Universidad Nacional
Federico Villarreal

Vicerrectorado de
INVESTIGACIÓN

ESCUELA UNIVERSITARIA DE POSGRADO

"MODELO DE IDENTIDAD DIGITAL BASADO EN EL PROGRAMA TIER DE INTERNET2 PARA GESTIONAR EL ACCESO A LOS SERVICIOS INFORMÁTICOS EN UNIVERSIDADES PÚBLICAS DE LA REGIÓN CUSCO"

TESIS PARA OPTAR EL GRADO ACADÉMICO DE:
DOCTOR EN INGENIERÍA DE SISTEMAS

AUTOR:
DARIO FRANCISCO DUEÑAS BUSTINZA

ASESOR:
DRA. JACKELINE ROXANA HUAMÁN FERNÁNDEZ

JURADO:
DRA. TAFUR ANZUALDO VICENTA IRENE
DR. BOLÍVAR JIMÉNEZ JOSÉ LUIS
DR. ROMERO ECHEVARRIA LUIS MIGUEL

LIMA – PERÚ
2020

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El objetivo de la investigación es determinar si el diseño del modelo de identidad digital basado en el programa TIER de internet2 influye en la gestión centralizada del acceso a los sistemas informáticos en universidades públicas de la región Cusco. Así mismo, para cumplir con el propósito de la investigación se aplicó metodologías de desarrollo de sistemas de información para diseñar el modelo de identidad digital y exclusivamente para la evaluación de adopción del modelo se utilizó la investigación de enfoque cuantitativo del tipo correlacional y cuasi-experimental con tamaño de muestra aleatoria de 38 entrevistados. En ese sentido, los resultados del diseño del modelo de identidad digital comprenden dos componentes. En primer lugar, el componente para gestionar el repositorio de datos basado en un sistema de directorio LDAP y un sistema de información de identidades. En segundo lugar, el componente para gestionar la autenticación y autorización se diseñó el sistema Portal Web de Autenticación Centralizada basada en Shibboleth, Agente de Autenticación de Sistemas Informáticos y soporte de identidades federadas. Por otro lado, el resultado de la evaluación de adopción del modelo en general es positiva. Entonces, diseñado los componentes para mejorar la gestión de repositorio de datos, autenticación y autorización de usuarios la hipótesis general es aceptada y por lo tanto el problema principal es resuelto.

Palabras claves: Modelo de Identidad Digital, Internet2, TIER, Trust and Identity in Education and Research, Universidad.

ABSTRACT

The objective of the research is to determine if the design of the digital identity model based on the TIER program of internet2 affects the management of access to computer services in public universities in the Cusco region. Likewise, in order to fulfill the purpose of the investigation, information systems development methodologies were applied to design the digital identity model and for the evaluation of the adoption of the model, the quantitative approach investigation of the correlational type with random sample size was used of 38 interviewees. The design results comprise two components. First, an LDAP directory system and an identity information system were designed to manage the data repository. Secondly, to manage authentication and authorization, the Centralized Authentication Web Portal based on Shibboleth and Computer Systems Authentication Agent was designed. Finally, on the evaluation of adoption of the model in general is positive. Then, with the design of components to improve data repository management, authentication and user authorization the general hypothesis is accepted and therefore the main problem is solved..

Keywords: Digital Identity Model, Internet2, TIER, Trust and Identity in Education and Research, University.

I. INTRODUCCIÓN

El presente estudio de investigación es un punto de partida para Universidades que aún no hayan implementado un sistema único de gestión de acceso a los sistemas informáticos de la universidad, puedan tomar como referencia el Programa TIER de Internet2 que está disponible para todas las universidades en el mundo. Además, para conocer la percepción del usuario sobre el nuevo procedimiento de acceso a los sistemas informáticos el presente estudio realiza una evaluación en base al Modelo de Adopción del Método (MAM) propuesto por (Moody, 2003).

En este sentido, se han investigado dos campos de estudios principales. El primer campo, es el referido a la Gestión de Identidad, Autenticación, Autorización y Acceso a Sistemas Informáticos. El segundo campo, es referido al Programa TIER (Trust and Identity in Education and Research) de Internet2 que está conformado por los componentes de Shibboleth, Grouper y COmanage. Por consiguiente, en base a los campos de estudio se diseñó el Modelo de identidad digital TIER de Internet2 cuyos elementos principales son un Sistema de Información de Identidades, Sistema de Directorio LDAP, Portal Web de Autenticación Centralizada, Agente de Autenticación de los Sistemas Informáticos y soporte de identidades federadas.

La estructura del documento de la presente tesis está conformada en principio por la introducción donde se plantea y describe el problema en base a la necesidad de la Universidad Pública de la Región Cusco y reforzado por estudios previos. Así mismo, se describen las limitaciones y justificación del estudio. Seguidamente, de desarrolla el marco teórico que describe de manera parsimoniosa las variables del

estudio. En esta misma línea, seguimos con el desarrollo del método donde se describe el tipo de estudio, la población, muestra, instrumentos, validaciones, análisis y procedimiento de prueba de hipótesis. Finalmente, se desarrolla la presentación de los resultados los cuales dan pie a la discusión de dichos resultados para luego finalmente concluir y expresar las recomendaciones necesarias del estudio.

1.1. Planteamiento del problema

En la era de la cuarta revolución industrial o transformación digital todos los procesos en las organizaciones deben y serán digitalizadas. En tal sentido, las soluciones informáticas disponible en las organizaciones progresivamente se integran a tecnologías emergentes como computación en la nube, Internet de la Cosas, Big Data, Inteligencia Artificial y entre otras. Por ejemplo, muchas organizaciones han externalizado el sistema de correo electrónico y almacenamiento utilizando servicios de computación en la nube.

Sin embargo, el hecho de disponer diferentes soluciones informáticas genera complejidad en la gestión de identidades y acceso a servicios digitales basada en múltiples usuarios y contraseñas. Además, cada servicio digital es desarrollado con diversas tecnologías que complica la interoperabilidad entre sistemas. Entonces, existe la necesidad de adoptar modelos capaces de proporcionar una identidad digital única que permita la autenticación y autorización al momento de acceder a los sistemas de información de la organización.

En el caso particular de las universidades existe una creciente necesidad de intercambiar datos y compartir recursos digitales para actividades académicas y de investigación. Además, las universidades cada vez asumen convenios con institutos y comunidades de investigación que gestionan repositorios digitales que almacenan publicaciones en diferentes áreas del conocimiento.

A pesar de los avances tecnológicos muchas organizaciones no han logrado modernizarse por la resistencia al cambio de sus integrantes. Entonces, al adoptar una nueva tecnología es necesario evaluar la percepción de los usuarios para tener éxito en el proceso de cambio.

1.2. Descripción del problema

A medida que las computadoras empezaron a compartir datos entre múltiples usuarios usando las redes de computadores surgieron los problemas de seguridad en la gestión o control de acceso. Así mismo, el problema se agudiza aún más puesto que los sistemas informáticos en las organizaciones se multiplican cada vez y trabajan de manera independiente provocando que los usuarios utilicen credenciales o cuentas diferentes para acceder a cada sistema.

Los problemas mencionados anteriormente no son ajenos a las Universidades, puesto que, una universidad tiene muchos usuarios que hacen uso de diversos Sistemas de Información orientadas al ámbito académico, administrativo y de investigación. Entonces, por el considerable número de usuarios y el constante cambio tecnológico de los sistemas de información se requieren métodos de autenticación y control de acceso más complejo.

Según (Nina et al., s. f.) en el caso de las universidades públicas de la región del Cusco específicamente en la Universidad Nacional de San Antonio Abad no es ajeno a la problemática de la gestión de identidades y el control de acceso a las soluciones informáticas. En primer lugar, la universidad progresivamente ha implementado según las necesidades de la institución o la disponibilidad de presupuesto diversos sistemas informáticos que necesitan diferentes credenciales de acceso. Por ejemplo, los servicios informáticos como: el Software Académico, Servicio Wi-Fi, Correo electrónico institucional, Biblioteca virtual, Repositorios digitales, Software Anti plagio y entre otros servicios requieren sus propias credenciales de acceso. En segundo lugar, los usuarios de la universidad para acceder a los servicios informáticos de la universidad deben elegir y recordar la credencial de acceso adecuada entre varias credenciales que ellos disponen. Entonces, esta situación provoca incomodidad y dificultades en el acceso a los sistemas informáticos de la universidad. En tercer lugar, los sistemas informáticos que utiliza la universidad fueron desarrollado en diferentes plataformas de Hardware y Software que generan complejidad en el intercambio de datos para crear un modelo de gestión de acceso centralizado de credenciales. En conclusión, es necesario adoptar un nuevo modelo de identidad digital que sea fácil de usar, útil y seguro para la gestión centralizada de identidades.

Tomando en cuenta los problemas descritos anteriormente la organización internacional Internet2 desarrollo el programa TIER (Trust and Identity in Education and Research) que es un conjunto de soluciones informáticas de fuente abierta para solucionar los problemas de gestión

centralizada de identidad, autenticación y autorización en los sistemas de información de las universidades. Por lo tanto, considerando que existe una solución para la gestión centralizada de identidades probada por muchas universidades del mundo el presente estudio plantea diseñar y evaluar la adopción del modelo de identidad digital basada en el programa TIER de Internet2 en las Universidades de la Región Cusco.

1.3. Formulación del problema

Problema general

¿De qué manera el diseño del modelo de identidad digital basado en el programa TIER de Internet2 influye en la gestión de acceso a servicios informáticos en universidades públicas de la región Cusco?

Problemas específicos

a) ¿De qué manera el diseño del modelo de identidad digital basado en el programa TIER de internet2 influye en la gestión del repositorio de datos para acceder a los servicios informáticos en universidades públicas de la región Cusco?

b) ¿De qué manera el diseño del modelo de identidad digital basado en el programa TIER de internet2 influye en la gestión de la autenticación y autorización de usuarios para el acceso a servicios informáticos de las universidades públicas de la región Cusco?

c) ¿Es posible que los usuarios adopten el modelo de identidad digital, basado en el programa TIER de internet2, para gestionar el acceso a servicios informáticos en la universidad pública de la región Cusco?

1.4. Antecedentes de la investigación

En el ámbito internacional tenemos importantes investigaciones principalmente en Latinoamérica y España.

En primer lugar, (Torres et al., 2017) en su estudio titulado Plataforma de Gestión de Identidad y Acceso Federado para la Universidad de Cuenca de Ecuador tuvo como objetivo desarrollar una plataforma de gestión de identidad y acceso federado basado en el programa Trust and Identity in Education and Research de Internet2 el estudio fue de enfoque aplicativo, de diseño no experimental. La población estuvo constituida por integrantes de la Universidad de Cuenca la muestra fue no probabilística, para la implementación se plantea una arquitectura orientada a servicios y las pruebas se realizan aplicando pruebas de conceptos que contemplan la configuración de los componentes de la plataforma en un ambiente controlado, el autor llego a la conclusión que el programa TIER permite que la Universidad de Cuenca cuente con una plataforma robusta para la gestión de identidad y acceso federado evitado el esfuerzo de un desarrollo en la universidad, pero siempre apegado a la innovación. Otro factor de éxito en este proyecto fue la adquisición de destrezas por parte del personal técnico involucrados.

En segundo lugar, (Mendieta et al., 2015) en su investigación titulada Sistema centralizado de gestión de usuarios para la Universidad del Tolima en

Colombia tuvo como objetivo centralizar la gestión de usuarios, permitiendo la sincronización de la información de datos personales en un único sistema de autenticación para las distintas aplicaciones con que cuenta la Universidad de Tolima. El estudio fue un enfoque de nivel aplicativo, de diseño no experimental. La población estuvo constituida por integrantes de la Universidad Tolima la muestra fue no probabilista de selección directa, la técnica estadística de recolección de datos fue el cuestionario, el autor llego a la conclusión de utilizar como principal componente de la solución un Single Sing On (SSO) que sirve para interactuar con las diferentes aplicaciones y así lograr un sistema de autenticación único. Además, el sistema Single Sing On, intercambia información sensible y protege estos datos mediante el uso de canales seguros, por lo que cualquier aplicación que gestione información sensible debe utilizar mecanismos para proteger tal información.

En tercer lugar, (Monedero et al., s. f.) en su trabajo de investigación titulado Implantación de LDAP como sistema de autenticación centralizada tuvo como objetivo implementar un sistema de autenticación centralizada basado en el Protocolo Ligero de Acceso a Directorios (LDAP) es estudio es de nivel aplicativo, de diseño no experimental. La población estuvo conformada por miembros de la Universidad de Cordoba de España, la conclusión del trabajo fue seleccionar como principal componente a OpenLDAP para implementar el servidor de directorio logrando un sistema de alta disponibilidad, fiabilidad y rendimiento. En particular, para el caso de la universidad de Cordoba ya disponía de una solución de acceso único de autenticación basado en directorios de UNIX (NIS) pero presentaba problemas

como limitaciones en las modificaciones de datos y delegar privilegios de administración.

En Cuarto lugar, (Penna et al., 2016) en su estudio titulado Implementación de un servicio de autenticación centralizado y gestión de identidades en la Universidad de la República en Uruguay, tuvo como objetivo implementar un servicio de autenticación centralizada, basada en un proveedor de identidad Shibboleth, la población estuvo constituido por aproximadamente 100000 estudiantes y 15000 funcionarios (docentes y no docentes), la conclusión del trabajo fue la implementación de un servicio de autenticación centralizada basada en un proveedor de identidad de Shibboleth y la referencia a la norma ISO 24760. Además, se trabajó con énfasis en seguridad de la información aplicando mecanismos de autenticación fuerte con certificados x.509 de cliente y Smart-cards. Actualmente, los servicios se encuentran en producción disponibles para toda la universidad.

Dentro de los antecedentes nacionales se identifican pocos trabajos en el tema de investigación.

En principio, (Díaz Barriga et al., 2015) en su estudio titulado Implantación de un servicio de autenticación basado en Shibboleth en la PUCP-Caso de Estudio, el problema que identifica corresponde a que los usuarios de las universidades necesitan recordar cada vez un mayor número de contraseñas para acceder a los servicios informáticos. En tal sentido, en la Pontificia Universidad Católica del Perú se implementó la herramienta de autenticación federada Shibboleth proporcionado por Internet2. En este sentido, el proceso

de implementación resulto en una herramienta de autenticación con tolerancia a fallas bajo un esquema de alta disponibilidad, pero con el riesgo de que el sistema presente comportamientos anómalos que afecte la percepción de seguridad de los usuarios.

Por otro lado, muy aparte del ámbito universitario existe implementaciones en otras empresas como el caso del Banco de Nación de Perú donde desarrollaron un Sistema de Administración de Acceso e Identidades para obtener un mayor control sobre los activos de información que gestiona 5500 usuarios a nivel nacional sobre 250 aplicaciones (Castro Velarde & Guzmán Salgado, 2010). Así mismo, el trabajo realizado sobre seguridad de la información en la empresa SNX S.A.C. que implementa un sistema de control de acceso (Rivas Arellano, 2016). Además, el trabajo realizado para la empresa Claro en la Región Puno donde se diseñó e implemento un servidor con el protocolo de acceso a directorios LDAP para la seguridad y control del personal que utilizan dispositivos de cómputo (Ccosi & Martin, 2018)

1.5. Justificación de la investigación

1.5.1. Justificación teórica

La presente investigación presenta justificación teórica, puesto que las variables gestión de acceso a sistemas informáticos y modelo TIER de Internet2 se sustenta en la teoría de Administración de Identidades y Control de Acceso (IAM).

El conocimiento teórico sobre Administración de Identidades y Control de Acceso, sirven para gestionar la identidad digital en los sistemas de información implementados en las organizaciones y en este caso particular la universidad. Así mismo, la Administración de Identidades y Control de Acceso se compone de un conjunto de procedimientos a ejecutar, tecnologías de Hardware y Software y políticas que permite realizar la gestión de las identidades de usuario y controlar el acceso a los diferentes recursos de las organizaciones.

Entonces, el presente estudio reafirma la importancia de gestionar un sistema de identidades para el acceso a los sistemas de información que continuamente es renovado con nuevas tecnologías como es el caso de la Computación en la Nube, Internet de las Cosas, Big Data, Inteligencia Artificial entre otros.

1.5.2. Justificación práctica

La transformación digital genera el uso de muchas aplicaciones de Software y diferentes dispositivos de Hardware que hacen necesario la gestión de identidades digitales para asegurar los datos personales y de las

organizaciones. En este sentido, muchas universidades en el mundo conocedores de la problemática de gestión de identidades digitales centralizada para acceder a los servicios informáticos ya crearon soluciones y brindan servicio de calidad a sus usuarios. Entonces, se justifica el presente trabajo para lograr que la Universidad Pública de la Región Cusco este a nivel de las mejores universidades del mundo y del país.

Por otro lado, el estudio es importante porque evalúa la adopción de un modelo de identidad digital basado en el programa Trust and Identity in Education and Research (TIER) de Internet2 que es utilizado en muchas universidades del mundo. Entonces, una solución basada en un estándar de Internet2 asegura la gestión adecuada de la identidad digital y por ende favorece a las actividades académicas, administrativas y de investigación de la universidad.

1.5.3. Justificación metodológica

La investigación presenta justificación metodológica puesto que plantea un problema de la sociedad y aplica el método científico para solucionar el problema en mención. En ese sentido, se plantea una investigación de enfoque cuantitativo, de tipo aplicada y diseño no experimental. Además, en la investigación se utilizó instrumentos de recolección de datos el cuestionario y análisis de datos de los sistemas de información implementados. Así mismo, los instrumentos de recopilación de datos fueron validados.

1.5.4. Justificación epistemológica

El presente estudio presenta justificación epistemológica, puesto que se sustenta en la Teoría General de Sistemas, transformación digital y ciberseguridad. Así mismo, no es posible el desarrollo de un sistema de información o software que en la actualidad no contemple las teorías antes mencionadas.

En ese sentido, la Teoría General de Sistemas engloba todas las aristas de investigación de la realidad y también del interior del ser como son los órganos de nuestro cuerpo humano. Además, es importante puntualizar sus características que corresponden a sistemas abiertos o cerrados, flexibles, permeables, centralizados, adaptables, estables entre otros (Ramírez, 1999).

La cibernética es una teoría de los sistemas de control basada en la transferencia de la información entre sistema, canal de comunicación, contexto y procesos de retroalimentación. En ese sentido, para la transferencia de la información se desarrollan continuamente diversas tecnologías que ya corresponde a una cuarta revolución industrial también denominada transformación digital. Por lo tanto, la transformación digital es definida como un proceso evolutivo que considera una serie de actividades continuas y graduales que define un cambio radical durante un periodo de tiempo. Además, requiere competencias digitales o habilidades tecnológicas poseídas o requeridas por las personas. En el proceso gradual se generan tecnologías digitales como cloud computing, big data, IoT entre otras. Otro componente de la transformación digital corresponde a los cambios en los modelos de negocio,

procesos operativos y experiencias de las personas. En conclusión, la transformación digital debe crear valor que corresponden a efectos y beneficios para toda la organización realizado como resultado del esfuerzo de la transformación digital.

Finalmente, la ciberseguridad que comprende la organización y recopilación de recursos, procesos y estructuras utilizados para proteger el ciberespacio y los sistemas habilitados para el ciberespacio. En ese sentido, en la presente investigación reforzamos el tema de ciberseguridad para convertirse en un dominio interdisciplinario y no un dominio técnico.

