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

SISTEMA DE INICIO DE SESIÓN ÚNICO PARA APLICACIONES EN DEPARTAMENTO ADMINISTRATIVO FINANCIERO DEL INSTITUTO DE CIENCIAS FORENSES DE GUATEMALA

Javier Alexander Chacón Samol
Asesorado por ingeniero Álvaro Giovanni Longo Morales

Guatemala, septiembre 2022

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

SISTEMA DE INICIO DE SESIÓN ÚNICO PARA APLICACIONES EN DEPARTAMENTO ADMINISTRATIVO FINANCIERO DEL INSTITUTO DE CIENCIAS FORENSES DE GUATEMALA

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

JAVIER ALEXANDER CHACÓN SAMOL
ASESORADO POR INGENIERO ÁLVARO GIOVANNI LONGO MORALES

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN CIENCIAS Y SISTEMAS

GUATEMALA, SEPTIEMBRE 2022

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANA	Inga. Aurelia Anabela Cordova Estrada
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. Kevin Vladimir Armando Cruz Lorente
VOCAL V	Br. Fernando José Paz González
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANA	Inga. Aurelia Anabela Cordova Estrada
EXAMINADORA	Inga. Floriza Felipa Ávila Pesquera de Medinilla
EXAMINADOR	Ing. Sergio Leonel Gómez Bravo
EXAMINADOR	Ing. Carlos Alfredo Azurdia Morales
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

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:

SISTEMA DE INICIO DE SESIÓN ÚNICO PARA APLICACIONES EN DEPARTAMENTO ADMINISTRATIVO FINANCIERO DEL INSTITUTO DE CIENCIAS FORENSES DE GUATEMALA

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería Ciencias y Sistemas, con fecha 05 de agosto de 2021.

Javier Alexander Chacón Samol

Guatemala 13 de julio de 2022

Ing. Oscar Argueta Hernández
Director de la Unidad de EPS
Facultad de Ingeniería
Universidad de San Carlos de Guatemala

Respetable Ing. Argueta:

Respetuosamente me dirijo a usted deseándole éxito en sus actividades cotidianas, por medio de la presente hago de su conocimiento que el estudiante JAVIER ALEXANDER CHACÓN SAMOL, quien se identifica con CUI No. 2243-35162-0101 y como estudiante universitario con número de carné 201212752, ha finalizado el informe final del proyecto EPS:

"SISTEMA DE INICIO DE SESIÓN ÚNICO PARA APLICACIONES EN DEPARTAMENTO ADMINISTRATIVO FINANCIERO DEL INSTITUTO DE CIENCIAS FORENSES DE GUATEMALA"

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

Sin otro particular me suscribo, atentamente,

F:_____

Ing. Álvaro Giovanni Longo Morales
longoalvarousac@gmail.com
Alvaro Giovanni Longo Morales
Ingeniero en Ciencias y Sistemas
Colegiado No. 15,845

Universidad de San Carlos de Guatemala

Facultad de Ingeniería
Unidad de EPS

Guatemala, 20 de julio de 2022.
REF.EPS.DOC.239.07.2022.

Ing. Oscar Argueta Hernández
Director Unidad de EPS
Facultad de Ingeniería
Presente

Estimado Ingeniero Argueta Hernández:

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, **Javier Alexander Chacón Samol, Registro Académico 201212752 y CUI 2243 35162 0101** procedí a revisar el informe final, cuyo título es **SISTEMA DE INICIO DE SESIÓN ÚNICO PARA APLICACIONES EN DEPARTAMENTO ADMINISTRATIVO FINANCIERO DEL INSTITUTO DE CIENCIAS FORENSES 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"

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, 20 de julio de 2022.
REF.EPS.D.227.07.2022.

Ing. Carlos Gustavo Alonzo
Director Escuela de Ingeniería Ciencias y Sistemas
Facultad de Ingeniería
Presente

Estimado Ingeniero Alonzo:

Por este medio atentamente le envío el informe final correspondiente a la práctica del Ejercicio Profesional Supervisado, (E.P.S) titulado **SISTEMA DE INICIO DE SESIÓN ÚNICO PARA APLICACIONES EN DEPARTAMENTO ADMINISTRATIVO FINANCIERO DEL INSTITUTO DE CIENCIAS FORENSES DE GUATEMALA,** que fue desarrollado por el estudiante universitario **Javier Alexander Chacón Samol, Registro Académico 201212752 y CUI 2243 35162 0101** quien fue debidamente asesorado por el Ing. Álvaro Giovanni Longo Morales 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"

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

Ing. Oscar Argueta Hernández
Director Unidad de EPS

/ra

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

Guatemala 26 de julio de 2022

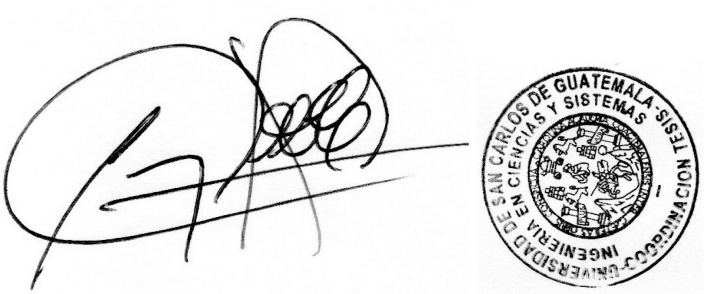
Ingeniero
Carlos Gustavo Alonzo
Director de la Escuela de Ingeniería
En Ciencias y Sistemas

Respetable Ingeniero Alonzo:

Por este medio hago de su conocimiento que he revisado el trabajo de graduación-EPS del estudiante **JAVIER ALEXANDER CHACÓN SAMOL** carné **201212752** y CUI **2243 35162 0101,** titulado: **"SISTEMA DE INICIO DE SESIÓN ÚNICO PARA APLICACIONES EN DEPARTAMENTO ADMINISTRATIVO FINANCIERO DEL INSTITUTO DE CIENCIAS FORENSES 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

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

LNG.DIRECTOR.178.EICCSS.2022

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, el visto bueno del Coordinador de área y la aprobación del área de lingüística del trabajo de graduación titulado: **SISTEMA DE INICIO DE SESIÓN ÚNICO PARA APLICACIONES EN DEPARTAMENTO ADMINISTRATIVO FINANCIERO DEL INSTITUTO DE CIENCIAS FORENSES DE GUATEMALA**, presentado por: **Javier Alexander Chacón Samol**, procedo con el Aval del mismo, ya que cumple con los requisitos normados por la Facultad de Ingeniería.

"ID Y ENSEÑAD A TODOS"

Msc. Ing. Carlos Gustavo Alonzo
Director
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, septiembre de 2022

Decanato
Facultad de Ingeniería
24189101- 24189102
secretariadecanato@ingenieria.usac.edu.gt

LNG.DECANATO.OI.629.2022

La Decana 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, al Trabajo de Graduación titulado: **SISTEMA DE INICIO DE SESIÓN ÚNICO PARA APLICACIONES EN DEPARTAMENTO ADMINISTRATIVO FINANCIERO DEL INSTITUTO DE CIENCIAS FORENSES DE GUATEMALA,** presentado por: **Javier Alexander Chacón Samol,** después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, autoriza la impresión del mismo.

IMPRÍMASE:

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANA
FACULTAD DE INGENIERÍA

Inga. Aurelia Anabela Cordova Estrada
Decana

Guatemala, septiembre de 2022

AACE/gaoc

ACTO QUE DEDICO A:

Dios	Por suplir todas las necesidades de una vida digna. Su fortaleza y sabiduría medios indispensables en este triunfo.
Mi esposa e hijo	Gabriela Pineda, por su inquebrantable confianza en mis capacidades y apoyo incondicional. Santiago Chacón, por sacudir completamente mi vida y motivarme a ser mejor persona cada día.
Mis padres	Jorge Chacón y Norma Samol, autores principales de mi vida. Este logro es fruto de su amor, dedicación, consejos y sacrificios.
Mis hermanas	Stephany Samol, Sofía Castillo y Gabriela Chacón, por ser mi alegría y la causa principal de superación personal y profesional.
Mis abuelos	Agustín Samol y María Juárez, por su notable ejemplo de trabajo y caridad. Juan Manuel Chacón (q. e. p. d.) y Carlota López (q. e. p. d.) por sus enseñanzas y cariño que siguen palpables.

