manejo de las distintas unidades que forman parte de la administración de la Facultad.

[1] Unidad de Divulgación. Facultad de Arquitectura. *Bosquejo histórico*. https://farusac.edu.gt/administracion/. Consulta: septiembre de 2018.

1.1.1. Reseña histórica

El primer Decano Interino de la Facultad fue el Arquitecto Roberto Aycinena Echeverría, convirtiéndose pocos años después en el primer Decano electo.

Fue a partir de 1971 que la Facultad cuenta con edificio propio, el actual edificio T-2. En 1972 se inicia un movimiento transformador en la enseñanza en la Facultad de Arquitectura, dando como resultado el Congreso de Reestructuración de Arquitectura -CRA- el 10 de Mayo de 1972. A partir del CRA el pensum tuvo un enfoque social humanístico, el cual fue adecuado luego de la experiencia del Terremoto de 1976. A partir del 1982, el pensum tuvo un enfoque tecnológico.

En 1987, en la administración del Arq. Eduardo Aguirre Cantero, se inicia el programa de Técnico en Diseño Gráfico, la carrera tuvo éxito rápidamente, el que se evidencio a través del posicionamiento laboral de sus primeros egresados.

En 1994 se realiza una readecuación sistematizada del Pensum de la carrera de Arquitectura, planteada como un trabajo integral y científico, creándose el pensum de estudios para la cohorte 1995-2000, aprobado por el Consejo Superior Universitario 18 de noviembre de 1994.

En 1998 se lleva a cabo una nueva propuesta de readecuación de la Licenciatura en Arquitectura, aprobada el 2 de Mayo de 2002 por Junta Directiva de la Facultad, iniciando su implementación en el año 2003.[2]

La Unidad de Control Académico, inició con el objetivo de atender las tareas correspondientes a la atención de estudiantes y personal docente. Conforme dicha unidad fue evolucionando, se incorporó personal de informática, este administra sistemas de Control Académico y sistemas que automatizan procesos de otras unidades.

1.1.2. Misión

En la Unidad Académica, de la Universidad de San Carlos de Guatemala, responsable de ordenar y producir conocimientos, formar profesionales creativos en el campo de la arquitectura y el diseño visual, con principios éticos, comprometidos y competentes, con especialidades para proponer soluciones para resolver los problemas de la sociedad en su ámbito; desempeñándose en el campo

[2] Unidad de Divulgación. Facultad de Arquitectura. *Bosquejo histórico*. https://farusac.edu.gt/administracion/bosquejo-historico/. Consulta: septiembre de 2018.

laboral con excelencia y disciplina por el bien de la cultura y el mejoramiento de planificación, organización, desarrollo espacial y comunicación visual[3].

1.1.3. Visión

Ser la institución líder en la formación de profesionales creativos y éticos en los campos de arquitectura, el diseño visual, especialidades y otros que demande la sociedad guatemalteca. Con programas académicos acreditados internacionalmente por su actualización, calidad y excelencia. Con capacidad de proponer soluciones para los problemas nacionales dentro de su ámbito y brindar una respuesta eficaz a los requerimientos del mercado laboral. Con un gobierno democrático, una administración efectiva y con capacidad de gestión y condiciones adecuadas de infraestructura, financiamiento y recursos tecnológicos[4].

1.1.4. Servicios que realiza

Contribuye con el desarrollo científico y social-humanístico del país en el área de la arquitectura y diseño gráfico, por medio de sus programas de docencia, investigación y extensión, en función de las características del medio y oportunidades y necesidades sociales. Contribuir en la solución de los problemas y necesidades de la sociedad guatemalteca en el ámbito de la arquitectura y el diseño gráfico[5].

1.2. Descripción de las necesidades

Dentro de las necesidades identificadas en la unidad al momento de la toma de requerimiento, se pueden detallar las siguientes:

[3] Unidad de Divulgación. Facultad de Arquitectura. Administración. https://farusac.edu.gt/administracion/. Consulta: septiembre de 2018.

[4] Unidad de Divulgación, Facultad de Arquitectura. *Bosquejo histórico*. https://farusac.edu.gt/administracion/. Consulta: septiembre de 2018.

[5] Op. cit.

1.2.1. Por parte del personal de informática de Control Académico

En entrevista con el personal de informática de control académico fueron recopiladas la siguiente lista de necesidades:

1.2.1.1. Reducir el uso de credenciales distintas para un mismo individuo

La Facultad de Arquitectura está en constante crecimiento informático, en los últimos semestres se ha solicitado al menos un practicante a la unidad de EPS de la Facultad de Ingeniería, y se han elaborado nuevas aplicaciones, se han integrado más usuarios y por lo mismo se han presentado más casos en que usuarios pierden u olvidan sus contraseñas. Es necesario simplificar el manejo de credenciales, para que el usuario final pueda mantener una contraseña segura en lugar de varias contraseñas con bajo nivel de seguridad.

1.2.1.2. Recuperación de contraseña

En la actualidad, la Facultad no cuenta con una funcionalidad que le permita recuperar la contraseña a ningún usuario, esto hace que el usuario, deba dirigirse a la unidad de informática a solicitar dicho cambio de forma presencial.

1.2.1.3. Promover el correo institucional

La Facultad de Arquitectura les brinda a todos los estudiantes un correo electrónico, vinculado a su número de carnet. De momento no ha sido

promocionado adecuadamente, lo cual hace que el estudiante desaproveche este recurso.

1.2.2. Por parte del usuario final

El usuario final que hace uso de los sistemas de la facultad de arquitectura presenta las siguientes necesidades:

1.2.2.1. Integrar la autenticación de los sistemas

Se ha visto la necesidad de contar con un único usuario y contraseña, porque conforme se han activado nuevos sistemas, los usuarios han tenido que utilizar una credencial diferente para cada uno, haciendo obligatorio primero: identificar qué sistema utilizará y luego identificar que usuario y contraseña le corresponde.

1.3. Priorización de las necesidades

Mediante el desarrollo de los recursos tecnológicos, la Facultad de Arquitectura, se ha hecho de un mayor número de sistemas que tienen a su cargo distintos tipos de tareas según su naturaleza. Las credenciales varían respecto a cada sistema y esto genera al usuario dificultades para manejar sus accesos. Se suma a esto, que las aplicaciones no tienen un manejo apropiado de sus usuarios.

Dada esta problemática la Unidad de Informática, ve necesario disponer de una plataforma de autenticación única, que permita el ingreso a través de una misma interfaz, de la que puedan hacer uso los sistemas que tienen a su cargo.

Como parte de los objetivos de mejora en el servicio a los usuarios que hacen uso de los distintos sistemas de la Facultad, se considera la integración de una plataforma de autenticación, esta consiste en proveer a los estudiantes, docentes y personal administrativo un acceso unificado para el ingreso a los diversos sistemas. Este acceso unificado será implementado a través de un Sistema de Autenticación Reducida (SSO, por sus siglas en inglés), que deberá proveer el servicio de autenticación integral.

La implementación, que satisfaga la problemática deberá considerar la configuración de un sistema de autenticación única, que integre a los usuarios que hacen uso tanto de la plataforma de docentes como del correo institucional.

2. FASE TÉCNICO PROFESIONAL

En el desarrollo de esta fase se indicarán los aspectos importantes que fueron tomados en cuenta para la implementación de la plataforma, y la descripción de las actividades que fueron realizadas durante la ejecución del proyecto.

2.1. Descripción del proyecto

Una plataforma de autenticación única, es un sistema complejo que comprende tanto aspectos de arquitectura de software, como desarrollo y comunicación. El proyecto consiste en el desarrollo de esta plataforma para que permita al usuario, autenticarse de forma centralizada y segura a las aplicaciones que se encuentran bajo la administración de la Unidad de Informática de la Facultad de Arquitectura.

El proceso de autenticación en las aplicaciones integradas será realizado ahora por la plataforma SSO, que proveerá los servicios de autenticación de usuario, gestión de sesiones y administración general de los usuarios.