1.6. Limitaciones de la investigación

La presente investigación aporta a las universidades nuevos modelos de identidad digital para sus procesos de seguridad de la información. Sin embargo, las limitaciones principales fueron la falta de acceso a fuentes bibliográficas actualizadas relacionadas al tema de estudio, puesto que, el tema de estudio integra experiencias particulares de las universidades. Además, en el ámbito nacional se observa con mayor énfasis la falta de estudios de investigación puesto que el tema es relativamente nuevo que recién va en estado inicial en algunas universidades de nuestro país.

En referencia al factor económico la investigación también presentó limitaciones que se logró superar, gracias a la perseverancia del investigador, colaboradores y en general a los miembros de la comunidad universitaria. Otro aspecto positivo es la colaboración de la organización Internet2 para el soporte y la disponibilidad de recursos técnicos y didácticos.

1.7. Objetivos de la investigación

Objetivo general

Determinar si el diseño del modelo de identidad digital basado en el programa TIER de internet2 influye en la gestión de acceso a servicios informáticos en universidades públicas de la región Cusco.

Objetivos Específicos

a) Identificar si el diseño del modelo de identidad digital basado en el programa TIER de internet2 influye en la gestión del repositorio de datos para acceder a los servicios informáticos en universidades públicas de la región Cusco.

b) Determinar si el diseño del modelo de identidad digital basado en el programa TIER de internet2 influye en la gestión de la autenticación y autorización de usuarios para el acceso a servicios informáticos de las universidades públicas de la región Cusco.

c) Determinar en qué medida los usuarios adoptan el modelo de identidad digital, basado en el programa TIER de internet2, para gestionar el acceso a servicios informáticos en la universidad pública de la región Cusco.

1.8. Hipótesis

General

El diseño del modelo de identidad digital basado en el programa TIER de internet2, influye de manera positiva en la gestión de acceso a servicios informáticos en universidades públicas de la región Cusco.

Especificas

a) El diseño del modelo de identidad digital basado en el programa TIER de internet2, mejora la organización y gestión del repositorio de datos para acceder a los servicios informáticos en universidades públicas de la región Cusco.

b) El diseño del modelo de identidad digital basado en el programa TIER de internet2, influye positivamente en la gestión de la autenticación y autorización de usuarios para el acceso a servicios informáticos de las universidades públicas de la región Cusco.

c) El modelo de identidad digital, basado en el programa TIER de internet2, es factible de ser adoptado por los usuarios para gestionar el acceso a servicios informáticos en la universidad pública de la región Cusco.

II. MARCO TEÓRICO

2.1. Marco conceptual

2.1.1. Sustento teórico de las variables: Modelo de identidad digital basado en el programa TIER de Internet2

2.1.1.1. Definición de Identidad digital

Según (El Maliki & Seigneur, 2007):

> "El carácter distintivo o personalidad de un individuo. Una identidad consiste en rasgos, atributos y preferencias sobre las cuales se pueden recibir servicios personalizados. Tales servicios podrían existir en línea, en dispositivos móviles, en el trabajo o en muchos otros lugares".

Según (Presidencia República Perú, 2018):

> "La identidad digital es aquel conjunto de atributos que individualiza y permite identificar a una persona en entornos digitales. Los atributos de la identidad digital son otorgados por distintas entidades de la Administración Pública que, en su conjunto, caracterizan al individuo".

Según (Veliz, 2015) define Identidad Digital como:

> "Aquella que, utilizada por las personas, naturales y jurídicas, posibilita identificarles de manera indubitable en medios no

presenciales, empleando para dicho fin un documento credencial electrónico (certificado digital)".

En este sentido la identidad digital es la representación de una entidad en un contexto particular. Así mismo, por mucho tiempo, una identidad digital fue considerada como el equivalente de la identidad en la vida real, pero no existe una relación obligatoria entre identidad en el mundo real y la identidad digital. En ese sentido, según (Apéstegui Culli, 2018) toda actividad de las personas en la web irá generando su identidad digital, de manera consciente o inconsciente. Finalmente para (Telefónica, 2013) la participación de la persona en el universo digital la complementa, ya que las herramientas online amplían las posibilidades y dotan a las personas de nuevas capacidades.

2.1.1.2. Modelo de adopción de métodos

También denominado MAM de las siglas del Inglés Method Evaluation Model y es desarrollado por (Moody, 2003) en base al Modelo de Adaptación de la Tecnología (TAM) desarrollado por (Davis, 1989). Por lo tanto, MAM es una estrategia para comprender y predecir la aceptación de una nueva manera de realizar sus actividades por medio de Tecnologías Informáticas. En este sentido, según (Pow Sang Portillo, 2012) para evaluar la aceptación se analizan 3 constructos que corresponden a los siguientes:

- **Facilidad del uso percibida**: Nivel de esfuerzo que una persona percibe al utilizar un método específico.

- **Utilidad percibida**: Nivel de eficacia de un método específico que es percibido por una persona para lograr sus objetivos propuestos.
- **Intención de uso**: Nivel de intencionalidad que tiene una persona para usar un método específico.

En la Figura 1, se ilustra los constructos que proponen el modelo y la relación que existe entre ellos. Así mismo, la adopción en la práctica del modelo consiste en determinar las percepciones de los usuarios que usan un determinado modelo. Por lo tanto, los constructos de MAM descritos anteriormente son variables de tipo psicológica.

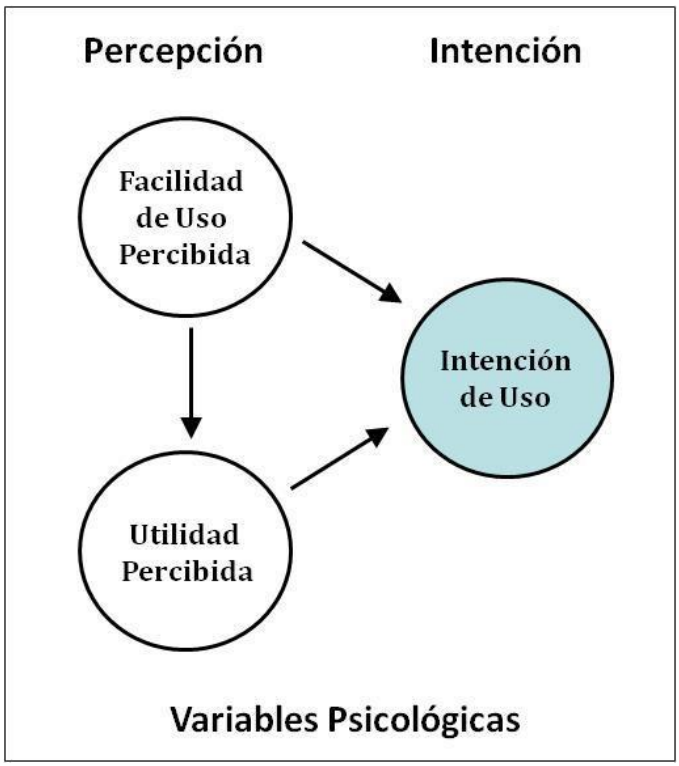

Figura 1. Modelo de Adaptación del Método propuesto por Moody

En conclusión, el Modelo MAM de Moodly considera que las percepciones de eficiencia o facilidad de uso y su efectividad en la utilidad

de un método inciden de manera significativa en la adopción de dicho método. Por lo tanto, se elige este modelo para determinar si es posible la adopción del modelo de identidad digital basado en el programa TIER de Internet2 en la gestión del acceso a servicios informáticos de la universidad.

2.1.1.3. Programa TIER de Internet2

Internet2 es una organización impulsada por instituciones de educación superior de los Estados Unidos y fundado en 1996. El propósito de Internet2 es generar una comunidad de tecnología avanzada y proporcionar un entorno de colaboración donde las instituciones universitarias desarrollan soluciones innovadoras para mejorar el servicio educativo y de investigación. Así mismo, Internet2 en la actualidad brinda servicios avanzados y personalizables de acceso libre para todas las instituciones educativas superiores. Internet2 presta servicios a 317 universidades de Estados Unidos, 60 agencias gubernamentales, 43 redes educativas que representan a más de 100 países (Internet2, 2019).

En este sentido, TIER son las siglas en Ingles de Trust and Identity in Education and Research, y es promovido por Internet2. Así mismo, TIER representa a un programa que integra un conjunto de Software de código abierto y buenas prácticas para gestionar la identidad y el acceso a recursos digitales en instituciones educativas (Internet2, 2019).

A través de los años, la comunidad de gestión de identidad y acceso de Internet2 desarrolló un conjunto de componentes de Software que se convirtió en un elemento fundamental dentro de la infraestructura informática de las universidades. En particular, Shibboleth, COmanage y Grouper han crecido por separado. Entonces, TIER se encargó de integrar cada uno de estos elementos utilizando APIs, estructuras de datos y desarrollo de aplicaciones comunes. También, TIER utiliza contenedores Docker para alojar los componentes de Software, que se configurarán para funcionar correctamente con InCommon Federation (InCommon Federation proporciona acceso seguro de inicio de sesión único a servicios locales y en la nube, y herramientas de colaboración global). En conclusión, TIER tiene el objetivo de construir una suite de gestión de identidad y acceso para educación e investigación. Además, TIER recopila un conjunto de buenas prácticas generadas en la comunidad para garantizar un acceso perfecto a los servicios digitales de investigadores, profesores, personal administrativo y estudiantes.

En la Figura 2, se muestra cómo la arquitectura TIER simplifica los procesos en el ambiente universitario y promueve la colaboración e investigación interinstitucional utilizando un conjunto de herramientas de código abierto y un conjunto de prácticas arquitectónicas en el ambiente universitario que responden a los desafíos planteado en actividades de identidad y control de acceso en instituciones de educación superior. Además, la arquitectura TIER proporciona herramientas, software y patrones arquitectónicos que permiten a las instituciones gestionar de

manera efectiva y segura el acceso a los recursos institucionales y fomentar la colaboración interinstitucional.

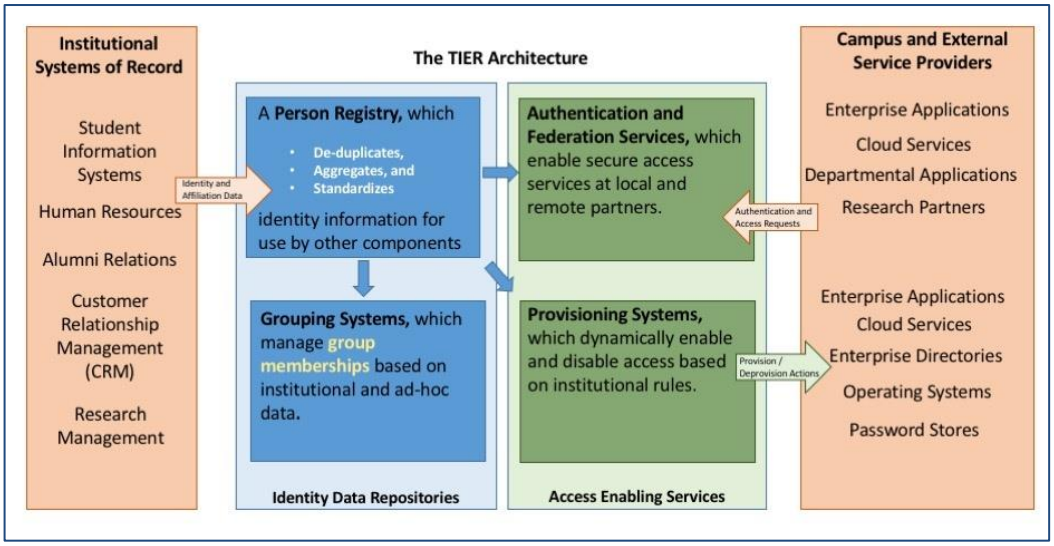

Figura 2. The business context for TIER

Tomado del Programa TIER de Internet2 https://www.internet2.edu.

2.1.1.4. Arquitectura referencial del Programa TIER

En la Figura 3, se muestra la arquitectura de referencia de TIER donde se describe los componentes funcionales para la gestión de la identidad y el acceso en una institución de educación superior. Estos componentes corresponden a:

- Componente para el Registro de persona (Entity Registry): Este componente permite registrar datos de profesores, estudiantes, personal administrativo y estudiantes.
- Servicios relacionados con la autenticación y la federación (Authentication and Federation Services): Componente que permiten el acceso de los usuarios a servicios de acceso comprobados que preservan la privacidad, tanto de forma local como remota.
- Servicio de grupos (Groups Service): Componente que permite gestionar conjunto o grupos de usuarios y para ello los identifica con un nombre que así mismo es utilizado para identificar y usar listas de correo y reglas de autorización.
- Aprovisionamiento (Provisioning Service): Componente que proporciona un único punto de administración para las cuentas de usuario en múltiples servicios y sistemas locales (por ejemplo, sistemas operativos heredados, bases de datos, etc.).
- Integración de Servicios con Messaging Queuing Service: Proporciona un mecanismo de comunicación entre los

componentes de la arquitectura basado en el modelo publicar-suscribir de esta manera se logra disponer una funcionalidad de entrega confiable.

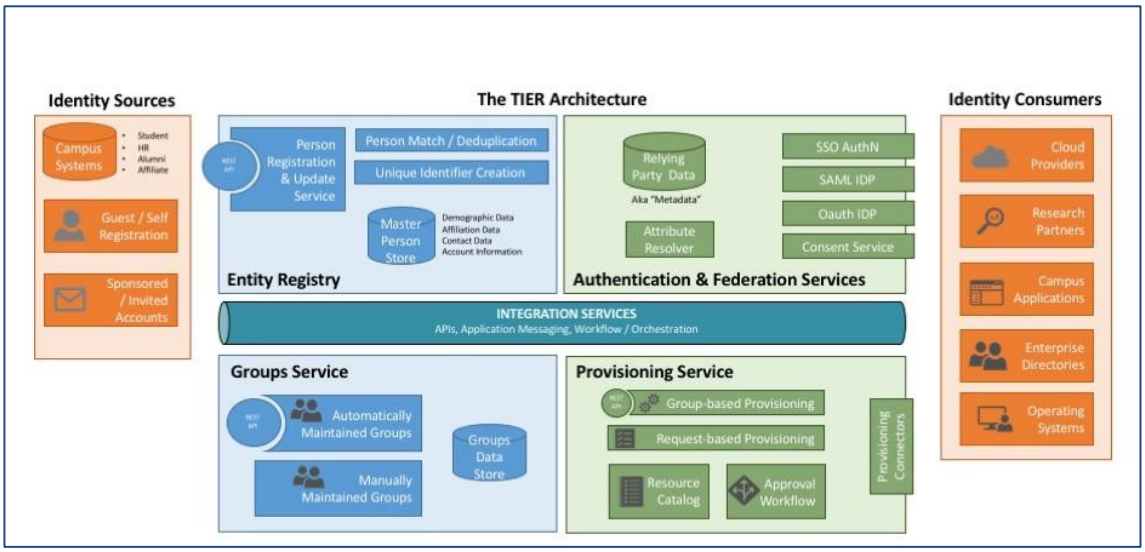

Figura 3. Arquitectura referencial del Programa TIER

Tomado del Programa TIER de Internet2 https://www.internet2.edu

Según (Torres et al., 2017) describe el programa TIER en base a tres aplicaciones Shibboleth, Grouper y COmanage. En este sentido, para la implementación de acceso centralizado a los servicios de su universidad recomienda que para gestionar la identificación y autorización utilizar Shibboleth. En este sentido, Shibboleth es un proyecto de fuente abierta que proporciona funcionalidades para implementar el inicio de sesión único y además permitir a las aplicaciones tomar decisiones para la autorización y acceso individual de recursos protegidos de manera que preserven la privacidad. Por otro lado, Grouper es la herramienta por excelencia para la gestión de control de acceso a grupos y rastrear

información como afiliaciones o roles en las aplicaciones de las universidades. Finalmente, COmanage es una herramienta de gestión de colaboración que permite a las organizaciones cumplir con sus objetivos de ciencia e investigación utilizando herramientas clave de colaboración en un marco seguro y efectivo. Así mismo, COmanage, aprovecha los servicios de administración de identidad federados, la autenticación y autorización de los miembros de la Organización de colaboración (CO) que se manejan en un proceso único y eficiente definido por el CO. Asu vez, este proceso crea automáticamente las cuentas y los controles de acceso para herramientas como wikis, calendarios, herramientas de conferencia y otras aplicaciones de dominio que están disponibles para los miembros de la organización.

Shibboleth

Shibboleth es una herramienta de código abierto que implementa un método para el inicio de sesión único o Single Sign-On (SSO) para aplicaciones Web que estén localizadas dentro la organización o pertenezcan a otras instituciones. Así mismo, Shibboleth se basa en el estándar de gestión de identidad federada denominada Security Assertion Markup Language (SAML).

Según el trabajo realizado por (Díaz Barriga et al., 2015) es posible identificar 3 elementos dentro de un sistema de autenticación basado en Shibboleth los cuales se describen a continuación:

- El Proveedor de Identidad (IdP): proporciona funcionalidades de inicio de sesión único en la web, autenticando de usuarios y suministro de datos a las aplicaciones, estas funcionalidades tienen un alcance más allá de la propia organización. En este sentido, IdP proporciona una respuesta simple de sí o no a una determinada solicitud de autenticación. También, IdP proporciona un conjunto completo de datos relacionados al usuario y los servicios requeridos y estos datos pueden ayudar al servicio a proporcionar una experiencia de usuario más personalizada y evitar que el usuario tenga que ingresar manualmente sus datos para acceder a los servicios.
- El Proveedor de Servicio (SP): Permite a las aplicaciones web, desarrolladas en distintas plataformas de Hardware y Software, integrar de forma nativa con servidores web de aplicaciones como por ejemplo Apache o IIS (Internet Information Service). Además, dicha estrategia de integración es débilmente acoplada con el fin de soportar las especificaciones del estándar SAML.
- El Servicio de Descubrimiento (DS): Proporciona una interfaz web que permite al usuario seleccionar qué proveedor de identidad utilizará para acceder a un proveedor de servicios. Así mismo, este producto se instala conjuntamente con un proveedor de servicios y permite que el servicio de descubrimiento lleve la misma interfaz de usuario y su correspondiente marca.

En la Figura 4, se ilustra la interacción de los componentes de Shibboleth. Por lo tanto, el proceso inicia cuando un usuario haciendo uso de un navegador web, solicita acceder a un contenido protegido, luego el Proveedor de Servicios redirige al usuario hacia el Servicio de Descubrimiento donde el usuario tendrá que elegir el nombre de la organización a la que pertenece. Así mismo, el navegador redirige al usuario al Proveedor de Identidad de su organización para que se autentique. Finalmente, una vez que la autenticación sea exitosa el Proveedor de identidad de la organización entregará al Proveedor de Servicio la mínima información necesaria sobre la identidad del usuario que permita al sistema la tomar decisiones sobre el los permisos a ser autorizados (Penna et al., 2016).