AGRADECIMIENTOS A:

Universidad de San Carlos de Guatemala	Por el privilegio de pertenecer a tan prestigiosa casa de estudios.
Facultad de Ingeniería	Por la formación académica, conocimientos y herramientas que me permiten el día de hoy desenvolverme como profesional
Mi familia	Con quienes comparto la alegría de este triunfo.
Mis amigos	Por su cariño y motivación durante mi carrera académica y profesional.
Ing. Álvaro Longo	Por su acompañamiento y asesoría para la realización de este trabajo.
Instituto Nacional de Ciencias Forenses de Guatemala	Agradecimiento especial al Ing. Willy Rosal e Ing. Irvin García por el apoyo recibido durante la ejecución de este proyecto.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

GLOSARIO

Compilar Proceso en desarrollo de *software* web que consiste en convertir el código fuente de una aplicación en un artefacto empaquetado con dependencias y librerías.

Desplegar Proceso en desarrollo de *software* que implica trasladar y configurar los artefactos en los servidores web.

Directorio activo Estructura abstracta para almacenar información descriptiva de los usuarios y manejo de credenciales en la red.

Framework En aplicaciones Microsoft, hace referencia a la versión de herramientas de desarrollo de *software*.

GIT Sistema de control de versiones descentralizada. Se utiliza para identificar en el desarrollo de *software* los cambios en los archivos e indicar fecha y hora de la modificación.

IIS Internet Information Services. Servidor web de Microsoft utilizado para publicar aplicaciones sobre servidores Windows.

Intranet	Es una red privada destinada para compartir recursos principalmente a los trabajadores de una organización.
ldap	Protocolo de comunicación hacia Microsoft Active Directory Domain.
Navegador web	Es una aplicación que habilita al usuario visualizar información de una página web.
Servidor web	Es un equipo de cómputo con recursos de gran potencia para exponer servicios web.
Software	Es un programa de cómputo que permite desarrollar tareas inteligentes con un propósito en específico.
SSO	Single Sign On. Es un esquema de autenticación que permite a varias aplicaciones autenticarse con una única sesión.
URL	Uniform Resource Locator. Es una dirección única para identificar recursos dentro de una red, principalmente de tipo web.

RESUMEN

El Instituto Nacional de Ciencias Forenses de Guatemala requiere una actualización en la arquitectura de sus aplicaciones, específicamente en el componente de autenticación. El objetivo es desacoplar este componente y centralizarlo para todo tipo de aplicación web del Departamento Administrativo Financiero.

Se implementa Keycloak como *software* de código abierto que además de ofrecer una interfaz centralizada para el inicio sesión, integra la conectividad por el protocolo ldap hacia el actual Directorio Activo de la institución. Esto habilita que el nuevo componente de autenticación funcione a través de las credenciales con las cuales los usuarios ingresan en su ordenador.

Posterior a la configuración se modifican las aplicaciones del Departamento Administrativo Financiero para integrar este nuevo mecanismo de autenticación. El usuario tiene la alternativa de realizar su inicio de sesión por SSO, sin perder el rol y los permisos de su usuario local.

Finalmente se compilan y despliegan las aplicaciones en ambientes productivos, donde se hace la entrega de los sistemas operando de manera correcta.

OBJETIVOS

General

Implementar un único sistema de autenticación para las aplicaciones en Departamento Administrativo Financiero (DAF) del Instituto Nacional de Ciencias Forenses de Guatemala (INACIF).

Específicos

1. Integrar, adecuar y desplegar las diferentes aplicaciones del DAF con el *software* de SSO Keycloak para la administración de identificación y acceso centralizado.

2. Permitir que los usuarios, a través de la herramienta SSO, utilicen las credenciales del actual Directorio Activo de INACIF para autenticarse a las diferentes aplicaciones (Usuario Federados).

3. Implementar componente para homologar los permisos de usuarios locales con usuarios de directorio activo. Los usuarios al autenticarse a través de SSO mantienen los permisos anteriores.

INTRODUCCIÓN

El Instituto Nacional de Ciencias Forenses de Guatemala (INACIF) es una institución pública que surge con el objetivo de unificar los servicios forenses periciales y garantizar la imparcialidad y confiabilidad de la investigación técnica científica. Esta institución tiene un ecosistema de sistemas de información que son heterogéneos en sus tecnologías e implementaciones. Dichos sistemas soportan los procesos y procedimientos de las diferentes áreas.

La autenticación es el componente en común de las aplicaciones, es decir, que todo aplicativo posee una sección de autenticación como puerta de entrada a sus operaciones. Este componente es importante para gestionar la identidad y acceso de los usuarios, pero ha sido desarrollado de acuerdo a las necesidades de cada aplicación e implementado con diferentes mecanismos de autenticación. El hecho que cada aplicativo tenga su propia forma de identificar a los usuarios repercute en que los usuarios poseen diferentes credenciales para cada aplicativo. Cada nueva aplicación al portafolio de la institución suma nuevas credenciales que el usuario debe memorizar. Cuando este conjunto de accesos no es controlado, surge malas prácticas y evidentes riesgos de seguridad, tales como: escribir una clave en una hoja de papel que pueda ser visto por cualquier persona; crear un archivo plano en la computadora con todas las credenciales, entre otras.

Para mitigar el riesgo actual del acceso a estas aplicaciones se realiza una actualización en la arquitectura de las aplicaciones. Esta modificación

permite centralizar el acceso a las aplicaciones y simplificar el proceso de autenticación con una única credencial.

1. FASE DE INVESTIGACIÓN

1.1. Antecedentes de la empresa

El Instituto Nacional de Ciencias Forenses de Guatemala (INACIF) es una institución que, mediante el desarrollo tecnológico y científico, fortalece y centraliza los servicios periciales forenses en Guatemala. Contribuye al sistema de justicia garantizando la imparcialidad y confiabilidad de las investigaciones e informes forenses. Los servicios que presta son específicamente requerimientos de jueces y fiscales, no actúa de oficio.

1.1.1. Reseña histórica

El INACIF surge por la necesidad de contar con una figura jurídica y técnica investigativa en el sector de justicia, que garantizara la confiabilidad e imparcialidad de las investigaciones forenses.

La institución unifica los servicios forenses periciales desde un enfoque técnico y científico, y lo realiza de manera autónoma. La evolución de sistemas informáticos permite a la institución incorporar nuevas herramientas tecnológicas en sus procesos para mejorar la eficiencia en sus actividades.

1.1.2. Misión

“Somos la Institución responsable de brindar servicios de investigación científica forense fundamentada en la ciencia y el arte, emitiendo dictámenes

periciales útiles al sistema de justicia, mediante estudios médico-legales y análisis técnico-científicos, apegados a la objetividad y transparencia."[1]

1.1.3. Visión

"Ser una Institución reconocida y altamente valorada a nivel nacional e internacional, por su liderazgo en las ciencias forenses, los aportes a la investigación científica, la calidad en la gestión institucional y el respeto a la dignidad humana."[2]

1.2. Servicios forenses

INACIF ofrece una serie de servicios periciales forenses de alta calidad y emite dictámenes técnicos científicos basados en sus investigaciones.

1.2.1. Clínica Forense

Realiza investigaciones relacionadas con evaluaciones médicas a personas vivas. En este tipo de investigaciones se determinan lesiones personales que un posible agresor ocasione a la integridad personal de un individuo, incluyendo agresiones sexuales. Servicios: reconocimientos médicos forenses, toma de muestras y levantamiento de indicios.