2.1.1. Funcionamiento de la plataforma

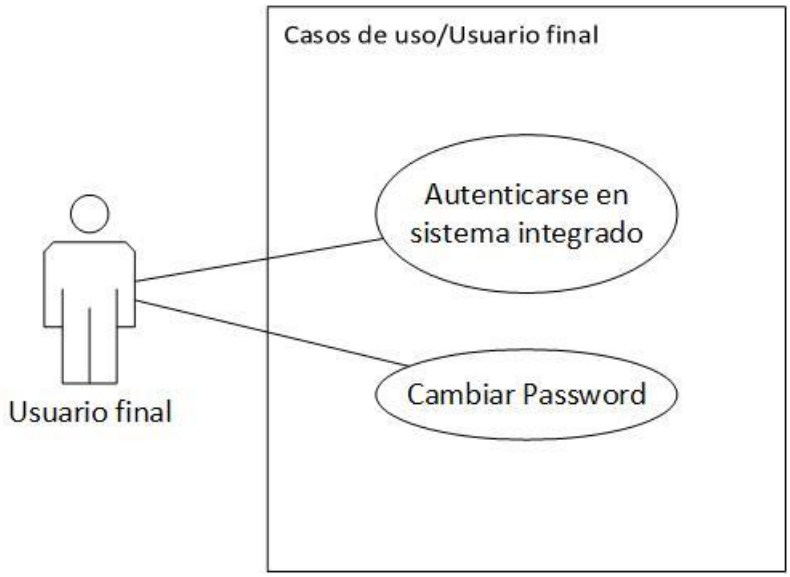
A continuación se describe a través de casos de uso, el funcionamiento de la plataforma desde la perspectiva de 3 tipos de usuarios:

- Usuario final
- Administrador de la plataforma
- Arquitecto de software

2.1.1.1. Funciones para el usuario final

Describe las actividades propias del funcionamiento de la plataforma orientada al usuario final, como lo es el ingreso a los sistemas y el cambio de contraseña por parte de los usuarios, como se describe en el siguiente caso de uso:

Figura 1. **CDU usuario final**



Fuente: elaboración propia, empleando Microsoft Visio 2013.

Tabla I. **Autenticarse en sistema integrado**

Código	Caso de Uso – 01
Nombre	Autenticarse en sistema integrado
Objetivo	El usuario se podrá autenticar a un sistema integrado en la plataforma de autenticación única.
Descripción	El usuario ingresa a su sistema por medio de un fácil y efectivo acceso.
Actores	Usuario final
Condiciones necesarias	• El usuario debe de tener acceso al sistema. • La aplicación en la que se quiere autenticar debe de estar integrada a la plataforma de autenticación única.
Escenario principal	1. El usuario ingresa en su explorador el link del sistema que quiere utilizar. 2. El sistema lo redirige hacia la plataforma de autenticación única. 3. El usuario ingresa sus credenciales. 4. Sí las credenciales son correctas la plataforma le permite el ingreso al sistema.
Escenario de excepción	4.a. Sí las credenciales del usuario son incorrectas el sistemas solicita al usuario que ingrese de nuevo su información.

Fuente: elaboración propia.

Tabla II. **Interfaz de cambio de contraseña**

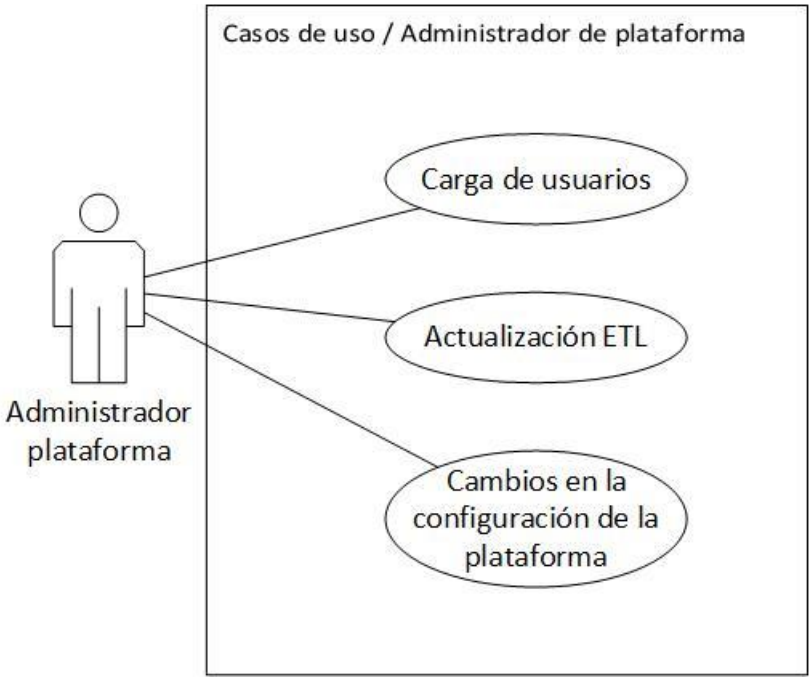
Código	Caso de Uso – 02
Nombre	Interfaz de Cambio de contraseña
Objetivo	Cambiar contraseña de usuario para acceder al sistema.
Descripción	El usuario cambia su contraseña a través de la plataforma de autenticación única.
Actores	Usuario final
Condiciones necesarias	• El usuario debe de tener acceso al sistema • El usuario debe de tener actualizado su correo electrónico personal, para poder realizar el cambio de contraseña.
Escenario principal	1. El usuario accede a la interfaz de autenticación única. 2. El usuario accede a la opción de recuperación de contraseña. 3. El sistema solicita al usuario que ingrese su CUI. 4. El sistema le envía al usuario un correo electrónico para restablecer su contraseña. 5. El correo electrónico redirige al usuario a la interfaz de cambio de contraseña. 6. El usuario ingresa su nueva contraseña y la confirma.
Escenario de excepción	1.a. Sí el sistema no reconoce al usuario le informará que su usuario no es válido.

Fuente: elaboración propia.

2.1.1.2. Funciones para el usuario administrador de la plataforma

Son las funciones que tiene a cargo el usuario que administra el sistema en producción. Este usuario consta con los permisos en los sistemas que administra la plataforma, y debe administrar, configurar y monitorear el correcto funcionamiento de la misma.

Figura 2. **CDU usuario administrador**



Fuente: elaboración propia, empleando Microsoft Visio 2013.

Tabla III. **Carga de datos servidor LDAP**

Código	Caso de Uso – 03
Nombre	**Carga de Usuarios**
Objetivo	Cargar el servidor LDAP de la plataforma de autenticación única con información actualizada de usuarios.
Descripción	El usuario de administrador debe de cargar los usuarios a través del sistema de ETL. TALEND Open Studio for Data Integration.
Actores	Usuario administrador de plataforma
Condiciones necesarias	• El usuario debe de tener acceso al Sistema para carga de información. • La nueva información debe de encontrarse en las base de datos correspondientes.
Escenario principal	1. El usuario comprueba que la información nueva debe de estar en la base de datos. 2. El usuario ejecuta el proceso de extracción, transformación y carga de la información. 3. El sistema debe realizar la extracción de la información hacia la base de datos relacional que consolida la información de todos los usuarios. 4. El sistema extrae nuevamente la información, la carga en el servidor LDAP. 5. El usuario verifica que la carga se haya realizado exitosamente.

Continuación de tabla III.

Escenario de excepción	1.a. Sí el usuario identifica que la información no está actualizada en la base de datos correspondiente; debe realizar la carga de dicha información. 5.a. Sí el sistema no carga la información de manera adecuada, debe proceder al mantenimiento del ETL.

Fuente: elaboración propia.

Tabla IV. **Actualización de ETL**

Código	Caso de Uso – 04
Nombre	Actualización de ETL
Objetivo	Actualizar herramienta para la carga de usuarios
Descripción	Es el grupo de tareas llevadas a cabo por el administrador de la plataforma, para actualizar el servidor LDAP con nuevos grupos de información que deben de ser tomados en cuenta.
Actores	Usuario administrador de plataforma
Condiciones necesarias	• El usuario debe de tener acceso al sistema para carga de información.
Escenario principal	1. El administrador debe de realizar los ajustes dentro de las funciones o realizar nuevas funciones dentro de las bases de datos afectadas. 2. Los nuevos parámetros deben de ser ingresados en la herramienta de ETL. 3. Se deben de realizar pruebas para revisar sí los ajustes fueron realizados exitosamente.

Continuación de tabla IV.

Escenario de excepción	6.a. Sí el sistema no reconoce al usuario, le informará que su usuario no es válido.

Fuente: elaboración propia.