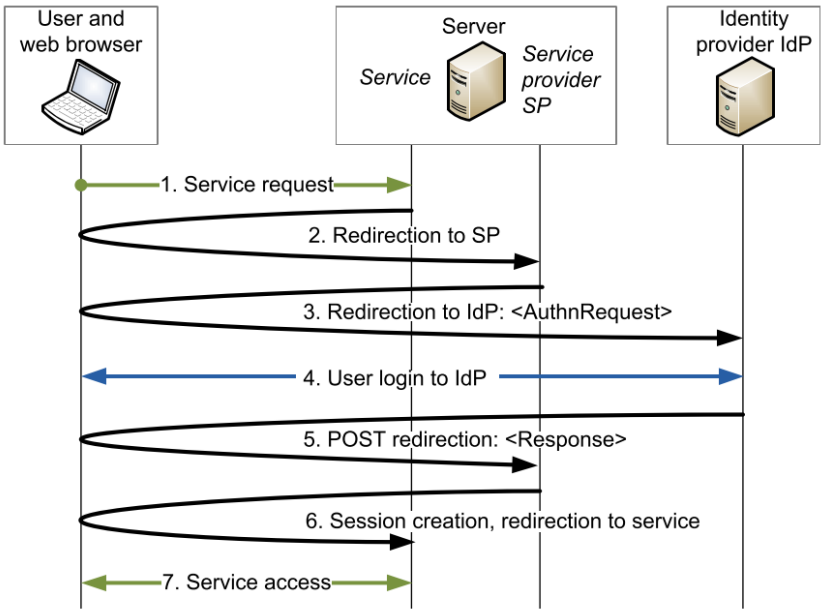

Figura 4. Interacción de componentes de Shibboleth

Tomado de (Díaz Barriga et al., 2015).

Grouper

Según (Internet2, 2019) Grouper es un sistema de gestión de acceso empresarial diseñado para un entorno de gestión altamente distribuido, heterogéneo y con esquema de información común a las universidades. Así mismo, Grouper puede crear grupos, roles y permisos para muchos fines. En primer lugar, Grouper puede ayudar a la coordinación y colaboración de grupos de trabajo utilizando listas de correo, wikis, calendarios con sus respectivos permisos para los usuarios. En segundo lugar, Grouper establece un solo punto de control donde los administradores pueden añadir, remover, modificar y otorgar permisos a los grupos de usuarios. En tercer lugar, Grouper puede proporcionar niveles de derechos o permisos para administrar grupos, por ejemplo, un investigador podría requerir gestionar su propio grupo añadiendo y eliminado a sus miembros de su equipo de investigación. Finalmente, los estudiantes pueden usar Grouper para configurar y administrar grupos para aplicaciones similares a medida que trabajan juntos en proyectos compartidos y trabajo en clase. Además, su personal de TI puede delegar la administración de grupos y habilitar a las principales colaboraciones para configurar y administrar sus propios grupos. En la Figura 5, se ilustra una visión general de Grouper.

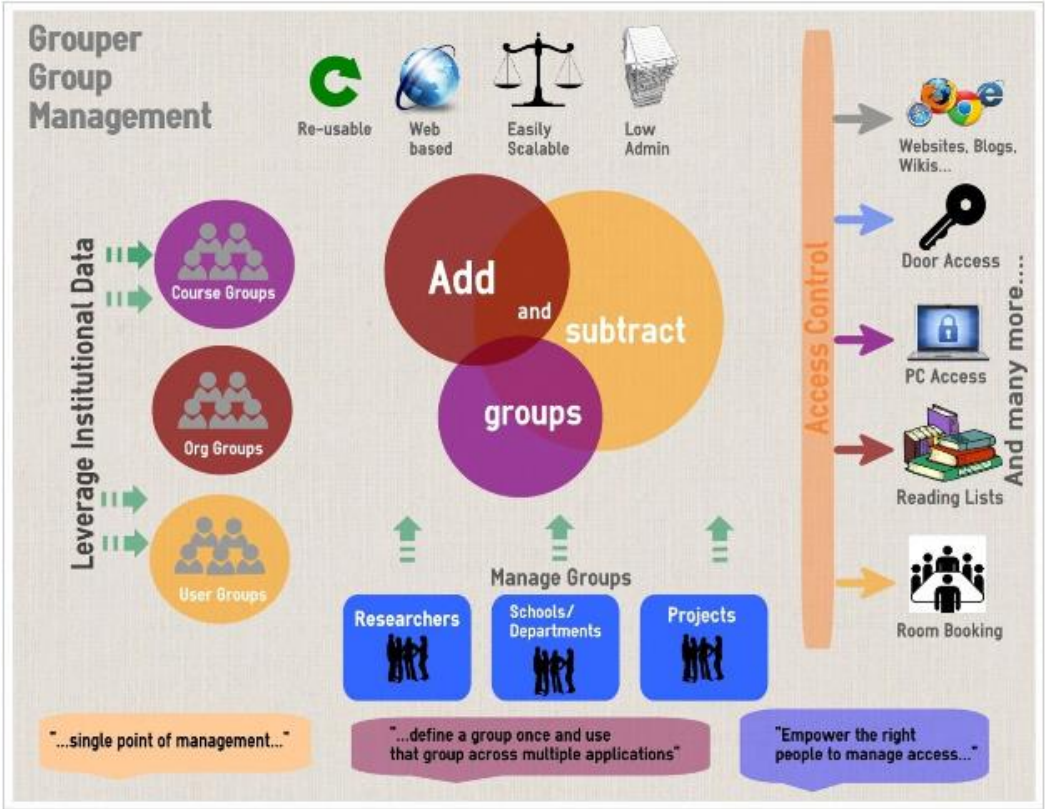

Figura 5. Sistema de Gestión de Grupos Grouper.

Tomado de (Internet2, 2019).

COmanage

COmanage es un conjunto de herramientas que proporciona facilidades a la gestión de identidades. Así mismo, los desarrolladores pueden seleccionar y personalizar una instancia de COmanage según sus necesidades de su organización. En la Figura 6, se muestra el propósito principal de COmanage es disponer de un registro o almacén de datos. Luego, en este almacén se guarda la información en una base de datos que disponga de una estructura de datos que soporte un servicio de directorios LDAP (Protocolo Ligero de Acceso a Directorios). Finalmente, las

aplicaciones pueden utilizar la información almacenada para tomar decisiones de control de acceso a sus recursos digitales.

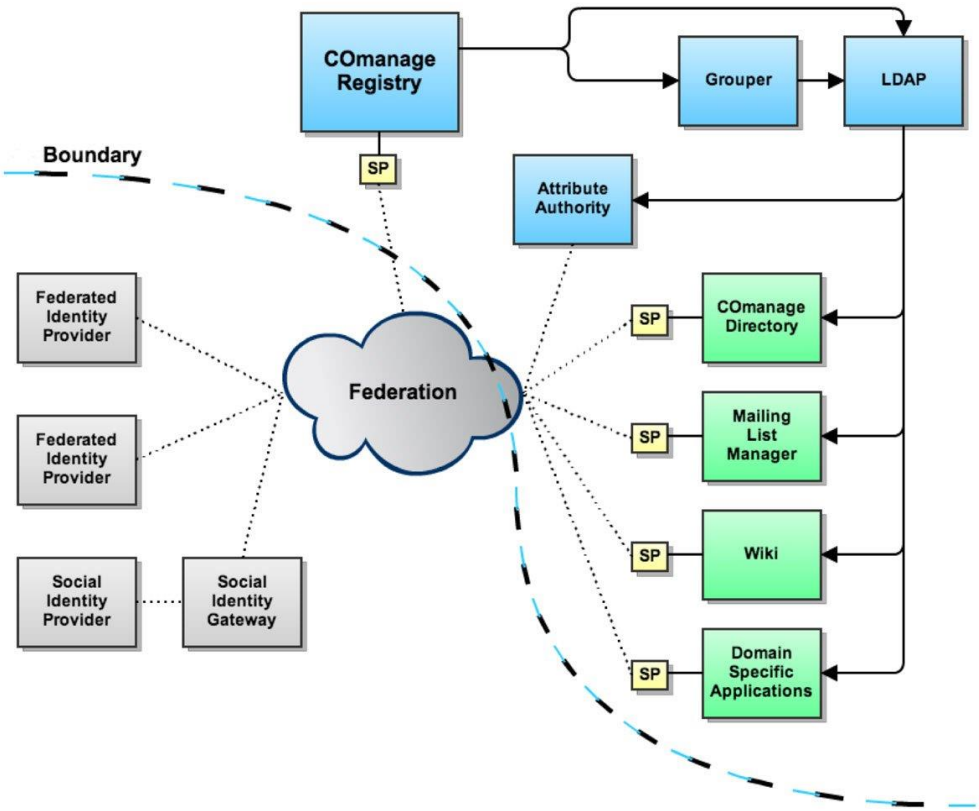

Figura 6. Funcionamiento de COmanage.

Tomado de (Internet2, 2019).

2.2.2. Sustento teórico e las variables: Gestión del acceso a sistemas informáticos

2.2.2.1. Definición de acceso a sistemas informáticos

El acceso a sistemas informáticos contempla actividades de Gestión de Identidad, procesos de autenticación y autorización. En principio, La gestión de identidad según (Penna et al., 2016) realiza actividades de alcance (delimitar el alcance de la identidad), autenticidad (mecanismos para evitar el robo de identidad), anonimato y seudónimo (evitar el rastreo de la identidad de usuarios).

2.2.2.2. Gestión de Identidad

Según la norma ISO 24760, "Information technology – Security techniques – A framework for identity management", define a la gestión de identidades como los procesos y políticas involucradas en el administración del ciclo de vida de la identidad digital. En este sentido, el ciclo de vida de identidad (Identity Lifecycle) se considera desde el registro inicial hasta el borrado de los datos de identidad. Además, en este ciclo de vida intervienen aplicaciones y herramientas para el mantenimiento y uso adecuado de la información que es necesario considerarlo. Por otro lado, en el ciclo de vida de la identidad es relevante cuidar la integridad, confidencialidad y disponibilidad de los datos. Entonces, para cumplir esta finalidad es necesario considerar las normas de protección de datos personales. También, es necesario tomar en cuenta el robo de la información de la identidad, y no solo ello sino también que

medidas se puedan aplicar para mitigarlo. En la Figura 7, se describe el ciclo de vida de la identidad digital.

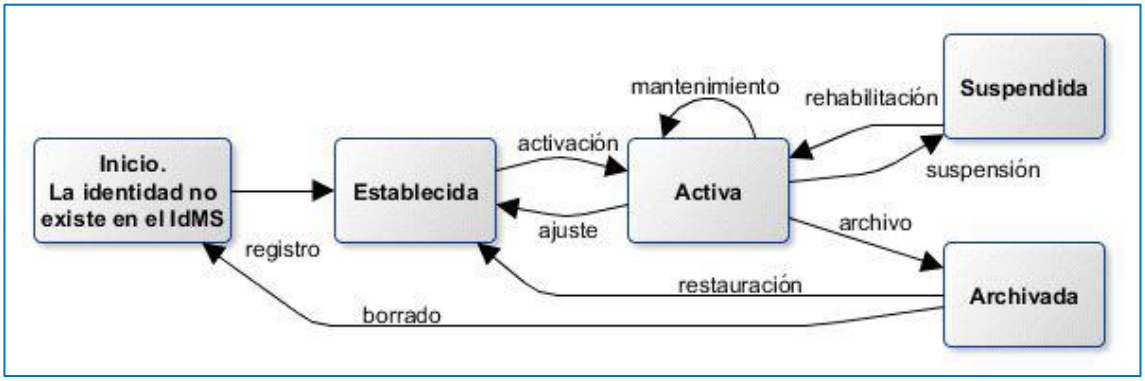

Figura 7. Modelo del ciclo de vida de las identidades.

Tomado de la (Norma ISO 24760-1).

Según el boletín de identidad digital de (Telefónica, 2013) Internet se ha convertido en un elemento esencial en la vida de las personas. Por otro lado, para (El Maliki & Seigneur, 2007) la facilidad de uso en la gestión de identidades puede generar riesgos en la seguridad. Por ejemplo, las contraseñas débiles que utilizan los usuarios en muchos sitios web provoca que el descubrimiento de vulnerabilidades sea exitoso. Por otro lado, para facilitar la interacción con entidades desconocidas, se propone un reconocimiento simple en lugar de la autenticación de una identidad en forma manual. Entonces, la facilidad de uso es mejor cuando no se realiza una tarea manual. En conclusión, en algunos casos puede haber un nivel de seguridad más débil, pero ese nivel puede ser suficiente para algunas acciones, como iniciar sesión en una plataforma de juegos para dispositivos móviles.

También, es importante tomar en consideración reglas en el nuevo paradigma de identidad centrado en el usuario, como son:

- Potenciar el control total de los usuarios sobre su privacidad
- Usabilidad, ya que los usuarios usan la misma identidad para cada transacción de identidad
- Dar una experiencia de usuario consistente gracias a la uniformidad de la interfaz de identidad
- Limitar los ataques de identidad, es decir, el phishing
- Limitar la accesibilidad / perturbaciones (reducción de spam)
- Revisar las políticas en ambos lados cuando sea necesario, proveedores de identidad y proveedores de servicios (sitios web)
- Grandes ventajas de escalabilidad ya que el Proveedor de Identidad no tiene que obtener ningún conocimiento previo sobre el Proveedor de Servicios
- Asegurar condiciones seguras al intercambiar datos
- Desacoplar la identidad digital de las aplicaciones
- Pluralismo de operadores y tecnologías.

2.2.2.3. Autenticación

Según la (Presidencia República Perú, 2018) La autenticación digital es el procedimiento de verificación de la identidad digital de una persona, mediante el cual se puede afirmar que es quien dice ser. Además, para el acceso a un servicio digital las instituciones de la Administración Pública deben adoptar los métodos de autenticación digital, tomando en

cuenta los niveles de seguridad a establecerse según la norma establecida. En la Figura 8, se ilustra el proceso de autenticación de usuarios.

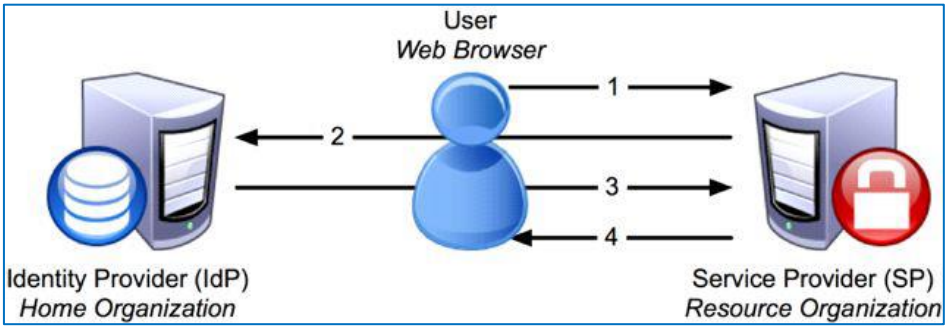

Figura 8. Proceso de autenticación de usuario.

Tomado del Programa TIER de Internet2

Por otro lado, Según (Conklin & Shoemaker, 2019) la autenticación es el proceso para determinar la identidad de un usuario. Por lo tanto, todos los procesos en un sistema de computo tienen una identidad asignada para que de esa manera se pueda emplear una funcionalidad de seguridad diferente. Además, la autenticación es un elemento fundamental de la seguridad, puesto que, proporciona mecanismos para determinar si un usuario esta o no autorizado para utilizar un sistema de cómputo. Finalmente, en sistemas donde muchos usuarios comparten una sola cuenta, ellos también comparten la autenticación y la identidad asociada a dicha cuenta.

Existen tres métodos generales usados en la autenticación los cuales son: Algo que tú sabes, algo que tienes y algo que tú eres. Por lo tanto, el mecanismo de autenticación más común es proporcionar algo que solo el usuario valido conoce. Así mismo, el ejemplo, más común de algo

que solo uno conoce es el nombre de usuario y una contraseña. Sin embargo, está técnica no es muy confiable puesto que el usuario comparte o elige contraseñas sencillas que pueden ser fáciles de adivinar. En consecuencia, es necesario utilizar otros mecanismos de autenticación más seguras. Por ejemplo, utilizar una ficha (token), una biometría estática o dinámica la localización física.

El mecanismo de autenticación por ficha o token implica el uso de algo que solo los usuarios válidos deberían tener en su poder. En los sistemas de cómputo el token o fichas son elementos encriptados que identifican a un usuario, pero el problema de los tokens es que sus propietarios pueden extraviarlo y así generar que un usuario no autorizado, utilizando el token ajeno, ingrese al sistema. Entonces, para solucionar el problema de la perdida del token es combinar el token con una contraseña o PIN, un ejemplo de este sistema combinado es las tarjetas utilizadas en los ATM o cajeros automáticos.

Otro mecanismo de autenticación es la biometría que considera algo que es único del usuario por ejemplo su voz, retina, estructura de su huella dactilar, pero la desventaja de estos mecanismos es el uso de un Hardware adicional y la falta de especificidad que se pueden lograr con otros métodos.

2.2.2.4. Autorización

Según (Conklin & Shoemaker, 2019) la autorización es el mecanismo para determinar que a la persona identificada se le ha otorgado

la autoridad para realizar las acciones solicitadas. Además, los sistemas de control de acceso se ponen en marcha para garantizar que sólo las personas autorizadas tengan acceso a la información, y que para que la información se mantenga intacta y disponible cuando sea necesario. Entonces, el propósito de los sistemas de control de acceso es evitar la modificación de la información por los usuarios no autorizados, permitir la modificación de la información por los usuarios autorizados, y preservar la consistencia interna y externa de los datos.

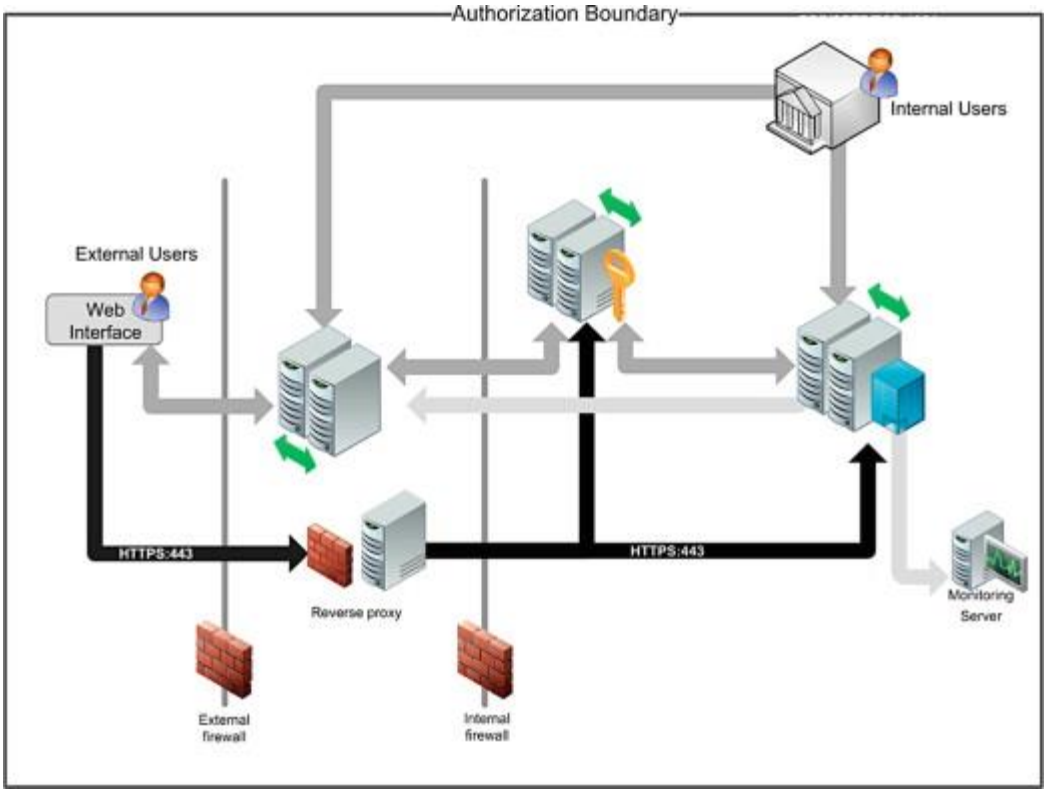

Figura 9. Proceso de autorización. Tomado de FISMA Center.

