# PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE ESMERALDAS

## ESCUELA DE SISTEMAS Y COMPUTACIÓN

**ESTUDIO DE CASO:**

**"ANÁLISIS DE FACTIBILIDAD DE PROCEDIMIENTO DE AUTENTICACIÓN ÚNICA PARA ACCEDER A LOS SERVICIOS INFORMÁTICOS DE LA PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR-SEDE ESMERALDAS"**

**PREVIO AL GRADO ACADÉMICO DE INGENIERÍA EN SISTEMAS Y COMPUTACIÓN:**


**AUTOR:**

BRYAN ALEXANDER SEVILLA DELGADO

**ASESOR:**

MGT. WILSON GUSTAVO CHANGO


Esmeraldas – Enero, 2018

Estudio de caso aprobado luego de haber dado cumplimiento a los requisitos exigidos, previo a la obtención del título de INGENIERO EN SISTEMAS Y COMPUTACIÓN.

## TRIBUNAL DE GRADUACIÓN

**Título: "**ANÁLISIS DE FACTIBILIDAD DE PROCEDIMIENTO DE AUTENTICACIÓN ÚNICA PARA ACCEDER A LOS SERVICIOS INFORMÁTICOS DE LA PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR-SEDE ESMERALDAS**"**

**Autor:** BRYAN ALEXANDER SEVILLA DELGADO

**Mgt. Gustavo Chango** **f.-…….……**
**Asesor/a**

**Mgt. Kléber Posligua** **f.-…….**
**Lector #1**

**Mgt. Jaime Sayago** **f.-…….**
**Lector #2**

**Director de Escuela**
**Mgt. Xavier Quiñónez Ku** **f.-…….**

**Ing. Maritza Demera Mejía** **f.- ……....**
**Secretaria General PUCESE**

**Esmeraldas, Ecuador, 2017**

## DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo, **BRYAN ALEXANDER SEVILLA DELGADO** portador de la cédula de identidad No. **0802314732** declaro que los resultados obtenidos en la investigación que presento como informe final, previo a la obtención del título de **"Ingeniero en Sistemas y Computación**" son absolutamente originales, auténticos y personales.

En tal virtud, declaro que el contenido, las conclusiones y los efectos legales y académicos que se desprenden del trabajo propuesto de investigación y luego de la redacción de este documento son y serán de mi sola, exclusiva responsabilidad legal y académica.

BRYAN ALEXANDER SEVILLA DELGADO
**C.I.: 0802314732**

# CERTIFICACIÓN

Mgt. Wilson Gustavo Chango Docente de la PUCESE, certifica que:

El estudio de caso realizado por BRYAN ALEXANDER SEVILLA DELGADO bajo el título "ANÁLISIS DE FACTIBILIDAD DE PROCEDIMIENTO DE AUTENTICACIÓN ÚNICA PARA ACCEDER A LOS SERVICIOS INFORMÁTICOS DE LA PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR-SEDE ESMERALDAS" reúne los requisitos de calidad, originalidad y presentación exigibles a una investigación científica y que han sido incorporadas al documento final, las sugerencias realizadas, en consecuencia, está en condiciones de ser sometida a la valoración del Tribunal encargada de juzgarla.

Y para que conste a los efectos oportunos, firma la presente en Esmeraldas, noviembre de 2017.

Mgt. Wilson Gustavo Chango
Asesor.

## DEDICATORIA

Dedico este trabajo a mi abuela Yolanda Ramírez Torres y a mi madre Lorena Delgado Ramírez, por su apoyo incondicional, siempre estar a mi lado en los momentos más difíciles y ser pilar fundamental en mi vida como estudiante universitario.

## AGRADECIMIENTO

A Dios por haberme dado la fortaleza y salud necesaria para llegar a este punto.

A mi abuela y madre por tener la fuerza, además de la paciencia necesaria para guiarme por el camino indicado, sin ellas este trabajo nunca hubiera podido ser finalizado

Agradezco a mis maestros y asesor por su tiempo brindado en la elaboración de esta investigación.

## RESUMEN.

La presente investigación se desarrolló con el objetivo de analizar la factibilidad de implementar un sistema de autenticación única que permita a los estudiantes acceder a los distintos servicios informáticos de la PUCESE. Se analizó las distintas herramientas y tecnologías que existen para la implementación de un procedimiento de autenticación único y de la misma forma fue necesario identificar la infraestructura tecnológica y el tipo de servicios informáticos que brinda la institución.

En la PUCESE los estudiantes utilizan principalmente cinco servicios web, los cuales son: sistema de consulta de notas, sistema de evaluación académica para estudiantes, Moodle, Microcurricular, correo electrónico institucional.

Durante la investigación se observó que las credenciales que asigna automáticamente la universidad a sus estudiantes, para ingresar a los distintos servicios web son en un alto grado vulnerables, debido a que el número de cédula o matrícula de un estudiante es información pública, que en manos equivocadas proporcionara acceso a información sensible y confidencial.

Finalmente la solución propuesta se desarrollará a un bajo costo, se usará casi en su totalidad software, infraestructura y herramientas brindadas por Microsoft de forma gratuita, debido al contrato campus agreement que existe entre la PUCESE y Microsoft, que permite a sus estudiantes y profesores tengan acceso a varias plataformas libremente, entre las que se encuentran Office 365, Microsoft Azure, entre otras.



**Palabras clave:** Single Sing On, PUCESE, protocolos de autenticación, aplicaciones web, credenciales, Active Directory.

# ABSTRACT.

The present research was developed with the objective of analyzing whether it is feasible to implement a unique authentication system to access the different computer services by PUCESE to its students. We analyzed the different tools and technologies that exist for the implementation of a unique authentication procedure. In the same way it was necessary to identify the technological infrastructure and what type of computer services the institution provides.

In PUCESE students mainly use five web services, which are: notes consultation system, academic system for students, Moodle, Microcurricular, institutional email.

During the investigation it was observed that the credentials that the university automatically assigns its students to enter the different web services are to a high degree vulnerable, because the number of a student's registration or enrollment is public information, that in the wrong hands provide access to sensitive and confidential information.

Finally, the proposed solution will be developed at a low cost, using almost all software, infrastructure and tools provided by Microsoft for free, because PUCESE belongs to the group of educational units eligible by Microsoft for their students and teachers to have access to several platforms freely, among which are Office 365, Microsoft Azure, among others.



**Keywords:** Single Sing On, PUCESE, authentication protocols, web applications, credentials, Active Directory.

# Índice General.

## Índice de figuras.

## 1. Justificación:

En las instituciones, los usuarios acceden a diferentes aplicaciones y/o servicios con diferentes roles y credenciales generando una gran posibilidad de olvido, ocasionando una no disponibilidad de los servicios, por esto es indispensable independizar la gestión de usuarios de las aplicaciones y/o servicios, independientemente de la tecnología de desarrollo y de los sistemas operativos.

La Pontificia Universidad Católica del Ecuador sede Esmeraldas ofrece varios servicios informáticos dentro de su arquitectura tecnológica; para el acceso a la diversidad de aplicaciones los usuarios manejan claves para cada una de ellas.

En la mayoría de aplicaciones utilizadas en la PUCESE, cuando un usuario olvida sus credenciales de acceso, el técnico encargado del reseteo/bloqueo de contraseñas debe solucionar estos inconvenientes, utilizando tiempo que puede ser aprovechando en labores más importantes.

La implementación de un procedimiento de autenticación única logra un aumento de seguridad debido a que el usuario ingresaría sus credenciales de identificación una vez para el uso de todos los recursos y servicios, de esta manera se evita que el usuario guarde sus contraseñas en algún lugar donde podría quedar expuesto a personas ajenas a dicha información.

La implementación de un sistema de logeo único permite:

- Reducir los tiempos de acceso a los distintos servicios informáticos brindados.
- Aumento en la productividad en el departamento de sistemas, debido a que los requerimientos por reseteo de contraseñas disminuirán significativamente, tiempo y personal que se pueden usar para proyectos de mayor importancia en la institución.
- La administración, gestión y mantenimiento de las credenciales por parte del encargado resulta mucho más fácil de llevar a cabo debido a que toda la información de usuarios, contraseñas, privilegios se encontraría centralizada y ordenada en directorios.

- Optimizar los tiempos de acceso a todas las aplicaciones y/o servicios de las instituciones.

# 2. Objetivos.

## 2.1. Objetivo General:

Analizar la factibilidad de implementar un sistema de autenticación único, para acceder a los distintos servicios informáticos estudiantiles, brindados dentro de la infraestructura tecnológica de la Pontificia Universidad Católica del Ecuador-Sede Esmeraldas.

## 2.2. Objetivos específicos:

- Analizar las distintas herramientas y tecnologías que existen para la implementación de un procedimiento de autenticación único.

- Identificar la infraestructura tecnológica con la que cuenta la PUCESE y qué tipo de servicios informáticos proporciona.

- Identificar las políticas de asignación de credenciales para el uso de los distintos servicios web por parte de la PUCESE a sus estudiantes.

## 3. Informe del caso.

En la actualidad las grandes y medianas empresas manejan varias aplicaciones y sistemas informáticos, usuarios con roles diferentes acceden a diferentes servicios por lo que la demanda de los usuarios por contar con una única credencial para el acceso a los diferentes servicios va en aumento, debido a la alta probabilidad que existe del olvido de varias contraseñas por parte de los usuarios. Aparece la necesidad de implementar una plataforma que brinde una autenticación única, con un alto nivel de seguridad y transparencia; al mismo tiempo que surgen algunas dudas ¿Cómo sería el servicio de Google si en cada ocasión para acceder a YouTube, Gmail, Drive se tuviera que ingresar las credenciales de usuario? ¿Los usuarios recordarían el usuario y contraseña para cada servicio? ¿Se utilizarían en la misma proporción que se lo hace hoy en día?

El uso de las nuevas tecnologías ha facilitado la vida del estudiante universitario, la necesaria presencia del estudiante en el aula de clases, entrega de tareas y exámenes en papel, entre muchos inconvenientes más, concluyeron con la necesidad de automatizar todas estas actividades en servicios o aplicaciones informáticas, como el Moodle.

En la Pontificia Universidad Católica del Ecuador Sede Esmeraldas (PUCESE) los estudiantes utilizan principalmente cinco servicios web, cada uno con sus características e importancia dentro de la institución. Las aplicaciones web son el sistema de consulta de notas, sistema de evaluación académica para estudiantes, Moodle, Microcurricular, correo electrónico institucional.

En el instante de que un estudiante es matriculado se le provee automáticamente de credenciales para acceder a cada uno de estos sistemas, cada credencial varía según las políticas de asignación que tiene la universidad.

El sistema de consulta de notas proporciona a los estudiantes un medio para consultar todas sus calificaciones obtenidas a lo largo de su vida universitaria de forma detallada, en cambio el sistema de evaluación académica permite realizar la evaluación semestral a los docentes y directores de escuela. Con la aplicación Microcurricular los estudiantes pueden

llevar un seguimiento del sílabo de todas las materias donde se encuentran matriculados, y de esta forma observar si se cumplen acorde a la planificación.

Los tres primeros sistemas antes mencionados cuentan con las mismas credenciales de inicio de sesión las cuales son el número de cédula como nombre de usuario y el número de matrícula como contraseña. La credencial de autenticación al Moodle está compuesta por el primer nombre, un punto y el apellido como nombre de usuario, el número de matrícula es la contraseña.

Considerando lo anterior, se observa que las credenciales que asigna automáticamente la universidad a sus estudiantes para ingresar a los distintos servicios web son en un alto grado vulnerables, debido a que el número de cédula o matrícula de un estudiante es información pública, que en manos equivocadas proporcionará acceso a información sensible y confidencial. Por ejemplo un estudiante en determinado caso, puede sustraer las tareas o exámenes subidos al Moodle, como también cualquier persona estaría en la capacidad de extraer las notas de todas las materias, calificar al docente con baja puntuación, por nombrar algunos casos que se pueden suscitar por la suplantación de identidad usando las credenciales de un usuario.

A esto se le suma la no disponibilidad de la opción para modificar las credenciales en los sistemas de notas, académico y Microcurricular, causando una falla de alto riesgo en la seguridad de la información, debido a que los datos utilizados como credenciales de inicio de sesión son de dominio público.

## 3.1. Sistema de inicio de sesión único para los servicios web.

En el interior de una organización, los usuarios utilizan los diferentes servicios y aplicaciones, cada uno con diferentes roles, por lo que la necesidad de tener una única credencial para ingresar a las aplicaciones crece constantemente.

> Al mismo tiempo que los encargados del desarrollo de software de las organizaciones no deberían ocuparse de la gestión y mantenimiento de identidades de los usuarios, puesto que ese tiempo sería restado de sus verdaderas responsabilidades como desarrollador de aplicaciones.(Sandoval & Javier, 2016)

> El desarrollo tecnológico avanza a pasos agigantados, consiguiendo que las personas accedan a la información de forma más sencilla, surgiendo la necesidad de métodos de autenticación eficaces y a su vez complejos, debido que se deberían tener varios usuarios/contraseñas por usuario dependiendo el rol que jueguen en la organización. La facilidad y comodidad que brinda el autenticarse una sola vez para tener acceso a todas las aplicaciones de una plataforma, se ha vuelto un requerimiento indispensable para los usuarios de cualquier empresa o institución. Asimismo estos sistemas de autenticación única deben proporcionar confianza, seguridad, transparencia y alta disponibilidad a la información. (Mendieta & Andrade Navarro, 2015)

> Según (Díaz Barriga, Ríos Kruger & Cohn Muroy, 2015) La Dirección de Informática Académica (DIA) de la Pontificia Universidad Católica del Perú ha creado y desarrollado varios sistemas informáticos dentro del campus de la universidad. Cada sistema solicita una credencial (usuario/contraseña) de autenticación diferente, esto origina un problema a los usuarios los cuales utilizan alrededor de ocho aplicaciones web al día. Con el objetivo de simplificar la tarea de autenticación, la DIA busca implementar un sistema *Single Sing On (SSO)* que permitiría a los usuarios acceder a las aplicaciones web, autenticándose una única vez.

Teniendo en cuenta lo anterior, las organizaciones donde existen varios servicios y aplicaciones, el principal inconveniente es recordar todas las credenciales asignadas por cada servicio web. Lo ideal sería que con una sola credencial de autenticación los usuarios accedan a un sistema que contengan toda la información de logeo.

## 3.2. Autenticación de usuarios.

Uno de los requisitos principales en la implementación de un sistema informático son los medios de seguridad, que deben ser los ideales para proteger el bien más importante de toda organización: la información.

Los medios utilizados deben proporcionar los mecanismos adecuados para identificar a individuos que intentan acceder al sistema, determinando procesos que van desde lo simple de una contraseña hasta lo complejo de un sistema de autenticación biométrico.

El objetivo primordial de un sistema informático no es identificar, más bien se trata de autenticar a un individuo, es decir; asegurar de que dicho individuo es quien dice ser.

> Las palabras identificar y autenticar son términos muy parecidos, pero para un ordenador hay una enorme diferencia: por ejemplo en un sistema biométrico para la identificación de usuarios basados en el reconocimiento de retina; la persona al mirar por el dispositivo lector, el sistema debe decidir si el usuario fue validado de forma correcta, es decir; es quien dice ser, a esto se le llama identificación. Pero, por lo general lo que se utiliza es que el usuario introduzca sus credenciales (usuario/contraseña) y también mire a través del lector de retina; este caso el sistema no tiene la labor de identificar a un usuario, sino autenticarlo: comprobar los parámetros de la retina con los guardados en una base de datos. (“RedIRIS - Autenticación de usuarios”, s/f)

Los procedimientos de autenticación se dividen en tres grandes grupos dependiendo del método que utilicen para identificar a los usuarios: algo conocido por el usuario, algo que posea el usuario y características físicas específicas que tenga el usuario.

Por ejemplo, algo conocido por el usuario puede ser una cadena de caracteres o contraseña que solo él conoce, la cédula de identidad es algo que el usuario posee y un escaneo de retina como característica física.

Un sistema de autenticación fiable debería combinar varios de estos métodos, como por ejemplo al momento de utilizar una tarjeta de débito se debe pasar la tarjeta por la ranura

del cajero automático identificando a que usuario pertenece, para después pedir una contraseña de 4 dígitos donde autenticará si la persona puede hacer uso del servicio.

Una vez determinada la forma de autenticación es indispensable enviar el token a los servicios o aplicaciones que se necesita acceder. Un token es un grupo de datos que contiene información que verifica la identificación de una persona al momento de acceder a una aplicación.

> Los tokens son dispositivos de seguridad adicional para nuestras transacciones en internet. Son una manera de reforzar, y también agilizar, la autentificación de nuestra persona en servicios que requieran contraseñas, PINs o firmas digitales. (Hinojosa, s/f)

Existen dos tipos, tokens de dispositivo y tokens de contraseñas.

Tokens de dispositivo: se conectan directamente al ordenador o que lo hacen por métodos como Bluetooth, aunque aquí también podríamos incluir los mensajes al móvil.

Tokens de contraseña: son los tokens de seguridad más populares, también conocidos como OTP Tokens (One-Time Password), generan claves que se van renovando cada cierto tiempo: disponemos, por ejemplo, de un número que sólo podremos usar una vez porque a los 30 segundos cambia.

El uso de los tokens necesita que las aplicaciones sean capaces de leer el token y trasladar la información que este contiene al servidor para posteriormente autentificar al usuario, muchas veces este procedimiento no es posible sin la implementación de un sistema Single Sign On debido a que no todas las aplicaciones son compatibles entre sí.

> Un sistema Single sign-on, posibilita a los usuarios ingresar a muchas aplicaciones y servicios con un único conjunto de credenciales, facilitándole la tarea de recordar varias contraseñas y disminuyendo el tiempo utilizado para reintroducirlas (Gonzales, Rodríguez & Nistal, 2009).

Entonces, podemos decir que el Single Sign On es un método de autenticación para acceder a varios sistemas con solo un proceso de identificación. Su utilidad radica en que se evita el

ingreso repetitivo de credenciales cuando se tienen varias aplicaciones que necesitan ser accedidas mediante usuarios y contraseña.

Las aplicaciones que usan Single Sign On solo admiten el ingreso de los usuarios que se autenticaron de forma exitosa, brindándole a este tipo de sistemas un control total del acceso de los usuarios a los servicios.

El objetivo primordial de implementar un sistema como el ya mencionado, es tener un único punto de registro y autenticación para todos los usuarios de una organización.

> Mediante la estructura que proporciona un SSO, las partes tecnológicas con las que se implementa, se encargan de autenticar y gestionar las entradas y salidas a los sistemas, elementos de red, servicios web o aplicaciones involucradas de forma transparente para los usuarios. Dependiendo de la manera en que la identidad y las credenciales de usuario son administradas, las soluciones de Single Sing On pueden variar entre sistemas centralizados y de identidad federadas. (Iglesias, 2004)

Las características principales de un sistema de inicio de sesión único o también conocido como Single Sign On son:

**Sencillez de uso**

Da la sencillez puesto que el usuario se autentica una única vez y el sistema le otorga el acceso a los servicios para los cuales está autorizado en la organización.

**Clara y Limpia**

Ejecuta el ingreso a los recursos de la aplicación de una forma transparente para los usuarios, debido a que el inicio de sesión se lo realiza automáticamente.