Tabla V. **Cambios en la configuración de la plataforma**

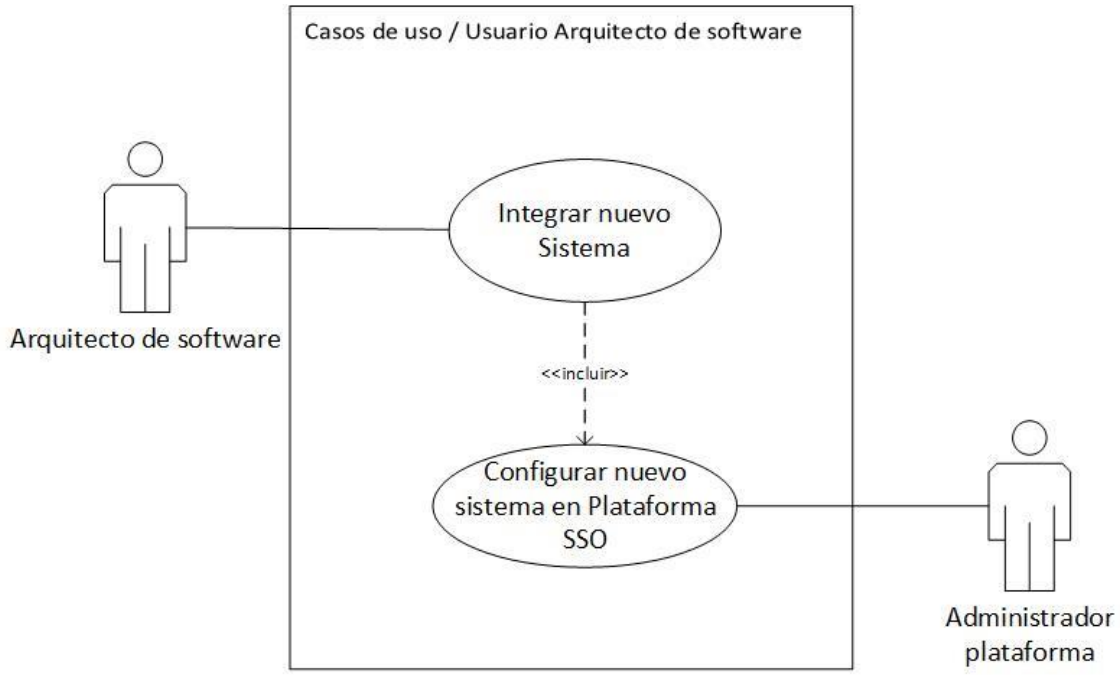
Código	Caso de Uso – 05
Nombre	Cambios en la configuración de la plataforma
Objetivo	Cambiar algún aspecto de la configuración inicial
Descripción	Este caso de uso identifica los cambios de la configuración inicial que se originan en base a algún requerimiento, partiendo de la configuración inicial.
Actores	Arquitecto de software
Condiciones necesarias	• El usuario debe de tener credenciales de administrador.
Escenario principal	1. El usuario debe de identificar el cambio en el manual técnico. 2. El administrador debe autenticarse con las credenciales de usuario administrador. 3. El usuario debe de realizar el cambio en la sección que corresponde. 4. El usuario verifica el cambio.
Escenario de excepción	4.a. Sí el cambio no fue realizado correctamente debe de iniciar el flujo.

Fuente: elaboración propia.

2.1.1.3. Funciones para el arquitecto de software

El arquitecto de software es el encargado de manejar la infraestructura disponible en la institución, y administrar los distintos servidores en los que está alojada la plataforma.

Figura 3. **CDU arquitecto de software**



Fuente: elaboración propia, empleando Microsoft Visio 2013.

Tabla VI. **Integración de nuevos sistemas a la plataforma**

Código	Caso de Uso – 06
Nombre	Integrar nuevo sistema
Objetivo	Integrar nuevo sistema a la plataforma
Descripción	Se integra una nueva aplicación a través del agente y de la configuración en la plataforma.
Actores	Arquitecto de software
Condiciones necesarias	• Se debe de contar con la colaboración del administrador de la aplicación. • Es necesario el acceso al servidor que se desea integrar y al instalador de un agente.
Escenario principal	1. El administrador de la plataforma debe de configurar el agente a integrar. 2. El arquitecto debe de instalar el agente 3. El arquitecto debe de configurar los permisos para el agente. 4. El arquitecto debe de configurar y reiniciar el servidor apache. 5. Se verifica funcionamiento correcto de la aplicación.
Escenario de excepción	5.a. En caso de funcionamiento no esperado verificar manual técnico.

Fuente: elaboración propia.

2.2. Investigación preliminar para la solución del proyecto

SSO, viene de las siglas en inglés Single Sign-On que en español se traduce como, autenticación única. Este sistema le permite al usuario final identificarse una sola vez, por medio de la plataforma y que la sesión se mantenga disponible, para el resto de aplicaciones que han sido integradas al mismo.

A los administradores y desarrolladores les simplifica la lógica de las aplicaciones, al consolidar la tarea de autenticación en una plataforma independiente, reduciendo así el tiempo de desarrollo.

Otra de las bondades que brinda esta herramienta es la seguridad lógica a través de una autenticación que determina las credenciales del usuario que ha ingresado al sistema, y la autorización que este tiene en los distintos sistemas.

2.2.1. Conocimientos básicos sobre sistemas de autenticación única

Para familiarizarnos con la herramienta de autenticación única es necesario conocer los conceptos de autenticación y autorización que son procesos que realiza la plataforma con los usuarios.

2.2.1.1. Autenticación

La autenticación es el proceso que realiza un usuario para identificarse dentro de un sistema. Para que un sistema le permita el acceso a un usuario debe cumplir por lo menos con uno de los siguientes factores:

- Factor de conocimiento: este primer factor indica que el usuario debe de tener algún conocimiento secreto, y saber plasmarlo en la interfaz de autenticación. El más claro ejemplo de esto son las contraseñas.

- Factor de posesión: otro factor que es utilizado para la autenticación es la posesión de algún instrumento que tenga algún tipo de clave de acceso.

- Factor de herencia: utiliza características físicas y únicas del usuario como huellas dactilares, lectura de retina, reconocimiento facial, etc.

2.2.1.2. Autorización

La autorización es una parte del sistema que le permite proteger los recursos de información, para que no puedan ser accedidos por aquellos usuarios a los que no se les ha otorgado los permisos necesarios. Los recursos incluyen archivos y otros objetos de datos, programas, dispositivos y funcionalidades de un sistema.

La autorización ocurre posterior a que el usuario ya ha sido autenticado o identificado dentro del sistema, y se utiliza para decidir si el usuario X tiene permiso de acceder al dato, funcionalidad o servicio.

2.2.2. Herramientas a utilizar

En esta sección se describen las herramientas utilizadas para el desarrollo de la plataforma de autenticación única

2.2.2.1. Servidor SSO OpenAM

Es una herramienta que administra y centraliza el acceso proveyendo las características necesarias, para brindar un adecuado funcionamiento de una plataforma de autenticación única.

La herramienta, OpenAM ha sido desarrollada en el lenguaje java y es una evolución de la herramienta OpenSSO de la empresa Sun Microsystems, perteneció a la empresa ForgeRock y en la actualidad cuenta con el respaldo de Open Identity Platform Community, quien le brinda mantenimiento y la distribuye bajo una licencia Común de Desarrollo y Distribución.

Otra de las características de OpenAM es permitir la integración de varias aplicaciones en un solo sistema de autenticación, proveyendo a cada una de las aplicaciones integradas, las herramientas necesarias para el seguimiento de las tareas propias de la plataforma.

2.2.2.2. OpenAM Web Policy Agents

El OpenAM web Policy Agent gestiona las políticas de OpenAM para la integración, y protege los recursos que en él se encuentran, interceptando las solicitudes de los usuarios que intentan acceder, y prohibiendo el acceso a usuarios no autenticados.

Fue creado con la finalidad de ser compatible totalmente con la herramienta OpenAM y desarrollado para servidores Apache. El objetivo de esta herramienta es, proveer una integración ágil para aplicaciones web, sirviendo como puente de comunicación entre la plataforma y el servidor de aplicaciones.

2.2.2.3. Servidor LDAP OpenDJ

OpenDJ es un servidor de directorios que implementa protocolo de acceso ligero LDAPv3, ha sido desarrollado en java y tiene sus orígenes en OpenDS originalmente para uso interno de Sun MicroSystems, y posteriormente convertirse en un proyecto de código abierto respaldado por Oracle Corporation.

Este proyecto, también fue desarrollado por la empresa ForgeRock y actualmente es Open Identity Platform Community quien le brinda soporte.

OpenDJ brinda un perfecto acoplamiento con la herramienta OpenAM y permite almacenar la información necesaria para el manejo de usuarios, dentro de la plataforma de autenticación única.

2.2.2.4. Talend Open Studio Integration for data Integration

Es una herramienta orientada a la extracción, transformación y carga (ETL), de datos de código abierto, que permite la integración de datos almacenados en distintas plataformas para sincronizarlos entre sí.

Talend provee una interfaz drag/drop que permite un intuitivo manejo de los componentes y las relaciones entre ellos, los proyectos se subdividen en Job y cada Job es un ETL por sí solo.

Debido a su robustez Talend provee soporte a una gran variedad de fuentes de datos como lo son bases de datos, documentos y servidores de directorios de acceso ligero (LDAP).

2.2.2.5. HAProxy

Herramienta que provee un servidor de alta disponibilidad para aplicaciones basadas en TCP y HTTP con capacidad para distribuir solicitudes en varios servidores, y realizar balanceo de carga entre los mismos.