Para lograr esto, se aplican los controles. Los controles ayudan a mitigar el riesgo y reducir la posibilidad de pérdida, y requiere de las combinaciones de controles para una defensa en profundidad. En ese

sentido, una forma de clasificar a los controles de acceso es mediante la descripción en la forma en que se implementan.

Después que el sistema de autenticación identifica a un usuario, el sistema de autorización toma el control y aplica los niveles de acceso predeterminado al usuario. La autorización es el proceso de aplicar reglas de control de acceso a un proceso de usuario y también determinar si un proceso especifico de usuario puede acceder a un objeto. Tres elementos son utilizados en la autorización: un solicitante (algunas veces referenciado como el sujeto), el objeto y el tipo o nivel de acceso a ser otorgado. El sistema de autorización debe identificar si un sujeto pertenece a un conjunto de sujetos asociados al sistema. Cuando un sujeto solicita acceso a un objeto, puede por ejemplo un archivo, un programa, un registro de datos, o cualquier otro recurso, el sistema de autorización crea el permiso ya sea para otorgar o denegar el acceso. El tercer elemento es el tipo de acceso solicitado que son comunes a acciones de leer, escribir, modificar, eliminar, o el derecho de otorgar permisos a otros sujetos para que tengan acceso a los recursos.

III. MÉTODO

3.1. Tipo de investigación

En primer lugar, el presente estudio es de tipo aplicativo, puesto que, diseñamos un modelo de identidad digital basado en el programa TIER de Internet2 para mejorar la gestión centralizada del acceso a los servicios informáticos de la universidad pública de la región Cusco.

En segundo lugar, para evaluar la aceptación del modelo por los usuarios de la universidad el presente estudio utiliza un enfoque cuantitativo del tipo correlacional y cuasi-experiemental con diseño pre-test y post-test con un solo grupo. Así mismo, las variables planteadas en el estudio correlacional están basados en el Modelo de Adopción de Métodos MAM descrito en la sección 2.1.1.2. del marco teórico.

3.2. Población y muestra

Población

La población objeto de investigación está conformada por 42 directores de las escuelas profesionales la Universidad Nacional de San Antonio Abad del Cusco. En este sentido, la justificación de elegir a los directores de las escuelas profesionales es porque utilizan la mayoría de los sistemas informáticos de la universidad por su cargo administrativo, docente e investigador.

Muestra

La técnica de muestreo que se utilizará en el estudio correlacional será el muestreo probabilístico aleatorio sin remplazo.

Así, para determinar el tamaño apropiado de la muestra aleatoria se ha considerado aplicar las técnicas probabilísticas teniendo en cuenta la siguiente fórmula:

$$n = \frac{(Z)^2 \ (P)(Q)(N)}{(E)^2 (N) + (Z)^2 (P)(Q)}$$

Dónde:

Z = Desviación Standard, medida en términos de niveles de confianza

E = Error de Muestreo

P = Probabilidad de ocurrencia de los casos (se asume p = 0.5)

Q = (1-P)

N = Tamaño de la población

n = Tamaño óptimo de la muestra

El procedimiento para determinar el tamaño de la muestra y su estratificación se muestra a continuación:

Factores del tamaño de la muestra

N = 42

P = 0.50

Q = 0.50

Z = 1.96

e = 0.05

A continuación, se muestra la determinación del tamaño óptimo de la muestra.

$$n = \frac{(1.96)^2 \ (0.50)\ (0.50)\ (42)}{(0.05)2\ (42) + (1.96)2\ (0.50)\ (0.50)} = \mathbf{37.86}$$

La muestra óptima resultó de acuerdo con los ajustes estadísticos con un total de 38 directores de las escuelas profesionales de la Universidad Nacional de San Antonio Abad del Cusco.

3.3. Operacionalización de variables

Definición de variables:

Modelo de identidad digital basado en el Programa TIER de Internet2:

Modelo con capacidades de gestión de repositorio de datos, autenticación de usuarios y autorización de permisos a usuarios basado en el programa TIER de Internet2, dicho modelo es una suite de aplicaciones y buenas prácticas para la gestión de identidades digitales en las universidades.

Gestión del acceso a los servicios informáticos:

Actividades que corresponden a los procesos de autenticación y autorización a diversos sistemas informáticos desarrollados en diferentes plataformas de

Hardware y Software. Así mismo, se evalúan su facilidad de uso, utilidad e intención de uso.

Tabla 1 *Definición y operación de las variables*

Variables	Indicadores
Modelo de identidad digital basado en el Programa TIER de Internet2	- Capacidad de inicio de sesión unificado - Capacidad de soporte del protocolo SSO y SAML - Capacidad de disponer funciones de proveedor de identidad - Capacidad de disponer funciones de proveedor de servicios - Capacidad de disponer de funciones de un servicio de descubrimiento - Capacidad para mantener automáticamente grupos - Capacidad para almacenar datos de grupos.
Gestión de acceso a los servicios informáticos	- Proporción de tiempo requerido para el acceso a los sistemas informáticos - Disponibilidad de seguridad y confiabilidad de los datos al acceder a los sistemas informáticos - Proporción de la cantidad de cuentas de usuario para acceder a los sistemas informáticos - Disponibilidad del servicio de recuperación de contraseñas - Existencia de un procedimiento para reportar el seguimiento y control de acceso

Nota: Fuente elaboración propia.

3.4. Instrumentos

En la presente investigación se empleó un cuestionario como instrumento de medición de las variables de investigación. Así mismo, el cuestionario es adaptado de (Abrahao, 2004) que se basa en el trabajo de (Moody, 2003) denominado Method Evaluation Model. Por otro lado, este cuestionario dispone de 14 preguntas de tipo cerradas con escala de Likert de 5 puntos. Además, cada pregunta fue formulada en formato de positivo a negativo y viceversa. Finalmente, las preguntas del cuestionario fueron localizadas aleatoriamente para evitar respuestas monótonas en los entrevistados. En el Anexo 2, se presenta el cuestionario para el presente estudio.

En la Tabla 2, se muestra la distribución de las preguntas según a las variables de estudio que corresponden a las percepciones de uso del modelo de identidad digital TIER de Internet2.

Tabla 2 *Definición y operación de las variables*

Percepción de eficiencia al usar el modelo de identidad digital	Pregunta 1, 3,4, 6 y 9
Percepción de eficiencia al usar el modelo de identidad digital	Pregunta 2, 5, 8, 10, 11 y13
Percepción de eficiencia al usar el modelo de identidad digital	Pregunta 7, 12, y 14

Nota: Fuente elaboración propia.

Confiabilidad del Instrumento

Para cuantificar el nivel de confiabilidad del instrumento se utiliza el coeficiente de Alfa de Cronbah. Tomando en consideración que el coeficiente

de Alfa de Cronbah varia entre 0 y 1. Además, los valores próximos a 1 indican gran fiabilidad. Sin embargo, para nuestro contexto de estudio será necesario alcanzar valores superiores a 0.7 de la escala de Alfa de Cronbah.

El procedimiento para el diseño del instrumento confiables consiste en cuatro pasos. En primer lugar, Escribir las preguntas para la primera versión del instrumento. En segundo lugar, aplicar la primera versión del instrumento realizando una prueba piloto a 10 sujetos. En tercer lugar, evaluar los resultados obtener las escalas de medición de Alfa de Cronbah y elegir las preguntas que son consistentes internamente. Finalmente, identificar las preguntas que no añaden valor y eliminarlas.

El alfa de Cronbach para el instrumento fue de 0.835.

Tabla 3 *Estadísticos de fiabilidad*

Alfa de Cronbach	N de elementos
,835	14

Nota: Fuente elaboración propia.

Validez del Instrumento

Un instrumento es válido cuando realmente es capaz de medir aquello para lo que ha sido concebido. Considerando, que el tamaño de la muestra es pequeño no podemos utilizar análisis factorial que por lo menos necesita un tamaño de muestra de 200 sujetos. Entonces, utilizamos la técnica de validación de análisis de correlación inter-item según (Campbell & Fiske,

1959). Además, según (Cohn Muroy, s. f.) el análisis de correlación inter-item analiza dos factores: Validez Convergente (CV) y Validez Divergente (DV) y dentro del cuestionario una pregunta se considera como válida si el valor de CV es mayor que su DV. En el Anexo 6, se presentan los datos utilizados para validar el instrumento.

Tabla 4 *Matriz de correlaciones inter-elementos*

	Facilidad de uso percibida					**Utilidad percibida**						**Intención de uso**			**General**		
	P1	**P3**	**P4**	**P6**	**P9**	**P2**	**P5**	**P8**	**P10**	**P11**	**P13**	**P7**	**P12**	**P14**	**VC**	**VD**	**Validez**
P1	1,0	0,2	0,7	0,3	0,2	-0,3	0,0	-0,2	0,3	0,0	-0,2	0,4	0,2	0,2	0,5	0,0	SI
P3	0,2	1,0	0,2	0,6	-0,1	0,3	0,3	0,0	-0,1	-0,3	0,1	-0,3	0,1	-0,1	0,4	0,0	SI
P4	0,7	0,2	1,0	0,2	0,6	0,3	0,2	0,2	0,4	-0,3	-0,1	0,3	0,2	0,7	0,6	0,2	SI
P6	0,3	0,6	0,2	1,0	0,0	0,3	0,2	0,0	0,2	0,0	0,3	-0,2	0,1	0,0	0,4	0,1	SI
P9	0,2	-0,1	0,6	0,0	1,0	0,1	0,0	0,3	0,2	-0,3	0,0	0,1	0,0	0,7	0,4	0,1	SI
P2	-0,3	0,3	0,3	0,3	0,1	1,0	0,7	0,5	0,4	0,1	0,6	0,0	0,3	0,4	0,6	0,2	SI
P5	0,0	0,3	0,2	0,2	0,0	0,7	1,0	0,8	0,7	0,4	0,9	0,5	0,9	0,5	0,7	0,3	SI
P8	-0,2	0,0	0,2	0,0	0,3	0,5	0,8	1,0	0,6	0,3	0,8	0,5	0,8	0,5	0,7	0,3	SI
P10	0,3	-0,1	0,4	0,2	0,2	0,4	0,7	0,6	1,0	0,7	0,6	0,9	0,6	0,4	0,7	0,4	SI
P11	0,0	-0,3	-0,3	0,0	-0,3	0,1	0,4	0,3	0,7	1,0	0,5	0,7	0,3	-0,2	0,5	0,0	SI
P13	-0,2	0,1	-0,1	0,3	0,0	0,6	0,9	0,8	0,6	0,5	1,0	0,4	0,8	0,3	0,7	0,2	SI
P7	0,4	-0,3	0,3	-0,2	0,1	0,0	0,5	0,5	0,9	0,7	0,4	1,0	0,6	0,3	0,6	0,3	SI
P12	0,2	0,1	0,2	0,1	0,0	0,3	0,9	0,8	0,6	0,3	0,8	0,6	1,0	0,5	0,7	0,4	SI
P14	0,2	-0,1	0,7	0,0	0,7	0,4	0,5	0,5	0,4	-0,2	0,3	0,3	0,5	1,0	0,6	0,3	SI

Nota: Fuente elaboración propia.

Según la Tabla 4, todas las preguntas que corresponden a los constructos percepción de uso del repositorio de datos, percepción de utilidad en la autenticación de usuarios y la intensión de uso de la autorización de permisos son válidas puesto que el valor de la validez de convergencia (VC) es mayor al valor de la validez de divergencia (VD).

3.5. Procedimientos

Para la aplicación del cuestionario previamente se desarrolló una capacitación de 20 horas lectivas a los directores de las escuelas profesionales.

Así mismo, el propósito de la capacitación fue para que los usuarios conozcan el uso del modelo de identidad digital basado en el programa TIER de Internet2. En este sentido, el contenido de la capacitación esta divido en dos módulos: El primero relacionado a la gestión de identificación, autenticación y autorización de usuarios, y el segundo relacionado a el acceso a los recursos digitales de educación e investigación.

Luego de la capacitación se aplicó el cuestionario tomando en cuenta el consentimiento informado a cada uno de los entrevistados y poniendo énfasis de que su participación es totalmente voluntaria. Así mismo, completada la aplicación del cuestionario se procedió a la codificación y tabulación de los datos. Seguidamente, con los datos tabulados y ordenados se procedió a su correspondiente análisis que consistió en verificar la normalidad de los datos y su correspondiente estadística descriptiva.

Finalmente, para completar el estudio se procedió con la prueba de hipótesis ejecutando los siguientes pasos:

1) Especificar las hipótesis alternas y nulas.
2) Utilizar el estadístico t-Student con nivel de significancia $p < 0.05$ para aceptar o rechazar la hipótesis nula.
3) Utilizar la regresión lineal múltiple para verificar si la intención de uso es motivada por la percepción de facilidad de uso y percepción de utilidad.
4) Realizar la prueba de hipótesis para cada hipótesis específica y luego recomponer las mismas para probar la hipótesis general.

3.6. Análisis de datos

Para el análisis de los resultados en principio se realizó la prueba de normalidad utilizando el estadístico de Shapiro-Wilk (Shapiro & Wilk, 1965) puesto que la muestra del estudio es pequeña. Además, la prueba de normalidad es necesaria para utilizar pruebas paramétricas de comparación de medias t-Student en la contrastación de las hipótesis. Finalmente, para determinar la correlación de las diferentes variables analizadas se utiliza el coeficiente de Pearson.

Para contrastar la hipótesis del estudio es necesario en principio contrastar las hipótesis específicas y luego componer las mismas para finalmente contrastar la hipótesis general. En este sentido, las hipótesis especificas se verifican en base a los puntajes de los constructos y si dichos puntajes son perceptiblemente mejores al puntaje medio de la escala de Likert 3. Es decir, que sus hipótesis nulas H_o y alternas H_a fueron definidas formalmente de la siguiente manera:

$$H_0: \mu \leq 3, \quad \propto = 0.05$$

$$H_a: \mu > 3$$

Donde α vale 0,05 que corresponde a la probabilidad de aceptar la hipótesis alternativa. El análisis de los datos fue llevado a cabo con la herramienta estadística SPSS.

IV. RESULTADOS

4.1. Sistema actual de la identidad digital en la Universidad Pública de la Región Cusco

En esta sección se considera a la Universidad Nacional de San Antonio Abad del Cusco en lo sucesivo UNSAAC, como objeto de estudio para describir el estado actual de la identificación digital para el acceso a los sistemas informáticos. En este sentido, La UNSAAC considerada la segunda más antigua del Perú está conformada por docentes, personal administrativo, estudiantes regulares y egresados. Así mismo, brinda formación en pregrado y posgrado distribuida en 10 facultades que las listamos a continuación:

1. Facultad de Arquitectura e Ingeniería Civil
2. Facultad de Ciencias
3. Facultad de Cs Administrativas, Contables, Económicas y Turismo
4. Facultad de Ciencias Agrarias
5. Facultad de Ciencias de la Salud
6. Facultad de Derecho y Ciencias Sociales
7. Facultad de Educación y Ciencias de la Comunicación
8. Facultad de Ing. Eléctrica, Electrónica, Informática y Mecánica
9. Facultad de Ing. de Procesos
10. Facultad de Ingeniería Geológica, Minas y Metalúrgica

Por otro lado, con la finalidad de entender la complejidad del proceso de identidad digital en la UNSAAC debemos puntualizar que los docentes, alumnos y administrativos son considerados como usuarios de los servicios de

la universidad. Además, la cantidad aproximada es de 20000 usuarios distribuidos en la sede central y filiales. También, en la UNSAAC los servicios informáticos progresivamente se han incrementado. En la Tabla 5, se describe la relación de las aplicaciones más importantes, además, quienes lo usan y cuál es su entorno y ubicación:

Tabla 5 *Resumen de Aplicaciones en la UNSAAC*

N°	**Servicio informático**	**Usuarios**	**Entorno**
1	Académico	Estudiantes, directores de departamentos académicos, Directores de Escuelas Profesionales, Profesores	Plataforma Framework .Net, SQL Server y PHP instalado en la propia organización
2	Acceso a la Red Inalámbrica	Todos los miembros de la comunidad	Active Directory – Servidor Implementado en la organización
3	Correo Electrónico Institucional	Todos los miembros de la comunidad	Plataforma Google - G Suite for Education
4	Biblioteca virtual	Todos los miembros de la comunidad	E-Libro – Servicio en la Nube
5	Sistema de anti plagio	Solo usuarios autorizados	URKUND – Servicio en la Nube

6	Repositorio Digital	Todos los usuarios de la universidad y público en general	Servidor Tomcat instalado en la organización

Para acceder a los servicios informáticos, se utiliza principalmente la Página Web principal de la UNSAAC, es importante precisar que para acceder a cada servicio es necesario disponer de un nombre de usuario y contraseña diferente para cada sistema informático. A continuación, ilustramos en las Figuras del 10 al 15 las ventanas de inicio de sesión para acceder a los principales servicios informáticos de la UNSAAC.

Figura 10. Portal Web de la UNSAAC y enlace a los sistemas informáticos más importantes.

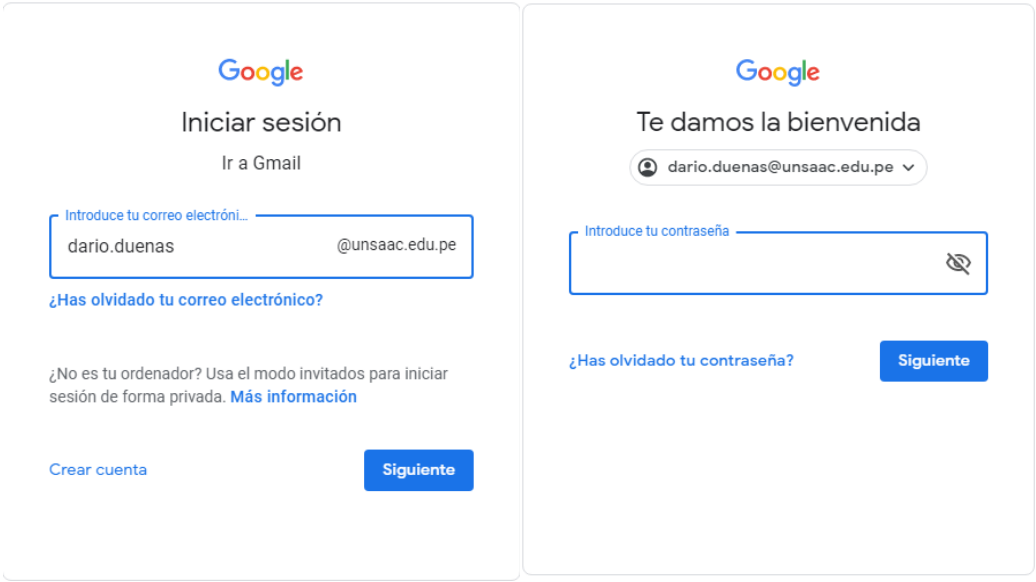

Figura 11. Ventana de Inicio de sesión para acceder al Sistema de Correo Electrónico Institucional de la UNSAAC.