**Multiplataforma**

Simplifica la manera de iniciar sesión y la forma de acceder a los recursos que se encuentran en la red desde diferentes plataformas.

**Fácil gestión**

A los administradores se les facilita la gestión de los recursos de la red, debido a que las credenciales de autenticación e información de los usuarios se encuentran sincronizada.

**Sistema seguro**

Independiente de la arquitectura que se utilice para implementar un sistema single sign on la información siempre se traslada por la red de forma cifrada.

Para los encargados de gestionar y desarrollar aplicaciones en una organización, tener un sistema de autenticación única, es una forma de simplificar a gran medida la lógica de sus aplicaciones, al poder encomendar la tarea de autenticación de los usuarios a un sistema totalmente independiente de las aplicaciones empleadas¨(Talledo, 2015).

Las desventajas de contar en una organización con un sistema de esta envergadura son muy pocas como: riesgos en la seguridad de todo el sistema, si el cliente utiliza una contraseña frágil. Dependiendo el tipo de sistema SSO implementado no es permitido el acceso al sistema desde varias estaciones de trabajo. En el caso de que la credencial es olvidada o perdida por parte del usuario no podrá acceder a ninguna aplicación dentro del sistema SSO hasta recuperarla.

Entre las principales ventajas de un SSO se encuentran, su fácil implementación dependiendo del sistema, prácticamente consiste en la instalación de un software en el computador que funciona como cliente, claro que depende la arquitectura, servicios utilizados e infraestructura tecnológica. Asimismo la estadía de un usuario en un sitio web que posea esta tecnología será más satisfactoria, en gran parte por el motivo que autenticándose una única vez brindará acceso a todos los servicios y aplicaciones disponibles. (Aguirre & Rosario, 2015)

Existen varios tipos de Single Sign On, entre los que se destacan: E-SSO, Web-SSO, Kerberos, Identidad Federada y OpenID. De los cuales el que más se ha popularizado es la implementación de Kerberos debido a las múltiples ventajas que brinda.

## 3.3. Kerberos

Kerberos es un protocolo de seguridad desarrollado en el Instituto de Tecnología de Massachusetts, al inicio con el objetivo de que dos computadoras conectadas en la misma red se pudieran autenticar entre si de forma segura y fiable. El nombre de Kerberos se deriva de la mitología griega, haciendo referencia al perro que custodiaba las puertas del reino de hades.

> Kerberos es un protocolo de autenticación basado en criptografía simétrica, eliminando la necesidad de enviar contraseñas a través de la red, proporciona un inicio de sesión único (SSO) a aplicaciones o servicios mediante el uso de los denominados *tickets*. Kerberos define un modelo de control de acceso donde un *cliente* que necesita ingresar a un *servicio* (denominado *servidor de aplicaciones*) debe acudir a un tercero, la *Key Distribution Center* (KDC) que es la encargada de autenticar y brindar tickets a usuarios. Kerberos crea una relación de confianza entre estos tres componentes. En resumen, el KDC comparte una contraseña secreta con el servicio y el cliente.(Méndez, Garcıa, López, & Millán, s/f)

El uso de Kerberos impide que la información y contraseñas viajen a través de la red de forma insegura, evitando ataques de reinyección o de *eavesdropping* por parte de personas no autorizadas que pretenden sustraer las contraseñas de los usuarios.

Entre las principales ventajas del uso del protocolo de seguridad Kerberos encontramos que la contraseñas no son transferidas por la red, sino que viajan a través de un sistema donde la información esta encriptada. Es decir; los usuarios solo utilizan las claves de acceso en el login, mientras que para encriptar y desencriptar la información enviada se crean contraseñas de forma dinámica conocidas como "secretos", esto evita varios tipos de ataques debido a que en la red solo queda rastro del secreto mas no de las credenciales de inicio de sesión.

El protocolo Kerberos es de libre uso, ya que se encuentra disponible de forma gratuita en el Instituto Tecnológico de Massachusetts para que cualquier persona pueda estudiar y

manipular el código fuente como mejor convengan en las plataformas que desee. Kerberos también tiene versiones de pago, a muy bajo costo.

Las desventajas que presenta implementar Kerberos en una organización radica en que las aplicaciones deben ser “kerberizadas”, es decir; su código fuente debe ser alterado con el objetivo de realizar las llamadas a las bibliotecas que usa Kerberos. Esto supone una inversión extra de recursos que no siempre es medible debido a que cada aplicación es diferente.

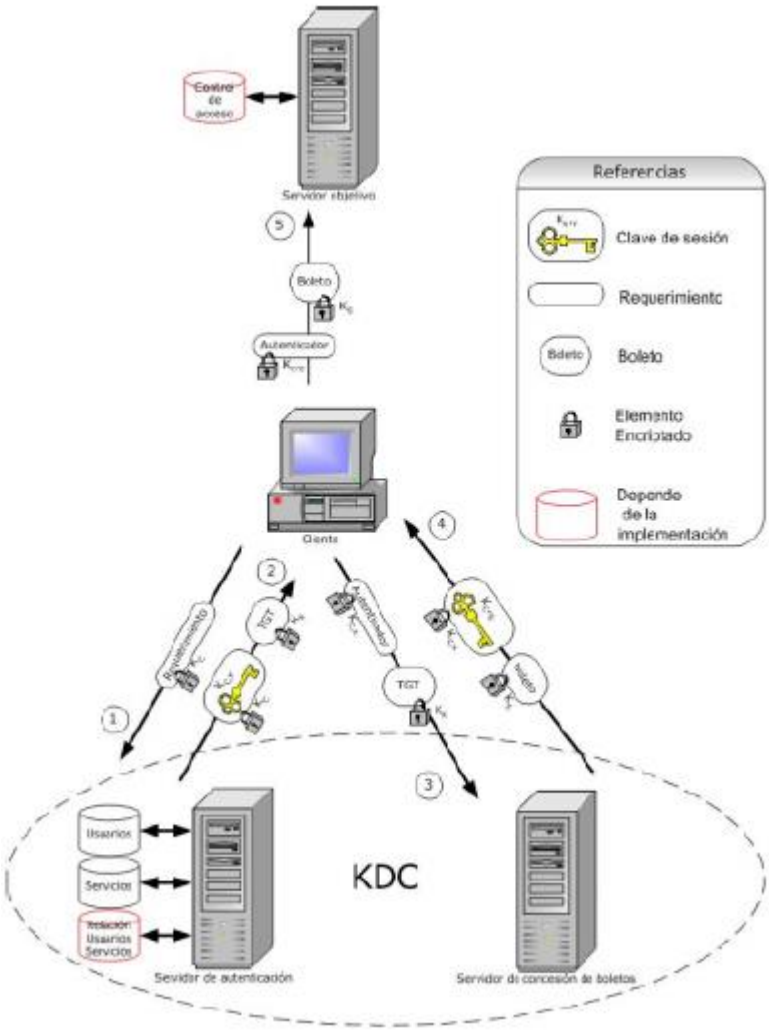


**Figura 1**. Protocolo Kerberos

Fuente: Funcionamiento de Kerberos (Vaca, 2014)

Si se extiende este concepto a la posibilidad de que un usuario con sus mismas credenciales accede a varios servicios compartidos entre diferentes organizaciones, se estaría hablando de una solución conocida como Identidad Federada.

## 3.4. Gestión de identidad Federada.

La identidad federada es una herramienta para afrontar la gestión de identidad en los sistemas informáticos. La diferencia entre otras herramientas del tipo Single Sign On es la libertad del usuario para poderse autenticar en servicios que pertenecen a varias organizaciones. De esta forma las organizaciones pueden compartir información sin depender de la arquitectura tecnológica, métodos de autenticación o tecnología de directorios como si lo hacen otras herramientas del tipo Single Sing On.

La principal finalidad de la gestión federada es posibilitar que los usuarios accedan y compartan información mediante distintos dominios de forma segura.

## 3.5. Security Assertion Markup Language (SAML)

> SAML es un marco de trabajo que permite expresar asertos acerca de la identidad, los atributos y las autorizaciones de un sujeto con el objetivo de facilitar las relaciones entre distintas empresas, así como las relaciones de estas con sus usuarios. Este marco de trabajo permite a las compañías crear identidades federadas, lo cual les facilita las tareas de gestión de perfiles, autenticación y autorización de usuarios. El caso típico de uso es el de Single-Sign-On (SSO), que permite a los usuarios acceder a diversos sitios en la federación con una única autenticación.(Sánchez Guerrero, 2009)

Los principales componentes que se presentan en un sistema de gestión federada basado en SAML son el proveedor de servicios, el proveedor de identidad y el usuario.

El proveedor de servicios es el encargado de proporcionar los servicios a los cuales el usuario está intentando acceder dependiendo de la información facilitada por el proveedor de identidad.

Proveedor de identidad: Contiene la infraestructura para autentificarse, es decir, es el encargado de modificar, eliminar o recuperar las credenciales según el usuario lo requiera. Si la autenticación es llevada a cabo de manera exitosa proporciona al proveedor de servicios la información necesaria para acceder a las aplicaciones.

## 3.6. Directorios.

En la actualidad, las personas y la sociedad en general necesitan de los sistemas informáticos para sostener las múltiples a aplicaciones que se usan a diario en las empresas o instituciones.

Para mejorar la administración de las aplicaciones web, la información de los recursos usados, usuarios y servicios, debe estar organizada de forma nítida y centralizada. La mayoría de esta información es manejada por varias aplicaciones dentro del sistema para lo cual debe estar siempre disponible y protegida.

> En la informática, un directorio es un modelo de base de datos que se compone de entradas y datos descriptivos acerca de cada entrada. El servicio de directorio LDAP se basa en un modelo cliente-servidor. La función de LDAP es permitir el acceso a un directorio existente. Proporciona un mecanismo utilizado para conectar, buscar y modificar directorios de Internet. (Enrique Tun, 2012)

Utilizando el protocolo LDAP es posible comunicar el agente Single Sign On y el directorio central donde se encuentra toda la información relacionado con los usuarios (nombre de usuario, contraseñas). La comunicación entre el usuario y el servidor LDAP no ocurre directamente, para ello será indispensable llamar a una API (application

programming interface) la cual crea un aviso para acceder al directorio utilizando el protocolo LDAP, una vez ingresado al directorio se da respuesta a la información pedida por la aplicación.

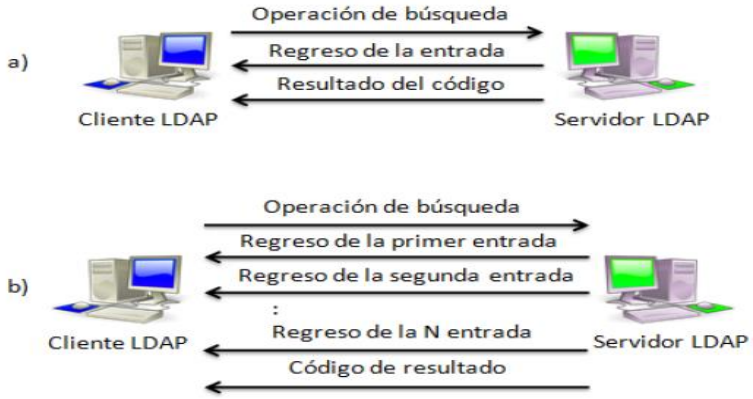


**Figura 2.** Interacción cliente – Servidor

Fuente: Directorios LDAP (Lozano, 2012)

## 3.7. Active Directory

Active Directory es el punto central de una red fundamentada en Windows, permite gestionar los ordenadores que se encuentran en la red, los usuarios, carpetas compartidas, servicios de autenticación y todos los recursos del sistema de forma centralizada haciendo uso de la tecnología LDAP.

> Active Directory también admite la administración descentralizada. Se pueden asignar permisos y conceder derechos de usuario de formas muy específicas. Por ejemplo, se pueden delegar privilegios administrativos para determinados objetos a los equipos de ventas y mercadotecnia de una organización.(L. F. Arias, s/f)

La solución Active Directory es la principal variante a un sistema basado en Kerberos + Ldap, debido a que AD contiene las características necesarias para reemplazar la implementación de estas dos tecnologías en una organización.

Active Directory se maneja como una base de datos que en su interior contiene la información de los objetos (credenciales, recursos, servicios de correo, etc.) que son gestionados por el administrador, el cual controla los permisos que los diferentes grupos de usuarios tienen sobre los objetos de la base de datos.

El principal beneficio que brinda Active Directory es su escalabilidad para cualquier cantidad de entornos y usuarios, es decir, que la base de datos que contiene la información de los objetos se puede replicar entre varios servidores o también llamados controladores de dominios.

Un controlador de dominio (DC) es un servidor que tiene instalado Windows server, donde se ejecuta Active Directory Domain Services. Se podría decir que actúa como director del dominio. Al momento de que un usuario solicita acceso a algún recurso que se encuentre dentro del dominio, el controlador del dominio consulta en su base de datos los permisos, derechos, accesos que tiene el usuario para poder hacer uso de los objetos.

Dominio en Windows server es un grupo lógico de ordenadores ejecutando versiones de Windows que comparten un directorio central conocido como ntds.dit. Todos estos ordenadores están registrados en la base de datos de Active Directory para que de esta forma puedan ser administrados.

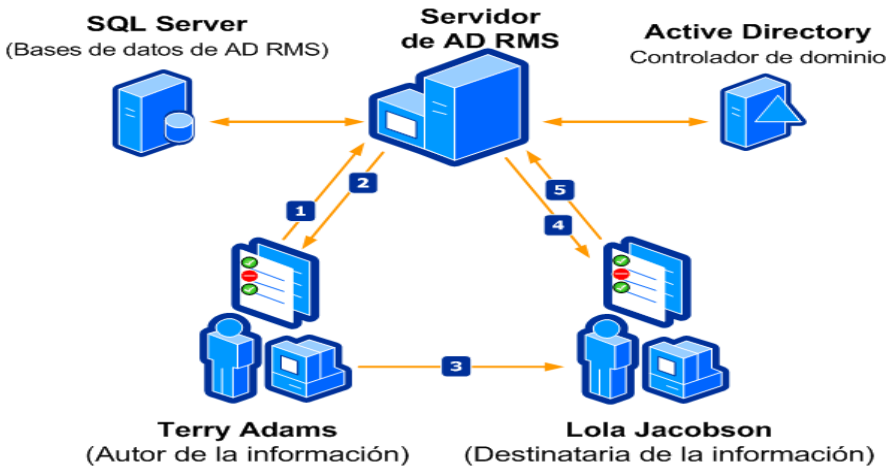


**Figura 3.** Funcionamiento de Active Directory

Fuente: Microsoft Active Directory Azure (Microsoft, s/f)

## 3.8. Active Directory Azure

Active Directory Azure es un servicio de microsoft para la administración y gestión de directorios e identidades de múltiples usuarios basados en la nube.

En una organización AD Azure representa una solución sencilla al problema del acceso a aplicaciones basadas en la nube como Office365, Dropbox, Yahoo!, Skype entre otras mediante un inicio de sesión único (SSO)

> Azure AD con unos cuantos clics puede ser integrado con un servidor de Windows Active Directory local, proporcionando a las organizaciones la competencia de aprovechar de mejor forma la cuenta de correo locales existentes para administrar el acceso a las aplicaciones SaaS basados en la nube. (Microsoft, s/f)

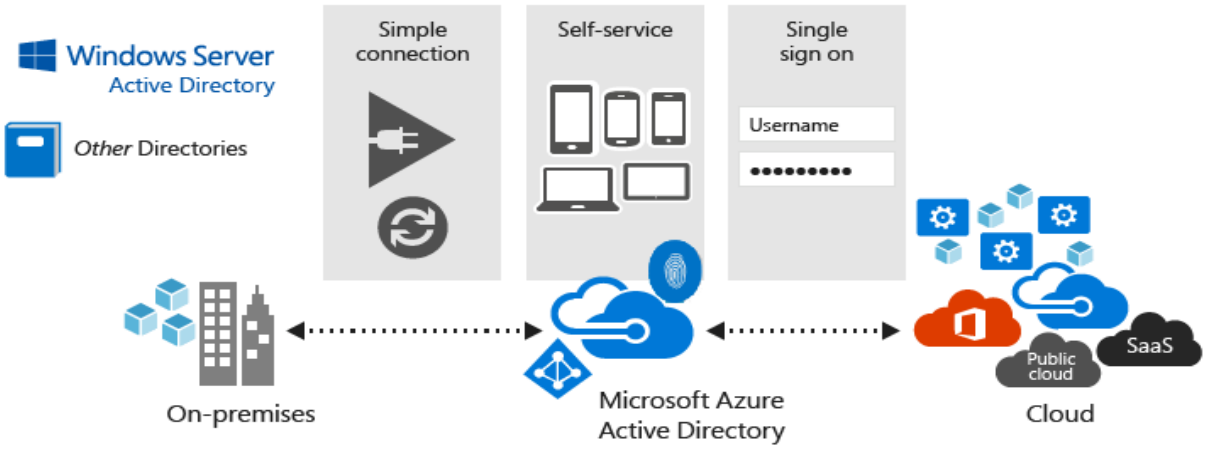


**Figura 4:** Integración de AD Azure

Fuente: Microsoft Active Directory Azure (Microsoft, s/f)

### Beneficios de AD Azure.

Una organización o empresa puede usar AD Azure para aumentar la productividad de los empleados, agilizar los procesos de TI, mejorar la seguridad y reducir los costos.

- Adaptación e integración rápida de servicios en la nube, proporcionando a los empleados y socios un inicio de sesión único
- Gestión fácil y segura para el acceso de los empleados a sus cuentas de redes sociales empresariales.
- Supervisar el uso de aplicaciones protegiendo el entorno de amenazas informáticas avanzadas con informes de seguridad y vigilancia.

## 3.9. Oauth 2.0

Es un protocolo que proporciona la autorización de forma segura, estándar y simple por parte de una aplicación hacia un usuario mediante el uso de una API (Aplication

Programming Interface) sin necesidad que el usuario comparta sus credenciales de autenticación con la aplicación cliente.

> Para (García, 2014) Oauth tiene como finalidad agregar una capa de seguridad a los servicios que brinda una API, de la misma forma resguarda los datos de los usuarios, permitiendo a un usuario otorgar un limitado acceso a aplicaciones de terceros. OAuth plantea preservar estos servicios y recursos, solicitando un código (token de acceso) el cual brinda la información de quién desea acceder y en nombre de quién.

Además ya no depende de las aplicaciones clientes para tener criptografía. Posee una clara separación de las funciones entre el servidor responsable de manejar las solicitudes de OAuth y el manejo del servidor de autorización del usuario.