2.3. Presentación de la solución al proyecto

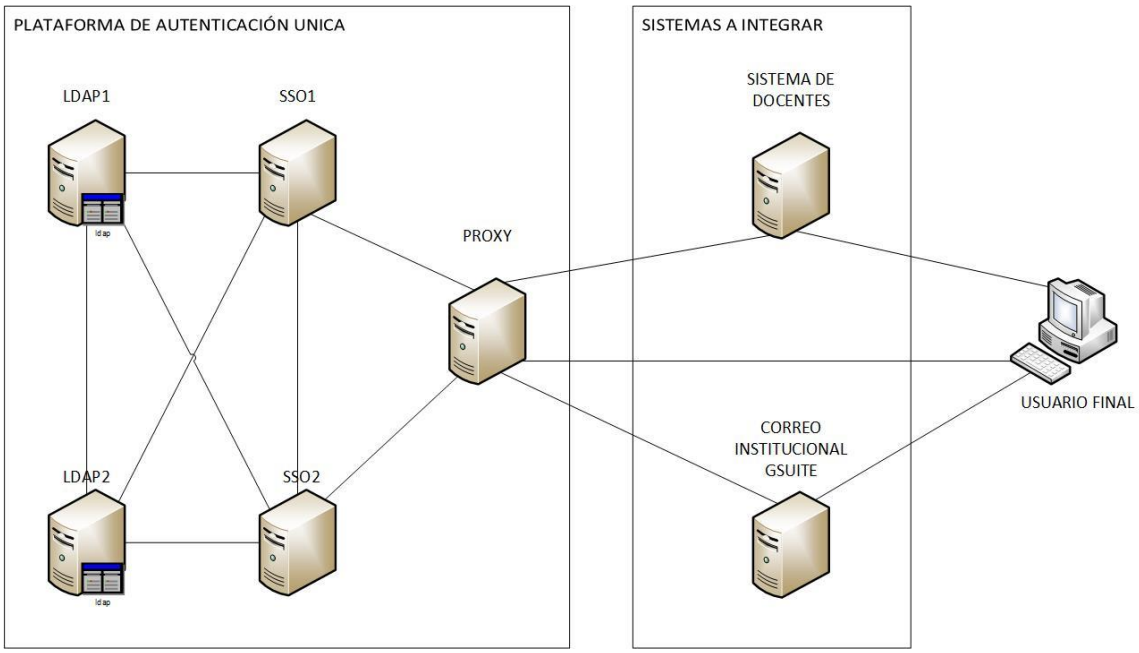
Para implementar la plataforma de autenticación única, es necesario definir la arquitectura de servidores que se utilizará. Asimismo se debe configurar de una forma ordenada cada una de las herramientas que la conforman y por último la integración de los sistemas.

2.3.1. Arquitectura de la plataforma

La plataforma debe de contar con una arquitectura estable y robusta que permita el acceso a cualquiera de los sistemas integrados, independientemente de las variaciones que pueda sufrir ésta en su ámbito de desempeño.

La plataforma atenderá estas variaciones a través de replicación y el balanceo de carga, evitando así complicaciones por perdida de algún servidor o la cantidad de usuarios accediendo a la plataforma.

Figura 4. **Arquitectura, plataforma de autenticación única**



Fuente: elaboración propia, empleando Microsoft Visio 2013.

La figura 4 detalla la arquitectura de la solución propuesta en ella, se consideran los siguientes componentes:

2.3.1.1. Servidores LDAP

Se contará con dos servidores LDAP, nombrados LDAP1 Y LDAP2 como se detalla en la figura 4, encargados de almacenar los datos. Dichos servidores tendrán comunicación directa con la herramienta de autenticación, y le brindará información sobre los usuarios que pueden hacer uso de la aplicación.

2.3.1.1.1. Replicación de la información

Los datos de los usuarios, serán almacenados en los servidores LDAP. LDAP1 Y LDAP2 replicarán datos entre sí con el objetivo de mantener la información consistente y que no exista dependencia directa a uno de ellos.

2.3.1.2. Servidores de autenticación

Se contará con dos servidores para el motor de autenticación única configurados con la herramienta OpenAM, SSO1 Y SSO2 de la figura 4, que replicarán la información entre sí, de esta forma ambos servidores podrán brindar el mismo servicio independientemente de cual se éste accediendo.

2.3.1.3. Proxy

El servidor proxy configurado con la herramienta haproxy, PROXY en la figura 4, será el encargado de realizar el balanceo de carga y de contener el certificado SSL, que provee seguridad a la plataforma de autenticación única.

2.3.1.3.1. Balanceo de carga

La tarea principal del proxy, es ser el puente de comunicación entre el cliente y la interfaz de autenticación única, es la herramienta que provee él balanceo de carga entre los dos servidores OpenAM a través de una política Round Robin.

2.3.1.4. Sistemas externos

Los sistemas externos, son aquellos que serán integrados a la plataforma de autenticación y que tendrán acceso a través de la misma interfaz. Para el caso del proyecto los sistemas externos son, el sistema de docentes y el sistema de cuenta de correo institucional Gsuite.

2.3.1.5. Usuario

El usuario en la figura 4, es la persona que intentará acceder a uno de los sistemas externos, utilizando un explorador web.

2.3.2. Desarrollo de la solución

Para el desarrollo de la solución es necesario llevar a cabo la siguiente lista de tareas:

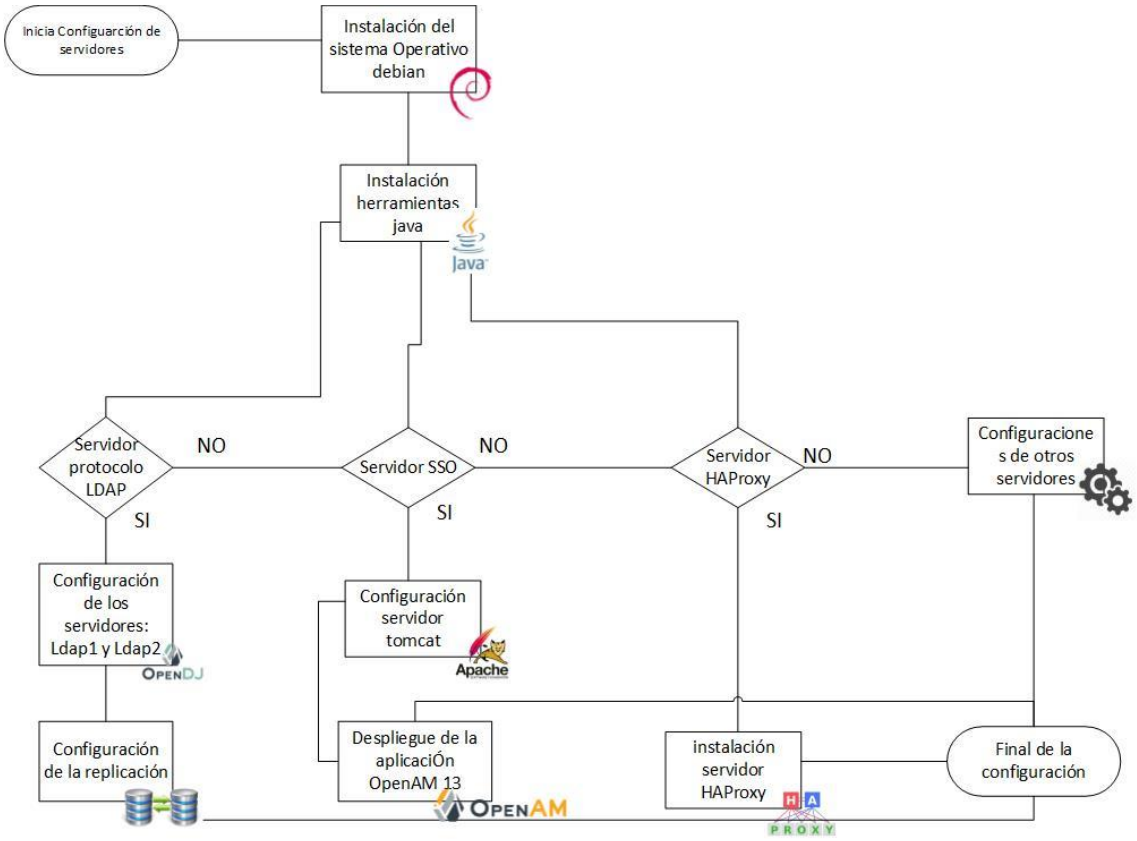
- Configuración inicial de los servidores
- Proceso de Extracción, Transformación y Carga (ETL)
- Configuración de la herramienta OpenAM
- Integración de sistemas
- Interfaz de cambio de contraseña
- Puesta en producción de la plataforma de autenticación

A continuación se detallan cada una de estas tareas:

2.3.2.1. Configuración inicial de los servidores

La configuración inicial de los servidores, consiste en la instalación básica del software necesario para el correcto funcionamiento de cada uno de estos. Cada servidor tiene una configuración particular según sea la función que cumpla dentro de la plataforma.

Figura 5. **Flujo configuración de servidores**



Fuente: elaboración propia, empleando Microsoft Visio 2013.

La figura 5, detalla el orden en el que se llevó a cabo la configuración para esta solución.