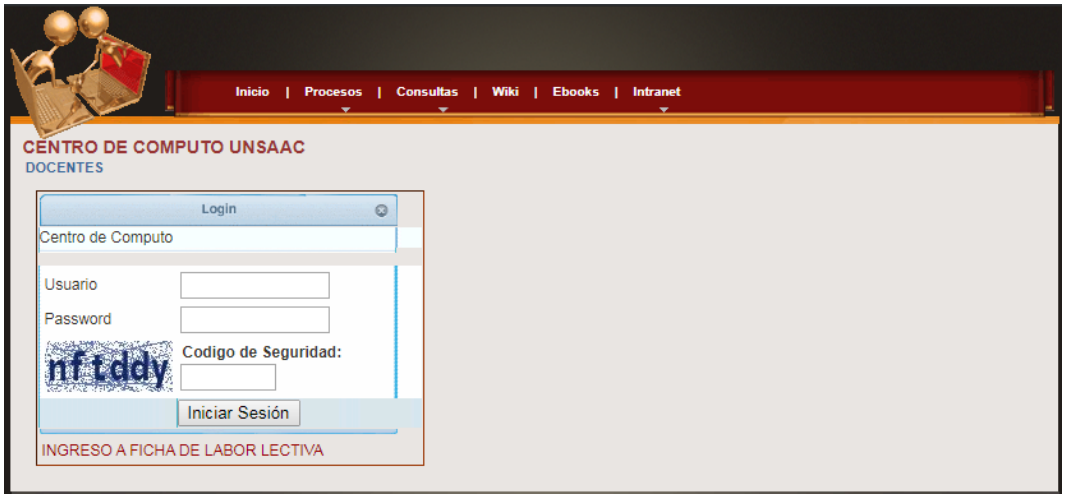

Figura 12. Ventana de Inicio de sesión para acceder al Sistema de Académico del Centro de Computo de la UNSAAC.

Figura 13. Ventana de Inicio de sesión para acceder a la Biblioteca Virtual de la UNSAAC.

Figura 14. Ventana de Inicio de sesión para acceder al Sistema de Anti-plagio de la UNSAAC.

Figura 15. Ventana de Inicio de sesión para acceder al Repositorio Digital de la UNSAAC.

De las ilustraciones anteriores se observa que los servicios informáticos están basados en diferentes plataformas y no tienen un estándar común y por ende generan islas de información y redundancia de datos. Además, está situación provoca incomodidades a los usuarios haciendo complejo el proceso de autenticación para acceder a un determinado servicio informático. En la Figura 16, se muestra un diagrama, se presenta el proceso actual de autenticación a los servicios informáticos de la UNSAAC donde se observa claramente que para el acceso a una determinada aplicación es necesario utilizar una cuanta de usuario y contraseña diferente para cada servicio.

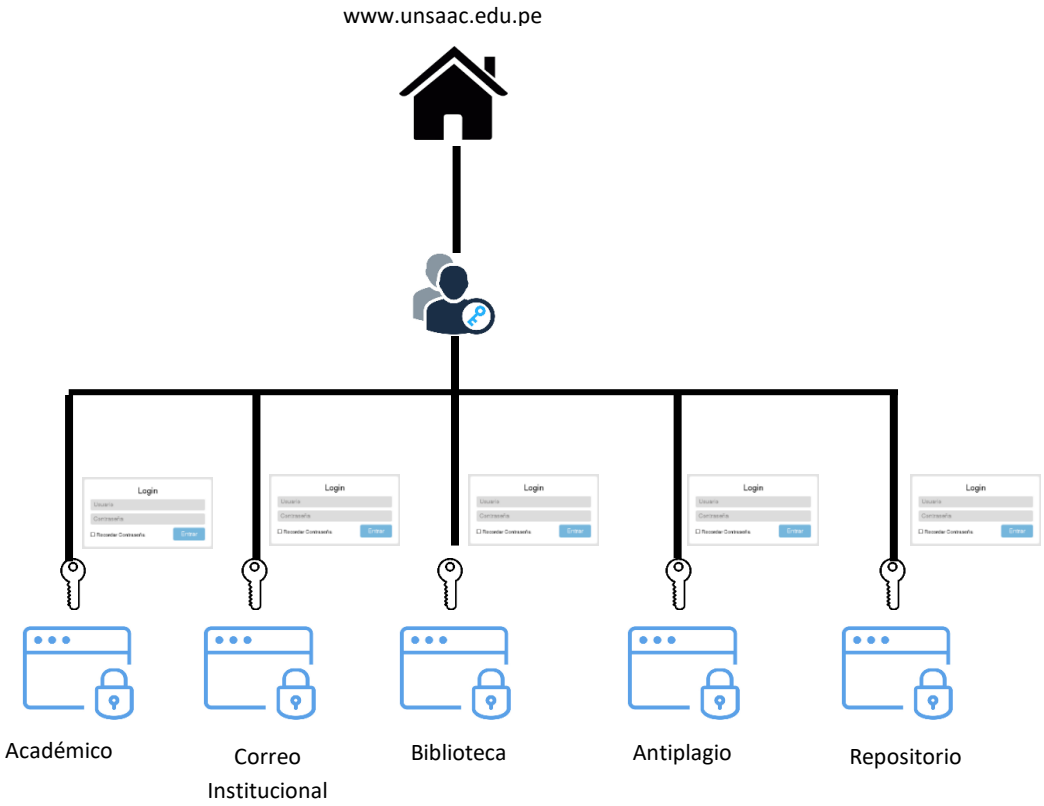

Figura 16. Esquema que describe el acceso a los principales sistemas informáticos de la UNSAAC.

4.2. Modelo de Identidad digital TIER para la Universidad Pública de la Región del Cusco

El propósito del modelo es permitir a los usuarios realizar una sola autenticación para que puedan acceder a los servicios informáticos de la universidad. En la Figura 17, se muestra el esquema de autenticación centralizada y el inicio de sesión único para acceder a los servicios informáticos de la universidad.

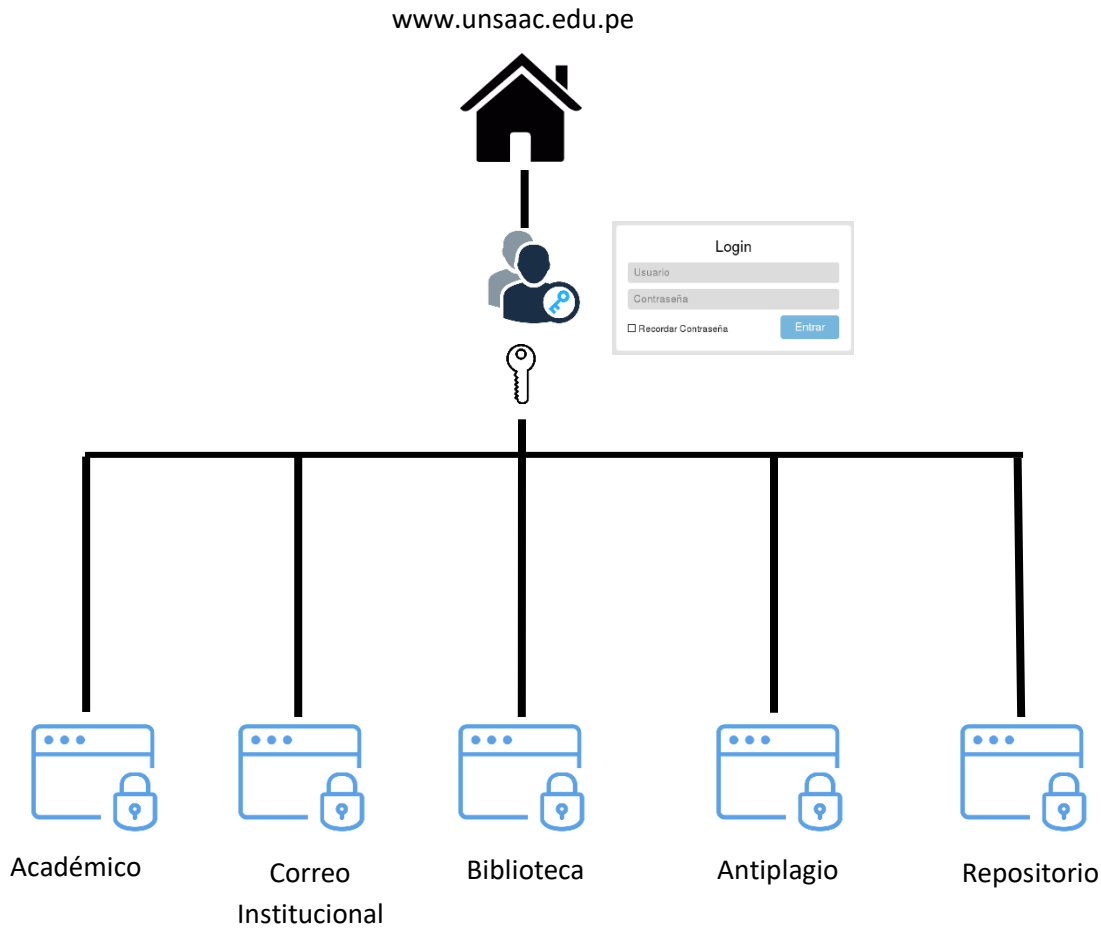

Figura 17. Esquema del nuevo modelo de identidad digital para el acceso a los principales sistemas informáticos de la UNSAAC.

4.2.1. Especificación de funciones del modelo de identidad digital TIER

Para ilustrar las funcionalidades del modelo se utiliza un diagrama de casos de uso donde describe la interacción de los usuarios con las entidades principales del modelo.

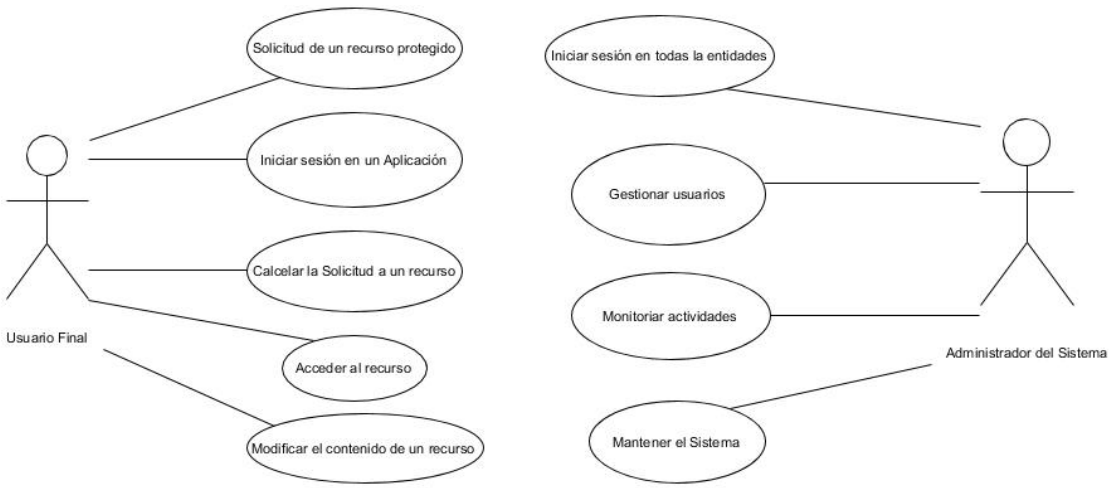

Figura 18. Funciones del nuevo modelo de identidad digital para el acceso a los principales sistemas informáticos de la UNSAAC.

En la Figura 18, describe la existencia de dos usuarios principales en primer lugar, está el usuario final que puede ser un docente, estudiante o administrativo que requiere acceder a una aplicación y solicitar un recurso digital. En segundo lugar, está el usuario administrador quien estará encargado de la administración de la arquitectura del modelo y controlara los usuarios que tienen derecho al acceso a los servicios informáticos.

4.2.2. Visión general del Modelo

Según las referencias descritas en el programa TIER de Internet2 para lograr la gestión adecuada del acceso a los sistemas informáticos, inicio de

sesión único y disponer de una autenticación centralizada es necesario plantear un modelo de gestión centralizada utilizando un agente de aplicación de usuario y Shibboleth Single Sign-On. En este sentido, el modelo puede aprovechar el mecanismo de gestión centralizada para establecer una base de datos centralizada y disponer una entrada de autenticación unificada para hacer la autenticación y gestión de identidad unificada del usuario. Por otro lado, el hecho de disponer en el modelo de un agente de aplicación de usuario los sistemas informáticos no necesitan realizar cambios en la aplicación del usuario, solo se necesitan configurar los filtros como una función proxy para realizar el inicio de sesión automático. Además, la ventaja del modelo es mantener los Sistemas Informáticos con sus propias bases de datos y también no realizar ningún cambio en el proceso de autenticación, puesto que, el mismo se realiza gracias a la incorporación de la función de autenticación unificada el cual completa el intercambio de información de autenticación de usuario de manera automática. También, los Sistemas Informáticos no necesitan tener múltiples datos de usuario en la base datos migrada de la base datos central, este hecho, permite reducir costos en procesos de migración de datos. Finalmente, facilita el despliegue de la autenticación unificada y la función de inicio de sesión único en el sistema de aplicaciones que ya se está ejecutando, lo cual es beneficioso para promover la transformación del sistema existente. Además, la coexistencia de la base de datos central distribuida y la base de datos local del sistema informático pueden garantizar funciones de seguridad, puesto que, es posible acceder a los sistemas informáticos aún si la base de datos central está bajo ataque.

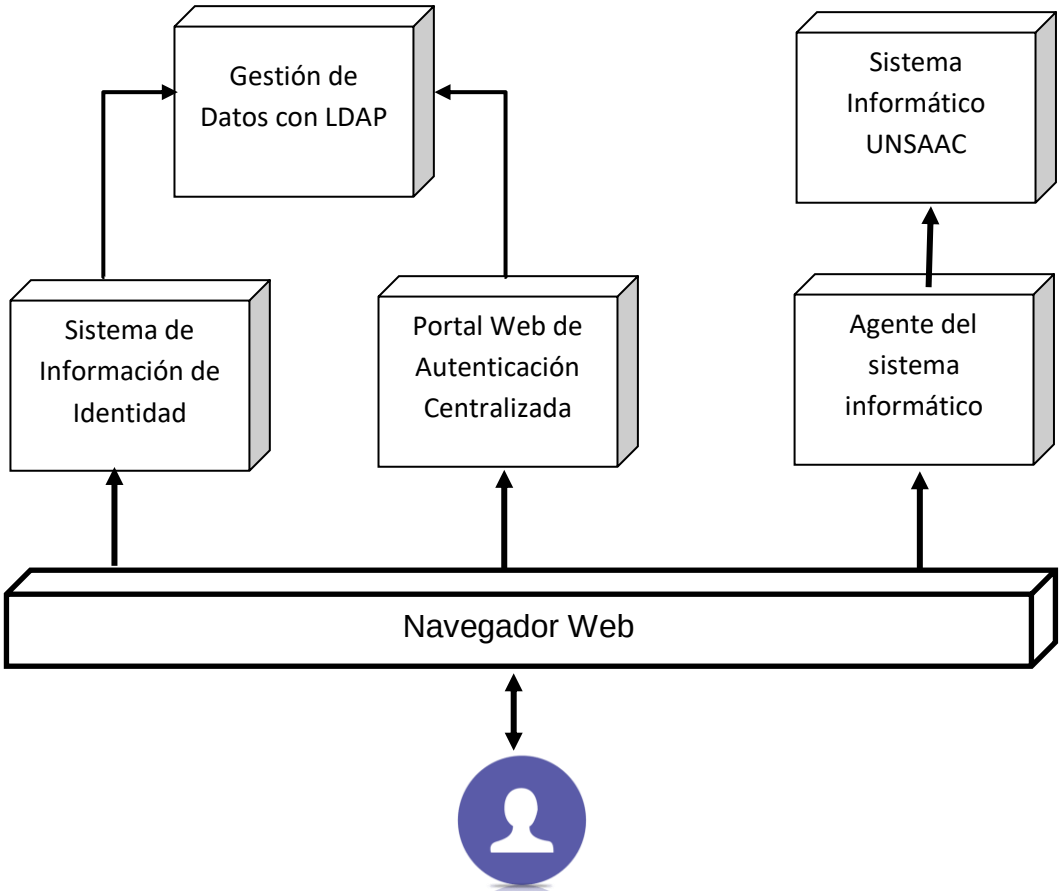

Figura 19. Modelo de identidad digital para el acceso a los principales sistemas informáticos de la UNSAAC.

El modelo está compuesto por el Portal Web de Autenticación centralizada, Sistema de Información de Identidades, Agente del Sistema Informático, Sistema de Directorio LDAP y un Navegador Web del Cliente. En la Figura 19, se muestra los componentes del Modelo según su arquitectura de Software.

4.2.3. Arquitectura de Hardware del Modelo

Con respecto, a la arquitectura de Hardware el modelo necesita dos Servidores Físicos que servirá como Proveedor de Servicio Shibboleth TIER,

Proveedor de Identidad Shibbolteh TIER, Sistema de Directorio LDAP, Portal Web Centralizado y Sistemas informáticos principales. En la Figura 20, se ilustra el diagrama de despliegue de los principales servidores del Modelo que pertenecen a la misma red y están interconectados con el protocolo TCP/IP.

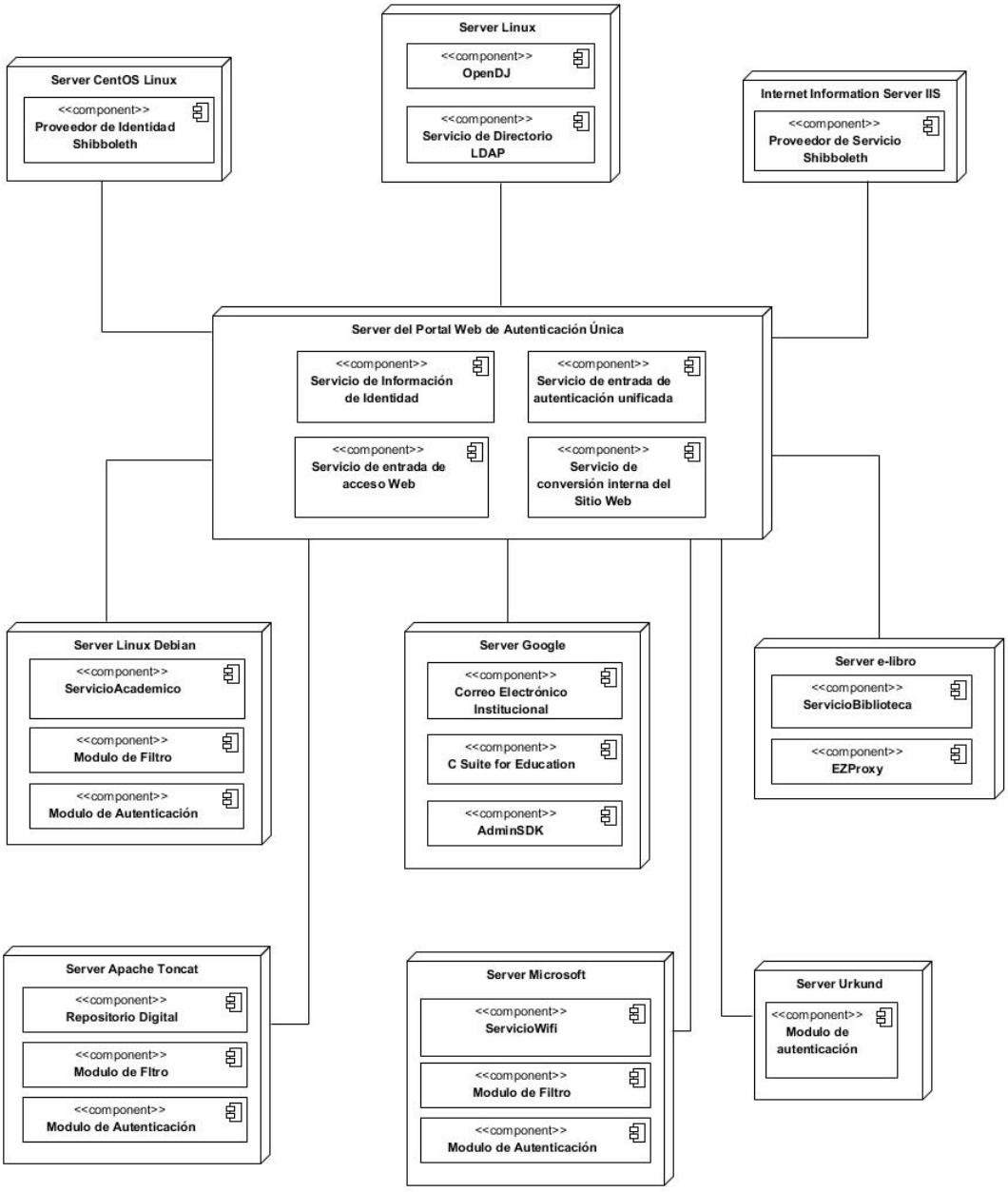

Figura 20. Arquitectura de Servidores del modelo de identidad digital para el acceso a los principales sistemas informáticos de la UNSAAC.