[1] Inacif. *Historia*. https://www.inacif.gob.gt/index.php/inacif/historia. Consulta: 5 de enero de 2022.
[2] Ibíd.

1.2.2. Tanatología

Realiza necropsias médico-legales para determinar la causa de muerte de un individuo, adicional incluyen en su reporte una serie de indicios que puedan orientar al investigador. Efectúa necropsias médico-legales a cadáveres exhumados según la autoridad competente lo requiera.

1.2.3. Odontología Forense

Determina lesiones de una persona específicamente en la cavidad oral, puede determinar el rango de edad e identificar personas fallecidas.

1.2.4. Antropología Forense

Reconocimientos antropológicos forenses que incluye análisis y estudio de restos óseos para determinar la causa de muerte o lesiones.

1.2.5. Psicología Forense

Realiza evaluaciones a personas involucradas en una agresión para determinar alternaciones o afecciones psicológicas que propiciaron el hecho (victimario) o secuelas del hecho (víctima).

1.2.6. Psiquiatría Forense

Evaluaciones para determinar condición mental, enfermedad mental, capacidad para asistir a juicio e incapacidades.

1.2.7. Balística

Evaluaciones para relacionar o desligar un arma de un hecho delictivo. Análisis sobre armas de fuego, casquillos, proyectiles, municiones, fragmentos, entre otros.

1.2.8. Fisicoquímica

Análisis por microscopía electrónica para determinar residuos de fulminantes, ubicando partículas de elementos químicos en muestras tomadas en manos de personas sospechosas de haber disparado un arma. Comparar fragmentos de pintura para relacionar partes de pintura automotriz con un vehículo sospechoso. Determinar presencia de combustibles en objetos o prendas para establecer si una persona pudo provocar un incendio. Otros estudios químicos específicos para confirmar evidencias.

1.2.9. Toxicología

Análisis para determinar la presencia de sustancias que pudieran causar daño o la muerte en alguna persona. Las pruebas se realizan en sangre, contenido gástrico, orina, entre otras.

1.2.10. Sustancias controladas

Análisis para confirmar sustancias dentro del grupo de drogas ilícitas típicas: cocaína, marihuana, heroína, morfina, anfetaminas, amapola y precursores.

1.2.11. Serología

Diagnóstico genérico para determinar la presencia de sangre, saliva, semen o espermatozoides. Estudios importantes en las investigaciones de posibles agresiones sexuales.

1.2.12. Genética

Análisis para establecer filiaciones por paternidad y maternidad, identificaciones de cadáveres cuando otros métodos no lo han confirmado plenamente.

1.2.13. Lofoscopía

Cotejo de impresiones digitales en documentos personales, revelado de huellas en objetos, obtención de huellas dactilares, cotejo de huellas en documentos con sospecha de alteración.

1.2.14. Vehículos

Investigaciones en vehículos involucrados en algún acto delictivo para determinar modificaciones referentes al chasis, motor o serie.

1.2.15. Lingüística y acústica

Las evaluaciones en este laboratorio determinan si los documentos escritos o comunicaciones orales evidencian denuncias como: discriminación racial, social, amenazas, insultos, coacciones, entre otras.

1.2.16. Documentoscopía

Se realizan pericias para determinar alternaciones en documentos y cotejo de firmas. Posibles modificaciones en escrituras, licencias, pasaportes, entre otros.

1.3. Descripción de necesidades

El Departamento Administrativo Financiero -DAF- posee un grupo de aplicaciones web que soportan procesos específicos de la institución e importantes en sus actividades diarias. Estas aplicaciones integran componentes de autenticación diferentes, por lo que cada aplicación implementa credenciales diferentes e independientes.

La institución requiere actualizar la arquitectura de sus aplicaciones, referente a autenticación. Esta arquitectura debe tomar en cuenta:

- Seleccionar un *software* que permita centralizar la autenticación de los usuarios a sus aplicaciones.

- Vincular el anterior *software* al actual directorio activo, esto permite que las credenciales de acceso sean las mismas con las que el usuario inicia sesión en sus equipos de cómputo.

- Modificar las aplicaciones existentes del DAF para integrar este nuevo componente.

2. FASE TÉCNICO PROFESIONAL

2.1. Investigación preliminar para la solución del proyecto

Para establecer el alcance de este proyecto es necesario definir los lineamientos y herramientas que permitan que su implementacion sea adecuada.

2.1.1. Aplicaciones Web

Las aplicaciones web son recursos tecnológicos que están disponibles y son accesibles a través del internet o intranet. No es necesario instalar ningún componente para utilizarlos porque procesan y trasladan la información por la red, únicamente se necesita un navegador web.

Dependiendo su naturaleza y objetivo existen diferentes tipos de aplicaciones como: compras de artículos en línea, páginas de publicidad, banca en línea, entre otras. Existe un grupo de aplicaciones consideradas “desarrollos a la medida” en la que diferentes entidades digitalizan y automatizan sus procesos, de acuerdo a sus propias necesidades.

2.1.1.1. Ventajas

- Disponibilidad: las aplicaciones web están inmediatamente disponibles bajo un dominio o dirección URL.

- Completa compatibilidad: existen diferentes navegadores web que cumplen adecuadamente los estándares de navegación y consumo de aplicaciones.

- Actualización inmediata: una actualización se realiza refrescando la página que el usuario visita en el momento. Esto se debe a que los ficheros de las aplicaciones se encuentran centralizadas en el servidor web.

- Multiplataforma: las aplicaciones web no dependen del sistema operativo o equipo utilizado, únicamente se necesita que el dispositivo a utilizar tenga un navegador web.

2.1.1.2. Riesgos

- Fuga de información: los recursos consultados pueden ser descargados o visualizados desde dispositivos o localizaciones no permitidas.

- Datos sensibles: dentro de la red también circulan información sensible: datos de tarjetas de créditos, datos de contacto, credenciales, entre otras. Inicialmente los datos viajaban sin ningún mecanismo de encriptación (http), posteriormente los sitios implementan certificados digitales (https) que permiten encriptar los datos que viajan sobre la red del punto de origen al destino, esto impide que la información sea legible, incluso si fuese capturada.

- Usuarios sin restricción de acceso: se necesita segmentar los accesos de acuerdo al rol del usuario. Por ejemplo: en una plataforma de banca virtual, un usuario no debe visualizar los datos de otros clientes como

saldos de otras cuentas y datos sensibles, únicamente lo que corresponde con el usuario que ingresó a la aplicación.

- Phising: sitios con apariencia de “legítimos” que buscan capturar datos sensibles o credenciales de acceso de plataforma para ser uso malicioso de dichos datos. Por ejemplo: un sitio con un dominio diferente de banca en línea que solicita usuario y clave de usuario, pero son aplicaciones ajenas.

2.1.2. Autenticación de aplicaciones

Las aplicaciones no públicas necesitan identificar al usuario que interactúa con el sistema. Los componentes de autenticación tienen la responsabilidad resguardar el acceso y brindar mecanismos de identificación. Existen datos que representan activos intangibles de gran valor para las instituciones, por ende, es importante gestionar la identidad y acceso de los usuarios.

El mecanismo de autenticación universal es usuario y clave, aunque existen otros mecanismos que permiten añadir otra capa de seguridad para validar la identidad del usuario, tales como: OTP, certificados PKI o token usb, biométricas, entre otras.

La página de inicio de sesión se convierte en la página de bienvenida de las aplicaciones web. Con objetivos maliciosos, terceros buscan aprovechar las vulnerabilidades de las aplicaciones para obtener información sensible de clientes o suplantar a usuarios.

2.1.3. Desarrollo de componente de autenticación

Las aplicaciones web en sus inicios planteaban arquitecturas monolíticas, su fundamento era que los diferentes componentes de una aplicación existiesen como un todo y el componente de autenticación no era excepción. De acuerdo a esta arquitectura, cada aplicación tiene su propio mecanismo de autenticación y desarrollado a la medida. Al aumentar la cantidad de aplicaciones web se evidenció que cada aplicativo contaba con componentes de autenticación distintos.