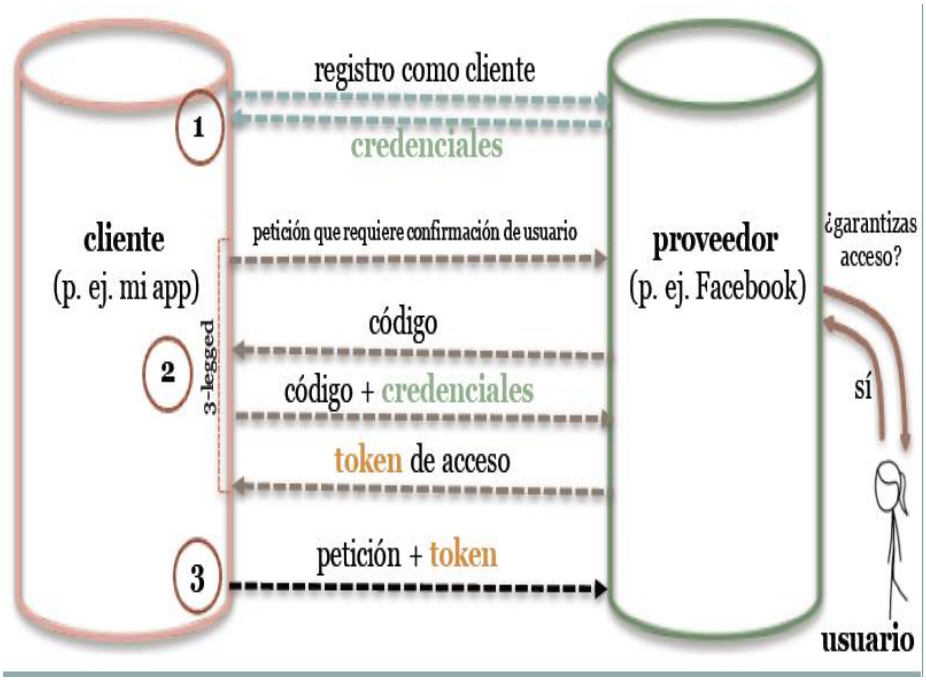


**Figura 5.** Funcionamiento de OAuth

Fuente: REST Avanzado (Santamaría, 2012)

## 3.10. OpenID

Es un protocolo digital descentralizado de inicio de sesión único que resuelve el problema de tener una única credencial de inicio de sesión individual para cada sitio web.

Con OpenID, un usuario puede registrarse una vez con un Identity Provider (IdP) de su elección y luego utilizar ese inicio de sesión en todos los sitios habilitados para OpenID. Como es un sistema descentralizado, un usuario puede registrarse con cualquier proveedor de identidad.

> OpenID es un método de autenticación en páginas web sin el requerimiento de tener una credencial de usuario para cada una de los sitios donde se quiere acceder. De esta manera OpenID concede permisos para que el usuario administre su identidad digital de forma centralizada, evitando la dificultad de contar con una identidad para cada una de las plataformas. OpenID es de código abierto y defiende la autenticación única de los usuarios en la red. Hay empresas que al detectar también estas deficiencias han creado los propios servicios de autenticación pero simplificando y mejorando la experiencia del OpenID.(Marta Serrat, s/f)

Un inicio de sesión OpenID es sencillamente una URL como http: //juan.miopenid.com/, que contiene un conjunto de etiquetas HTML que identifican el proveedor de identidad de un usuario.

Además de la ventaja de tener un solo inicio de sesión y una contraseña que no necesitan ser anotados en cualquier lugar para ser recordado, OpenID también tiene otra importante ventaja de seguridad: como la mayoría de los usuarios solo usarán un inicio de sesión de OpenID, la autenticación de ese inicio de sesión puede hacerse extremadamente segura. En la actualidad, es costoso para los sitios web proporcionar a sus usuarios características de seguridad individual de forma adicional, tales como certificados de cliente, tarjetas inteligentes o SecurIDs. Sin embargo, con OpenID un Proveedor de Identidad puede ser capaz de permitirse el lujo de poner el tiempo y dinero en la obtención de una sola "puerta de entrada" en lugar de tener decenas de sitios de seguridad individuales. Esto tiene el potencial de aumentar enormemente la seguridad de nuestros inicios de sesión diarios.

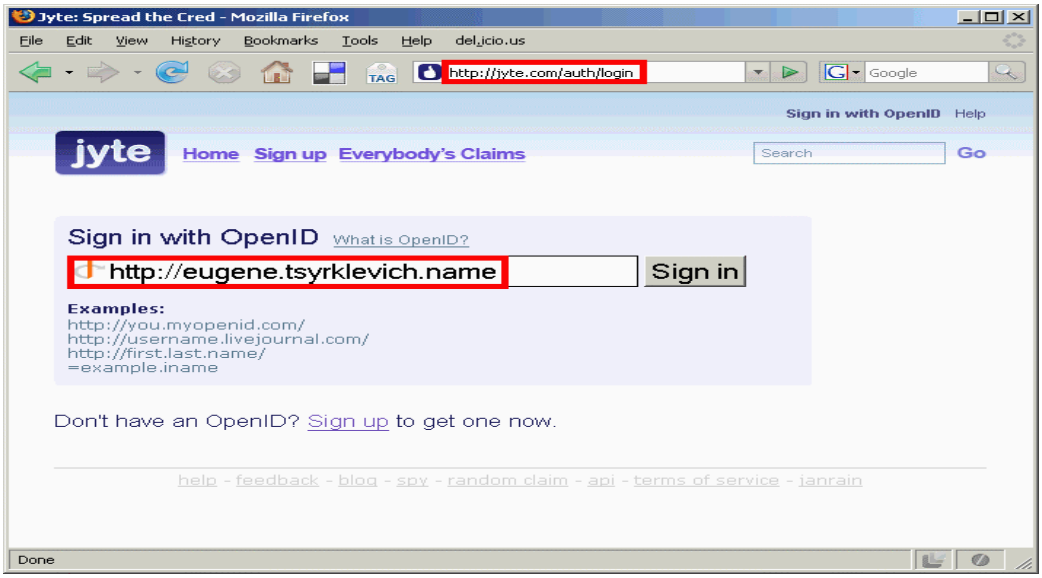


**Figura 6.** Login usando OpenID

Fuente: Single sign-on for the internet (Tsyrklevich & Tsyrklevich, 2007)

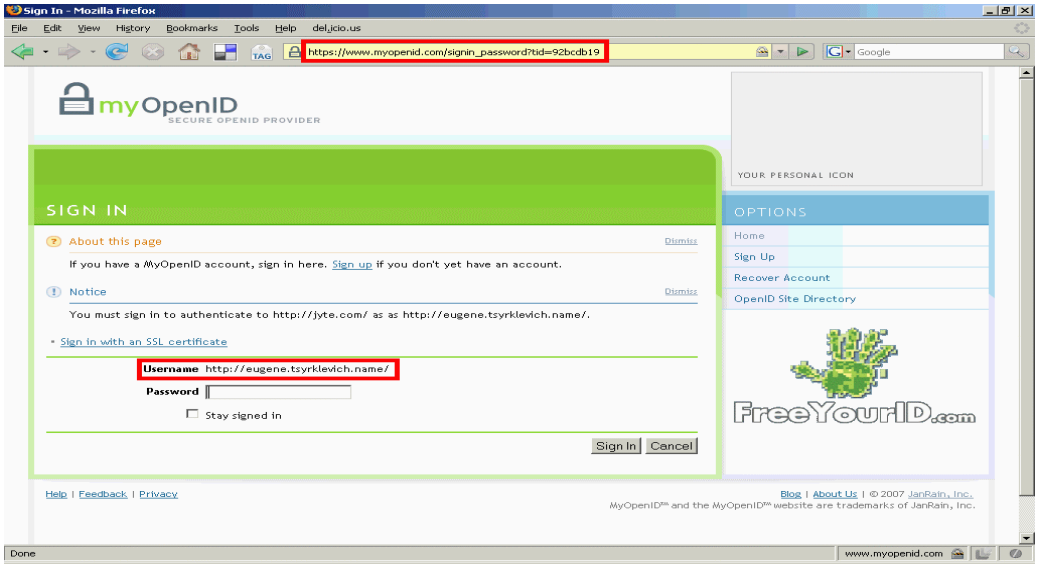


**Figura 7.** Proveedor Idp

Fuente: Single sign-on for the internet (Tsyrklevich & Tsyrklevich, 2007)

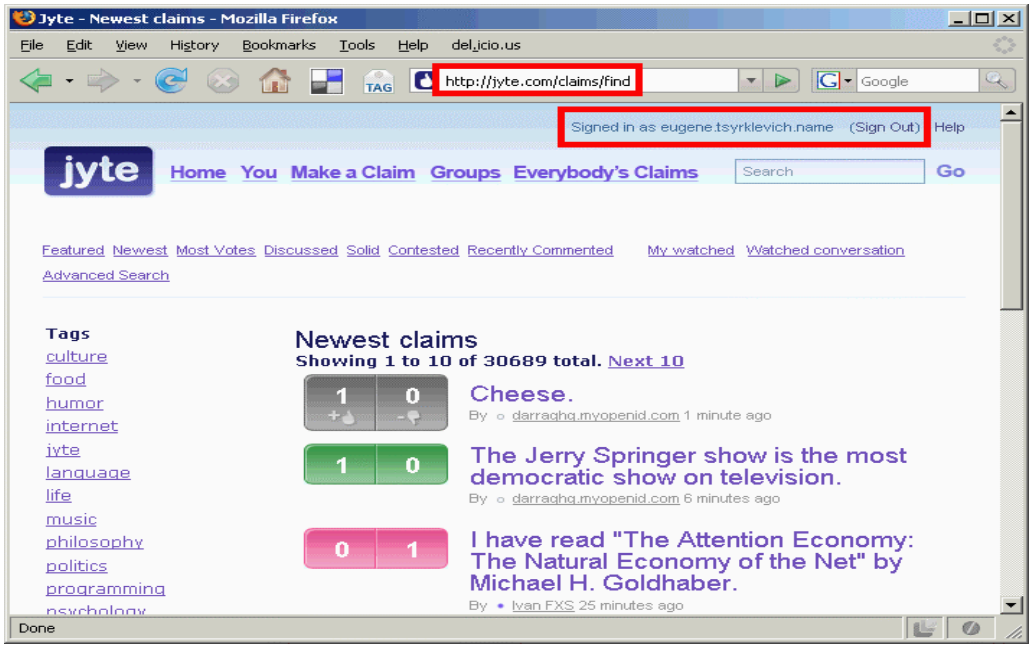


**Figura 8.** Usuario logeado correctamente

Fuente: Single sign-on for the internet (Tsyrklevich & Tsyrklevich, 2007)

## 3.11. OpenID Connect

El protocolo OpenID Connect, lanzado en febrero de 2014, se puede utilizar a través de numerosas plataformas, incluyendo móvil.

Principalmente se utiliza para la autenticación delegada, de forma que si el sitio a consumir es compatible con OpenID, el consumidor no necesita crearse una identidad para consumir la información, siendo únicamente necesario facilitar las credenciales obtenidas en cualquier otro sitio compatible, donde el que ofrece la información deberá verificar la credencial recibida. Este sistema requiere que la conversación entre el que solicita la autenticación y el que la ofrece sea de forma segura. Así mismo una de sus mayores ventajas reside en su facilidad de uso en los navegadores actuales mediante XRI. (“El reto de los sistemas de autenticación y autorización: ¿cómo elegir el más adecuado? | MINCOM”, s/f)

Es un estándar abierto para la autenticación que está diseñado para trabajar en conjunto con las capacidades de autorización de Oauth 2.0. Es esencialmente una capa de identidad construida encima de OAuth2 que permite la verificación de la identidad de un usuario final. Esto se logra mediante la adición de un testigo de identidad a la autorización de Oauth 2.0

En muchos sentidos OpenID Connect representa el futuro de la autenticación y autorización en especial porque fue desarrollado para aplicaciones móviles nativas y servicios web.

## 3.12. Protocolos de seguridad AAA

Los servicios de seguridad de red de autenticación, autorización y contabilidad por sus siglas en ingles AAA (Authentication, Authorization y Accounting) proporcionan el marco principal para configurar el control de acceso en dispositivos de red.

Authentication: Los usuarios y administradores deben probar que son quien dicen ser, utilizando combinaciones de nombre de usuario y contraseña, tarjetas token, preguntas de desafío y respuesta entre otros métodos.

Authorization: Una vez identificado el usuario, los servicios de autorización determina a que recursos puede acceder determinado usuario y que operaciones está habilitado para realizar.

Accounting: La contabilidad registra lo que el usuario hace, incluyendo a los elementos a los que accede, la cantidad de tiempo que accede al recurso, todos los cambios que se realizaron y de qué forma fueron usados.

> Los tipos de protocolos basados en AAA que existen son tres principalmente: RADIUS, TACASC, DIAMETER. (Escalona, 2012)

El protocolo de seguridad AAA más implementado es RADIUS, debido a una de sus principales características de brindar un control sobre la conexión de los usuarios, enviando

notificaciones de cuando inicia y termina la misma, con el propósito de crear un informe sobre el consumo del usuario con su respectiva factura.

> RADIUS es un protocolo cuya infraestructura de red se basa en un modelo cliente-servidor, donde los servicios de autenticación, autorización y contabilidad son administrados por un equipo proveedor de recursos, en este caso el servidor RADIUS, y los clientes son aquellos que acceden a los servicios ofrecidos. De esta manera se tiene una gestión centralizada que permite mejorar el nivel de seguridad de la red. (Vaca, 2014)

El servidor RADIUS se ocupa de tomar las solicitudes de los usuarios para acceder a la red, comprobando que las credenciales sean válidas, en base al directorio que contiene toda la información relacionada con los usuarios de la organización. Finalmente si la verificación fue llevada de forma exitosa, se envía toda la información necesaria para poder brindar el servicio solicitado.

Los mensajes que se envían desde el cliente al servidor en una comunicación usando RADIUS, viajan de forma encriptada, usando una clave secreta denominada “secreto compartido” que nunca es transmitida por la red para impedir intercepciones de personas maliciosas.

> A razón del desmesurado desarrollo de internet y la presentación de tecnologías nuevas de acceso, incluidas las inalámbricas, DSL, Mobile IP y Ethernet, routers y servidores de acceso los cuales son muy complejos, demandando nuevos requerimientos en los protocolos AAA, como por ejemplo manejar políticas para varios servicios, incapaz cubrirlas con RADIUS y TACACS+ es que surge DIAMETER, considerado por algunos el sucesor de RADIUS. (Escalona, Protocolos de control de acceso RADIUS, 2012)

Diameter es un protocolo basado en Radius, brinda servicios fundamentados en autenticación, autorización y auditoria (AAA). Sus principales ventajas y mejoras con respecto a su antecesor son mayor seguridad, reducción de margen de error de pérdidas de mensajes, fácilmente entendible, es decir, que posibilita implementar el protocolo fuera del marco de trabajo AAA.

## 3.13. Arquitecturas para implementar un sistema de autenticación único.

Hay varios tipos de arquitecturas donde se pueden implementar un sistema de inicio de sesión único. Cada arquitectura tiene sus propias características, que la hace más adecuada dependiendo el tipo de organización y los recursos informáticos, económicos o de infraestructura que esta posea.

> Existen cinco tipos de arquitecturas para implementar un SSO que para (Iván M. Caballero, 2013) son Password vault, administración centralizada con almacenamiento local, administración y almacenamiento de credenciales centralizados, arquitectura SSO totalmente distribuida, administración y almacenamiento de credenciales centralizados garantizando alta disponibilidad y redundancia.

Donde la arquitectura más básica y sencilla de implementar es Password vault, las credenciales se almacenan en las estaciones que funcionan como clientes, cuando el usuario desea acceder a las aplicaciones las credenciales se administran de forma local. No permite acceder a los sistemas desde múltiples estaciones de trabajo.

El almacenamiento y administración de credenciales tanto de forma local como en un servidor central presenta muchas ventajas con respecto al Password vault, la administración es centralizada y permite el acceso a las aplicaciones web desde cualquier estación de trabajo.

En los últimos años la arquitectura que se ha popularizado es la totalmente distribuida, presenta muchas ventajas sobre las antes mencionadas, su principal característica radica en que la base de datos está separada del servidor, es decir, los procesos se realizan en módulos independientes, varios servidores implementando balanceo de carga, múltiples bases de datos creando redundancia. Una de sus desventajas es el alto costo económico que genera implementarla.

La arquitectura Single Sign On que se desee implementar en cualquier organización dependerá de muchos factores como la complejidad, recursos disponibles, grado de flexibilidad, costos, requerimientos específicos entre muchos más.

> Un sistema SSO diseñado de manera correcta tiene características que permiten realizar un proceso de autenticación bajo todos los ambientes sin importar el diseño o plataforma.
>
> Esto significaría que una organización no tendría que poseer sistemas paralelos para realizar el procedimiento de ingreso a aplicaciones diseñadas en distintos ambientes, lenguajes y arquitecturas. (Iván M. Caballero, 2013)

# 4. Metodología.

La presente es una investigación tecnológica, debido que para la implementación de un sistema de autenticación única para los servicios web en la PUCESE, fue indispensable emplear conocimientos teóricos-prácticos encontrados en distintas investigaciones, con el fin de obtener la mayor cantidad de información útil posible, y de esta forma lograr el mejor resultado para la institución.

También podemos decir que es una investigación de campo, dado que para definir la actual situación de la PUCESE, en torno a la manera de cómo sus estudiantes gestionan varias cuentas para ingresar a los diferentes servicios web y aplicaciones, se utilizó una intervención concreta del investigador para recolectar la información necesaria de manera directa y acudir a los lugares donde suceden los eventos.

> (Arias, 1999) indica que la investigación de campo se basa en la recopilación de datos de forma directa en la realidad donde ocurren los hechos, sin manipular o controlar ninguna variable.

También se utilizó el método analítico – sintético, con el cual se analizó los datos obtenidos del estudio y se realizó una síntesis de los mismos.

> Para (Romero, 2017) el método analítico combina el proceso formal de resolución con el método científico para lograr la resolución del problema. El problema, analítico parte de la división de un todo en muchas partes para estudiarlas por separado, en tanto que el método sintético reúne un conjunto de conceptos para formular una solución global.

Se utilizó la investigación cualitativa con la finalidad de describir las características de un fenómeno, ya que permitió obtener datos de las aplicaciones y servicios web utilizados por los estudiantes, cada una de sus características y la arquitectura donde son implementadas.

> Según (Martinez, 2006) la investigación cualitativa trata de identificar la naturaleza profunda de las realidades, su estructura dinámica, aquella que da razón plena de su comportamiento y manifestaciones. De aquí, que lo cualitativo (que es el todo integrado) no se opone a lo cuantitativo (que es sólo un aspecto), sino que lo implica e integra, especialmente donde sea importante.

## 4.1. Instrumentos y técnica.

Una de las técnicas empleadas para la recolección de datos fue la observación, considerada como una herramienta que se usa tanto en las investigaciones cuantitativas como cualitativas. En nuestro caso la observación ayudó a conocer de forma más detallada el funcionamiento y forma de autenticación de todos los servicios web utilizados por los estudiantes de la PUCESE.

> La observación científica consiste en la percepción sistemática y dirigida a captar los aspectos más significativos de los objetos, hechos, realidades sociales y personas en el contexto donde se desarrollan normalmente. Proporciona la información empírica necesaria para plantear nuevos problemas, formular hipótesis y su posterior comprobación. (Hernandez, s/f)

Como método de recopilación de información también se usó la entrevista, que fue realizada a uno de los principales desarrolladores de software del departamento de TIC, de

esta manera se logró obtener datos fundamentales para conocer de forma más detallada y profunda la arquitectura sobre la cual corre la infraestructura tecnológica de la PUCESE. Información sobre servidores, servicios web utilizados por los estudiantes, sistemas operativos, cableado estructurado fueron parte de los datos recogidos durante la entrevista.

La entrevista fue basada en la investigación de (Velandia, Ángel, Barona Ríos, & García Ponce de León, 2010) donde se analizan los patrones de disponibilidad de infraestructura y equipamiento informático, así como los modos de apropiación y uso de las TIC por parte de los empleados en una institución.