Por otro lado, los Sistemas Operativos necesarios para el modelo consiste de varias aplicaciones tanto de Linux, Windows y otras plataformas, cada una juega un rol importante en la ejecución del sistema. Por lo tanto, la falla de uno de los sistemas operativos o plataforma afecta a todo el sistema, en principio se requiere de sistema operativo Windows Server instalado en cada Servidor Físico. Seguidamente, en cada uno de los sistemas operativos instalados debemos desplegar e instalar diversas aplicaciones, como se describe a continuación:

En el Servidor de Proveedor de Servicio:

- Sistema Operativo Microsoft Windows Server y todas las aplicaciones necesarias para instalar el Proveedor de Servicio.
- Servidor de Aplicaciones en la Plataforma Microsoft (Puede ser Internet Information Service o IIS). En dicho servidor se desplegará la entidad de Proveedor de Servicio, Los certificados SSL y una aplicación simple para testear el inicio de sesión.
- Shibboleth Service Provider para aplicaciones Web y con protección de recursos.

En el Servidor de Proveedor de Identidad:

- Sistema Operativo Microsoft Windows Server y todas las aplicaciones necesarias para instalar el Proveedor de Identidad.
- Plataforma Java especialmente el cliente JRE.
- Servidor de Aplicaciones Apache Tomcat como contenedor de Servlets con SSL habilitado.

- Shibboleth Identity Provider para gestionar identidades y proporcionar autenticación a recursos de usuarios.
- OpenLDAP Server que es la base de datos donde se registra toda la información de usuarios y los enlaces a sitios autorizados.

4.3. Diseño del Repositorio de Datos para la gestión de acceso a los Sistemas Informáticos en la Universidad Pública de la Región del Cusco

4.3.1. Sistema de Directorio o Gestión de Datos LDAP

El modelo dispone de una base de datos LDAP que es un directorio centralizado de datos. Así mismo, dicha base de datos almacena datos del usuario y los sistemas informáticos a los que los usuarios pueden acceder. También, el sistema de información de identidad y el Portal Web de Autenticación Centralizada interactúan con la base de datos LDAP a través de la interfaz de acceso a la base de datos. Además, la finalidad de utilizar una base de datos LDAP en vez de utilizar una base de datos relacional es la ventaja de simplificar la implementación y también LDAP es usualmente utilizado para autenticación.

La base de datos del directorio LDAP almacena entradas que corresponde a objetos que contiene toda la información básica para docentes, estudiantes, personal administrativo. Por ejemplo, para cada entrada almacena su nombre de usuario, nombres de la persona, contraseña, dependencia, correo electrónico, número de teléfono, y entre otros. Así mismo, las entradas están organizadas en forma jerárquica y cada entrada tiene sus propios atributos. En la Figura 21, se muestra el modelo de directorio LDAP para la universidad.

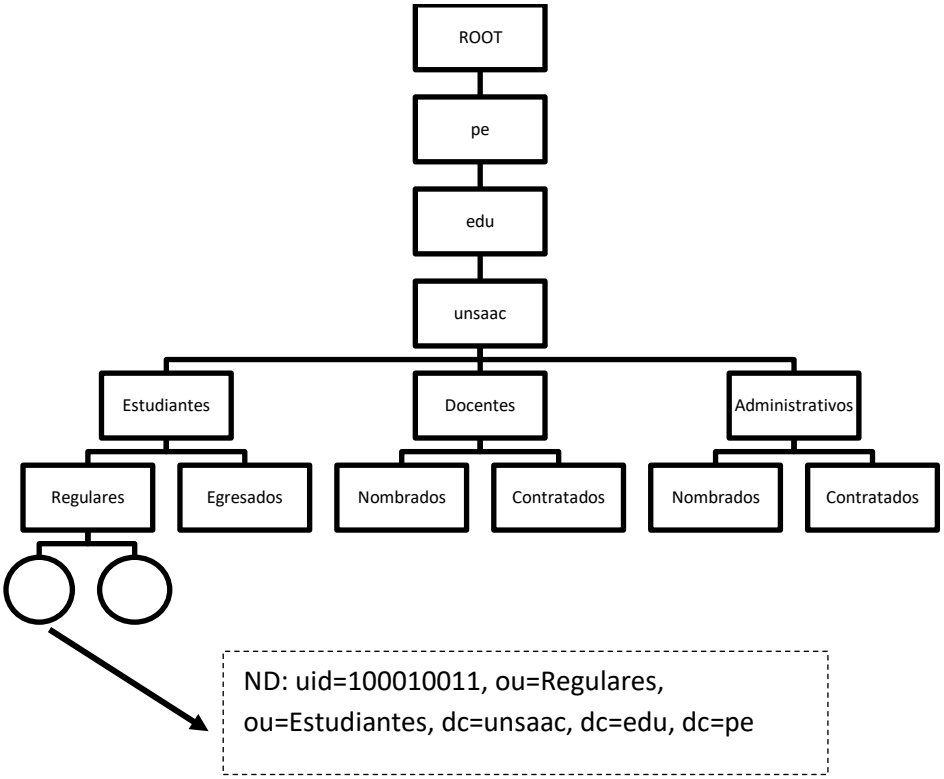

Figura 21. Árbol de directorio de información LDAP para el modelo de identidad digital.

En la Figura 22 y 23, se muestra el repositorio de datos basado en el directorio LDAP en funcionamiento y con la solicitud de datos de los usuarios.

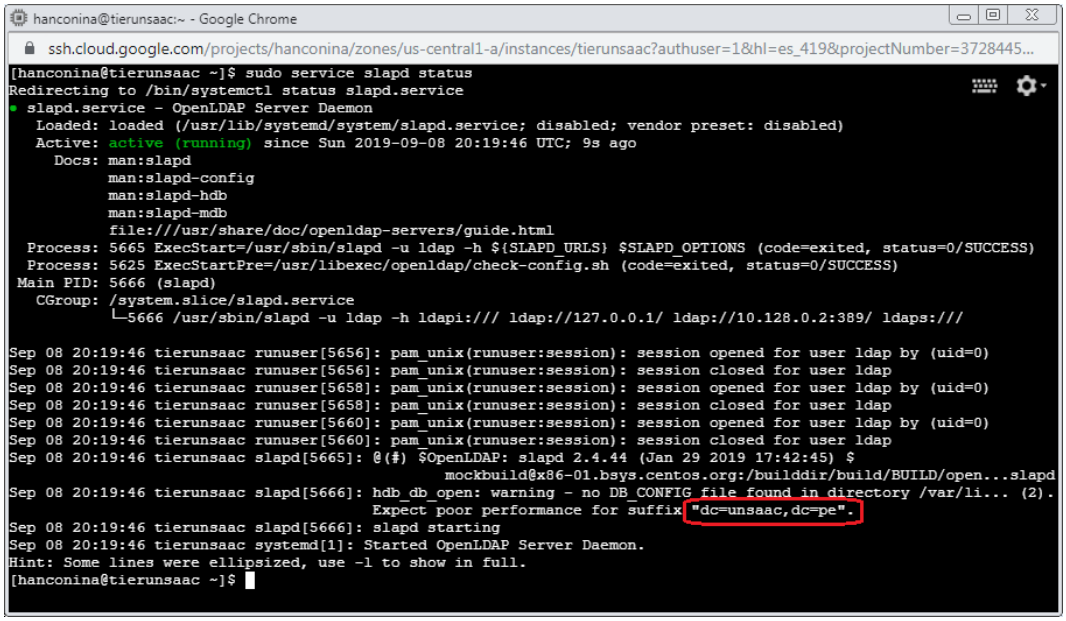

Figura 22. Repositorio digital habilitado para el esquema de directorio LDAP de la Universidad.

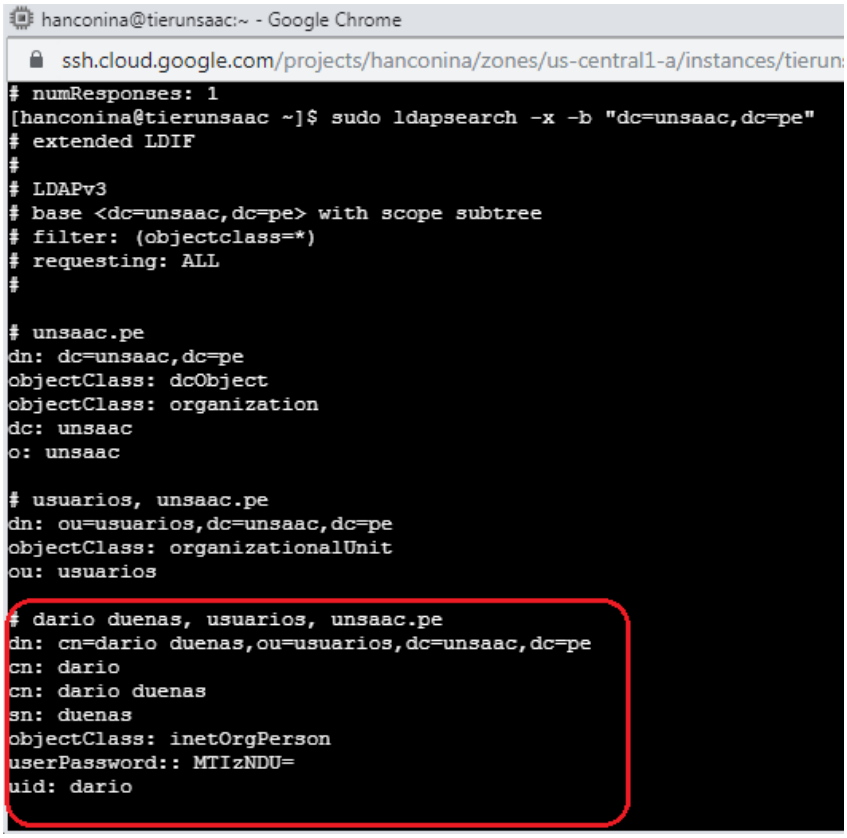

Figura 23. Acceso a datos del directorio LDAP de la Universidad.

4.3.2. Sistema de Información de Identidades

Para mejorar la gestión de directorio LDAP de la Universidad es necesario un Sistema de Información de Identidades que Permite gestionar usuarios y disponer de un administrador para añadir, eliminar, modificar, y entre otras operaciones sobre los usuarios quienes necesitan la autenticación y el inicio de sesión único. Así mismo, este administrador puede adicionar, eliminar, modificar, y entre otras operaciones sobre aquellas aplicaciones que los usuarios acceden. Por otro lado, cualquier usuario debe pasar por el sistema de información de identificación antes de completar el inicio de sesión único para acceder a un determinado sistema informático de la universidad. Así mismo, cualquier sistema informático de la universidad debe pasar también por el sistema de información de identificación antes de que este brinde servicios al usuario. En la Figura 24, se ilustra como el sistema de información de identidades interactúa con otros componentes del modelo.

4.4. Diseño de componentes de Autenticación y Autorización de usuarios para la gestión de acceso a los Sistemas Informáticos en la Universidad Pública de la Región Cusco

4.4.1. Portal Web de Autenticación Centralizada

El Portal es parte de la gestión centralizada y se utiliza para proporcionar una entrada de certificación uniforme a los usuarios cuando desean acceder a un determinado sistema informático de la universidad. A través del Portal, el usuario solicita la información de inicio de sesión y así realizar la autenticación de identidad unificada antes de acceder al sistema informático. En la Figura 24, se ilustra los componentes relacionados al portal de autenticación. A continuación, se describe el funcionamiento de componentes relacionados a la autenticación y autorización.

- **Servicio de entrada de autenticación unificada:** El usuario recupera la identidad de autenticación del navegador de internet para luego solicitar una entrada al servicio de entrada de autenticación unificada. En el navegador se crea un objeto de sesión que se almacena en un Cooked.

- **Servicio de entrada de acceso Web**: Provee una entrada de inicio de sesión al sistema informático indicando los permisos que el usuario dispone en la aplicación. El usuario, tiene una solicitud HTTP para acceder al sistema informático a través del Navegador de Internet.

- **Servicio de conversión interna del sitio**: En ocasiones cuando el usuario no puede acceder a un sistema informático se redirige al módulo de conversión interna y sus principales funciones corresponde a:

    - Chequear el encabezado del Cookie de la solicitud HTTP para determinar si el usuario ha completado la autenticación.

    - Generar aserciones para el usuario quien tiene completado su inicio de sesión único y la aserción contiene sentencias de autenticación de usuario y declaración de atributos. Los atributos de autenticación contienen el nombre de usuario y la contraseña que son necesarios para la autenticación en el sistema informático.

    - Generar un formulario, y crear una respuesta POST y enviarla al módulo de filtro en el sistema informático.

- **Módulo de autenticación**: Completa el inicio de sesión del usuario en el sistema informático. El módulo de autenticación es como un proxy para analizar las solicitudes y redirigir al sistema que corresponde el inicio de sesión.

- **Módulo de Filtro**: Verifica si los atributos de autenticación del usuario están certificados para acceder al Sistema Informático de la universidad.

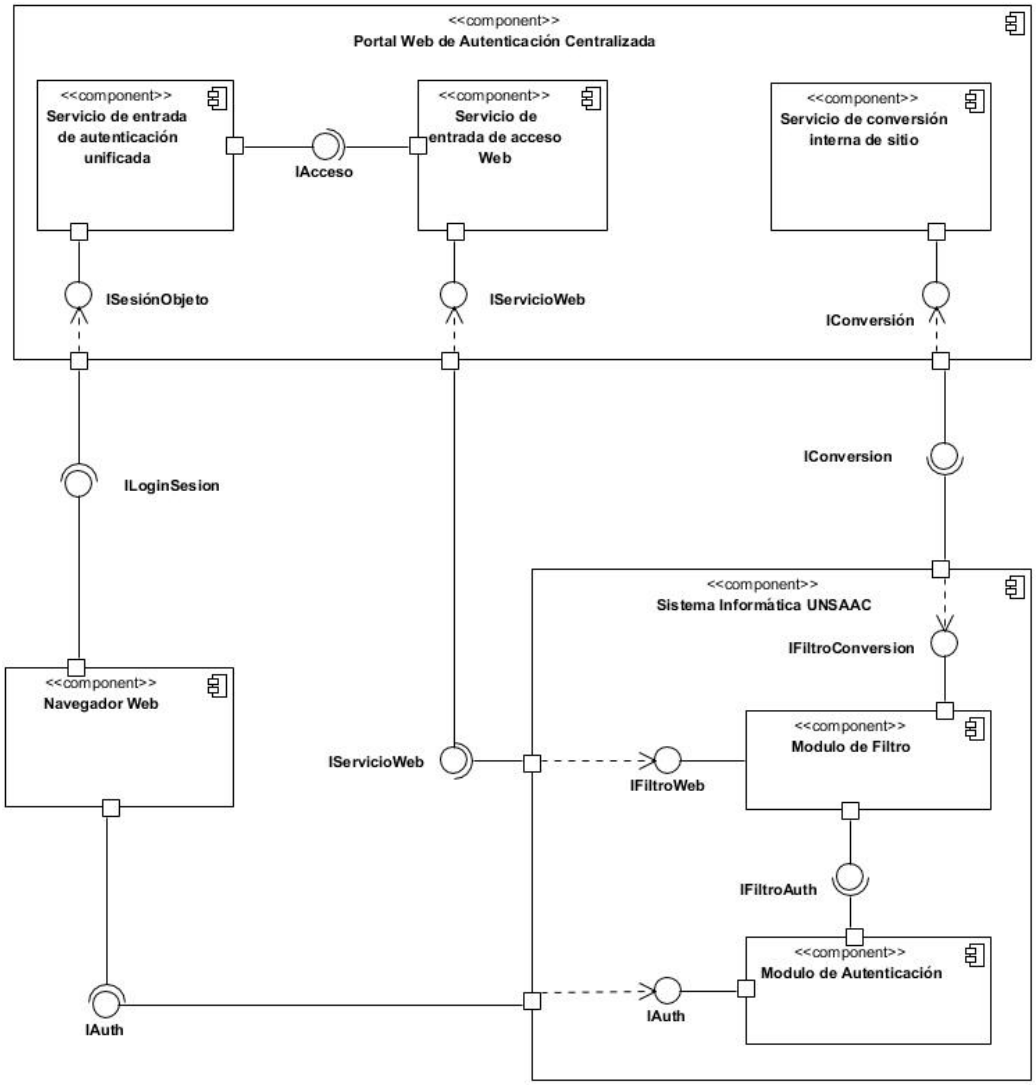

Figura 24. Diagrama de Componentes para la Autenticación y Autorización del modelo.

4.4.2. Agente del sistema informático

Es un filtro desplegado junto al sistema informático, que se comporta como una capa intermedia que implementa un agente de autenticación. El módulo de agente de autenticación según la solicitud del usuario determina si el usuario procede su autenticación única y automáticamente accede a la aplicación o sistema informático de la universidad, Además, el módulo de

agente de autenticación interactúa con el Portal Web de autenticación centralizada para conocer la información de identificación que esta almacenada en la base de datos centralizada.

En este sentido, para lograr el propósito de autenticación única la estructura del modelo según el programa TIER debe consistir en tres entidades principales: Un Agente de Usuario (AU), Un Proveedor de Servicios (PS) Shibboleth y Proveedor de Identidad (PI) Shibboleth. Asu vez, dichas entidades interactúan de la siguiente manera:

1. En primer lugar, mediante una URL segura (HTTPS) el usuario solicita un recurso protegido por un Proveedor de Servicio.
2. Seguidamente, el Proveedor de Servicio recibe la solicitud, atiende y envía una solicitud de autenticación al Proveedor de Identidad puesto que su rol es identificar y autenticar al usuario.
3. A continuación, el Proveedor de Identidad recibe la solicitud, la atiende y envía un retorno sobre el resultado de la autenticación al Proveedor de Servicios con la autorización del usuario para acceder al recurso protegido.
4. Finalmente, el Proveedor de Servicio recibe y responde y otorga el recurso al usuario. Así mismo, el recurso es un archivo, aplicación, datos u otro.