El desarrollo de este componente heterogéneo tiene una consecuencia importante en este estudio: cada aplicación tendrá su propio conjunto de credenciales, esto implica que cada usuario tendrá una credencial diferente por cada aplicación.

2.1.4. Directorio activo

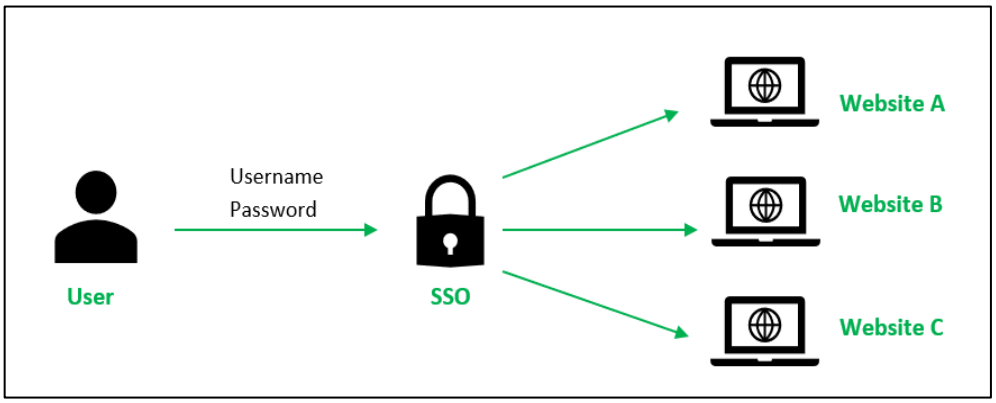
Un directorio es una estructura abstracta que almacena información arbitraria en la red. Un servicio de directorio como Active Directory Domain Services de Microsoft provee la funcionalidad de almacenamiento de datos en el directorio y hacerlo disponible en la red. Es común utilizarlo para almacenar información de usuarios, credenciales, e información adicional de identidad: número de teléfono, puesto, código de empleado, entre otras. Con esta información permite a equipos de cómputo, registrados en la red, autenticarse en un dominio específico.

2.1.5. Single Sign On (SSO)

Es un servicio de sesión y de autenticación que permite, con un único conjunto de credenciales (usuario y clave, regularmente), autenticarse a múltiples aplicaciones. Es la implementación de una arquitectura más desacoplada que permite delegar la responsabilidad de identidad de acceso.

SSO está bajo el acuerdo de Administración de Identidad Federada (FIM) y utiliza el estándar Oauth como intermediario en el proceso de autenticación. El proceso consiste en que una aplicación delega la responsabilidad de autenticación a un tercero. Oauth es el estándar de comunicación entre estos componentes en la validación y negociación. El objetivo es centralizar la autenticación a múltiples aplicaciones.

Figura 1. **Modelo SSO**



Fuente: LIMA, Acervo. *Introducción del Inicio de Sesión Único.* https://es.acervolima.com/introduccion-del-inicio-de-sesion-unico-sso/. Consulta: 2 de enero de 2022.

Las ventajas principales de SSO son: reducir la cantidad de credenciales, minimizar el riesgo en phising y reducir la carga operativa en informática en cuanto a resolver problemas de inicio de sesión.

2.1.6. SSO y directorio activo

Ambos componentes son independientes y pueden utilizarse en conjunto para aprovisionar una capa de autenticación centralizada y que las credenciales de acceso sean del propio directorio activo, esta configuración es denominada “federar” usuarios a través de Single Sign On.

2.1.7. KeyCloak y Microsoft Active Directory

SSO y Directorio Activo son conceptos teóricos y existen varias herramientas para su implementación. Para objeto de estudio se hace referencia a Directorio Activo al *software* desarrollado por Microsoft Active Directory Domain Services y KeyCloak para la implementación de SSO.

KeyCloak es una herramienta de administración de acceso e identidad de código abierto. Esta herramienta permite la implementación de Single Sign On y la federación de usuarios hacia servidores Microsoft Active Directory. INACIF posee un servidor que se utiliza para la autenticación de sus colaboradores en la intranet, a través de sus equipos de cómputo.

2.2. Presentación de la solución al proyecto

La solución al problema de múltiples cuentas por usuarios es unificar los componentes de autenticación. Para centralizarlo se utiliza Keycloak para

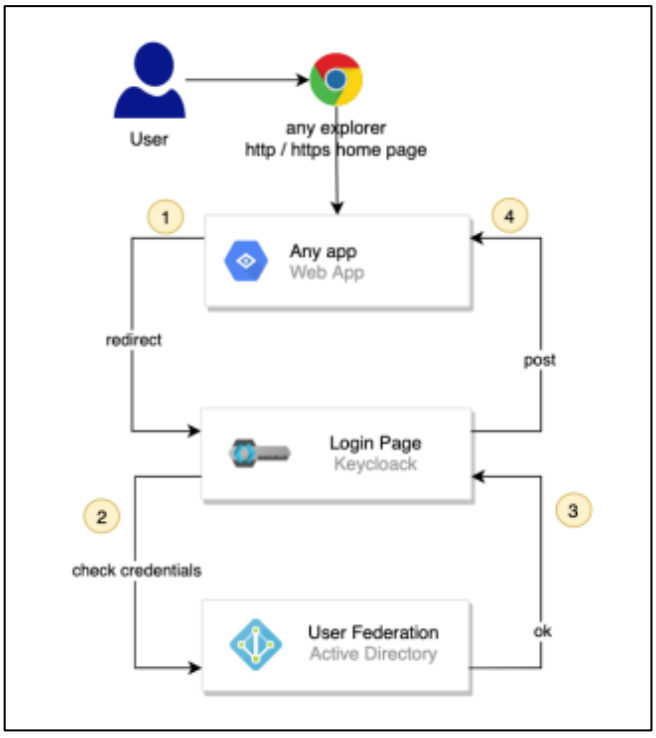
aprovisionar un solo método de autenticación y se integra hacia Directorio Activo por protocolo ldap.

Todo colaborador de INACIF posee usuario en el Directorio, dicho usuario es esencial para iniciar sesión en los equipos desde la red, por ende, estas serán las credenciales seleccionadas en el proceso de unificación de credenciales.

2.2.1. Flujo de autenticación propuesto

Toda aplicación deberá seguir el siguiente estándar de autenticación:

Figura 2. **Flujo de autenticación propuesto**



Fuente: elaboración propia, empleando Draw.io.

- La página de inicio de las aplicaciones redirecciona al usuario a un formulario de autenticación de Keycloak.

- El usuario ingresa credenciales conocidas en el dominio.

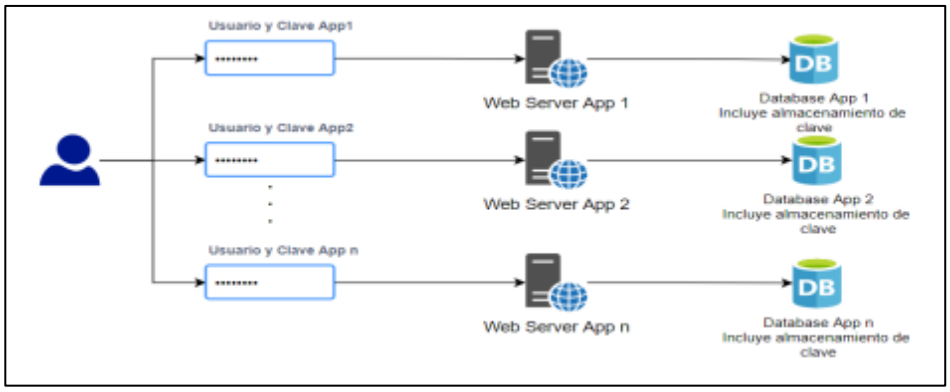
- Keycloak a través de la federación de usuarios sincroniza los usuarios y permita consultar las credenciales hacia el Directorio Activo existente en INACIF.