De la misma manera fue usada la investigación de ("Guía Técnica Diagnóstico de Sistemas de Información | RNI - Red Nacional de Información", 2013) debido a que ofrecen una propuesta lógica, sistémica y concreta que permite identificar las necesidades que presentan las entidades nacionales y territoriales en los diferentes componentes asociados a un sistema de información.

## 5. Diagnóstico.

En la PUCESE existen cinco servicios web utilizados por los estudiantes que al momento de ser matriculados en el primer nivel se les asigna automáticamente una credencial de autenticación para los sistemas de consulta de notas, sistema de evaluación académica para estudiantes, Moodle, MicroCurricular y correo electrónico institucional.

Para el sistema de evaluación académica para estudiantes, consulta de notas y Microcurricular las credenciales de autenticación son el número de cédula como nombre de usuario y el número de matrícula como contraseña, las cuales no pueden ser cambiadas o modificadas.

El sistema de consulta de notas permite a los estudiantes conocer todas sus calificaciones obtenidas, la interfaz de la aplicación consta de cuatro secciones para realizar las consultas de notas: récord completo, récord anual, notas de medio semestre y cultura física.

Récord completo visualiza de forma detallada todas las notas que el estudiante ha obtenido durante todos los semestres que ha sido matriculado, indicando la materia, número de faltas, número de intentos, número de créditos y si la materia fue aprobada o no dependiendo de la calificación final.

Récord anual nos permite seleccionar el año del cual queremos consultar las calificaciones, una vez seleccionado la opción deseada, visualiza de forma detallada las notas de todas las materias que el estudiante curso durante ese año.

Notas de medio semestre da la posibilidad de observar las notas parciales, notas de exámenes y faltas de las materias que se están cursando en el actual semestre.

Cultura Física nos permite consultar de forma detallada la calificación de la materia, pero solo si se encuentra matriculado en la asignatura.

El sistema de evaluación académica para estudiantes, es una aplicación en donde se puede realizar la evaluación semestral obligatoria a los docentes y director de escuela esta evaluación se basa en calificar el desempeño de los maestros que imparten las materias que el estudiante está cursando en el actual semestre, de la misma manera con el director de escuela de la carrera. En caso de no realizar esta evaluación, los estudiantes son sancionados tanto académica como económicamente.

Dicho sistema solo es habilitado una vez en cada semestre, es decir; que el resto del semestre los estudiantes podrán logearse pero no tendrán la opción de realizar la evaluación al docente o al directo de escuela.

La aplicación de Microcurricular fue creada con el objetivo de que los estudiantes lleven un seguimiento al sílabo de todas las materias que estén cursando en el semestre, esta aplicación también permite descargar el sílabo por parte de cualquier usuario, pero solos dos pueden calificar si el sílabo está siendo ejecutado de forma correcta o no, por el docente a cargo de la asignatura correspondiente. El director de escuela de cada carrera elige a los dos estudiantes encargados de calificar.

El Moodle es un software utilizado por los educadores o capacitadores para la creación de cursos virtuales y entornos educativos con el objetivo de mejorar la comunicación con el docente, la entrega de tareas y la forma de evaluar.

El Moodle es una herramienta indispensable durante las horas de clases, puesto que la mayoría de trabajos, tareas, exámenes, material de estudio se encuentran dentro de esta plataforma.

Las credenciales de los estudiantes son asignadas automáticamente al ingresar al primer nivel, en este caso la credencial de autenticación al Moodle está compuesta por el primer nombre, un punto y el apellido como nombre de usuario, el número de matrícula es la contraseña. Esta credencial se puede modificar en la sección de herramientas que brinda la aplicación.

La PUCESE brinda a sus estudiantes un correo electrónico institucional, el cual es entregado en la proforma al momento de matricularse. Generalmente está compuesto por el primer nombre, un punto, el primer apellido seguido del signo arroba y el nombre de dominio pucese.edu.ec, por ejemplo: *bryan.sevilla@pucese.edu.ec*

Como contraseña para el uso de este correo electrónico es asignada inicialmente una contraseña, posteriormente cuando el estudiante se autentique por primera vez el sistema automáticamente le pedirá que cambie la contraseña por una nueva.

Adicionalmente con esta cuenta de correo electrónico el estudiante puede hacer uso de la plataforma Office 365, junto con todas sus herramientas como Microsoft Word, Excel, PowerPoint, OneDrive con 1TB de almacenamiento gratuito, Access, las cuales se podrán instalar hasta en máximo 5 dispositivos como computadoras de escritorios, tablets, móviles entre otros.

Actualmente en la PUCESE se está implementando un sistema de autenticación, donde la estación de trabajo y el office 365 usaran la mismas credenciales de acceso, empleando el estándar abierto Oauth 2.0, Active Directory Local y Active Directory Azure, es decir, ingresando las credenciales en el equipo se podrán usar todas las herramientas que brinda el paquete de office 365 sin necesidad de logearse nuevamente.

Como servidor de correo electrónico es usada la plataforma informática en la nube Microsoft Azure, este servicio permite alojar servidores y aplicaciones en la nube a través de máquinas virtuales simulando como si estuvieran físicamente en la misma red, de esta forma se logra reducir los costos y recursos necesarios para sostener un servidor de este

tipo. A diferencia de comprar y dar mantenimiento al hardware que comprende la infraestructura tecnológica en la institución, la alternativa nube brinda la disminución de costos en equipos, reducción en consumo de electricidad, soporte técnico y mantenimiento.

> Entre las ventajas de Microsoft Azure se encuentran la disminución de costes de operación y aprovisionamiento de las aplicaciones, la respuesta rápida a cambios en las necesidades de los clientes y el negocio, la capacidad para escalar según las necesidades de la aplicación, etc. (Matute & Mamfredy, 2012)

La mesa de ayuda o también conocido como *help desk* dentro de la PUCESE está organizado de tal manera que: el soporte técnico a las aplicaciones de Moodle y Microcurricular es realizado por una persona, mientras que otra se encarga de dar soporte al correo electrónico, sistema de evaluación académica y sistema de consulta de notas.

El soporte a nivel usuario de todas las aplicaciones es llevado a cabo por otro empleado que brinda asistencia a todos los requerimientos de los usuarios, sin embargo si el requerimiento en el sistema de consulta de notas es complejo, es decir, se necesita acceder de forma directa a la base de datos del sistema y modificarla, es necesario la intervención del encargado del soporte técnico de dicha aplicación.

## 5.1. Arquitectura de aplicaciones.

> La Arquitectura de Software puede ser vista como la estructura del sistema en función de la definición de los componentes y sus interacciones; es considerada como plan de diseño del sistema, debido a que es usada como guía para el resto de las tareas de la etapa de desarrollo. (Astudillo, s/f)

Las aplicaciones de sistema de evaluación académica para estudiantes, sistema de consulta de notas, Microcurricular están desarrolladas en el lenguaje de programación orientado a objetos Visual Studio .NET, usando el entorno para aplicaciones web de Microsoft ASP.NET y Sql Server como gestor de base de datos. El servidor web que esta

implementado es Internet Information Services (IIS); este servicio convierte a un PC en un servidor web para Internet o una intranet, es decir, que en los ordenadores que tienen este servicio instalado se pueden publicar páginas web tanto local como remotamente.

Las aplicaciones web se modelan mediante lo que se conoce como modelo de capas, una capa representa un elemento que procesa o trata información. Los sistemas mencionados anteriormente están diseñados en 3 capas, donde su objetivo principal es la separación de la capa de presentación, capa de negocio y la capa de datos. La ventaja primordial radica en la separación de roles, es decir, resulta más fácil reemplazar o modificar una capa sin afectar a los módulos restantes.

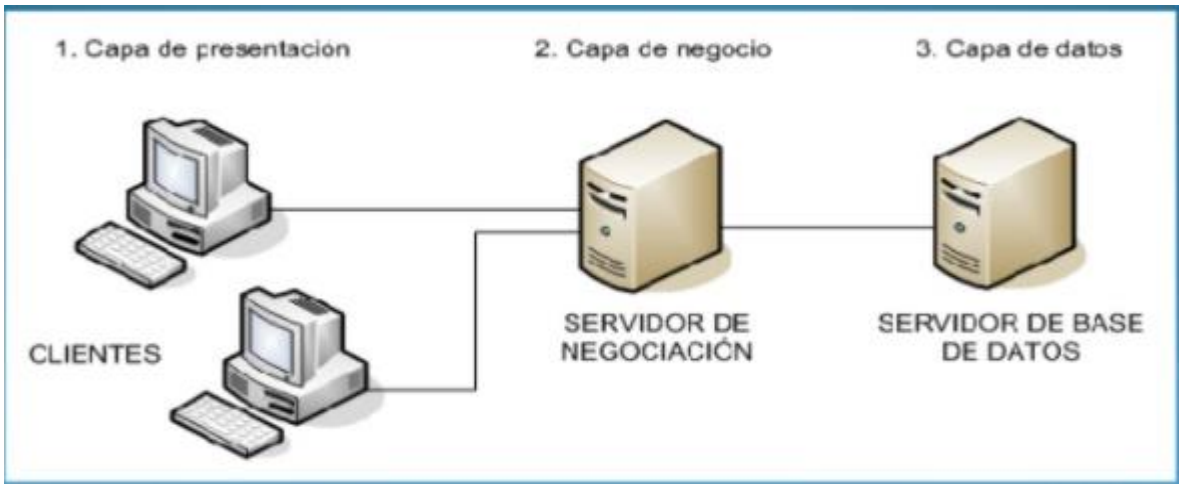


**Figura 9.** Arquitectura de software: Modelo 3 capas.

Fuente: Arquitectura 3 capas (Fani Calle, s/f)

## 5.2. Mapa de red de la PUCESE.

La PUCESE cuenta con 56 switch marca Hewlett-Packard y D-link, existen dos redes: el campus de la avenida Eugenio Espejo y el campus de Santa Cruz.

Todas las estaciones de trabajo y las aplicaciones que utilizan, tanto empleados administrativos como estudiantes, son controladas por la implementación de Active Directory Local que posee la institución.

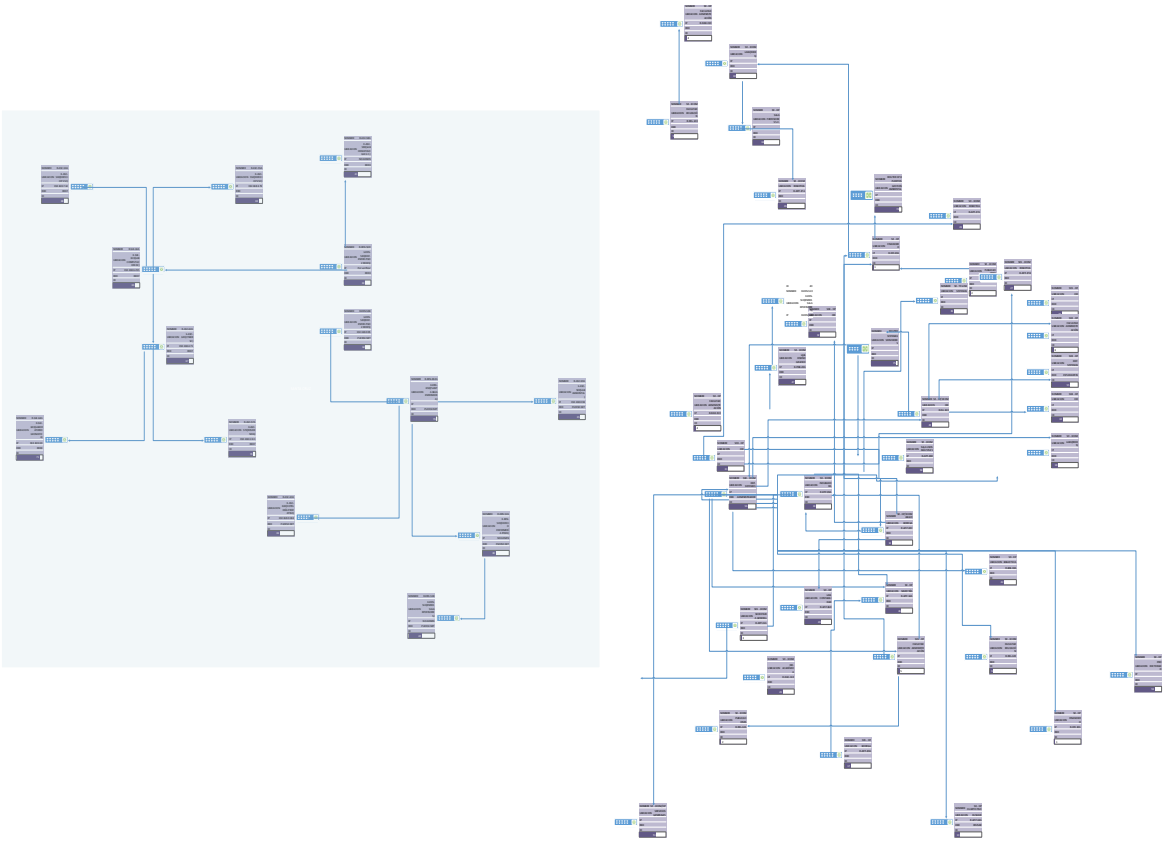

**Figura 10**. Mapa de red campusa avenida Eugenio Espejo y Santa Cruz.

Mediante la entrevista realizada a uno de los principales responsables de la infraestructura tecnológica de la PUCESE se pudo conocer que físicamente todas las aplicaciones están alojadas en un solo servidor, pero lógicamente se encuentran separadas debido a que cada una está instalada en una máquina virtual distinta con su propio sistema operativo y características únicas.

El sistema de evaluación académica para estudiantes, consulta de notas y Microcurricular corren bajo una máquina virtual con sistema operativo Windows, mientras que el Moodle se encuentra en una máquina virtual Linux. En la PUCESE existe un convenio con

Microsoft, lo que habilita el uso de los diferentes entornos de desarrollo integrado (IDE) y gestores de bases de datos como Visual Studio, Sql server entre otras herramientas, restringiendo en cierta medida la posible migración de todos los sistemas a software libre.

También se pudo llegar a conocer que existen cinco servidores de producción y cinco servidores de ambiente de pruebas conectados de forma independiente en un pequeño data center. Los servidores en ambientes de pruebas son utilizados en su mayoría por los estudiantes que se encuentran en etapas de prácticas pre-profesionales, con el objetivo de crear aplicaciones web o modificar las que ya existen, todo esto antes de ser aprobados por el jefe del departamento de TIC para finalmente llevar estos servicios a un servidor de producción.

La arquitectura de software cliente-servidor es preponderante en la institución, dado que todas las aplicaciones se encuentran implementadas bajo este modelo, las aplicaciones que corren sobre este tipo de arquitectura presentan una ligereza considerable, debido a que el consumo, administración y carga de recursos son realizados de forma directa por el servidor.

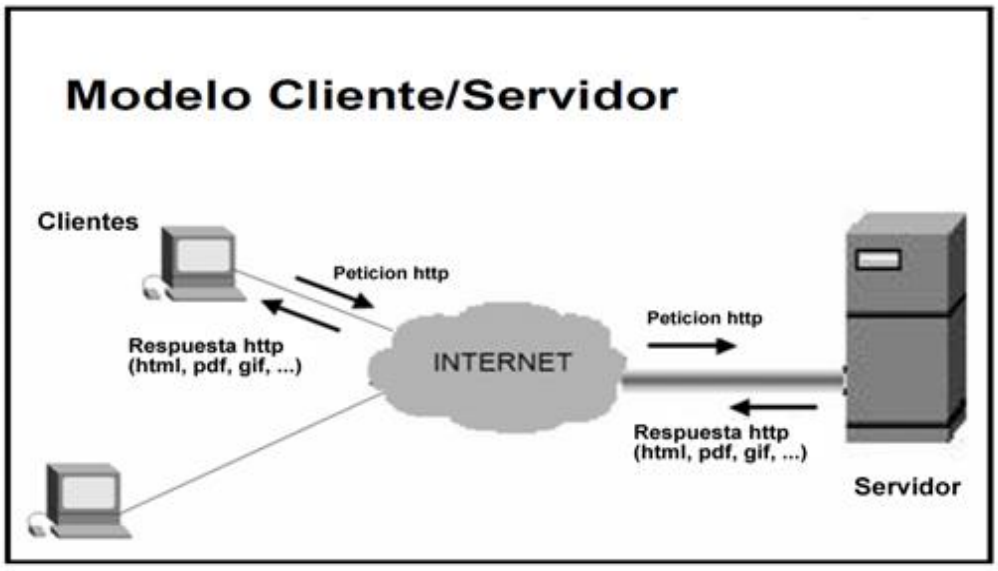


**Figura 11.** Modelo Cliente - Servidor

Fuente: Desarrollo de aplicaciones Web / Arquitectura aplicación Web (Carrera, 2009)

Con el avance de la tecnología el número de sitios individuales que requieren registro ha aumentado drásticamente, se está haciendo evidente que la actual situación de autenticación es insostenible. Para hacer frente a las decenas de inicios de sesión individuales y contraseñas requeridas por diferentes sitios, los usuarios se ven obligados a anotar sus inicios de sesión o reutilizar el mismo nombre de usuario y contraseña para cada sitio web. Esto es claramente indeseable ya que crea múltiples puntos de ataques, y un único sitio hackeado tiene el potencial de comprometer completamente la identidad digital de un usuario en Internet hoy en día.