Para cumplir los requisitos de seguridad el protocolo SSL debe ser habilitado tanto en el Proveedor de Servicios y el Proveedor de Identidad, de

esta manera protegemos la información que entre ellos se intercambia. En la Figura 25, se ilustra la interacción entre las entidades principales del sistema.

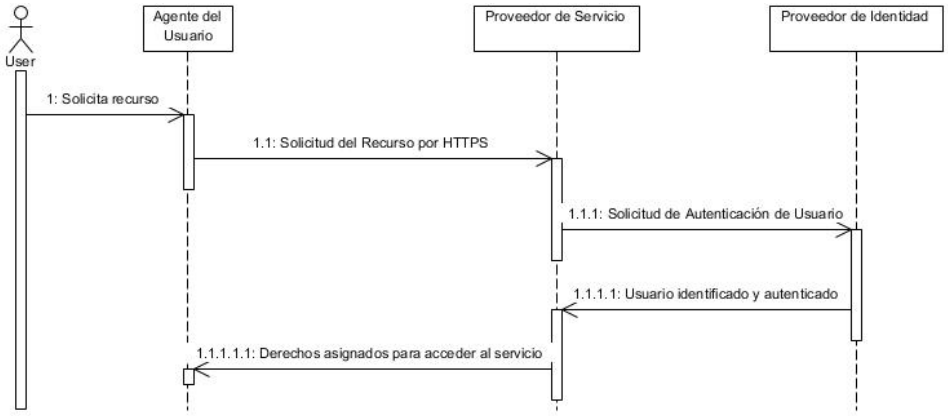

Figura 25. Diagrama de secuencia de los componentes del Agente del Sistema Informático.

Por otro lado, es importante tomar en cuenta algunas características para SSO o Inicio de Sesión Único (Single Sing-On) que Shibboleth utiliza:

- Atributos de usuario: Estos atributos sirvan para que el Proveedor de Servicios y el Proveedor de Identidad intercambien datos. En este sentido, los atributos que se consideran corresponden a el correo electrónico del usuario, número de teléfono, nombre de grupo y el cargo que tiene en la organización.
- Shibboleth metadata: corresponde a metadatos del Proveedor de Servicios y Proveedor de Identidad y corresponde a Mensajes de URL, ID de la entidad, Información de Encriptado, entre otros.
- Federación Single Sign On con Shibboleth: Corresponde a mecanismos que permitirán actuar al Proveedor de Servicios y el

Proveedor de identidad con aplicaciones que este fuera de la organización es decir pertenezcan a otra red.

- Perfiles Shibboleth: Define un conjunto de funciones que pueden ser realizadas.
- Shibboleth Binding: Define el formato de como los mensajes son encaminados a un determinado receptor. Por ejemplo, se puede utilizar un HTTP POST.

4.4.3. Sistema informático UNSAAC

Representa a un servicio digital que la universidad brinda a docentes, estudiante, personal administrativo y público en general. Por consiguiente, los sistemas informáticos de la universidad son diversos y con el pasar de los años se viene incrementando.

4.4.4. Navegador Web

Es la aplicación que permite a los usuarios del sistema acceder a los servicios de la universidad. Así mismo, el único requisito del navegador es soportar Cookie, protocolo seguro de comunicación SSL y JavaScript.

4.4.5. Soporte de identidades federadas

La universidad dispone de servicios implementados dentro del dominio de la organización y otros que accede como software como servicio en la nube. Por ejemplo, el Sistema Académico, Repositorio Digital y directorio activo para el acceso a Wi-fi son implementados en la universidad, por otro lado, el

sistema de correo electrónico institucional, sistema antiplagio y biblioteca virtual son servicio en la nube.

Entonces, bajo dicha situación de los servicios informáticos y por recomendación del programa TIER de Internet2 es necesario plantear un modelo basado federaciones de identidad.

Un sistema de gestión de identidad federada, consiste en componentes de software y protocolos que manejan el ciclo de vida de la identidad digital de una persona. Así mismo, esta arquitectura proporciona al usuario la ilusión de que existe una única autoridad de identificación. Además, si el usuario tiene muchas identidades no es necesario que conozca todas, entonces, solo una identidad es suficiente para tener acceso a todos los servicios en el dominio federado. También, el modelo de identidad federada se basa en un conjunto de Proveedores de Servicios denominada como círculo de confianza, seguridad mutua y autenticación simple o SSO (Single Sign-On). Los sistemas federados admiten múltiples proveedores de identidad y un sistema distribuido para almacenar información de identidad y acceso rápido a los recursos. En la Figura 26, se ilustra un esquema de federación de dominios.

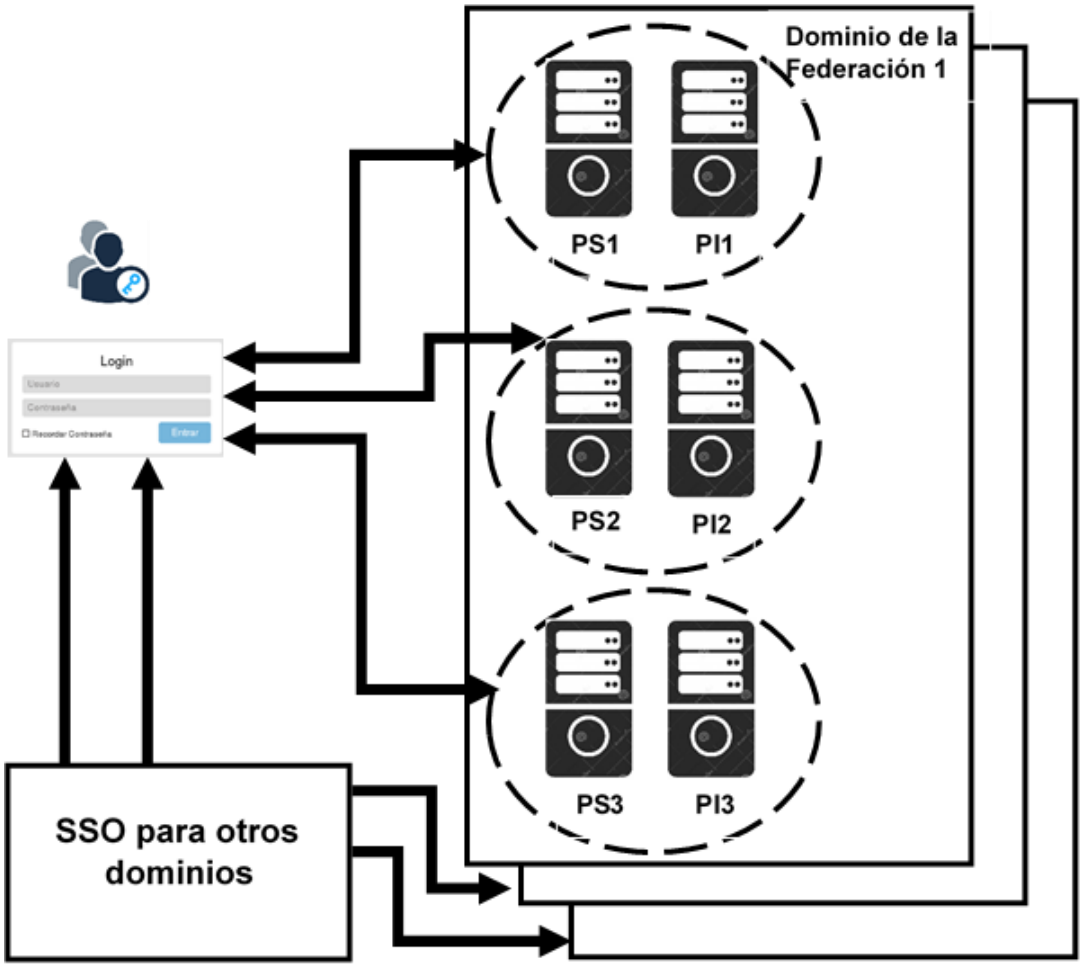

Figura 26. Diagrama de secuencia de los componentes del Agente del Sistema Informático.

4.4.6. Interfaz de usuario del Portal Web

En la Figura 27 y 28, se ilustra un prototipo de la ventana de inicio de sesión del portal web de autenticación única y una sesión iniciada por un usuario listo para poder acceder a los diferentes sistemas informáticos de la universidad.

Figura 27. Ventana de Inicio de Sesión del Portal de Autenticación Única.

Figura 28. Sesión abierta en el portal web de autenticación.

4.5. Influencia del modelo de identidad digital en la gestión de acceso a los servicios informáticos

4.5.1. Proporción de tiempo requerido para el acceso a los sistemas informáticos

Tabla 7 *chi-cuadrado para la proporción de tiempo*

Pruebas de chi-cuadrado

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	1,583[a]	1	,208		
	,891	1	,345		
	1,609	1	,205		
				,346	,173
	1,563	1	,211		
	76				

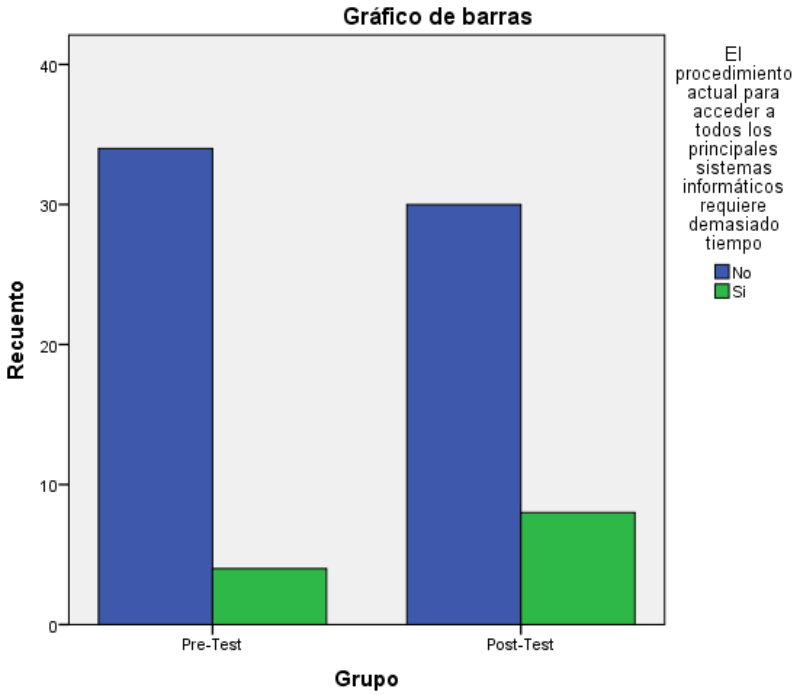

Figura 29. El procedimiento actual para acceder a todos los principales sistemas informáticos requiere demasiado tiempo

En la Tabla 7 y Figura 29, se ilustra la existencia de demasiado tiempo para realizar el procedimiento de acceso a los principales sistemas informáticos de la Universidad. El resultado y las comparaciones en las etapas del pre-test y

post-test demuestran que no existen diferencias significativas al utilizar o no utilizar el modelo de identidad digital.

4.5.2. Disponibilidad de seguridad y confiabilidad de los datos al acceder a los sistemas informáticos

Tabla 8 *chi-cuadrado para la disponibilidad de seguridad y confiabilidad*

Pruebas de chi-cuadrado

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	7,664[a]	1	,006		
	6,440	1	,011		
	7,805	1	,005		
				,011	,005
	7,563	1	,006		
	76				

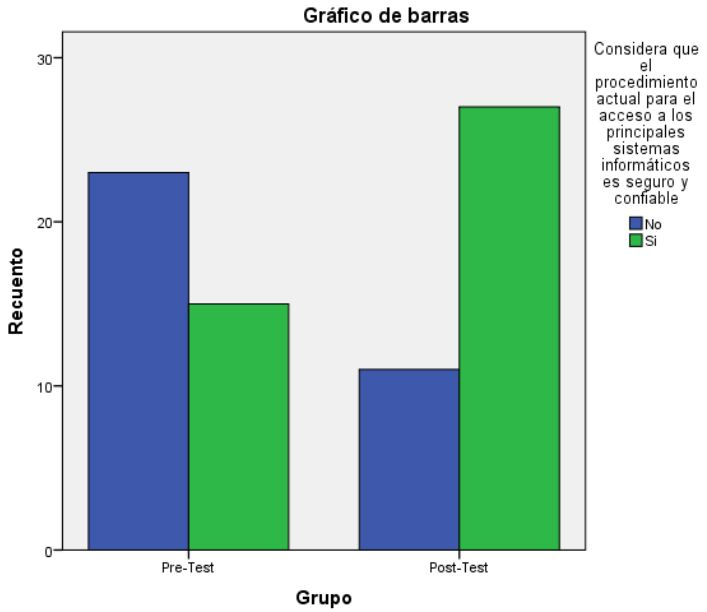

Figura 30. Considera que el procedimiento actual para el acceso a los principales sistemas informáticos es seguro y confiable

Según los datos de la Tabla 8 y Figura 30 los resultados indican que existe diferencias significativas en la seguridad de los datos que son proporcionados por el nuevo modelo de identidad digital basado en TIER.

4.5.3. Proporción de la cantidad de cuentas de usuario para acceder a los sistemas informáticos

Tabla 10 *chi-cuadrado para la proporción de cuentas de usuario*

Pruebas de chi-cuadrado

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	41,263[a]	1	,000		
	38,368	1	,000		
	46,173	1	,000		
				,000	,000
	40,720	1	,000		
	76				

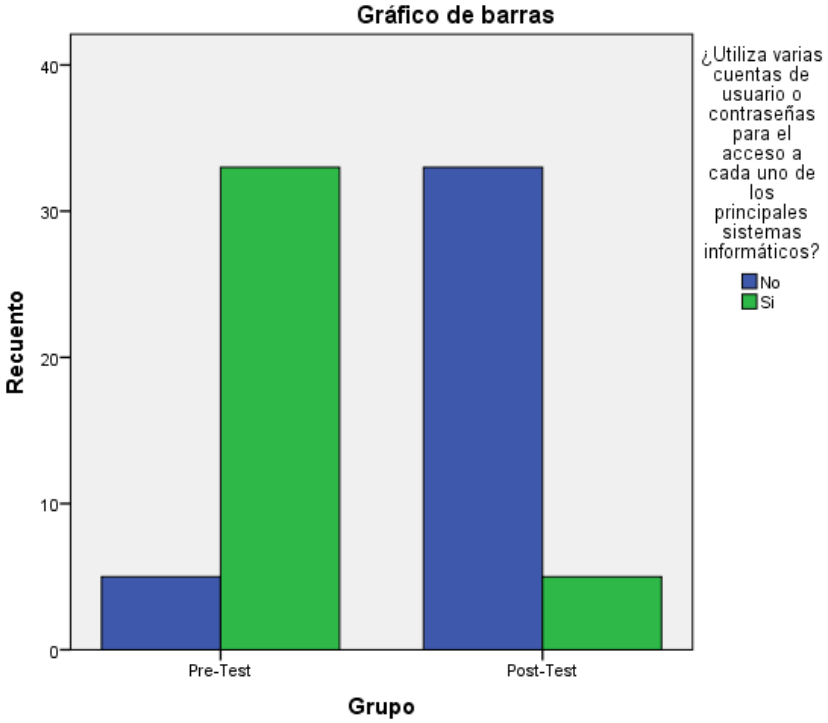

Figura 31. ¿Utiliza varias cuentas de usuario o contraseñas para el acceso a cada uno de los principales sistemas informáticos?

Según los resultados la proporción de cuentas de usuarios en su gran mayoría se ilustra según la Tabla 10 y Figura 31 que se utiliza una sola cuenta para acceder a los servicios informáticos de la Universidad. En este sentido, se demuestra la principal virtud del nuevo modelo de identidad digital que es la utilización de una sola cuenta de usuario para acceder a todos los sistemas informáticos de la universidad.

4.5.4. Disponibilidad del servicio de recuperación de contraseñas

Tabla 11 *chi-cuadrado para la disponibilidad del servicio de recuperación de contraseñas*

Pruebas de chi-cuadrado

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	7,773[a]	1	,005		
	6,531	1	,011		
	7,926	1	,005		
				,010	,005
	7,670	1	,006		
	76				

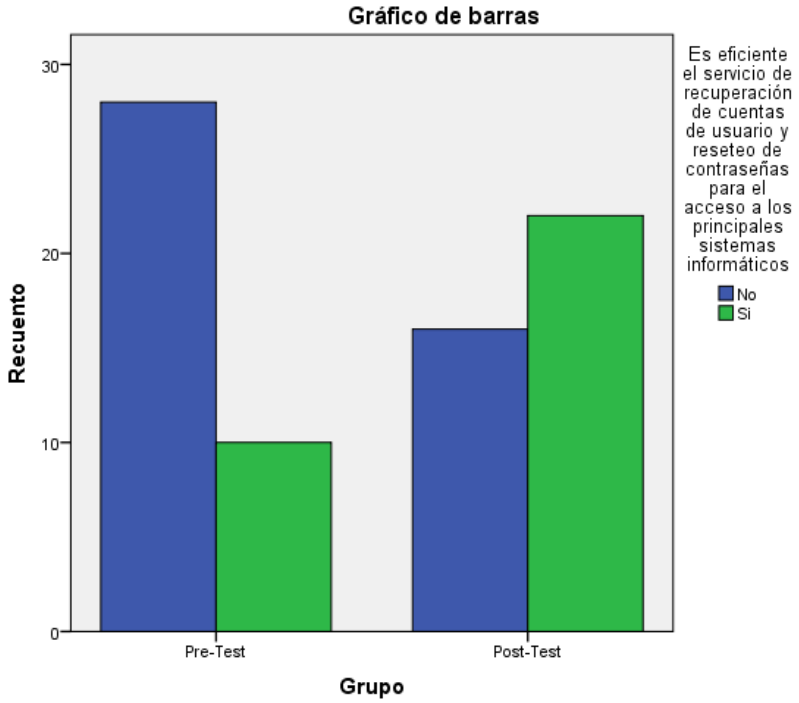

Figura 32. Es eficiente el servicio de recuperación de cuentas de usuario y reseteo de contraseñas para el acceso a los principales sistemas informáticos

Por otro lado, para el caso de la recuperación de contraseñas según las evaluaciones del pre-test y post-test se puede observar según los resultados de la Tabla 11 y Figura 32 que se mejora el proceso de recuperación de contraseña puesto que es uno de los componentes más importantes del nuevo modelo de identidad digital basado en TIER.

4.5.5. Existencia de un procedimiento para reportar el seguimiento y control de acceso

Finalmente, el procedimiento para reportar el seguimiento y control de acceso a pesar de estar implementado en el modelo no es percibido como una ventaja por los usuarios según los resultados del pre-test y post-test ilustrados en la Tabla 12 y Figura 35.