- Al verificar las credenciales correctas debe redireccionar a la plataforma otorgando accesos al mismo.

2.2.2. Experiencia de usuario en implementación

El usuario actualmente ingresa al formulario de autenticación de cada aplicación web. Estas credenciales son almacenadas y validadas por la propia aplicación. Las claves de acceso son distintas para cada aplicación.

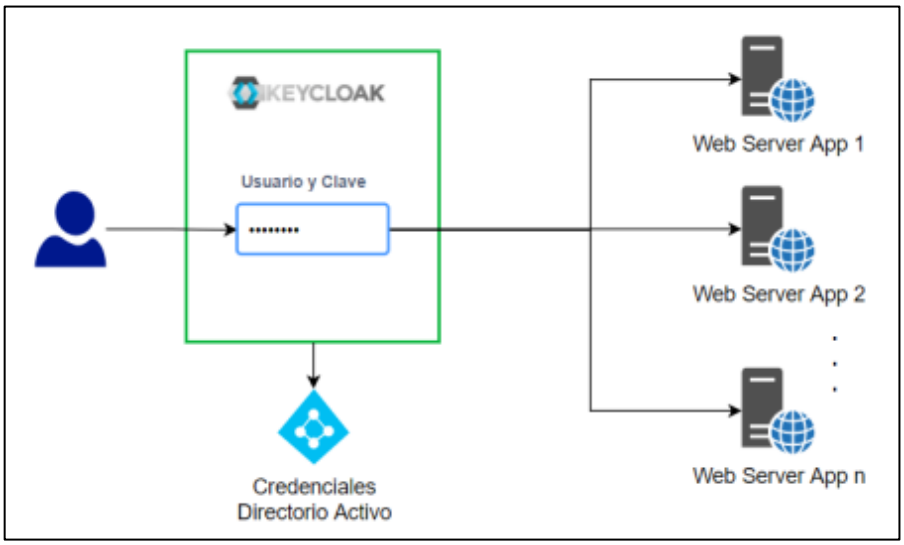
Figura 3. **Arquitectura actual del componente de autenticación**



Fuente: elaboración propia, empleando Draw.io.

Posterior a la implementación de Keycloak e integración en las diferentes aplicaciones, el usuario ingresa a un único formulario de autenticación y las claves de ingreso para cualquier aplicación son las mismas que utiliza para iniciar sesión en sus equipos de cómputo. Los accesos y permisos de cada aplicación en esta integración funcionan de manera transparente, independientemente del tipo de autenticación a utilizar. La homologación de usuarios se realiza al identificar al colaborador y sus permisos a través de los atributos: código de empleado o DPI.

Figura 4. **Arquitectura propuesta para autenticación**



Fuente: elaboración propia, empleando Draw.io.

2.2.3. Mejoras en directorio activo

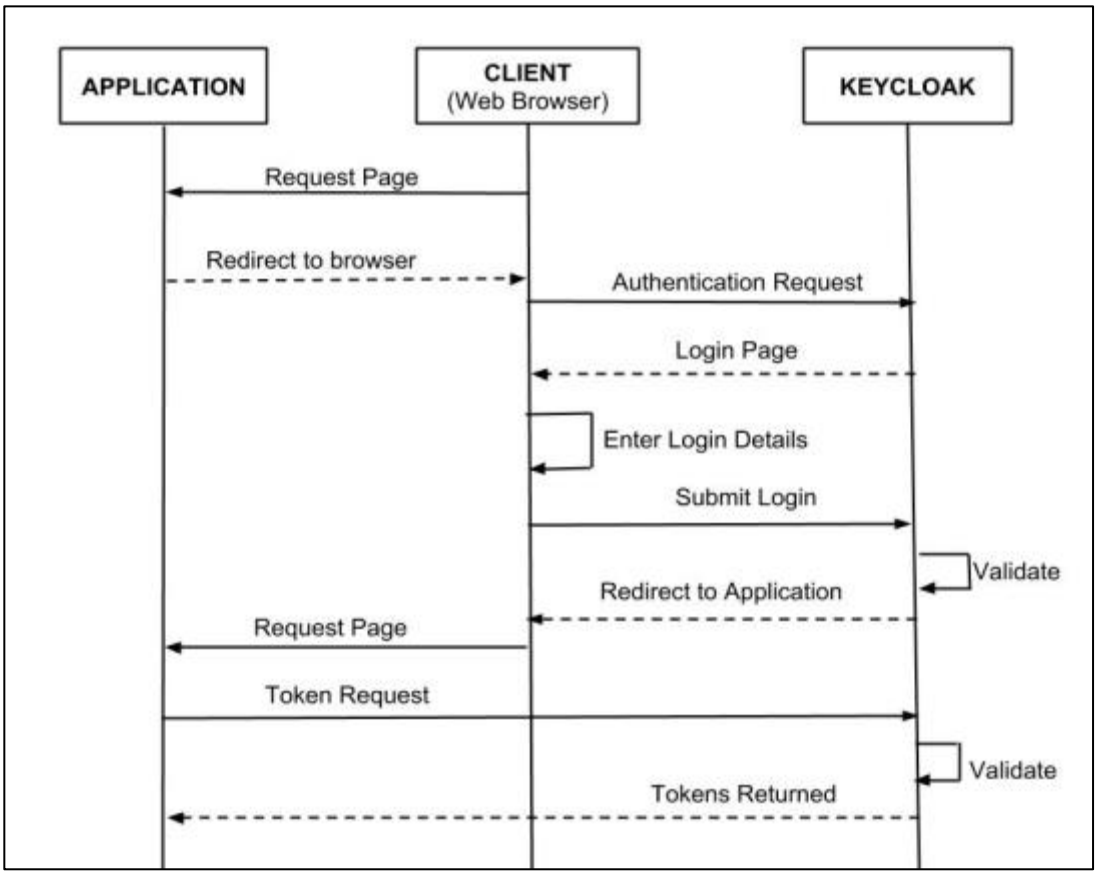
Para homologar los usuarios locales de las aplicaciones y los usuarios en el SSO se requiere modificar algunas propiedades. La solicitud inicial es

madurar la información de los usuarios agregando algunos atributos principales: código de empleado y DPI.

2.2.4. Protocolo y estándar de comunicación

Keycloak es una componente independiente y las aplicaciones necesitan interactuar con dicho componente. El estándar de comunicación es oAuth2.0.

Figura 5. **Diagrama de secuencia de SSO en Keycloak**



Fuente: CoMakeIT. *Quick guide to using Keycloak for identity and Access management.* https://www.comakeit.com/blog/quick-guide-using-keycloak-identity-access-management/.Consulta: 2 de enero de 2022.

2.2.5. Integración en aplicaciones existentes

Las aplicaciones del Departamento Administrativo Financiero del INACIF necesitan modernizar su componente de autenticación. Para cada aplicativo se analiza y de manera estratégica se modifica el código fuente para añadir la funcionalidad de SSO.

Tabla I. **Aplicaciones Web en Departamento Administrativo Financiero**

Nombre de aplicación	Tecnología
Sistema de Documentos de la Unidad de Gestión y Acreditamiento de la Calidad	.net Framework
Sistema de Actualización de datos de los Empleados	.net Framework
Firmas electrónicas	.net Framework
Sistema de Compras	.net Framework

Fuente: elaboración propia, empleando Microsoft Excel.

2.3. Planificación

Para el desarrollo y seguimiento del proyecto se proyectan actividades generales en la fase de ejecución.

Tabla II. **Planificación de proyecto**

Recurso	Ago	Sept	Oct	Nov	Dic	Ene
Instalación de Keycloak e integración con Directorio Activo	**X**					
Integración de SSO aplicación 1		**X**				
Integración de SSO aplicación 2			**X**			
Integración de SSO aplicación 3				**X**		
Integración de SSO aplicación 4					**X**	
Certificación y entrega de aplicaciones en ambientes productivos						**X**

Fuente: elaboración propia, empleando Microsoft Excel.