> Una primera solución evidente al problema de la autenticación sería el uso de algún tipo de certificado personal (basado, por ejemplo, en el estándar X.509) emitido y validado por alguna autoridad central de confianza. Si bien este tipo de certificados son útiles para gestiones con determinadas entidades, no son prácticos en general para el acceso a servicios de Internet, ya que requerirían la presencia de autoridades centrales de confianza aceptadas globalmente que validen la identidad del usuario, y además implicarían gestiones administrativas previas para obtener el certificado que complicarían el proceso. (Sánchez, 2011)

Por lo que han surgido los protocolos de autorización y autenticación en Internet; a continuación se muestra una tabla con los más importantes y reconocidos del mercado.

| Protocolo | OpenID | Oauth 2.0 | SAML |
|---|---|---|---|
| Propósito | Proporciona una capa de autenticación sobre OAuth2.0 | Permite la autorización delegada de recursos de Internet | Permite a 2 entidades web intercambiar datos de autenticación y autorización |
| Tipo o formato de | JSON | Binarios, JSON, | XML |

| | | | |
|---|---|---|---|
| Tokens | | SAML | |
| Autorización | No | Si | Si |
| Autenticación | Si | Depende de OpenID Connect | Si |
| Año de creación | 2005 | 2006 | 2001 |
| Versión actual | OpenID Connect | Oauth 2.0 | SAML 2.0 |
| Transporte | HTTP, XRDS | HTTP | XML, HTTP, SOAP |
| Peligros en la seguridad | Suplantación de identidad<br><br>Los proveedores de identidad OpenID tienen un registro de todos los nombres de usuarios, si se logra descifrar la cuenta tendrá a acceso a todas las aplicaciones | Suplantación de identidad<br><br>OAuth 2.0 no admite la firma, el cifrado, la verificación del cliente. En su lugar, se basa por completo en TLS para la confidencialidad. | Firma XML<br><br>Si se duplica es posible suplantar a cualquier usuario. |
| Su uso más adecuado | Inicio de sesión único de aplicaciones para usuarios finales. | Autorización de las API. | Inicio de sesión único para empresas<br><br>Nota: no se adapta bien para |

| | | | |
|---|---|---|---|
| | | | aplicaciones móviles |
| Pide la aprobación del usuario | Si | Si | No |
| Token contiene información del usuario | Si | No | Si ( a causa de la firma) |
| Admite aplicaciones integradas y móviles | Si | Si | No |
| Integración con Azure Active Directory | Media | Media | Facil |
| Costo por integrar con Azure Active Directory | No | No | Si |
| Protocolo abierto o privado (pagado) | Abierto | Abierto | Abierto |

**Tabla 1.** Comparación de protocolos de autenticación.

Fuente: Federated Identities: OpenID vs SAML vs OAuth (Koussa, 2013)

Considerando la Tabla 1, se asignó un valor (peso) cuantitativo a cada una de las características que presentaba dichos protocolos. Los valores van del 1 al 5, teniendo al 1 como la calificación más baja y el 5 como la más alta; dicha calificación se basó en la

situación actual de la PUCESE y las necesidades tecnológicas que presenta. De la misma manera también se tuvo en consideración la arquitectura de las aplicaciones web en estudio y su capacidad de integración con cada uno de los protocolos de autenticación.

| Protocolo | OpenID | Oauth 2.0 | SAML |
|---|---|---|---|
| Propósito | 3 | 5 | 3 |
| Tipo o formato de Tokens | 5 | 5 | 4 |
| Autorización | 0 | 5 | 5 |
| Autenticación | 5 | 3 | 5 |
| Transporte | 5 | 5 | 5 |
| Peligros en la seguridad | 3 | 5 | 3 |
| Su uso más adecuado | 3 | 5 | 1 |
| Pide la aprobación del usuario | 5 | 5 | 0 |
| Token contiene información del usuario | 5 | 5 | 5 |
| Admite aplicaciones integradas y móviles | 5 | 5 | 0 |
| Integración con Azure | | | |

| | | | |
|---|---|---|---|
| Active Directory | 3 | 3 | 5 |
| Costo por integrar con Azure Active Directory | 5 | 5 | 0 |
| Protocolo abierto o privado (pagado) | 5 | 5 | 5 |
| Total | **52** | **61** | **41** |

**Tabla 2.** Pesos de características en protocolos de autenticación.

Fuente: Federated Identities: OpenID vs SAML vs OAuth (Koussa, 2013)

Estos protocolos surgen por la necesidad de unir todos los métodos de autenticación de usuario. El inconveniente radica en el momento que los usuarios deseen acceder a algún servicio tienen que registrarse, ingresando su información personal y creando una credencial para dicho sitio. Entre más cuentas son creadas y más servicios se usan, las probabilidades de robo de identidad crecen, tanto porque no siempre las credenciales usadas son del todo seguras, o debido a que las herramientas de seguridad que brindan los proveedores de servicios no son suficientes.

Una de las formas para resolver este problema se basa en que el usuario ingrese sus credenciales de acceso una única vez y de este modo también pueda acceder a los demás servicios, sin el requisito de volver a ingresar las credenciales o tener que registrarse en algún proveedor de servicios, a esto se lo conoce como SSO.

Los aspectos que se definieron en la Tabla 1 muestran que los tres protocolos presentan muchas semejanzas entre sí, con muy pocas diferencias y cada uno cumpliendo con su propósito de manera ideal. En el caso de la PUCESE el protocolo que más cumple con las necesidades de la organización es Oauth 2.0, según el resultado presentado en la Tabla 2.

También se observa que Oauth aparte de ser un estándar de autorización que permite a otras aplicaciones acceder a información del usuario sin dar a conocer sus credenciales, también brinda los beneficios de autenticación del protocolo OpenID.

Oauth 2.0 está siendo utilizado actualmente con el personal administrativo de la PUCESE, mediante un sistema que aún se encuentra en fase de pruebas, donde mediante el logeo en la plataforma Office 365 también se tiene acceso a la estación de trabajo sin necesidad de ingresar las credenciales de autenticación nuevamente.

La suscripción institucional a Office 365 incluye otra a Active Directory Azure, esto permite la fácil integración si desea sincronizar contraseñas o configurar un sistema de inicio de sesión único con su entorno local.

El principal inconveniente de SAML es su costo al integrarlo con Active Directory Azure, a pesar de su fácil integración. Active Directory Azure incorpora la herramienta de inicio de sesión único federado que permite a las aplicaciones redirigirse a Azure Active Directory para la autenticación de usuario en lugar de preguntar siempre por las credenciales. Esto se puede utilizar para aplicaciones que soportan protocolos tales como SAML 2.0, WS-Federation, u OpenID Connect, entre otros.

## 5.3. Diagramas de proceso de autenticación actual.

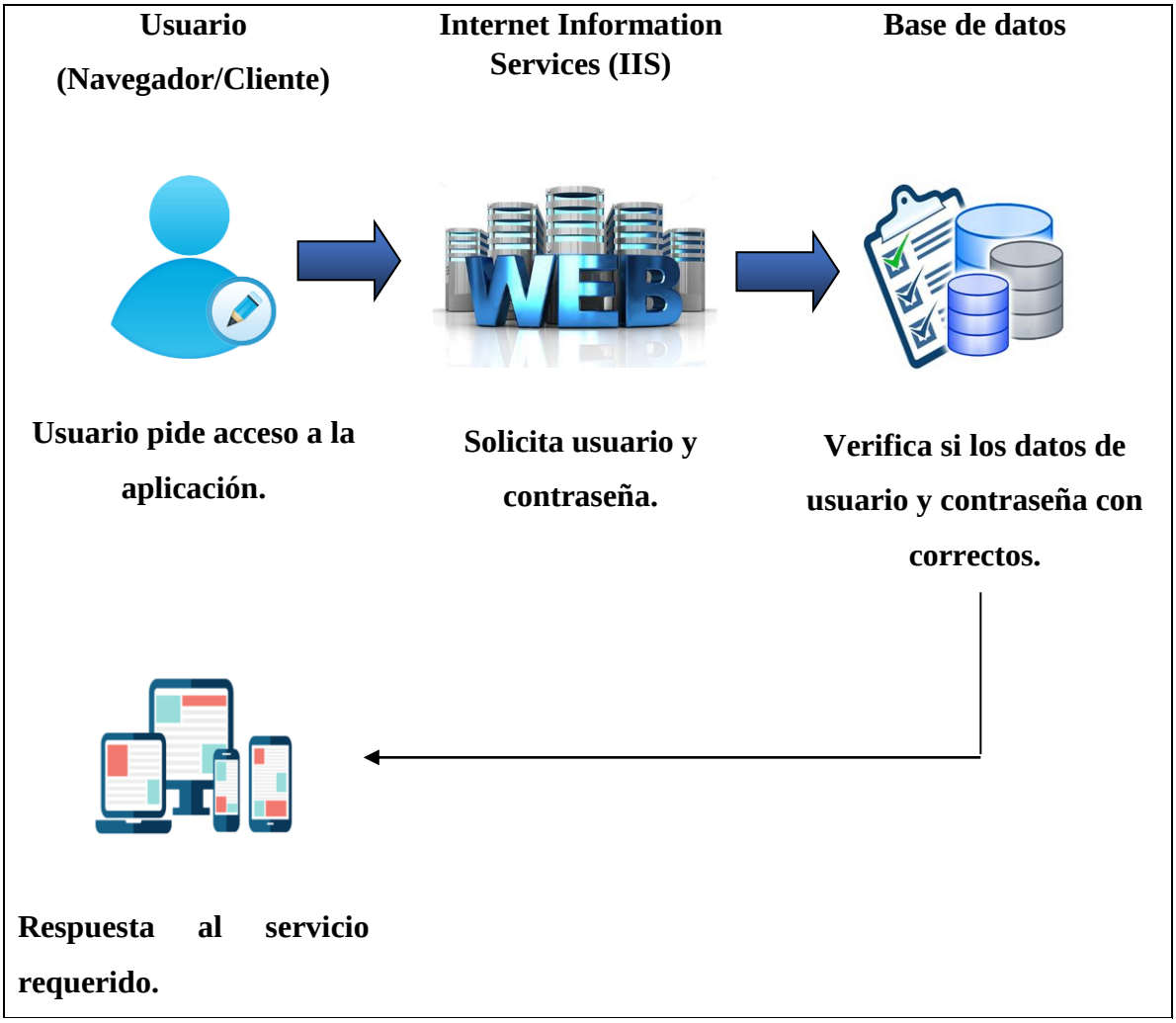


**Figura 12**. Proceso de autenticación – Sistema de consulta de notas.

Fuente: Elaboración propia basada en el escenario actual del caso de estudio

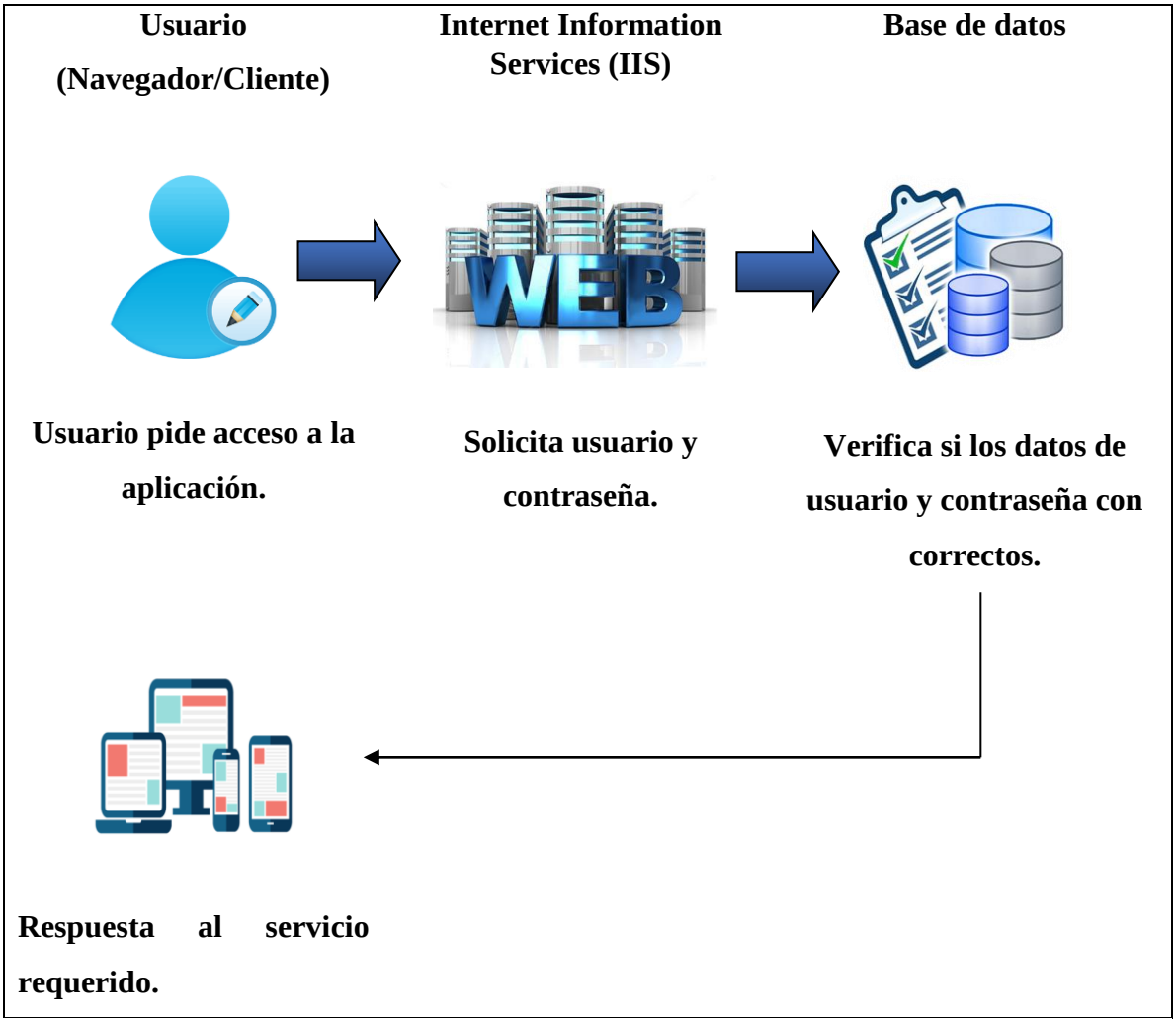


**Figura 13**. Proceso de autenticación – Sistema de evaluación académica.

Fuente: Elaboración propia basada en el escenario actual del caso de estudio

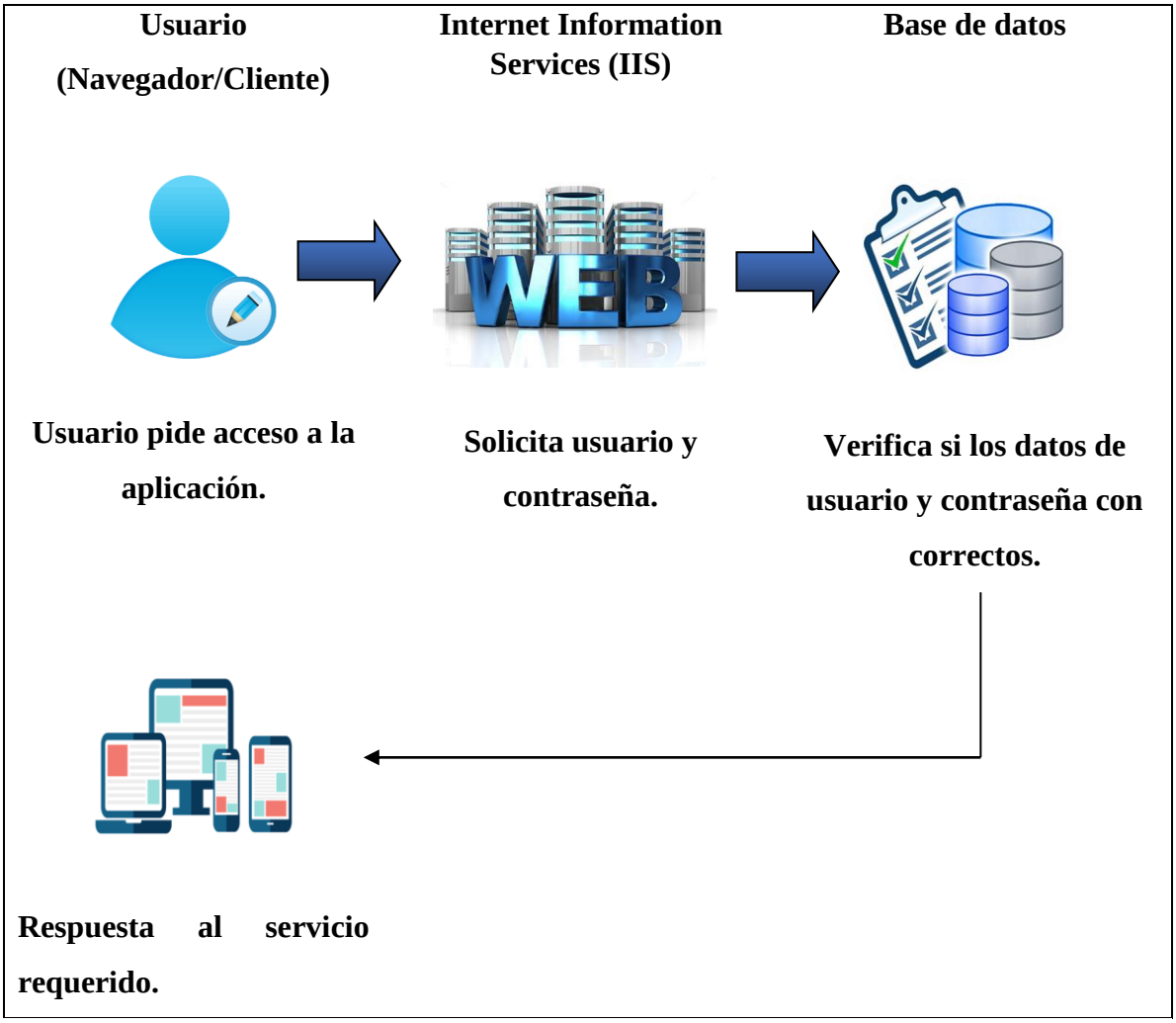


**Figura 14**. Proceso de autenticación – Aplicación Microcurricular.

Fuente: Elaboración propia basada en el escenario actual del caso de estudio

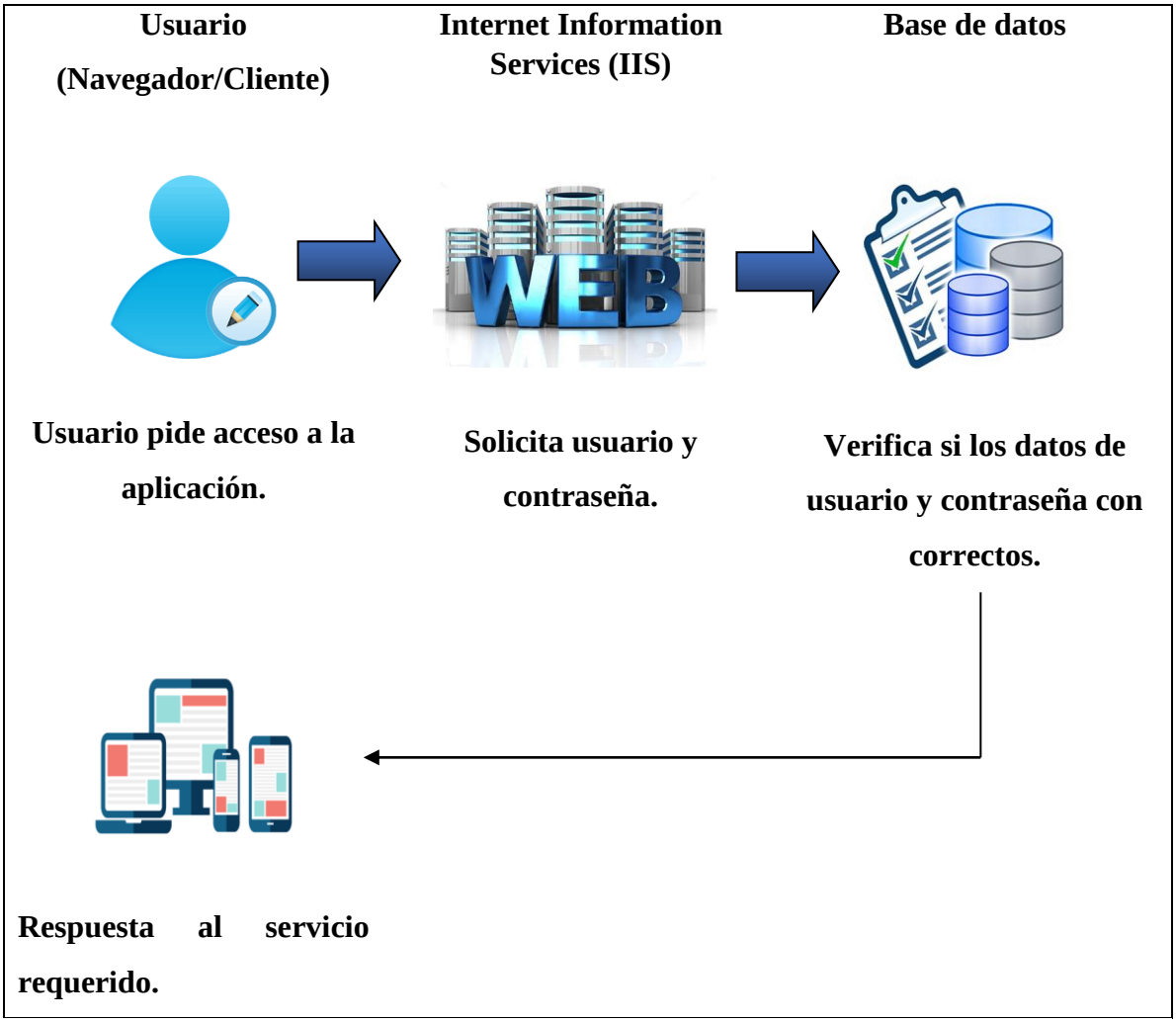


**Figura 15**. Proceso de autenticación – Aplicación Moodle.

Fuente: Elaboración propia basada en el escenario actual del caso de estudio

## 6. Propuesta de intervención.

Entre la PUCESE y Microsoft existe un contrato campus agreement, el cual permite que los estudiantes, profesores tengan acceso a la plataforma de Office 365 de forma gratuita, al

mismo tiempo esta suscripción también permite el uso de muchas soluciones informáticas entre las que se encuentran Active Directory Azure.