2.3.2.1.1. Configuración genérica de los servidores

Es la configuración inicial que tendrán todos los servidores, a partir de esta se realiza el resto de la instalación, dependiendo de su rol en la plataforma. Esta configuración consta de la instalación del sistema operativo debían 8, seguido de la instalación del Java Developer Kit (JDK), básico para las herramientas OpenAM y OpenDJ.

2.3.2.1.2. Servidores con protocolo LDAP

Se refiere a los servidores que almacenaran los datos de los usuarios del SSO. Estos servidores tendrán instalado el sistema LDAP (OpenDJ), y se configuran de forma separada para después configurar la replicación y así integrar ambos, de forma que estos cuenten con la misma información.

2.3.2.1.3. Instalación de servidores SSO

La herramienta OpenAM 13 debe de ser desplegada en un contenedor web, por lo que se realiza la instalación de Tomcat8 en los dos servidores en que se publicará, luego se carga la aplicación de OpenAM en el contenedor, para después ser configurada a través de su asistente.

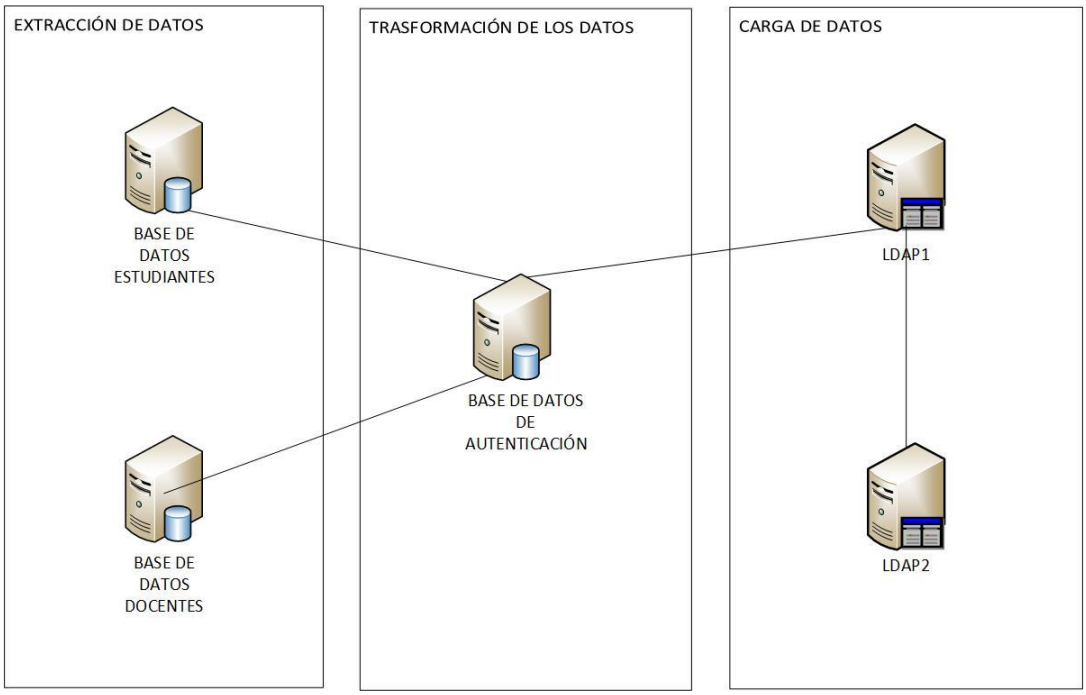
2.3.2.1.4. Instalación Haproxy

Se instala la herramienta haproxy, en el servidor encargado del balanceo de carga. Dicha configuración junto a la configuración del SSO permitirá realizar el balanceo de carga dentro de la plataforma.

2.3.2.2. Proceso de Extracción, Transformación y Carga (ETL)

En la figura que se presenta a continuación, se detallan las fuentes de las que se extraen los datos y el flujo que lleva hasta terminar en una replicación entre los servidores LDAP1 y LDAP2. Esto se hace necesario debido a que los datos se encuentran distribuidos donde para fines de la solución, es necesario integrarlos.

Figura 6. **Modelo de extracción de datos**



Fuente: elaboración propia, empleando Microsoft Visio 2013.

2.3.2.2.1. Definición inicial

Contempla las tareas de migración de los datos que se encuentra actualmente en la base de datos de origen, hacia una nueva fuente de datos adaptada a los requerimientos de la herramienta SSO y por medio de ella la plataforma basará su autenticación.

Este tipo de cambios deben de llevarse a cabo tanto al inicio del sistema en producción, como periódicamente para mantener la información actualizada en ambos sistemas.

Debe desarrollarse políticas de ETL para todas las aplicaciones que deseen integrarse al sistema, porque la plataforma autentica a partir de una única fuente de datos, según ha sido implementado para este proyecto.

2.3.2.2.2. Extracción de la información

Para manejar la autenticación, el gestor necesita la información de los usuarios que estarán acreditados, para utilizar los sistemas integrados a la plataforma.

Tabla VII. **Información para la extracción de datos**

Sistemas integrados	Usuarios	Base de datos
Sistema de docentes	Docentes	Base de datos de docentes
Sistema de correo institucional G Suite	Docentes, estudiantes, administrativos	Base de datos de docentes, estudiantes y administrativos.

Fuente: elaboración propia.

Según se puede observar en la tabla VII, los usuarios que es necesario que migren al sistema de directorios del SSO son: estudiantes, docentes y administrativos para la herramienta G Suite, y solo docentes para el sistema de docentes.

El proceso de extracción, obtiene los datos de la base de datos de docentes y la base de datos de estudiantes, para después unificarla en una nueva base de datos en donde convergen también los datos de administrativos, denominada en la figura 6 “Base de datos de Autenticación”. De la Base de datos de Autenticación se hace la nueva carga y transformación, hacia la herramienta LDAP en donde finaliza el proceso.

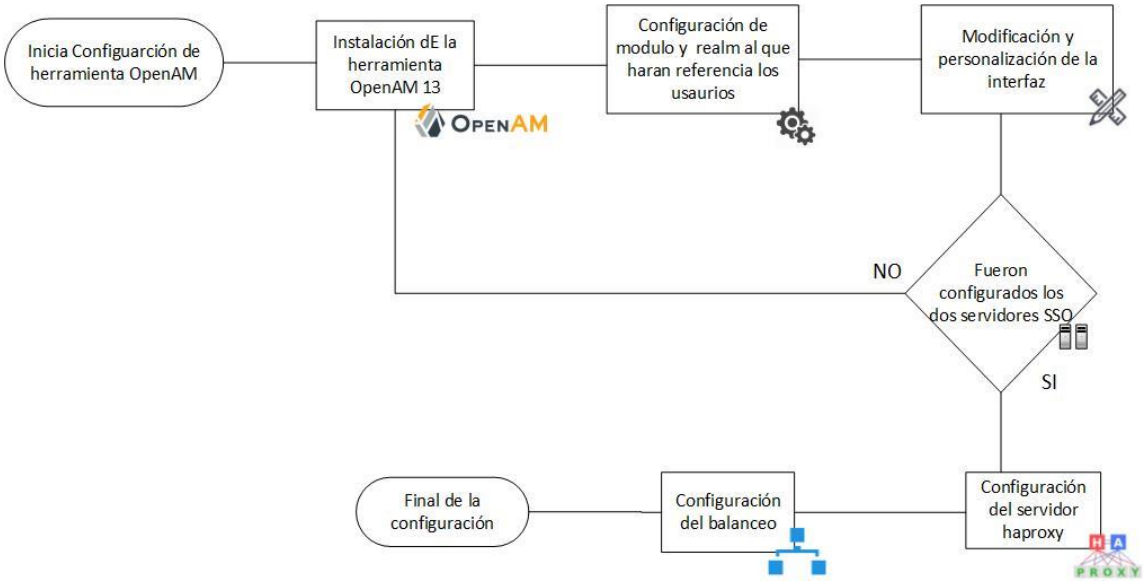
2.3.2.2.3. Puesta en marcha

El proceso de ETL, debe de ser ejecutado por primera vez cuando se despliegue en producción la plataforma de autenticación. Después de la primera carga, el proceso deberá de ser repetido periódicamente para tener integridad entre la información de la base de datos, y la fuente de datos LDAP.

2.3.2.3. Configuración de la herramienta OpenAM

En la figura 7 se presenta un diagrama de las actividades necesarias para realizar la configuración de la herramienta OpenAM.

Figura 7. **Flujo configuraciones herramienta OpenAM**



Fuente: elaboración propia, empleando Microsoft Visio 2013.

2.3.2.3.1. Instalación y configuración inicial de la herramienta

Esta es la configuración principal necesaria, para el correcto funcionamiento del SSO, en esta se deben definir los grupos de usuario y las fuentes de datos involucrados en el proceso. La información propia de la aplicación fue configurada para ser almacenada directamente en los servidores SSO, mientras que la fuente de datos para los usuarios a la que hará referencia el sistema será el servidor LDAP.