2.4. Costos del proyecto

Para este proyecto se establece la siguiente proyección de costos. Esta proyección incluye el detalle de los recursos económicos necesarios para su ejecución.

Tabla III. **Detalle de costos del proyecto**

Recurso	Cantidad	Costo unitario	Subtotal
Macbook pro 13 ” 8 GB de RAM 256 SSD	1	Q15 000,00	Q15 000,00
Monitor 24”	1	Q1 500,00	Q1 500,00
Teclado y mouse inalámbricos	1	Q500,00	Q500,00
Mensualidad de internet de 15mb	6	Q350,00	Q2 100,00
Proporción de cuota de energía eléctrica	6	Q200,00	Q1 200,00
Servidores virtualizados Linux con 8GB de RAM 2 cores y 80GB disco	2	Q10 000,00	Q20 000,00
Salario de Ingeniero de *software*	6	Q15 000,00	Q90 000,00
Asesoría de facultad de ingeniería	6	Q4 000,00	Q24 000,00
Total			**Q154 300,00**

Fuente: elaboración propia, empleando Microsoft Excel.

2.5. Beneficios del proyecto

Además de alcanzar los objetivos de este proyecto, existe una serie de beneficios adicionales para las aplicaciones tecnológicas de la institución.

2.5.1. Usabilidad

Se facilita al usuario el acceso a las aplicaciones. Necesita una única clave para ingresar a todas las aplicaciones del departamento, por lo que podrá despreocuparse de recordar cada credencial por aplicación.

2.5.2. Disminuir riesgos en seguridad

Se disminuye el riesgo de malas prácticas como escribir credenciales en papel, cuadernos o archivos planos, que pueden materializarse en fuga de información o suplantación de identidad.

2.5.3. Componente centralizado y reutilizable

SSO es un estándar de industria y su implementación escala en número de aplicaciones y tipo de aplicaciones. Keycloak es agnóstico a la tecnología de la aplicación que desea integrarse.

2.5.4. Actualización de aplicaciones

Las aplicaciones del departamento tienen una versión de Framework obsoleta y requieren de la actualización para utilizar SSO. Las aplicaciones se benefician indirectamente en este proyecto para instalación de parches de seguridad, obsolescencias y mantenimiento.

2.6. Desarrollo de proyecto

La implementación de este proyecto abarca la instalación de Keycloak como herramienta de gestión SSO, configuaración de plataforma, conexión hacia Directorio Activo, adecuación de código fuente y publicación de aplicaciones del Departamento Administrativo Financiero de INACIF.

2.6.1. Configuración Keycloak

La primera fase de desarrollo contempla las configuraciones necesarias en el servidor de Keycloak.

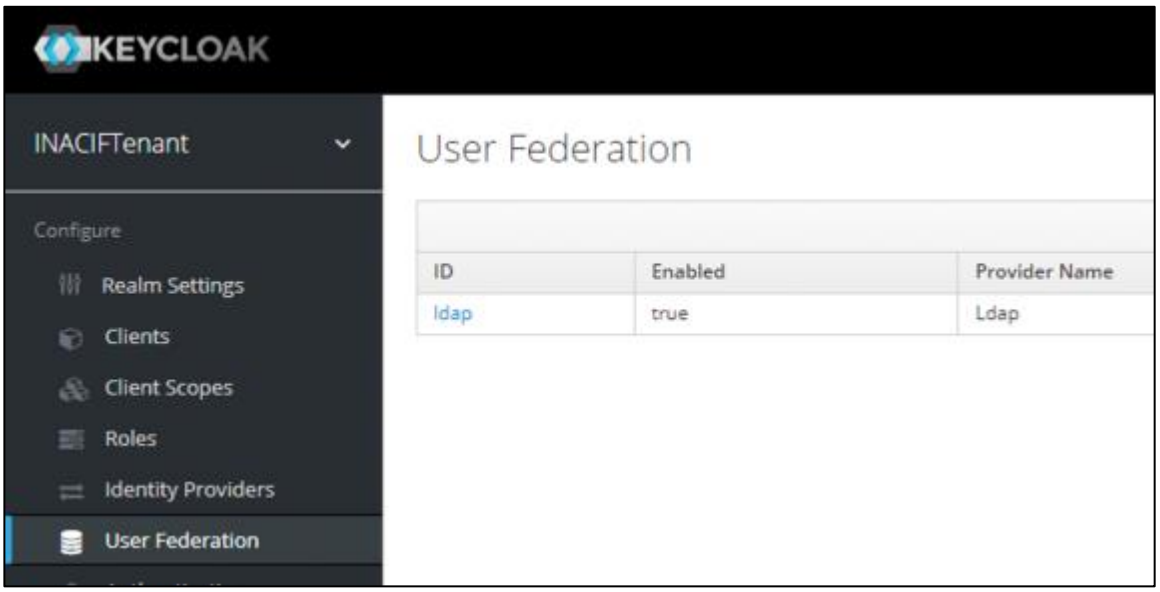
2.6.1.1. Supuestos

Se cuenta con una instancia inicial de Keycloak sin ninguna configuración. Se brinda el acceso con usuario privilegiado para realizar las configuraciones.

2.6.1.2. Usuarios federados

Se requiere configurar la instancia de Keycloak para sincronizar usuarios del Directorio Activo de INACIF a esta plataforma. Dicha configuración identifica la Unidad Organizacional (OU) de los usuarios y se establece en modo de lectura. La herramienta es capaz únicamente de leer atributos de usuarios, pero no modificarlos.

Figura 6. **Conectividad Keycloak y Microsoft Active Directory**

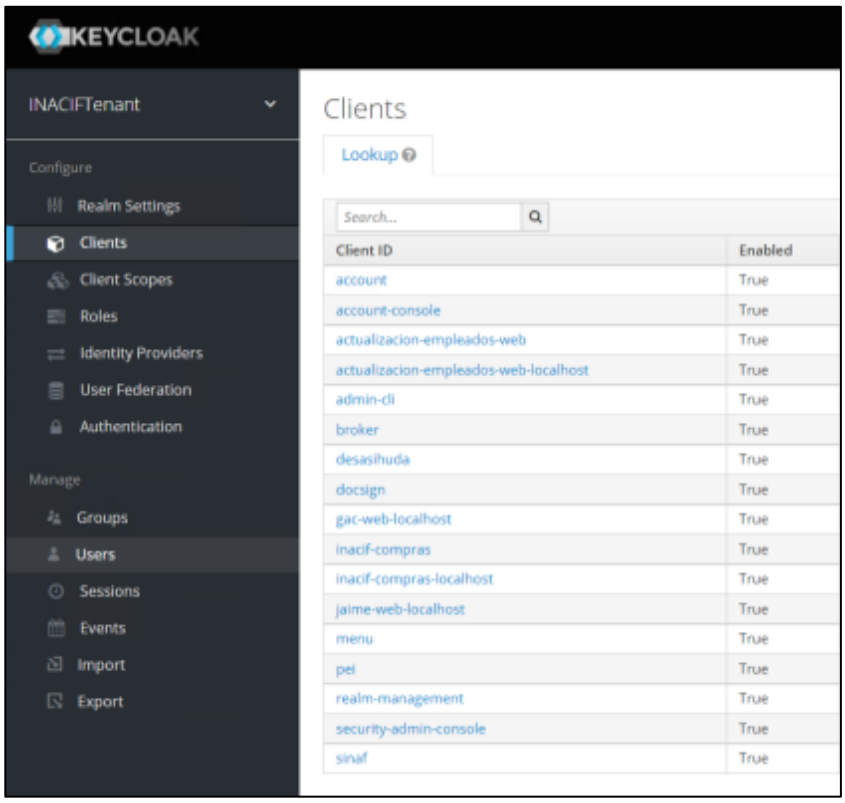


Fuente: INACIF. *Consola administrativa de Keycloak*. *Sección de usuarios federados.* https://www.keycloak.org/docs/15.0/server_admin/. Consulta: 2 de enero de 2022.