Active Directory Azure es un servicio de microsoft para la administración y gestión de directorios e identidades de múltiples usuarios basados en la nube.

En una organización AD Azure representa una solución sencilla al problema del acceso a aplicaciones basadas en la nube como Office365, Dropbox, Yahoo, Skype entre otras mediante un inicio de sesión único (SSO)

Una vez realizada la investigación se pudo observar que se encuentra implementado el Active Directory (AD) de forma local, la cual tiene como función controlar los recursos a los cuales acceden los usuarios dentro de la institución, y que las estaciones de trabajo se encuentren bajo un mismo dominio.

Active Directory Azure también incluye un conjunto de herramientas para la gestión de identidades, como autenticación única de usuarios, autorización a recursos compartidos y gestión de contraseñas.

Con el fin de aprovechar todos los recursos tecnológicos disponibles en la institución, sin tener que llegar a la contratación de equipos nuevos, software costoso o herramientas diseñadas específicamente para la autenticación de usuario, surge la necesidad de implementar Active Directory Azure en combinación con algunas herramientas y protocolos de autenticación, como la solución ideal para la gestión del acceso e inicio de sesión único tanto a aplicaciones basadas en la nube como aquellas alojadas en los servidores de la Universidad.

Tanto Active Directory Azure como la implementación de un Active Directory local son sistemas de directorios que almacenan la información de los usuarios, recursos utilizados, los procesos de inicio de sesión, la autenticación y la autorización, búsquedas de directorios.

Los primeros pasos que se deben realizar para lograr crear un Sistema de autenticación única con Active Directory Azure es integrarla con el AD local, esto proporcionara una

identidad común para los usuarios de Office 365, la estación de trabajo local, Azure y aplicaciones SaaS con soporte para integrarlas con Active Directory.

## 6.1. Software an a service (SaaS)

> SaaS, *Software-as-a-Service*, es un modelo de repartición del software que brinda a sus clientes el ingreso a aplicaciones a través de la nube (internet). El software se entrega como servicio, de manera que el cliente no tiene que ocuparse del mantenimiento de las aplicaciones. Para el usuario, este modelo da la posibilidad de minimizar recursos y costos.
>
> Las aplicaciones y servicios no tienen soporte físico y se ingresan a través de la red para su uso on-line, es decir, se ejecutan en servidores del proveedor en forma de alojamiento web (*hosting*). Detrás puede existir métodos de optimización de la infraestructura tales como la virtualización de servidores o la computación en la nube también conocida como *Cloud-Computing* con la que a veces se confunde el SaaS.(Bravo, 2009)

Ventajas de SaaS.

**Obtener acceso a aplicaciones sofisticadas:** Con SaaS, incluso aplicaciones empresariales sofisticadas, como ERP y CRM, están al alcance de organizaciones que no cuentan con recursos para comprar, implementar y administrar la infraestructura y el software necesarios.

**Pagar solo por lo que usa:** También ahorra dinero, porque el servicio SaaS permite escalar o reducir los recursos en función del nivel de uso.

**Usar software de cliente gratuito:** Los usuarios pueden ejecutar la mayoría de las aplicaciones SaaS directamente desde un explorador web sin necesidad de descargar e instalar ningún software.

**Obtener acceso a los datos de las aplicaciones desde cualquier parte:** Con los datos almacenados en la nube, los usuarios pueden obtener acceso a su información desde cualquier equipo o dispositivo móvil conectado a Internet.

La integración es llevada a cabo mediante AD Azure Connect, una herramienta la cual permite integrar directorios locales con Azure Active Directory.

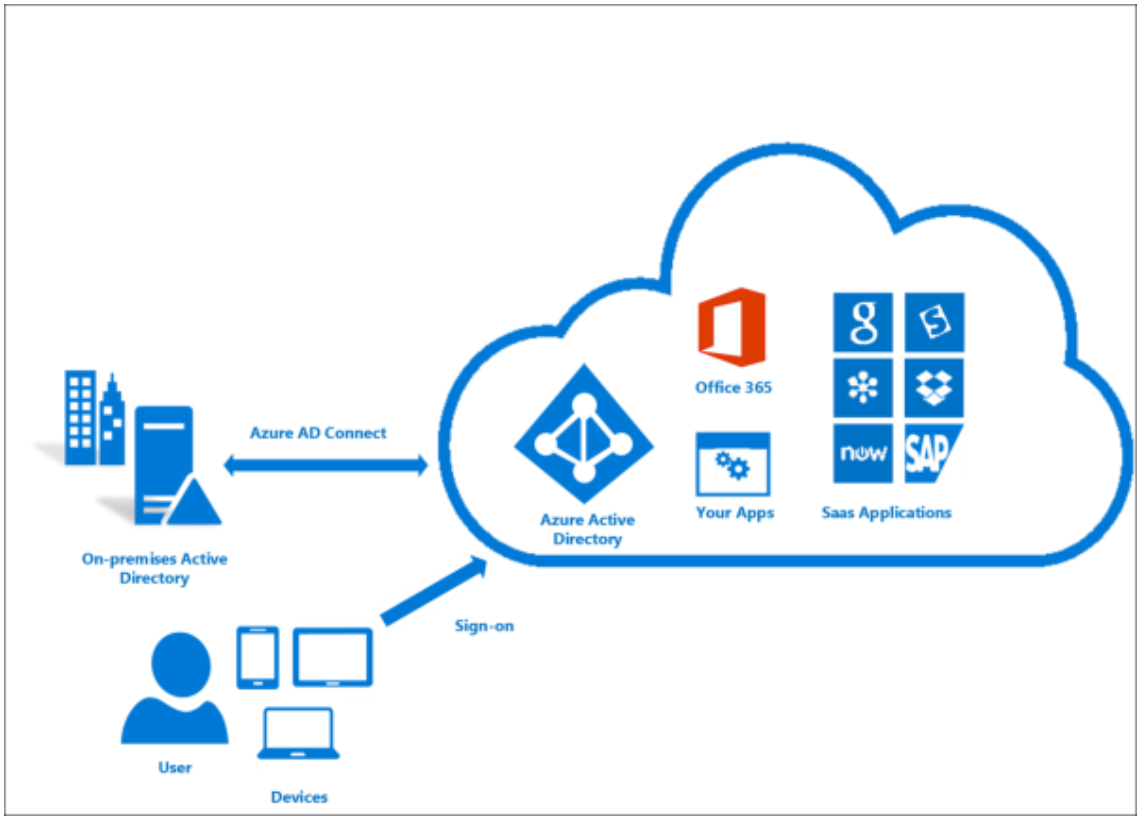


**Figura 16.** Funcionamiento Active Directory Connect

Fuente: Microsoft Active Directory Azure (Microsoft, s/f)

Azure Active Directory Connect se constituye de tres componentes principales: los servicios de sincronización, el componente opcional de servicios de federación de Active Directory y el componente de supervisión denominado Azure AD Connect Health.

Una vez conectada una instancia de Active Directory local con una instancia de Azure AD se pueden sincronizar las contraseñas, lo que permite iniciar sesión en los servicios de ambas instancias utilizando la misma contraseña. Las ventajas más significativas de integrar los directorios locales con el AD Azure son el aumento de productividad de los usuarios y la reducción de costos en asistencia técnica.

Active Directory Azure recibe tres formas diferentes de iniciar sesión en las aplicaciones:

El inicio de sesión único federado, inicio de sesión único basado en contraseña, inicio de sesión único existente.

**Inicio de sesión único** federado posibilita a las aplicaciones re direccionarse a Active Directory Azure para la autenticación del usuario en lugar de solicitar su propia contraseña. Esto es compatible con aplicaciones que admiten protocolos como SAML, WS-Federation u OpenID Connect, es el modo más apropiado de inicio de sesión único.

**Inicio de sesión único basado en contraseña** permite el almacenamiento seguro de la contraseña de la aplicación mediante una extensión de navegador web o una aplicación para móviles. Esto aprovecha el proceso de inicio de sesión existente proporcionado por la aplicación, pero permite a un administrador gestionar las credenciales sin necesidad que el usuario conozca la contraseña.

**Inicio de sesión único existente** permite que Active Directory Azure aproveche cualquier inicio de sesión único existente que se haya configurado para la aplicación, pero permite que estas aplicaciones se vinculen a los portales del panel de acceso de Office 365 o Active Directory Azure.

En el momento que se suprime un usuario o cambia su información en Azure AD, estas modificaciones también se ven reflejadas en las aplicaciones SaaS y en el Active Directory Local dentro de la empresa u organización. Esto significa que la sincronización fue llevada con éxito, permitiéndole al administrador controlar de forma más simplificada la gestión de identidad de los usuarios.

## 6.2. Uso de la galería de aplicaciones Azure AD

La Galería de aplicaciones de Active Directory de Azure brinda un catálogo de aplicaciones que permiten una forma de inicio de sesión único con Azure Active Directory. Entre las aplicaciones aceptadas se encuentran Dropbox, Citrix, Docusing.

Una lista de aplicaciones posibilitan el inicio de sesión único federado usando protocolos de autenticación como SAML, WS-Federation, y OpenID Connect.

Una vez que se haya encontrado la aplicación deseada en la galería, se deben seguir algunos pasos en AD Azure para habilitar el inicio de sesión único.

## 6.3. Implementación de aplicaciones integradas Azure AD a los usuarios

Azure AD proporciona varias formas personalizables de implementar aplicaciones para los usuarios finales en una organización:

- Panel de acceso Azure AD
- Lanzador de aplicaciones de Office 365
- Inicio de sesión directo para aplicaciones federadas

El panel de acceso en https://myapps.microsoft.com es un portal basado en la Web que permite a un usuario final con una cuenta de organización en Azure Active Directory ver e iniciar aplicaciones basadas en la nube a las que se les ha concedido acceso por parte de Azure Administrador de AD.

El Panel de acceso está separado del Portal de administración de Azure y no requiere que los usuarios tengan una suscripción de Azure o una suscripción de Office 365.

## 6.4. Lanzador de aplicaciones de Office 365

Para las empresas que han implementado Office 365, las aplicaciones asignadas a los usuarios a través de Azure AD también aparecerán en el portal de Office 365 en https://portal.office.com/myapps . Esto facilita que los usuarios de una organización inicien sus aplicaciones sin tener que utilizar un segundo portal y es la solución de lanzamiento de aplicaciones óptima para las instituciones que usan Office 365.

## 6.5. Inicio de sesión directo para aplicaciones federadas

La mayoría de las aplicaciones federadas que admiten conexiones SAML 2.0, WS-Federation o OpenID también admiten la opción de que los usuarios inicien en la aplicación y, a continuación, accedan a través de Azure AD, ya sea mediante redirección automática o haciendo clic en un link para iniciar sesión.

Azure Active Directory (Azure AD) facilita la autenticación para los administradores y desarrolladores de aplicaciones, debido a que brinda la identificación como un servicio, con compatibilidad para usar protocolos de autenticación tales como OAuth 2.0 y OpenID Connect, además de bibliotecas de código abierto para varias plataformas.

Azure AD es el proveedor de identidad, responsable de verificar la identidad de usuarios y aplicaciones que existen en el directorio de una organización y, en última instancia, emitir tokens de seguridad tras la autenticación exitosa de esos usuarios y aplicaciones.

Una aplicación que desea externalizar la autenticación de Azure AD debe estar registrada en Azure AD, que guarda e identifica de forma exclusiva la aplicación en el directorio.

Los desarrolladores pueden utilizar las bibliotecas de autenticación de AD Azure de código abierto para facilitar la autenticación.

## 6.6. Bibliotecas de autenticación de Active Directory de Azure

La biblioteca de autenticación de AD de Azure (ADAL) posibilita a los desarrolladores de de software cliente autenticar de forma sencilla a los usuarios en el Active Directory (AD) en la nube o en las instalaciones locales y, a continuación, obtener tokens de acceso para resguardar las llamadas de la API. ADAL tiene muchas características que facilitan la autenticación para los desarrolladores, como soporte asíncrono, caché de tokens configurable que almacena tokens de acceso y tokens de renovación, renovación automática de token cuando un token de acceso expira y un token de actualización está disponible y más. Mediante el manejo de la mayor parte de la complejidad, ADAL puede ayudar a un desarrollador a centrarse en la lógica empresarial de su aplicación y gestionar fácilmente los recursos sin ser un experto en seguridad.

## 6.7. Ejemplos de código de Azure Active Directory

Microsoft Azure Active Directory (Azure AD) permite agregar autenticación y autorización a sus aplicaciones web y API web. Para esto brinda varios ejemplos de código, donde se indica detalladamente como usarlos e integrarlos con cualquier aplicación dependiendo el caso. Para ello se muestran distintos escenarios admitidos por AD Azure donde estos ejemplos de código resultan útiles.

- **Explorador web a aplicación web:** un usuario tiene que iniciar sesión en una aplicación web
- **Aplicación de una sola página (SPA):** un usuario tiene que iniciar sesión en una aplicación de una sola página
- **Aplicación nativa a API web:** una aplicación nativa que se ejecuta en teléfonos, tabletas o equipos tiene que autenticar un usuario para obtener recursos de una API web
- **Aplicación web a API web:** una aplicación web tiene que obtener recursos de una API web.

### Explorador web a aplicación web

Estos fragmentos de código muestran como realizar la autenticación única desde un navegador web a una aplicación web usando Active Directory Azure.

| Idioma / Plataforma | Muestra | Descripción |
|---|---|---|
| Cnet | WebApp-OpenIDConnect-DotNet | Utilice OpenID Connect (middleware OpenID Connect OWIN de ASP.Net) para autenticar usuarios de un inquilino de Azure AD. |
| Cnet | WebApp-MultiTenant-OpenIdConnect-DotNet | Una aplicación web multi-tenant .NET MVC que utiliza OpenID Connect (middleware OpenID Connect OWIN de ASP.Net) para autenticar usuarios de varios inquilinos Azure AD. |
| Cnet | WebApp-WSFederation-DotNet | Utilice WS-Federation (middleware OWIN de WS-Federation de ASP.Net) para autenticar usuarios de un inquilino de Azure AD. |

**Figura 17.** Ejemplo de código 1 – Explorador web a aplicación web

Fuente: Microsoft Active Directory Azure (Microsoft, s/f)

## Aplicación de una sola página (SPA)

En este ejemplo se observa cómo realizar la autenticación en un sistema de una sola página utilizando las bibliotecas ADAL

| Idioma / Plataforma | Muestra | Descripción |
|---|---|---|
| JavaScript, C # /. NET | SinglePageApp-DotNet | Utilice ADAL para JavaScript y Azure AD para proteger una aplicación de una página basada en AngularJS implementada con un back-end de API web ASP.NET. |

**Figura 18.** Ejemplo de código 2 – Aplicación de una sola página

Fuente: Microsoft Active Directory Azure (Microsoft, s/f)

## Aplicación nativa a la API Web

Los ejemplos de código mostrados a continuación presentan como añadir la autenticación y autorización para aplicaciones nativas que llaman a API web, utilizando las bibliotecas ADAL, Oauth 2.0 y AD Azure.

| Idioma / Plataforma | Muestra | Descripción |
|---|---|---|
| Javascript | NativeClient-MultiTarget-Cordova | Utilice el complemento ADAL para Apache Cordova para crear una aplicación Apache Cordova que llame a una API web y utilice Azure AD para la autenticación. |
| Cnet | NativeClient-DotNet | Una aplicación .NET WPF que llama a una API web protegida mediante el uso de Azure AD. |
| Cnet | NativeClient-WindowsStore | Una aplicación de Windows Store que llama a una API web asegurada con Azure AD. |
| Cnet | NativeClient-WebAPI-MultiTenant-WindowsStore | Una aplicación de Windows Store que llama a una API web de múltiples inquilinos que está protegida con Azure AD. |
| Cnet | WebAPI-OnBehalfOf-DotNet | Una aplicación cliente nativa que llama a una API web, que obtiene un token para actuar en nombre del usuario original y, a continuación, utiliza el token para llamar a otra API web. |
| Cnet | NativeClient-WindowsPhone8.1 | Una aplicación de Windows Store para Windows Phone 8.1 que llama a una API web asegurada por Azure AD. |
| ObjC | NativeClient-iOS | Una aplicación de iOS que llama a una API web que requiere la autenticación de Azure AD. |
| Cnet | WebAPI-ManuallyValidateJwt-DotNet | Una aplicación cliente nativa que incluye lógica para procesar un token JWT en una API web, en lugar de utilizar middleware OWIN. |

**Figura 19.** Ejemplo de código 3 – Aplicación Nativa a API Web

Fuente: Microsoft Active Directory Azure (Microsoft, s/f)

**Aplicación Web a la API Web**

Estos ejemplos de código presentan la manera de usar OAuth 2.0 en Azure AD para crear aplicaciones Web que llaman a las API de la Web.

| Idioma / Plataforma | Muestra | Descripción |
|---|---|---|
| Cnet | WebApp-WebAPI-OpenIDConnect-DotNet | Llame a una API web con los permisos del usuario que haya iniciado sesión. |
| Cnet | WebApp-WebAPI-OAuth2-AppIdentity-DotNet | Llame a una API web con los permisos de la aplicación. |
| Cnet | WebApp-WebAPI-OAuth2-UserIdentity-Dotnet | Añada autorización con OAuth 2.0 en Azure AD a una aplicación web existente para que pueda llamar a una API web. |
| JavaScript | WebAPI-Nodejs | Configure un servicio de REST API integrado con Azure AD for API protection. Incluye un servidor Node.js con una API Web. |

**Figura 20.** Ejemplo de código – Aplicación Web a la API Web

Fuente: Microsoft Active Directory Azure (Microsoft, s/f)

## 6.8. API de gestión de Office 365

Las API de administración de Office 365 utilizan Azure AD para proporcionar autenticación segura a las aplicaciones de la organización. Para acceder a las API de administración de Office 365, debe registrar su aplicación en Azure AD y, como parte de la configuración, especificar los niveles de permisos que necesita su aplicación para acceder a las API.