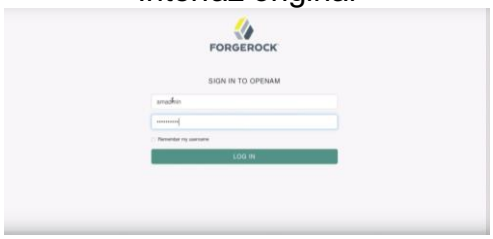
La herramienta OpenAM 13, permite agrupar los usuarios en grupos llamados Realm que pueden tener su origen en distintas fuentes de datos. Para este proyecto se realizó un único grupo denominado raíz (“/”) en el que se encuentra toda la información de los sistemas involucrados hasta el momento.

2.3.2.3.2. Modificación y personalización de la interfaz

La configuración de la interfaz, es el grupo de tareas y configuraciones con las que realizaremos la personalización de los aspectos visuales que brinde un diseño agradable y descriptivo, familiar para el usuario, y la edición de avisos para que sean más personalizados, según los requerimientos definidos.

Figura 8. **Interfaz personalizada**

Interfaz original



Interfaz actual

Fuente: elaboración propia.

2.3.2.3.3. Configuración del proxy

En la configuración del proxy, se instala el certificado SSL y se configura el balanceo de carga para que pueda seguir trabajando correctamente, independiente de si alguno de los dos servidores deja de funcionar. Para el balanceo de carga, se debe contar con los dos servidores SSO.

2.3.2.4. Integración de sistemas

El sistema de docentes de la facultad de arquitectura y el correo institucional (G Suite) serán integrados a la plataforma de autenticación única de la siguiente manera:

2.3.2.4.1. Integración sistema de docentes

Primero se tuvo un periodo de conocimiento del sistema para identificar de qué forma sería afectado por la integración, alcance y tipo de usuarios que hacen uso del mismo. Después, se deben realizar las tareas de integración como lo son, la creación de una librería que permita obtener la información de los campos, la adaptación de la misma librería al sistema y por último, las tareas que completan la integración dentro del sistema.

Figura 9. **Flujo integración sistema de docentes**

Fuente: elaboración propia, empleando Microsoft Visio 2013.

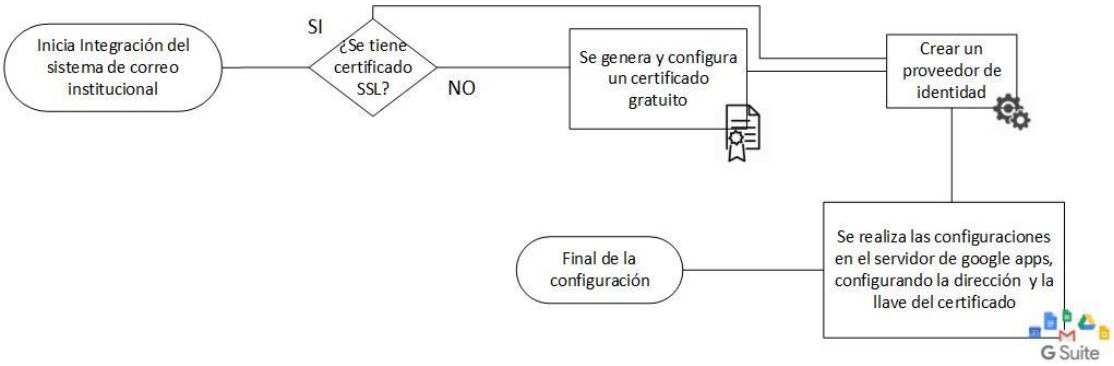
2.3.2.4.2. Integración de G Suite al SSO

Actualmente, la Facultad de Arquitectura provee a sus usuarios una cuenta de correo institucional, gracias al servicio G Suite de Google orientado a

todos los usuarios. La configuración de la plataforma es soportada por OpenAM y esto permite un proceso de integración personalizado con la herramienta.

La figura 9, detalla los pasos necesarios para realizar la integración de la herramienta G Suite a la plataforma de autenticación única.

Figura 10. **Flujo integración con G Suite**



Fuente: elaboración propia, empleando Microsoft Visio 2013.

2.3.2.5. Interfaz de cambio de contraseña

La interfaz de cambio de contraseña, implica tareas de configuración por medio de la herramienta OpenAM. Configurando así que el usuario a través de la interfaz de autenticación, pueda recuperar su contraseña por medio de un correo electrónico enviado a la cuenta de correo personal.

2.3.2.6. Puesta en producción de la plataforma de autenticación

Durante el desarrollo se trabajó en un entorno virtualizado, en donde se configuraron los servidores que forman parte de la arquitectura de la plataforma

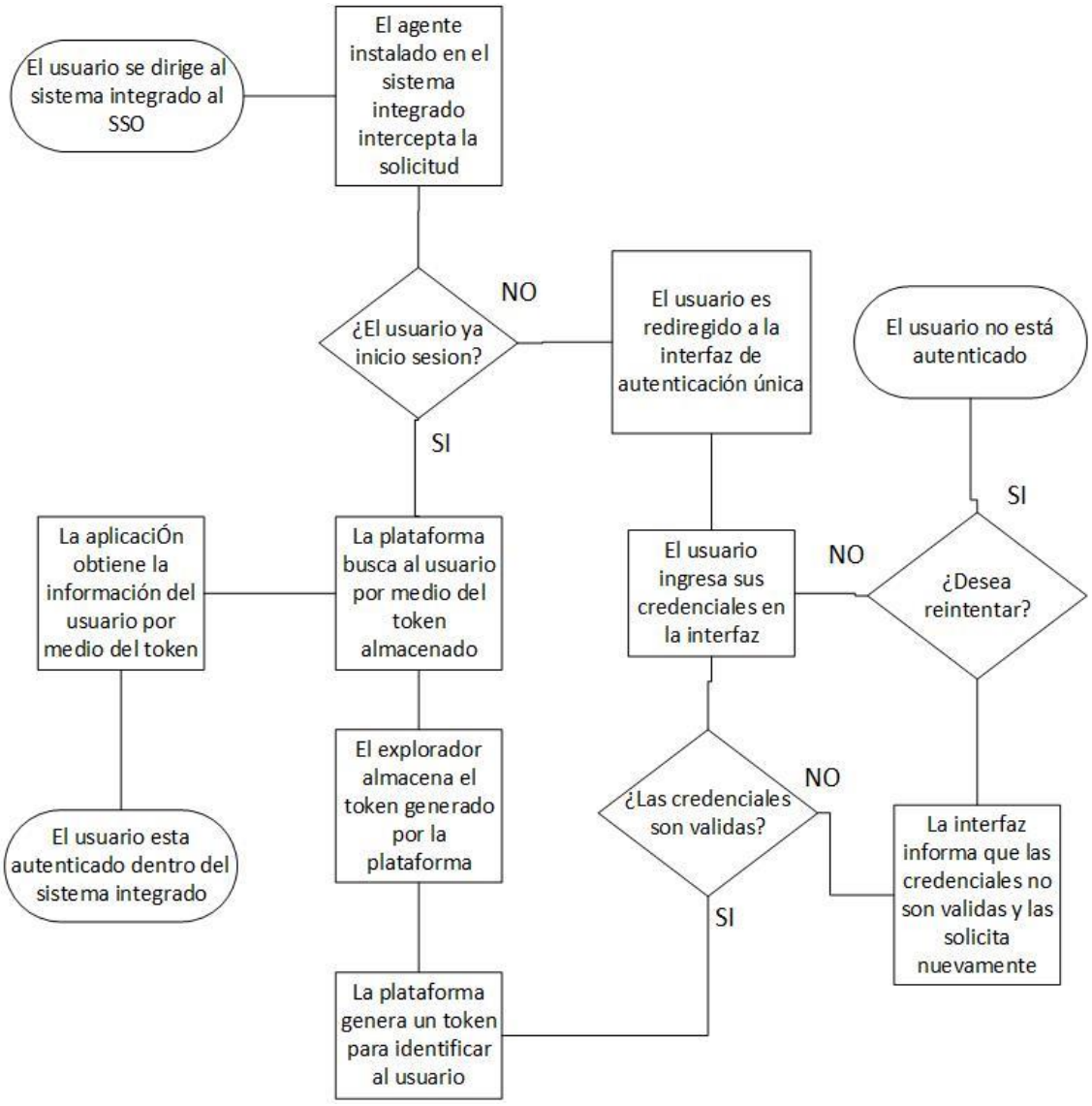
y el servidor de docentes. Dentro de las tareas de puesta en producción se realizaron las siguientes:

- Integrar en un ambiente de producción los servidores que forman parte de la arquitectura del SSO.
- Realizar la migración de usuarios de producción al sistema de directorios LDAP.
- Integrar el sistema de docentes a la plataforma SSO. Se debe replicar los cambios realizados en el ambiente de desarrollo.
- Integración herramienta Gsuite. Se debe activar la autenticación en la plataforma, a través de la configuración del administrador.