2.6.1.3. Clientes

Cada aplicación web hace referencia a un cliente dentro de Keycloak. Un cliente contiene todas las propiedades de una aplicación web y el acceso a integrarse. Algunas propiedades importantes son: dirección de la aplicación web (URL), protocolo de conexión, tipo de acceso, entre otros.

Figura 7. **Listado de aplicaciones en Keycloak**



Fuente: INACIF. *Consola administrativa de Keycloak*. *Sección de usuarios federados.* https://www.keycloak.org/docs/15.0/server_admin/. Consulta: 2 de enero de 2022.

2.6.2. Integración de SSO en aplicaciones actuales

La segunda fase de desarrollo implica la integración de SSO a las aplicaciones existentes del Departamento Administrativo Financiero de INACIF.

2.6.2.1. Alcance

Se contempla la modificación de código fuente, integración de SSO, despliegue en ambientes productivos y certificación de las cuatro aplicaciones del departamento.

2.6.2.2. Entorno de desarrollo

Las aplicaciones por integrar son plataformas Microsoft con lenguajes de programación CSharp y Visual Basic. Algunas plataformas tienen versiones obsoletas, parte de este proyecto es migrar a las versiones más recientes para soportar la integración con SSO. Estas aplicaciones utilizan como herramienta auxiliar de desarrollo Devexpress 2016, *software* que facilitan el desarrollo de controles en las aplicaciones web.

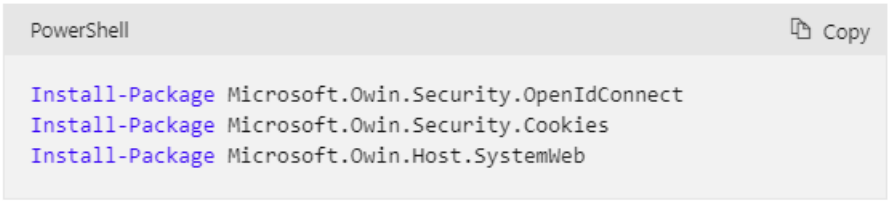
El IDE para desarrollo por defecto es Visual Studio en su versión gratuita 2019. Se requiere migración de aplicaciones con Visual Studio versión 2008 o 2010. El marco de trabajo en el desarrollo de estos proyectos es .net Framework, que funciona exclusivamente en ambientes Windows.

La publicación de los servicios web se realiza en servidores Windows Server 2016 con IIS instalado.

2.6.2.3. Gestor de paquetes

NuGet es el gestor de paquetes para aplicaciones .net por defecto. Es el encargado de instalar y actualizar todas las dependencias de *software* con terceros que una aplicación posea. Se utiliza para la instalación de las librerías de SSO

Figura 8. **Instalación de librerías SSO**

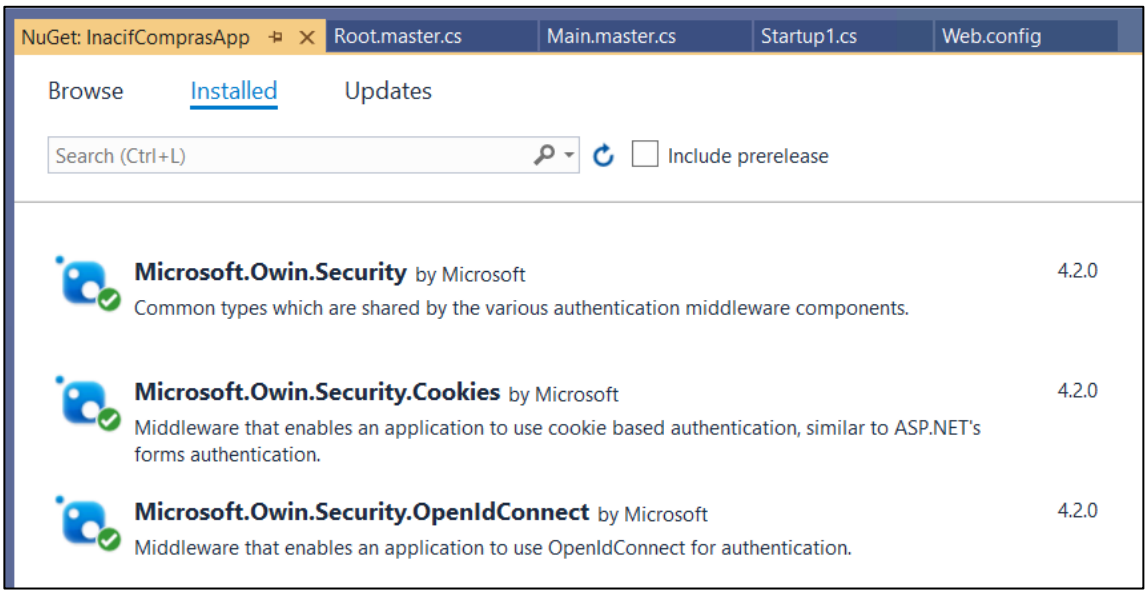


Fuente: Microsoft. *Add sign-in to Microsoft to an ASP.NET web app.* https://docs.microsoft.com/en-us/azure/active-directory/develop/tutorial-v2-asp-webapp.Consulta: 2 de enero de 2022.

2.6.2.4. Librerías

SSO expone varios protocolos con los cuales un cliente puede interactuar con este componente. Para el desarrollo de este proyecto se realiza a través del protocolo OpenId. Se utilizan las librerías nativas de Microsoft: Microsoft.Owin.Security.OpenId Connect, Microsoft.Owin.Security.Cookies y Microsoft.Owin.Host.SystemWeb. Estas librerías encapsulan y abstraen la implementación de SSO a las aplicaciones web existentes.

Figura 9. **Librerías NuGet**

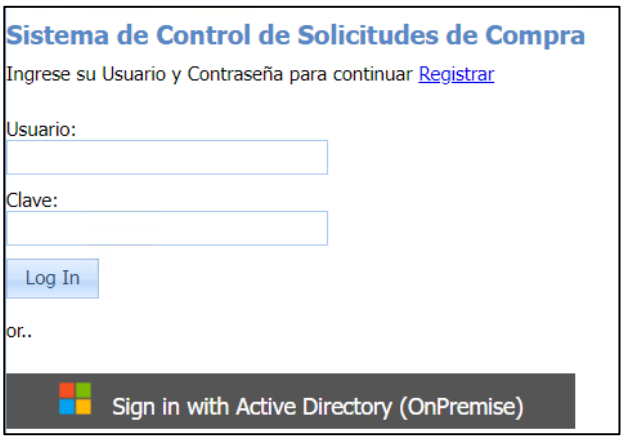


Fuente: Visual Studio Community 2019. *Gestor de paquetes NuGet.* https://www.google.com/search?q=Visual+Studio+Community+2019.+Gestor+de+paquetes+. Consulta: 8 de enero de 2022.

2.6.2.5. Dualidad en autenticación

Las integraciones de SSO en las aplicaciones contemplan una dualidad de autenticación, lo que permitirá a los usuarios decidir el mecanismo para identificarse: ingresar mediante las credenciales de la aplicación local o hacer uso del SSO con credenciales del directorio activo. Esta dualidad es exclusivamente en el inicio de sesión, después de ello el usuario mantiene el rol y permisos.

Figura 10. **Aplicaciones web con dos métodos de autenticación**



Fuente: INACIF. *Aplicación de Sistema de Control de Solicitudes de Compra.* https://www.inacif.gob.gt/. Consulta: 8 de enero de 2022.