Luego es necesario configurar las propiedades de la aplicación en Azure AD, generar una nueva clave, obtener un certificado X.509 para habilitar llamadas de servicio a servicio, especificar los permisos que necesita su aplicación para acceder a las API de administración de Office 365. Después solicitar un token de acceso mediante el código de autorización y/o mediante las credenciales de cliente, esto último basándose en el protocolo de autenticación Oauth 2.0.

Azure Active Directory (Azure AD) utiliza OAuth 2.0 para permitirle autorizar el acceso a aplicaciones Web y APIs Web, sin utilizar ninguna de nuestras bibliotecas de autenticación, ni los ejemplos de código mostrados anteriormente.

## 6.9. Secuencia de autorización de Oauth 2.0

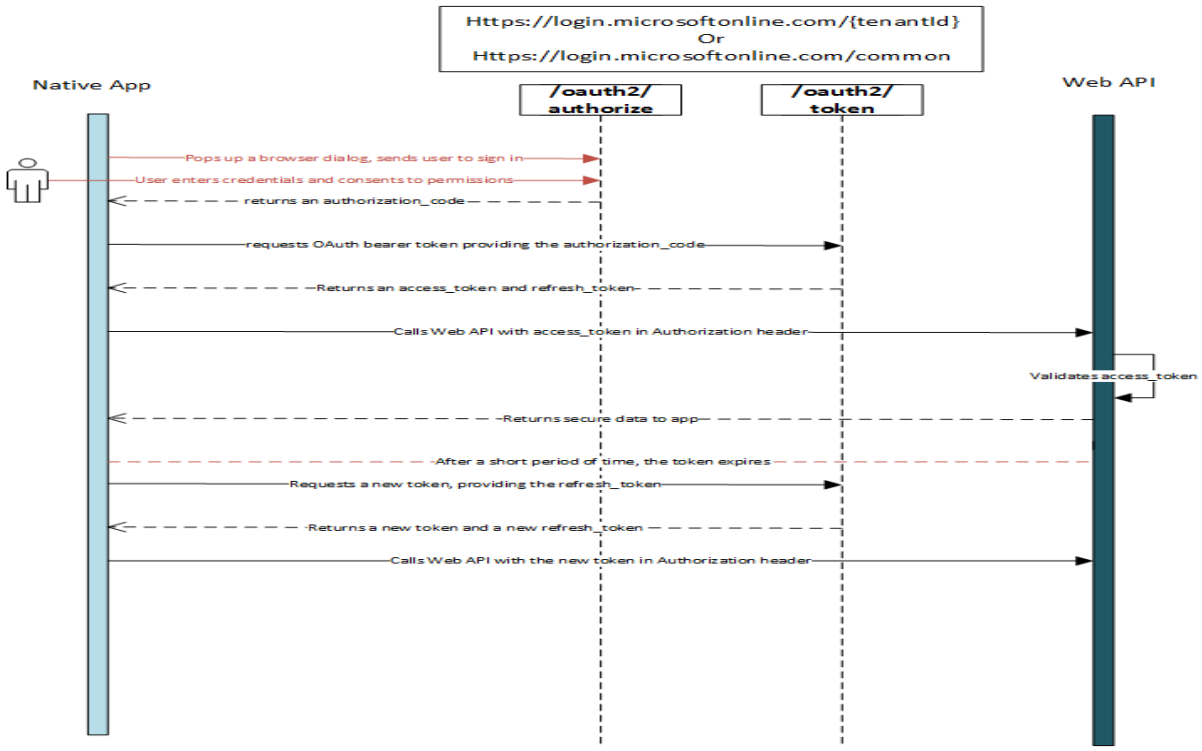


**Figura 21.** Autorización de Oauth 2.0

Fuente: Microsoft Active Directory Azure (Microsoft, s/f)

La secuencia de autorización comienza con el cliente dirigiendo al usuario al */authorize*, en esta solicitud, el cliente indica los permisos que necesita adquirir del usuario.

Luego se le pide al usuario que introduzca sus credenciales y acepte los permisos indicados en el parámetro de consulta (*scope*). Una vez que el usuario se autentique y conceda el consentimiento, Azure AD le enviará una respuesta a su aplicación en la dirección de su solicitud.

Ahora que ha adquirido un código de autorización y ha recibido permiso del usuario, puede canjear el código de un token de acceso al recurso deseado enviando una solicitud.

Una vez que se ha adquirido con éxito un *access token*, puede utilizar el token en las solicitudes a las API de Web, al incluirlo en el encabezado de cualquier aplicación.

Considerando los anterior, se observa que existe tres formas para unificar la autenticación entre varias aplicaciones usando Active Directory Azure, las cuales son bibliotecas de autenticación, ejemplos de código listos para implementarse y acceso a aplicaciones web utilizando la API de gestión de Office 365.

En el caso de la PUCESE lo ideal es usar la API de gestión de Office 365 basado en OAuth 2.0, la cual aparece como una de las soluciones más optimas y beneficiosas a implementar, debido a que permite añadir una aplicación propia de la organización, por ejemplo el sistema de consulta de notas y el sistema de evaluación académica para estudiantes, de una forma sencilla e intuitiva para el administrador de los servicios web de la institución.

El protocolo Oauth 2.0 permite el acceso al contenido por parte de un usuario a una aplicación web. Le brinda permisos a las API para que pueda consumir la información de dicha aplicación, delegando la autenticación del usuario al servicio que aloja la cuenta, es decir, a Active Directory Azure.

La integración de Moodle y Microcurricular con el Office 365 proporciona a los profesores y estudiantes una plataforma de aprendizaje para aumentar la productividad, esto se logra mediante el inicio de sesión único federado que brinda AD Azure.

Se observa que primero se debe conectar la instancia de Active Directory local con la de Active Directory Azure, para después incorporar Correo institucional, Office 365, Moodle y Microcurricular utilizando el inicio de sesión único federado de AD Azure. La API de gestión de Office 365 se encargara de integrar el sistema de consulta de notas y el sistema de evaluación académica, de esta forma se tendrá una única credencial de autenticación para acceder a las cinco aplicaciones web antes mencionadas, la cual será la misma que se usaba para ingresar al correo institucional; es decir, dirección de correo Hotmail y contraseña.

Al tratarse de una cuenta de correo electrónico de Microsoft, generara confianza al usuario al momento de ingresar sus credenciales de autenticación, además el portal de logeo tiene una interfaz amigable, donde sobresale el logotipo de la institución en este caso la PUCESE.

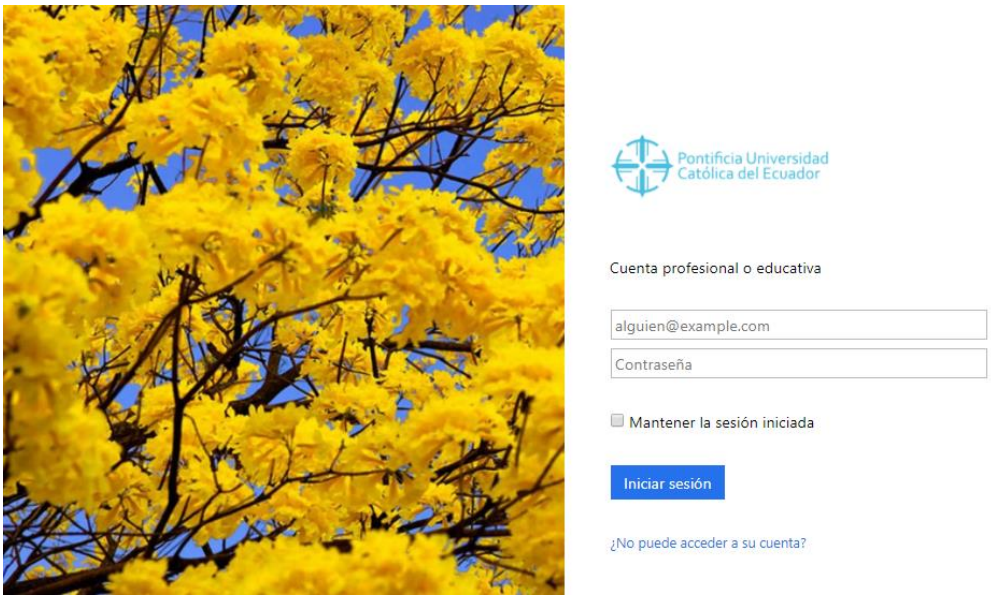


**Figura 22.** Portal de inicio de sesión Office 365

Fuente: Microsoft Active Directory Azure (Microsoft, s/f)

Adicionalmente se deberá brindar capacitación a todos los estudiantes, para informar sobre la nueva forma de iniciar sesión en todos los servicios web, de esta forma todo el estudiantado estará al tanto del nuevo sistema de inicio de sesión único implementado en la institución; haciendo hincapié en la importancia de crear una contraseña segura y robusta.