2.3.3. Funcionamiento de la interfaz de autenticación

En el diagrama de flujo de la figura 10, se detalla el funcionamiento de la interfaz de autenticación única, teniendo como objetivo determinar si el usuario ya ha iniciado sesión o identificar al usuario, validando que las credenciales sean correctas.

Figura 11. **Detalle del funcionamiento, plataforma de autenticación única**



Fuente: elaboración propia, empleando Microsoft Visio 2013.

Al momento de autenticar a los usuarios la interfaz les brinda un Token identificador, el cual internamente queda asociado a la identidad del usuario que utiliza el sistema.

Cuando un usuario ya autenticado por medio de la plataforma entra a uno de los sistemas integrados, su navegador hace llegar a las aplicaciones su Token, este está asociado internamente a la identidad del usuario que hace uso del sistema.

Es tarea del agente comprobar la presencia y validez del Token, y será la propia aplicación integrada quien obtendrá los atributos de identidad, consultando a la plataforma SSO por medio de peticiones post.

2.4. Costos del proyecto

A continuación se detallan los costos que tomó el desarrollo y puesta en marcha de la plataforma, tomando en cuenta tanto al recurso humano como al equipo necesario para la realización y puesta en producción del proyecto.

2.4.1. Cálculo de costos en recurso humano

Contempla los gastos que el proyecto requiere en términos de recurso humano. El recurso humano que se contempla en esta sección es:

- Epesista
- Asesor
- Personal de la institución

Tabla VII. **Costo recurso humano, desarrollo de SSO**

Descripción	Cantidad de recursos	Tiempo - Mes	Costo unitario	Subtotal
Toma de requerimientos e investigación. (Epesista)	1	1	Q10 000,00	Q10 000,00
Toma de requerimientos e investigación. (Epesista)	1	5	Q10 000,00	Q50 000,00
Asesor técnico y experto en la herramienta. (Asesor)	1	6	Q5 000,00	Q30 000,00
Capacitación del personal. (Personal de la institución).	1	1	Q2 000,00	Q2 000,00
			Total	Q92 000,00

Fuente: elaboración propia.

2.4.2. Cálculo de costos en equipo

En esta etapa, se toma en cuenta los gastos que el proyecto tuvo durante el desarrollo, por parte del equipo físico del que se hizo uso.

Tabla VIII. **Costo de equipo, desarrollo de SSO**

Descripción	Tiempo - Mes	Costo unitario	Subtotal
Costos de electricidad, red e internet.	6	Q300,00	Q1 800,00
Alojamiento en servidores.	6	Q1 000,00	Q6 000,00
		Total	Q7 800,00

Fuente: elaboración propia.

2.4.3. Cálculo total de costos

En esta categoría, se toman en cuenta los gastos que el proyecto tuvo durante el desarrollo, por parte del recurso humano y físico.

Tabla IX. **Costos totales, desarrollo de SSO**

Descripción	Subtotal
Costes de recurso humano.	Q92 000,00
Costes de equipo	Q7 800,00
Total	Q99 800,00

Fuente: elaboración propia.

2.5. Beneficios del proyecto

La plataforma de autenticación única presenta distintos beneficios, según el rol que desempeña el usuario en la institución:

2.5.1. Beneficios para el usuario final

- La implementación del SSO evita que el usuario necesite recordar varias contraseñas.
- Por la cantidad de sistemas que tienen a su cargo, los usuario anteriormente necesitaban tener varias contraseñas, esto provoca que creen contraseñas sencillas y fáciles de recordar, estas muchas veces son inseguras. Por esto el SSO permite tener una única contraseña segura.
- El SSO permite acceder a varios recursos que pertenezcan al listado de sistemas asignados al usuario, siendo necesaria así una única asignación y evitando que el usuario deba iniciar sesión en cada uno de estos sistemas.
- Se realizó una mejora bastante notable en la experiencia del ingreso a las distintas aplicaciones utilizadas en la Facultad de Arquitectura por parte de los usuarios, reduciendo tiempo sin perder la seguridad.
- Se brindó a todos los usuarios una interfaz de recuperación de contraseña, con este nuevo beneficio los usuarios no necesitan acudir a Control Académico a gestionar esta acción como anteriormente se hacía.
- Se promovió dentro de los grupos de usuarios de la Facultad, el interés por el uso de la herramienta GoogleApps, de las cuales ya se disponía y no se aprovechaba de manera adecuada.

2.5.2. Beneficios del administrador de la plataforma

- Proporciona la administración de políticas centralizada y respaldo para las credenciales de usuario, a través de una implementación del protocolo ligero de acceso a directorios LDAP OpenDJ.
- La integración a una plataforma ya existente le permite tener una integración sólida, que no requiere de desarrollo largo y complejo.

- Reducción de tiempo utilizado por parte del encargado. Los casos de cambio de contraseña se reducirán, debido a la sincronización de contraseñas entre las distintas aplicaciones.

2.5.3. Beneficio del arquitecto

- La integración de los sistemas no interfiere con su autonomía. La labor del agente es realizar la comunicación entre la plataforma de autenticación y el servidor, en el que se encuentra alojada el sistema que se desea integrar.

3. FASE DE ENSEÑANZA Y APRENDIZAJE

3.1. Capacitación

La capacitación fue dirigida al personal de informática sobre el uso de la herramienta, la administración de la misma y las posibles dudas que se pueden encontrar por parte de los usuarios finales.

La herramienta de autenticación única utilizada, provee a los usuarios administradores la opción de configurar un ambiente más personalizado, según sean las características de los usuarios.

3.1.1. Carga de usuarios

Contempla el ETL inicial que debe de ser tomado en cuenta al momento de pasar a producción. Este ETL consiste en la carga de datos inicial con la que empezará a trabajar el sistema.

Cada vez que se requiere agregar nuevos usuarios se hará un barrido de todos los nuevos datos en la base de datos, y se incrementarán los nuevos usuarios y nueva información, exceptuando las contraseñas que ya se encuentran en la base de datos.

3.1.2. Configuraciones habituales al sistema

Contempla las configuraciones más frecuentes que pueden existir en el sistema.

3.1.3. Configuraciones de integración

Se capacita las características principales que se deben de tomar en cuenta como las librerías a utilizar y el agente a instalar, al momento de integrar un nuevo sistema a la plataforma de autenticación.

3.2. Material elaborado

El material elaborado son las herramientas de ayuda e información entregadas a la institución, para la configuración y uso del sistema. Este material va orientado tanto al usuario administrador, como para el usuario final.

3.2.1. Manual de usuario

La capacitación al usuario final se hará por medio de manuales y video tutoriales, porque es una explicación corta y es un cambio pequeño para el usuario. Estos medios visuales permiten una mayor capacidad de alcance y se divulgará, a través de la unidad de difusión perteneciente a la Facultad de Arquitectura.

El manual de usuario, está orientado al uso de la plataforma por parte del usuario final. Comprende el uso de las diferentes características integradas

como lo son: la autenticación a la plataforma y el cambio de contraseña. Para más detalle sobre este tutorial, puede dirigirse a la sección de anexos.

3.2.2. Manual técnico

Este recurso está orientado al administrador de la aplicación, además detalla la configuración realizada durante el desarrollo del proyecto y los aspectos importantes de la lógica del sistema; detalla la formación de la plataforma y provee una guía en la integración de nuevos sistemas. El mismo fue integrado directamente al equipo técnico de la Facultad de Arquitectura, porque por medidas de seguridad se concluyó que no fuera público.

CONCLUSIONES

1. Se establecieron las bases de una plataforma de autenticación única para los usuarios de la Facultad de Arquitectura. Esta brinda el ingreso a los diferentes sistemas que tiene a su cargo de una manera cómoda, rápida y segura.

2. Los servidores que contienen la plataforma SSO fueron integrados a un proxy, con el fin de realizar balanceo de carga y de esta forma volver a la plataforma más robusta y estable, proveyendo garantías para la inclusión de nuevos sistemas.

3. Esta plataforma fue desarrollada para que el usuario realice una autenticación de forma rápida y sencilla, a través de una interfaz visualmente atractiva, flexible y fácil de utilizar.

4. El usuario podrá ingresar de manera segura a su cuenta, de forma que la plataforma identifica los datos de cada usuario de manera inequívoca, mientras la comunicación se realiza con datos cifrados, cumpliendo así con normas exigentes de seguridad.

5. La plataforma SSO tiene la capacidad de atender a todos los sistemas informáticos de la Facultad de Arquitectura, por medio de su herramienta de integración Web Policy Agent. En el desarrollo de la plataforma se realizó la integración del sistema de docentes como guía para futuras integraciones.

RECOMENDACIONES

1. Al momento de realizar una integración de un nuevo sistema, es necesario hacer un estudio previo de los usuarios involucrados, y así encontrar la mejor forma de integrar estos al proceso de ETL ya realizado.