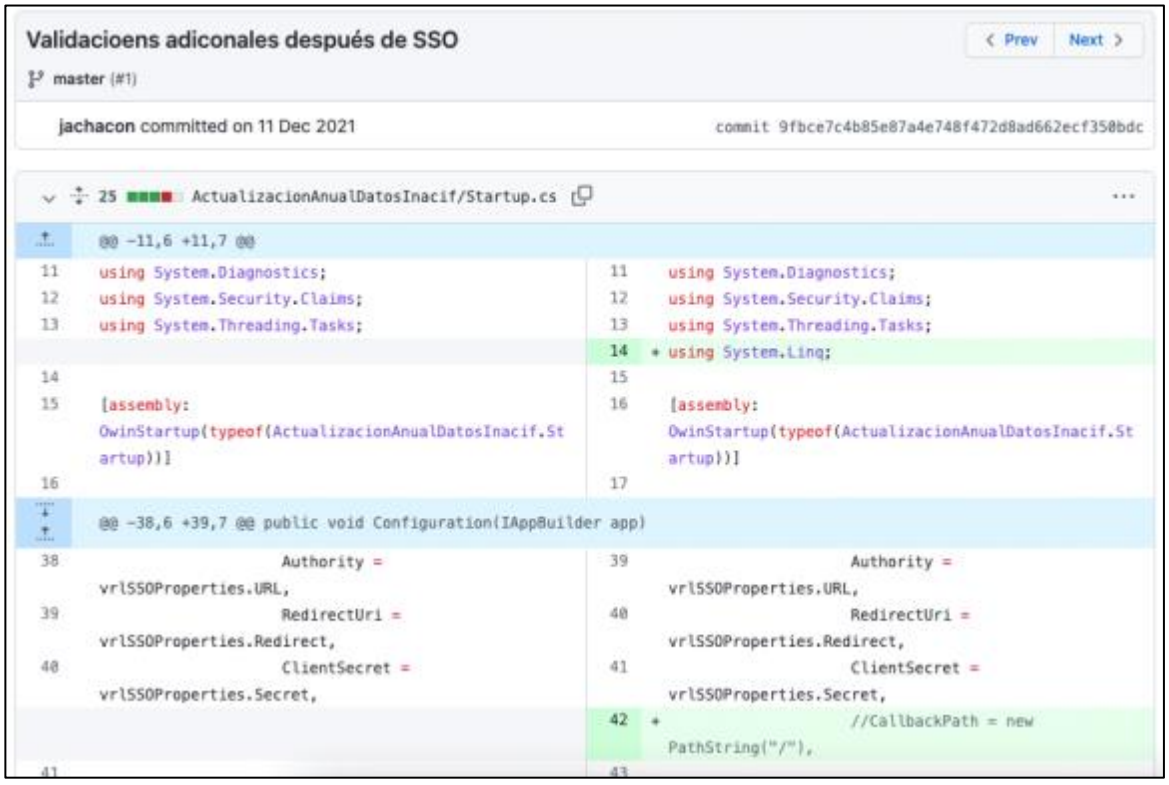
Figura 11. **Autenticación SSO**

Fuente: INACIF. *Página de inicio de sesión en Keycloak*. https://www.inacif.gob.gt/. Consulta: 8 de enero de 2022.

2.6.2.6. Control de Versiones

Para la gestión de modificaciones al código fuente se utiliza la estrategia de ramificación “Trunk Based Development”. Se cuenta con una rama principal que contiene el código fuente antes de iniciar el proyecto, se desarrollan los cambios en ramas aisladas y posteriormente se integran las funcionalidades en la rama principal. Para comparar, revisar y autorizar los cambios se utiliza Pull Request, funcionalidad en Github para integrar cambios entre ramas.

Figura 12. **Integraciones de código fuente**



Fuente: Github. *Pull Request que evidencia las modificaciones en las aplicaciones del DAF.* https://aws.amazon.com/es/blogs/aws-spanish/aws-single-sign-on-sso-la-proxima-evolucion/. Consulta: 2 de febrero de 2022.

3. FASE ENSEÑANZA APRENDIZAJE

3.1. Entregables

Los resultados de este proyecto se evidencian a través de la entrega de código fuente, servidores productivos y aplicaciones operando de manera adecuada.

3.1.1. Código fuente

Se hace entrega de cuatro repositorios de código fuente bajo el control de versiones GIT. En estos artefactos es posible evidenciar a través del histórico las modificaciones realizadas al código fuente de las aplicaciones, fecha y hora del mismo.

3.1.2. Artefactos en ambiente productivo

Se despliegan las cuatro aplicaciones en ambientes productivo: traslado de ficheros a servidor, instalación y configuración en servidor web IIS. Se entrega de manera adicional, una página web con el listado de aplicaciones disponibles y facilitar al usuario la navegación entre plataformas.

3.1.3. Servidor Keycloak

Se hace entrega de servidor que contiene la instalación de Keycloak con todas las configuraciones para operar SSO a través de usuarios federados y los

diferentes clientes, que representan las aplicaciones migradas a este nuevo modelo de autenticación.

3.1.4. Certificación

Se realiza acompañamiento en la certificación en ambientes productivos, adecuaciones que garanticen la usabilidad y experiencia de usuario en esta integración.

CONCLUSIONES

1. Se implementa y configura el SSO sobre Keycloak para centralizar la identidad de acceso y se modifican todas las aplicaciones del Departamento Administrativo Financiero del INACIF para incorporar el nuevo mecanismo de autenticación. Al añadir esta funcionalidad se mantiene el inicio de sesión tradicional. El usuario tiene la capacidad de decidir si utilizar las credenciales de la aplicación o hacerlo vía SSO.

2. Se realiza la integración de Keycloak hacia el Directorio Activo de INACIF. La sincronización de los usuarios a esta plataforma permite que las credenciales a utilizar en el SSO sean las alojadas en este Directorio. Esto es conocido como usuarios federados.

3. Se añaden los atributos de código de empleado y CUI en el Directorio Activo. Una carga masiva modifica los usuarios de todos los colaboradores de INACIF, esto permite a los usuarios mantener su rol y permisos, independientemente del método de identificación que utilicen: local o SSO.

RECOMENDACIONES

1. Ampliar el catálogo de aplicaciones existentes de otras áreas de la institución y estandarizar el SSO para desarrollo de nuevos proyectos tecnológicos.

2. Declarar el Directorio Activo como único repositorio de metadatos de los colaboradores. Permitiría a otras aplicaciones obtener información centralizada. Actualmente la información personal de los colaboradores es almacenada de manera independiente y repetida, posible riesgo de la integridad de los datos.

3. Realizar prueba de concepto de la administración de permisos dentro de Keycloak y evaluar la centralización de roles en la herramienta; similar al desacoplamiento de inicio de sesión de las aplicaciones.

BIBLIOGRAFÍA

1. INACIF. *Historia: Antecedentes, misión y visión.* [en línea]. <https://www.inacif.gob.gt/index.php/inacif/historia.>. [Consulta: 2 de enero de 2022].

2. _____. *Guía completa de servicios.* [en línea]. <https://www.inacif.gob.gt/docs/uip/InformacionPublicadeOficio-numeral06-01.pdf.>. [Consulta: 2 de enero de 202.].

3. Microsoft. *Add sign-in to Microsoft to an ASP.NET web app.* [en línea]. <https://docs.microsoft.com/en-us/azure/active-directory/develop/tutorial-v2-asp-webapp>. [Consulta: 8 de enero de 2022].

4. Red Hat. *Keycloak: Open Source Identity and Access Management.* [en línea]. <https://www.keycloak.org/>. [Consulta: 5 de enero de 2022].

5. _____. *Keycloak: Server Administration Guide.* LDAP and AD. [en línea]. <https://www.keycloak.org/docs/latest/server_admin/#_ldap.>. [Consulta: 2 de enero de 2022].

6. TERAVAINEN, Taina. *Single Sign On.* [en línea]. <https://searchsecurity.techtarget.com/definition/single-sign-on>. [Consulta: 8 de enero de 2022].