## 6.10. Diagramas de proceso de autenticación con Azure.

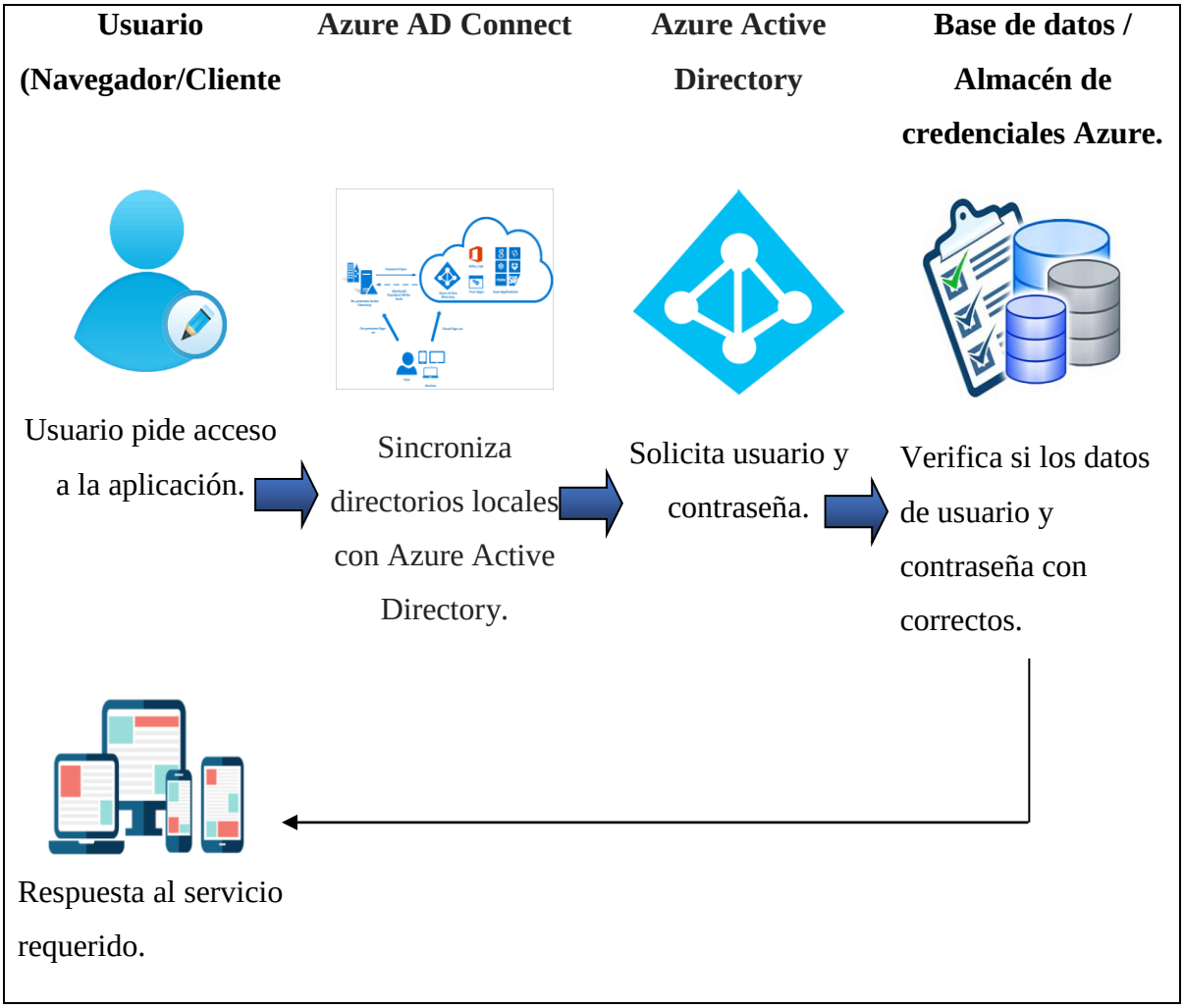


**Figura 23**. Proceso de autenticación - Sistema de consulta de notas.

Fuente: Elaboración propia basada en el escenario actual del caso de estudio

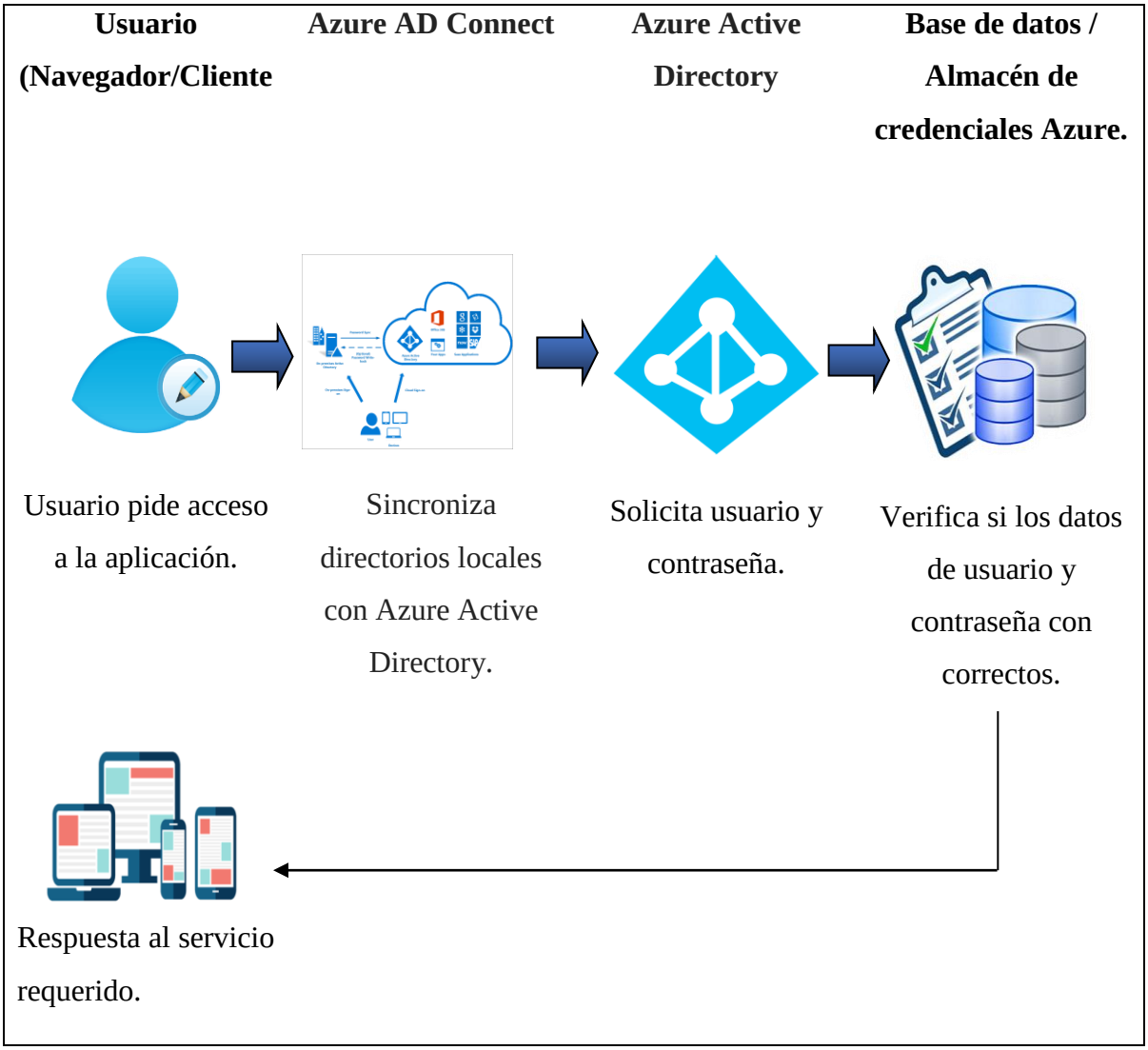


**Figura 24**. Proceso de autenticación - Sistema de evaluación académica.

Fuente: Elaboración propia basada en el escenario actual del caso de estudio

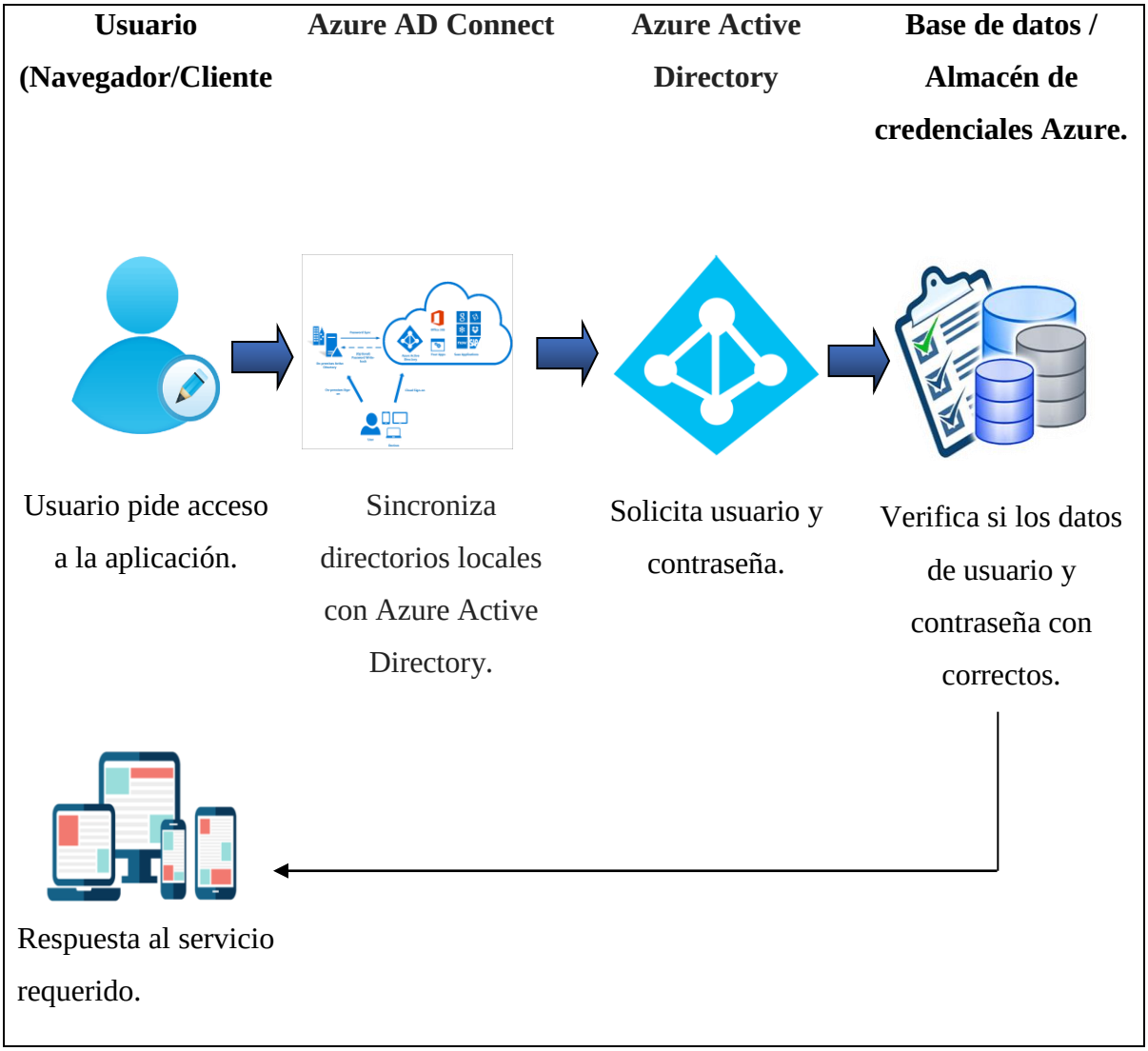


**Figura 25**. Proceso de autenticación – Aplicación Microcurricular.

Fuente: Elaboración propia basada en el escenario actual del caso de estudio

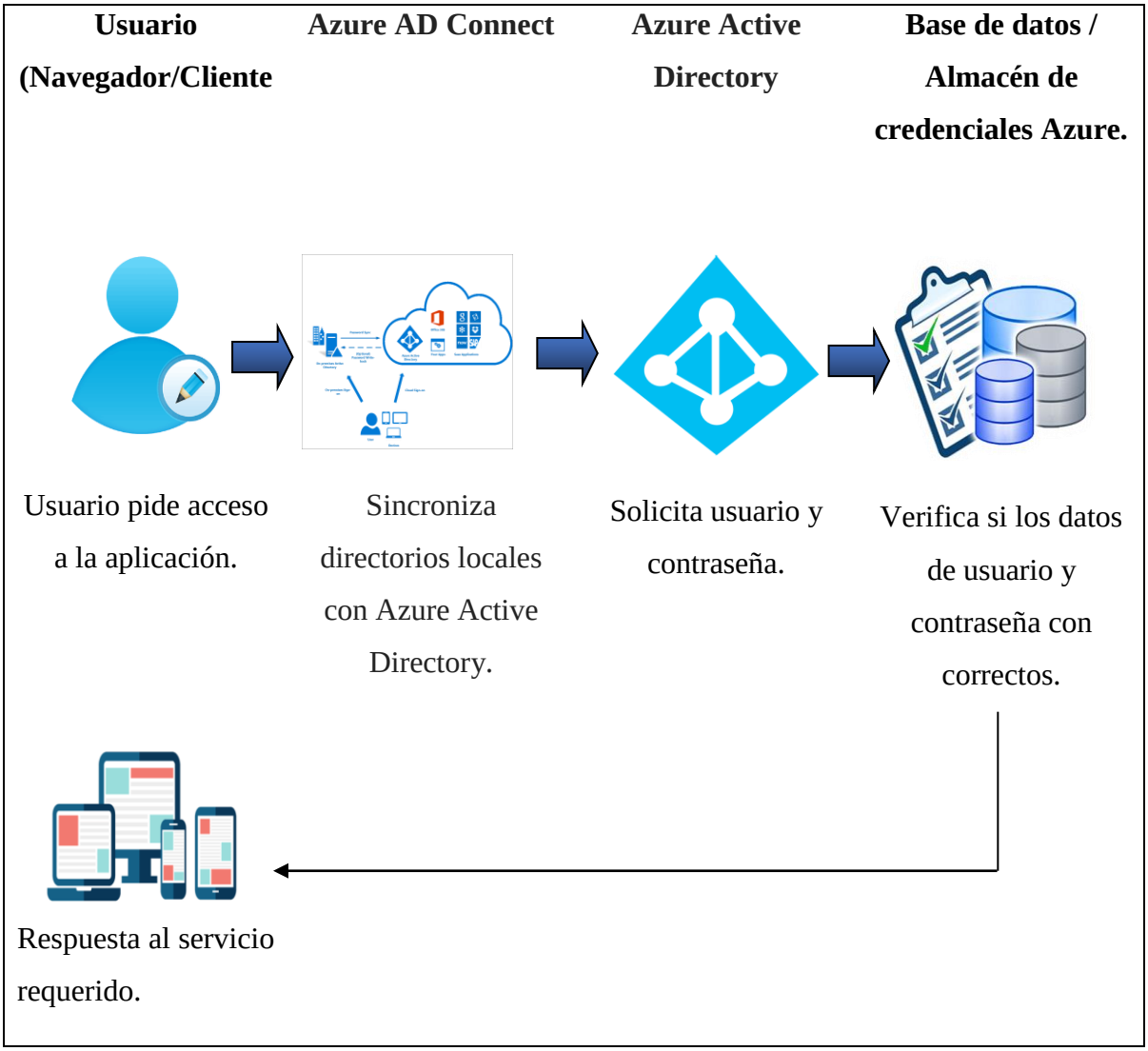


**Figura 26**. Proceso de autenticación – Aplicación Moodle.

Fuente: Elaboración propia basada en el escenario actual del caso de estudio

## 7. Conclusiones.

La autenticación es fundamental para la seguridad de los sistemas informáticos. El uso de un método de autenticación fuerte que no revele la contraseña es imprescindible.

Mediante el análisis de las distintas herramientas, tecnologías y protocolos que existen para implementar un sistema de autenticación única, se logró definir la solución ideal para la institución. Un sistema de autenticación basado en Active Directory Azure y Oauth 2.0 es el adecuado para la autenticación del usuario en el presente entorno.

Identificando todos los procesos, equipos y entidades que intervienen en la infraestructura tecnológica de la PUCESE se obtuvo información valiosa, que ayudo al desarrollo de la investigación. Actualmente el procedimiento de asignación de credenciales a los estudiantes no es realizada de manera adecuada, puesto que la información establecida como nombres de usuarios y contraseñas es de dominio público.

Finalmente la solución propuesta se desarrollará a un bajo costo, debido a que casi en su totalidad se usara software, plataformas, infraestructura y herramientas brindadas por Microsoft de forma gratuita.

## 8. Recomendaciones.

Dentro de una organización es de vital importancia garantizar el acceso a los servicios y proteger la identidad de los usuarios, asegurando que el usuario es quien dice ser.

La autenticación multifactor es un método de autenticación que requiere más de un método de verificación y agrega una segunda capa de seguridad al acceso de los usuarios. Funciona requiriendo dos o más métodos de verificación: algo conocido por el usuario, algo que posea el usuario y características físicas específicas que tenga el usuario.

Azure MultiFactor Authentication (MFA) es la solución de verificación en dos pasos de Microsoft. MFA ayuda a proteger el acceso a datos y aplicaciones. Proporciona

autenticación robusta a través de una gama de métodos de verificación, incluyendo llamadas telefónicas, mensajes de texto o verificación de aplicaciones para móviles. Además se puede integrar de manera fácil con Active Azure Directory.

Adicionalmente de tener un sistema de autenticación con una única credencial, es recomendable contar con un segundo método de verificación, de este modo si una persona malintencionada logra descifrar las credenciales de autenticación del usuario, no conseguiría acceder al sistema debido a que no posee el otro método de verificación.

## REFERENCIAS.


Aguirre, A., & Rosario, M. D. (2015, diciembre 1). *ESTUDIO Y ANÁLISIS DE FACTIBILIDAD DE LA SOLUCIÓN TIPO SINGLE SIGN-ON PARA PEQUEÑAS Y MEDIANAS EMPRESAS* (Thesis). Universidad de Guayaquil. Facultad De Ciencias Matemáticas y Físicas. Carrera de Ingeniería En sistemas computacionales. Recuperado a partir de http://repositorio.ug.edu.ec/handle/redug/11431

Arias, F. G. (1999). *El proyecto de investigación*. Fidias G. Arias Odón. Recuperado a partir de https://books.google.es/books?hl=es&lr=&id=88buBgAAQBAJ&oi=fnd&pg=PR7&dq=que+es+investigacion+de+campo+&ots=09ezmV9Pr4&sig=RG34Dlq2bZlo9F4Dwu_jxbzc05s

Arias, L. F. (s/f). Introducción a las infraestructuras de Active Directory. Recuperado a partir de http://www.academia.edu/6586371/Introducci%C3%B3n_a_las_infraestructuras_de_Active_Directory

Astudillo, H. (s/f). Arquitectura de Software.

Bravo, Á. H. (2009). El SaaS y el Cloud-Computing: una opción innovadora para tiempos de crisis. *REICIS. Revista Española de Innovación, Calidad e Ingeniería del Software*, *5*(1), 38–41.

Carrera, Abdon. (2009). Desarrollo de aplicaciones Web / Arquitectura aplicación Web. Recuperado el 7 de junio de 2017, a partir de http://daw-fiec.pbworks.com/w/page/16963465/Arquitectura%20aplicaci%C3%B3n%20Web

Díaz Barriga, O., Ríos Kruger, G., Cohn Muroy, D., & others. (2015). Implantación de un servicio de autenticación basado en Shibboleth en la PUCP-Caso de Estudio. Recuperado a partir de http://documentas.redclara.net/handle/10786/1003

El reto de los sistemas de autenticación y autorización: ¿cómo elegir el más adecuado? | MINCOM. (s/f). Recuperado el 28 de junio de 2017, a partir de http://www.mincom.gob.cu/?q=node/1739

Escalona, L. S. B. (2012). Protocolos de control de acceso RADIUS. *Revista Telem@tica*, *10*(1). Recuperado a partir de http://www.revistatelematica.cujae.edu.cu/index.php/tele/article/view/51

Fani Calle. (06:51:51 UTC). *Arquitectura 3 Capas*. Tecnología. Recuperado a partir de https://es.slideshare.net/Decimo/arquitectura-3-capas

García, Alvaro, Á., & others. (2014). *Implementación de un proveedor de autorizaciones OAuth 2.0 con Scala* (B.S. thesis). Recuperado a partir de https://repositorio.uam.es/handle/10486/661016

Guía Técnica Diagnóstico de Sistemas de Información | RNI - Red Nacional de Información. (2013). Recuperado el 24 de mayo de 2017, a partir de http://rni.unidadvictimas.gov.co/node/45

Hernandez, A. (s/f). Tecnicas e Instrumentos de la Investigacion. Recuperado a partir de http://www.academia.edu/9310612/Tecnicas_e_Instrumentos_de_la_Investigacion

Hinojosa, K. D. S. (s/f). TOKENS DE SEGURIDAD.

Iglesias, L. (2004). Single Sign On (Tesis). Facultad de Informática. Recuperado a partir de http://hdl.handle.net/10915/3911

Iván M. Caballero, J. C. M. (2013, mayo 7). Consideraciones para implementar una arquitectura single sign-on. Recuperado el 24 de mayo de 2017, a partir de http://www.criptored.upm.es/guiateoria/gt_m142j.htm

Koussa, S. (2013, julio 16). Federated Identities: OpenID vs SAML vs OAuth. Recuperado el 20 de septiembre de 2017, a partir de https://softwaresecured.com/federated-identities-openid-vs-saml-vs-oauth/

Marta Serrat, A. G. (s/f). La gestión de la identidad digital: una nueva habilidad informacional y digital. Recuperado el 22 de junio de 2017, a partir de http://www.tabuladecimal.info:8080/xmlui/bitstream/handle/123456789/206/giones2%5b2%5d.htm?sequence=2&isAllowed=y

Martínez, M. (2006). La investigación cualitativa (síntesis conceptual). *Revista de investigación en psicología*, *9*(1), 123–146.

Matute, M., & Mamfredy, R. (2012). *Microsoft Windows Azure como Plataforma para Prestación de Servicios, Soluciones y Computación en la Nube* (B.S. thesis). Quito: Universidad Israel, 2012. Recuperado a partir de http://190.11.245.244/handle/47000/576

Méndez, A. P., Garcıa, F. P., López, R. M., & Millán, G. L. (s/f). Federacion de servicios kerberizados en eduroam. Recuperado a partir de http://globaltraining.mondragon.edu/recsi2012/es/programa/recsi2012_submission_53.pdf

Mendieta, H. D., & Andrade Navarro, F. (2015). Sistema centralizado de gestión de usuarios para la Universidad del Tolima. Recuperado a partir de http://repository.unad.edu.co/handle/10596/3623

*MF0493_3 - Implantación de aplicaciones web en entorno internet, intranet y extranet*. (2015). Ediciones Paraninfo, S.A.

Microsoft. (s/f). What is Azure Active Directory? Recuperado el 4 de julio de 2017, a partir de https://docs.microsoft.com/en-us/azure/active-directory/active-directory-whatis

RedIRIS - Autenticación de usuarios. (s/f). Recuperado el 8 de mayo de 2017, a partir de https://www.rediris.es/cert/doc/unixsec/node14.html

Romero, M. L. (2017, julio 18). ¿Qué es el método analítico-sintético? Recuperado el 27 de octubre de 2017, a partir de https://www.lifeder.com/metodo-analitico-sintetico/

Sánchez Guerrero, R. (2009). Estudio y puesta en marcha de una infraestructura de gestión de identidad federada basada en SAML 2.0. Recuperado a partir de http://e-archivo.uc3m.es/handle/10016/8497

Sánchez, J. (2011). Sistemas de autenticación y autorización en internet. *Trabajo de investigación realizado en el Master" Interacción Persona Ordenador" de la Universidad Española de Lleida-Junio*.

Sandoval, Y., & Javier, F. (2016). Implementación de un sistema de inicio de sesión único (SSO) en una empresa de telecomunicaciones del Ecuador. Recuperado a partir de http://www.dspace.espol.edu.ec/handle/123456789/34307

Santamaría, Rodrigo. (2012). REST avanzado. Recuperado a partir de http://vis.usal.es/rodrigo/documentos/soa/REST%20avanzado.pdf

Tsyrklevich, E., & Tsyrklevich, V. (2007). Single sign-on for the internet: A security story. *July and August*, *340*. Recuperado a partir de http://www.orkspace.net/secdocs/Conferences/BlackHat/USA/2007/OpenID%20-%20%20Single%20Sign-On%20for%20the%20Internet-paper.pdf

Velandia, T., Ángel, S., Barona Ríos, C., & García Ponce de León, O. (2010). Infraestructura tecnológica y apropiación de las TIC en la Universidad Autónoma del Estado de Morelos: Estudio de caso. *Perfiles educativos*, *32*(127), 105–127.

Cezar, L. (2012). *Universidad Nacional Autonoma de Mexico.* Obtenido de SISTEMA CENTRALIZADO DE AUTENTICACIÓN DE USUARIOS PARA LA SUBDIRECCIÓN DE SEGURIDAD DE LA INFORMACIÓN UNAM-CERT: http://www.ptolomeo.unam.mx:8080/xmlui/handle/132.248.52.100/2662

Escalona, S. (2012). Protocolos de control de acceso RADIUS. *Revista Telemática*, 10.

Vaca, W. (2014). *CONTROL DE ACCESO Y ADMINISTRACIÓN DE RECURSOS DE RED MEDIANTE UN SERVIDOR AAA EN EL GAD MUNICIPAL DE URCUQUI USANDO SOFTWARE LIBRE.* Obtenido de http://repositorio.utn.edu.ec/bitstream/123456789/4337/2/04%20RED%20043%20ART%C3%8DCULO%20CIENT%C3%8DFICO%20ESPA%C3%91OL.pdf

# ANEXOS

## Anexo 1

### Entrevista al encargado de desarrollo de software.

La presente entrevista tuvo como finalidad conocer el funcionamiento de las aplicaciones web que manejan los estudiantes en la PUCESE, así mismo también se logró determinar de manera más detallada la infraestructura tecnológica con la que cuenta la institución.

1. **¿Número de aplicaciones web utilizadas por los estudiantes?**

a) Moodle
b) Sistema de consulta de notas
c) Evaluación al docente

d) Microcurricular
e) Correo electrónico

**2. ¿La instalación de las aplicaciones es?**

**a) Cliente/servidor**
b) Monousuario
c) Otro

**3. ¿Quién le presta soporte a estas aplicaciones?**

El soporte técnico a las aplicaciones de Moodle y Microcurricular es realizado por una persona, mientras que otra se encarga de dar soporte al correo electrónico, sistema de evaluación académica y sistema de consulta de notas.

El soporte a nivel usuario de todas las aplicaciones es llevado a cabo por otro empleado que brinda asistencia a todos los requerimientos de los usuarios, sin embargo si el requerimiento en el sistema de consulta de notas es complejo, es decir se necesita acceder de forma directa a la base de datos del sistema y modificarla es necesario la intervención del encargado del soporte técnico de esta aplicación.

**4. ¿Qué tipos de servidores son utilizados en la PUCESE?**

**a) Servidor de aplicaciones**
b) Servidor de Archivos
**c) Servidor de Base de Datos**
d) Servidor de Comunicaciones
e) **Servidor de Correo** WINDOWS AZURE MICROSOFT
f) Servidor Espejo
g) Servidor de Impresión
h) Servidor de Respaldo
**i) Servidor de Web**
j) Servidor Proxy
k) Otro (explicar)

Físicamente todas las aplicaciones están en uno solo, pero lógicamente se encuentran separadas debido a que cada una está instalada en una máquina virtual distinta con su propio sistema operativo y características únicas.
Como servidor de correo se usa la plataforma informática empresarial Microsoft Azure.

5. **¿Qué tipo de conexión tienen estos servidores?**

a) **Independiente (stand alone)**
b) Cluster (Si el servidor está conectado con otros servidores que pueden ser vistos como un sistema único.)

Existen cinco servidores de producción y cinco servidores de ambiente de pruebas conectados de forma independiente en un pequeño data center.

6. **¿Número de servicios que corren bajo Windows?**

Microcurricular, sistemas de notas, sistema de evaluación al docente.

7. **¿Número de servicios que corren bajo Linux?**

Moodle

8. **¿Qué tipo de cableado estructurado existe en la PUCESE?**

**a) Cableado de Voz**
**b) Cableado de Datos**
**c) Wireless**
d) Corriente regulada
e) Otro (explicar)

**¿En qué tipo de arquitectura de software son implementados las aplicaciones y servicios?**

a) **Arquitectura cliente servidor**
b) Arquitectura orientada a objetos (SOA)
c) Arquitectura de tres niveles

Todas las aplicaciones son implementadas en el modelo cliente- servidor.

9. **¿En qué tipo de arquitectura de sistemas están organizados los componentes de la infraestructura tecnología de la PUCESE?**

a) Centralizada
**b) Descentralizada**
c) Distribuida

## Anexo 2

# CERTIFICADO DE INVESTIGACION.

Certifico que el estudiante BRYAN ALEXANDER SEVILLA DELGADO con el número de cédula 0802314732 ha elaborado su investigación en el departamento de TIC en la PUCESE bajo mi supervisión, para el trabajo de tesis: "ANÁLISIS DE FACTIBILIDAD DE PROCEDIMIENTO DE AUTENTICACIÓN ÚNICA PARA ACCEDER A LOS SERVICIOS INFORMÁTICOS DE LA PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR-SEDE ESMERALDAS"

MBA. Marc Grob.
Jefe del departamento de TIC