2. Dado que el sistema es escalable por naturaleza, se recomienda tener una planificación para la integración de nuevos sistemas a la plataforma, de manera que esta integración sea progresiva y que se tenga en cuenta la información con que ya cuenta el sistema de directorios del LDAP.

3. En la evaluación de la plataforma se debe de tomar en cuenta el desarrollo de una interfaz paralela, que permita la administración de permisos y roles mediante la cual se pueda listar las aplicaciones de las que el usuario tiene acceso, así como el enlace a las mismas.

BIBLIOGRAFÍA

1. CRAIG, Mark, et.al. *OpenAM Installation Guide.* [en línea]. <http://openam.forgerock.org/openam-documentation/openam-doc-source/doc/install-guide/index.html>. [Consulta: 13 de abril de 2018].

2. Staff de Wikipedia. *OpenAM.* [en línea]. <https://en.wikipedia.org/wiki/OpenAM>. [Consulta: 15 de octubre de 2018].

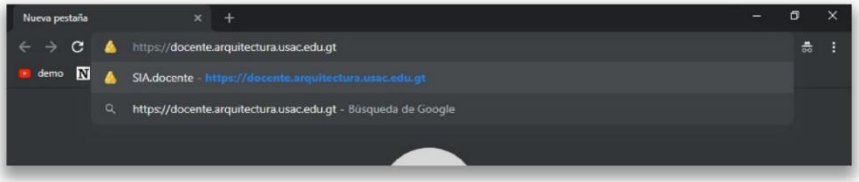
3. Staff de ForgeRock. *OpenAM Web Policy Agent 4.* [en línea]. <https://backstage.forgerock.com/docs/openam-web-policy-agents/4/web-users-guide/>. [Consulta: 13 de abril de 2018].

4. Unidad de Divulgación, Facultad de Arquitectura. *Administración.*[en línea]. <https://farusac.edu.gt/administracion//>. [Consulta: 13 de abril de 2018].

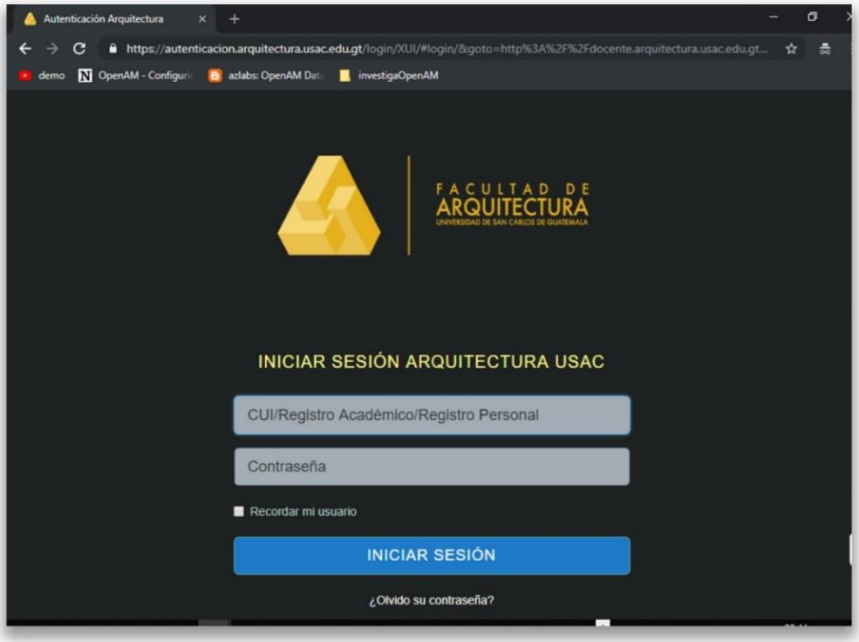
APÉNDICES

Apéndice 1. **Flujo de la Interfaz de Autenticación**

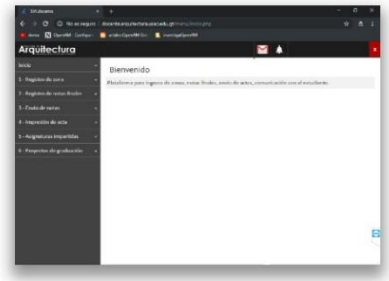
Paso1: El usuario intenta entrar al sistema de docentes o al correo institucional



Paso2: El sistema lo redirecciona a la interfaz de autenticación única



Paso 3: La plataforma lo redirecciona al sistema de docentes

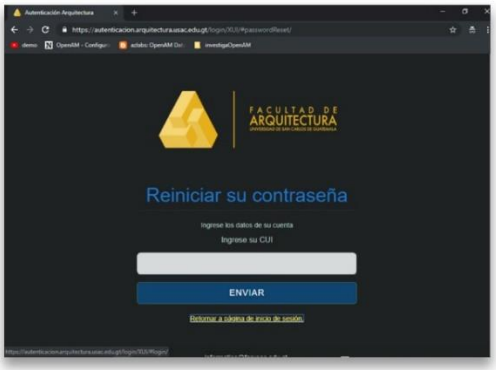


Paso 4: El sistema lo redirecciona al sistema de correo institucional

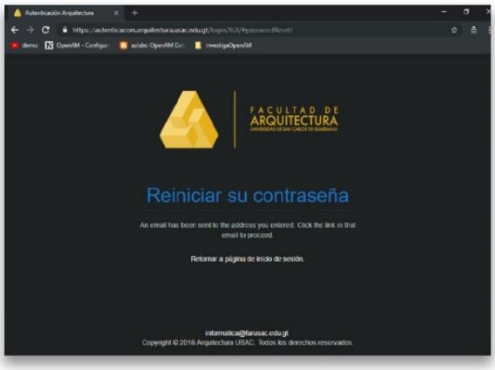
Fuente: elaboración propia, empleando Adobe Photoshop CS6.

Apéndice 2. **Flujo de restablecimiento de contraseña**

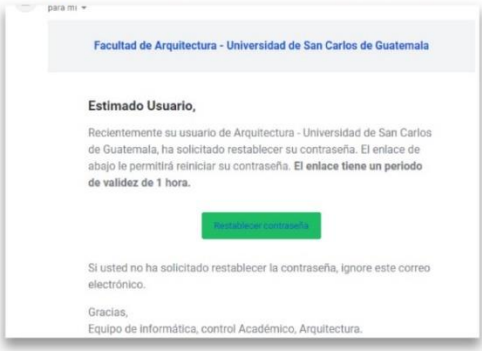
Paso 1: El usuario ingresa su número de CUI para que el sistema lo identifique.



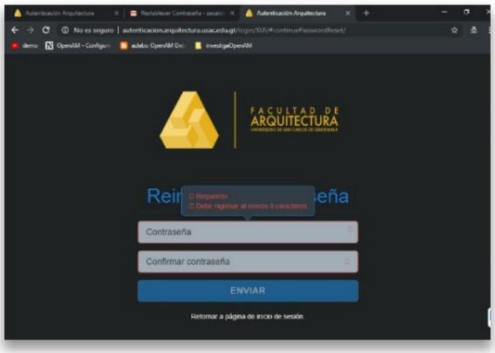
Paso 2: El sistema le envía al usuario un correo electrónico.



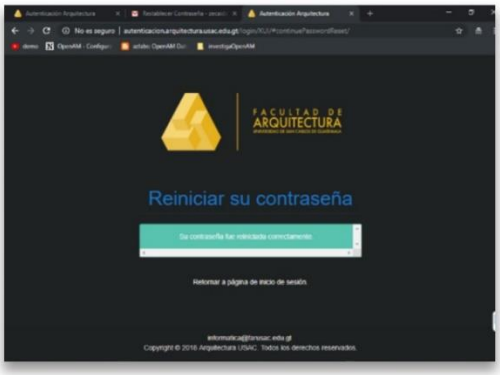
Paso 3: En su correo electrónico personal el usuario se dirige al link para restablecer la contraseña.



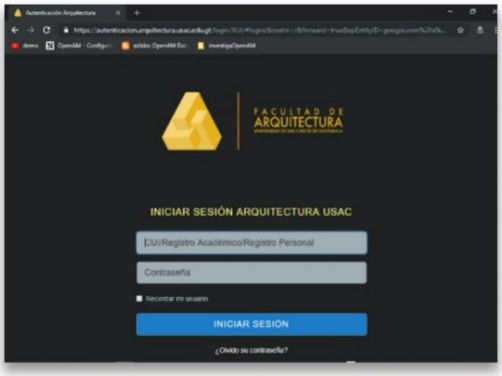
Paso 4: El Sistema solicita que ingrese y confirme la nueva contraseña.



Paso 5: El sistema le indica al usuario que ha restablecido la contraseña satisfactoriamente.



Paso 6: El usuario intenta ingresar de nuevo al sistema.



Fuente: elaboración propia, empleando Adobe Photoshop CS6.