Tabla 12 *chi-cuadrado para la disponibilidad del soporte de seguimiento*

Pruebas de chi-cuadrado

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	1,916[a]	1	,166		
Corrección por continuidad[b]	1,331	1	,249		
Razón de verosimilitudes	1,924	1	,165		
Estadístico exacto de Fisher				,249	,124
Asociación lineal por lineal	1,891	1	,169		
N de casos válidos	76				

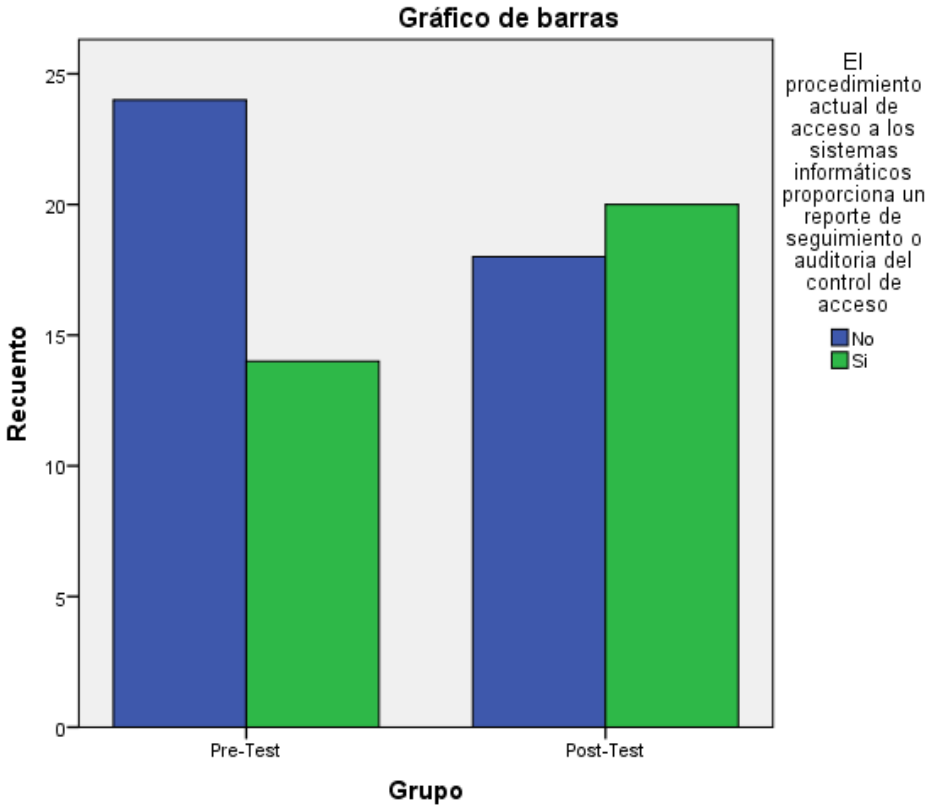

Figura 33. El procedimiento actual de acceso a los sistemas informáticos proporciona un reporte de seguimiento o auditoria del control de acceso

4.6. Evaluación de la adopción del modelo de identidad digital por los usuarios de la Universidad Pública de la Región del Cusco

4.6.1. Evaluación de la facilidad de uso percibida

Para llevar a cabo la evaluación de la percepción de los usuarios de la Universidad, se empleó como base al Modelo de Adopción de Métodos (MAM) descrito en la sección 2.1.1.1. del marco teórico. Según el modelo MAM el constructo de percepción de facilidad de uso mide el esfuerzo del usuario al utilizar un procedimiento especifico.

Por lo tanto, para evaluar la percepción de facilidad de uso de cada usuario entrevistado que utilizó el modelo de identidad digital TIER de Internet2, en la gestión del acceso a los servicios informáticos se aplicó la siguiente formula:

$$FUP(Facilidad\ de\ uso\ percibida)_i = \frac{\sum_{k=1}^{n} p_j}{n} \qquad 1 \leq p \leq 5 \qquad n = 5$$

$$1 \leq i \leq 38 \quad i, k \in N$$

Está formula es referenciada del trabajo de tesis de (Fernandez, 2007).

Donde: p_j corresponde al puntaje que fluctúa entre 1 y 5 para la k-ésima pregunta. Así mismo, n es la cantidad de preguntas del cuestionario que fueron consideradas para el constructo percepción de facilidad de uso (Pregunta 1, 3, 4, 6 y 9 del cuestionario) y $FUP\ (Facilidad\ de\ uso\ percibida)_i$ representa el valor promedio de la percepción de facilidad de uso por cada i-ésimo usuario entrevistado. En el

Anexo 4, se detallan los resultados de los puntajes asignados por cada usuario entrevistado.

Luego de obtener los puntajes se realiza un análisis descriptivo sobre los valores obtenidos del constructo $FUP\ (Facilidad\ de\ uso\ percibida)_i$ que se representan en la Tabla 6. En este sentido, se observa que el valor de la media es 3.79 y dicho valor es claramente superior al valor 3 que es el puntaje medio de la percepción de facilidad de uso. Además, el rango de valores fluctúa entre el valor mínimo de 1,40 y un valor máximo de 5. Por otro lado, el valor de la desviación estándar corresponde a un valor de 0,88 respecto a la media, lo que significa que la mayoría de las observaciones se encuentran dispersas a no más de 0.44 de desvió a cada lado de la media. En la Figura 29, se observa una distribución homogénea, pero aparece valores extraños cercanos al puntaje 1.

Tabla 6 *Descripción de datos sobre la percepción de facilidad de uso*

Variable	**Mínimo**	**Máximo**	**Media**	**Desv. típ.**
Facilidad de uso percibido (FUP)	1,40	5,00	3,79	0,88

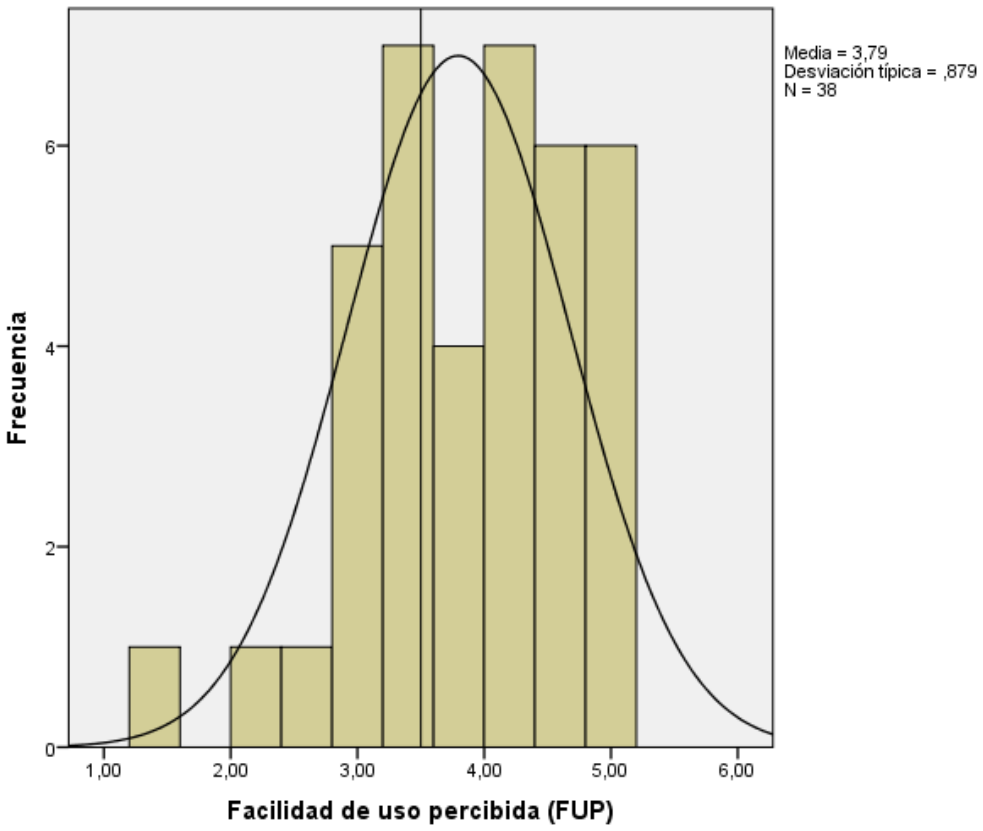

Figura 29. Diagrama de Frecuencias para la facilidad de uso percibida.

Los datos descriptivos manifiestan una facilidad de uso positiva al utilizar el modelo de identidad digital. Sin embargo, para generalizar estos resultados es necesario probar la hipótesis especifica formulada de la siguiente manera:

H1: *Los usuarios perciben que el modelo de identidad digital, basado en el programa TIER de internet2, es fácil de usar en la gestión del acceso a servicios informáticos en la universidad pública de la región Cusco.*

$$H1_0: \mu \leq 3, \quad \propto = 0.05$$

$$H1_a: \mu > 3$$

Los datos que corresponden a la percepción de facilidad de uso presentan una distribución normal según la prueba de bondad de ajuste de Kolmogorov-Smirnov. En la Tabla 7, muestra el estadístico Kolmogorov-Smirnov que muestra una significancia mayor a 0.05 por lo tanto los datos corresponden a una distribución normal. Por otro lado, en la Figura 30, los puntos caen aproximadamente sobre X=Y, entonces los datos provienen de una distribución normal.

Tabla 7 *Prueba de normalidad para los datos de facilidad de uso percibido*

	Kolmogorov-Smirnov		
	Estadístico	gl	Sig.
Facilidad de uso percibido (FUP)	,125	38	,140

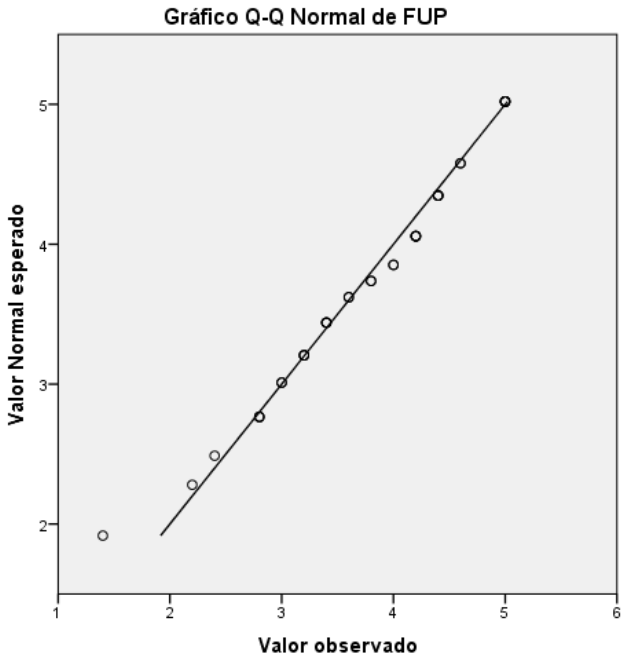

Figura 30. Dispersión de datos de la facilidad de uso percibida.

Finalmente, la prueba de t-student fue utilizada para verificar $H1_0$: $\mu \leq 3$. Así mismo, los resultados obtenidos en la Tabla 8, permiten rechazar la hipótesis nula $H1_0$, puesto que el valor del estadístico t-student está fuera del intervalo de confianza, siendo el nivel de significancia alto ($p < 0.05$). Entonces, podemos afirmar con el 95% de confianza que el modelo de identidad digital es fácil de usar para la gestión del acceso a los servicios informáticos de la Universidad, de tal forma, que la hipótesis especifica es contrastada.

Tabla 8 *Prueba de T-Student para la Facilidad de uso Percibida (FUP)*

	Prueba para una muestra					
	Valor de prueba = 0					
	t	gl	Sig. (bilateral)	Diferencia de medias	95% Intervalo de confianza para la diferencia	
					Inferior	Superior
FUP	26,6	37	,000	3,79	3,51	4,08

4.6.2. Evaluación de la utilidad percibida

Para evaluar la utilidad percibida, se procedió en primer lugar a calcular el promedio o media de los puntajes asignados por cada sujeto, aplicando una fórmula similar a la utilizad en la evaluación de la percepción de facilidad de uso. Así mismo, seis preguntas del cuestionario fueron consideradas para evaluar la utilidad percibida (Pregunta, 2, 5, 8, 10, 11 y 13).

Obtenido los puntajes se realiza un análisis descriptivo de los datos observados del constructo $UP(Utilidad\ percibida)_i$ que se representan en la Tabla 9. Por consiguiente, se observa que el valor de la media es 3.98 y dicho valor es claramente superior a 3 que es el puntaje medio de la utilidad percibida. También, el rango de valores varía entre el valor mínimo de 2,50 y un valor máximo de 5. Además, el valor de la desviación estándar corresponde a un valor de 0,66 respecto a la media, lo que significa que la mayoría de las observaciones se desvían sin exceder de 0.33 respecto a cada lado de la media. En la Figura 31, se observa una distribución homogénea sin valores extremos.

Tabla 9 *Descripción de datos sobre la utilidad percibida (UP)*

Variable	Mínimo	Máximo	Media	Desv. típ.
Utilidad percibida (UP)	2,50	5,00	3,98	0,66

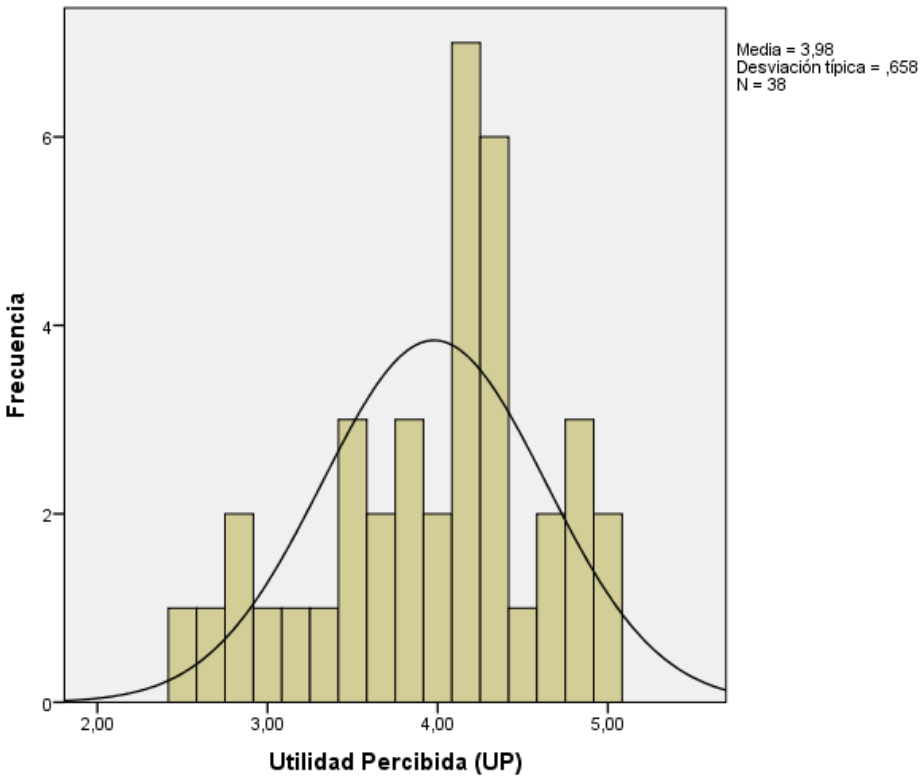

Figura 31. Diagrama de Frecuencias para la utilidad percibida.

Los datos descriptivos manifiestan que la utilidad percibida es positiva al utilizar el modelo de identidad digital. Por consiguiente, para generalizar estos resultados es necesario probar la hipótesis especifica formulada de la siguiente manera:

H2: *El modelo de identidad digital, basado en el programa TIER de internet2, es percibido por los usuarios como útil para gestionar el acceso a servicios informáticos en la universidad pública de la región Cusco.*

$$H2_0: \mu \leq 3, \quad \propto = 0.05$$

$$H2_a: \mu > 3$$

En la Figura 32, con respecto a los datos de la utilidad percibida los puntos caen aproximadamente sobre X=Y, entonces los datos provienen de una distribución normal.

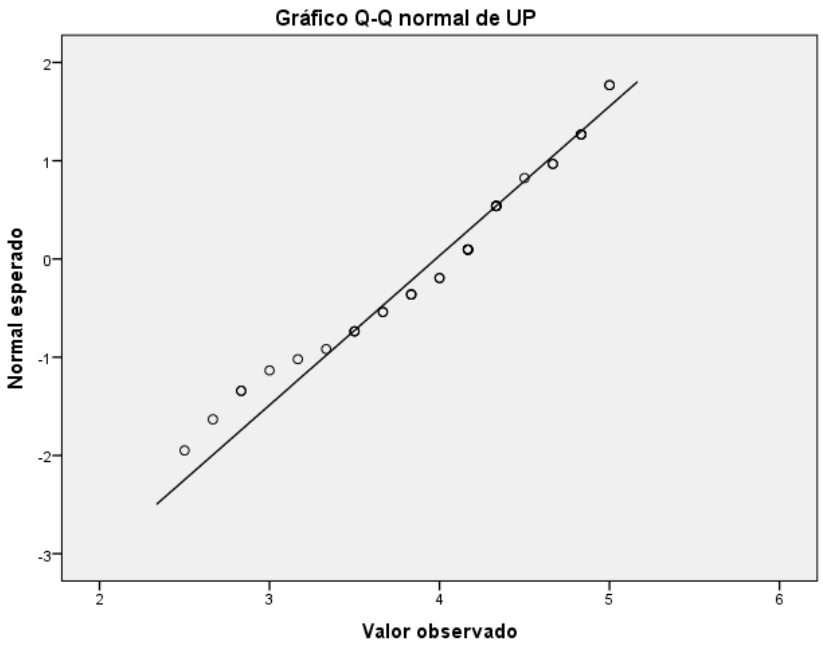

Figura 32. Dispersión de datos de la Utilidad percibida.

En conclusión, la prueba de t-student fue utilizada para verificar $H2_0: \mu \leq 3$. Así mismo, los resultados obtenidos en la Tabla 10, permiten rechazar la hipótesis nula $H2_0$, puesto que el valor del estadístico t-student está fuera del intervalo de confianza, siendo el nivel de significancia alto ($p < 0.05$). Entonces, podemos afirmar con el 95% de confianza que el modelo de identidad digital es fácil de usar para la gestión del acceso a los servicios informáticos de la Universidad, de tal forma, que la hipótesis especifica es contrastada.

Tabla 10 *Prueba de T-Student para la Utilidad percibida (UP)*

	Prueba para una muestra					
	Valor de prueba = 0					
	t	gl	Sig. (bilateral)	Diferencia de medias	95% Intervalo de confianza para la diferencia	
					Inferior	Superior
UP	37,28	37	,000	3,98	3,76	4,19

4.6.3. Evaluación de la intención de uso

Al igual que en las anteriores evaluaciones, con el fin de representar un valor representativo de los puntajes asignados por cada uno de los sujetos que usaron el modelo de identidad digital, se calculó el promedio aplicando una fórmula similar a la utilizada en la percepción de facilidad de uso, con la excepción de que n para este caso es igual a 3 preguntas que corresponden a (Pregunta 7, 12, 14).

El análisis descriptivo de los valores obtenidos del constructo $ITU\ (Intención\ de\ Uso)_i$ que se representan en la Tabla 11. En este sentido, se observa que el valor de la media es 4.33 y dicho valor es claramente superior al valor 3 que es el puntaje medio de la intención de uso según la escala de Likert. Además, el rango de valores fluctúa entre el valor mínimo de 2,67 y un valor máximo de 5. Por otro lado, el valor de la desviación estándar corresponde a un valor de 0,65 respecto a la media, lo que significa que la mayoría de las observaciones se encuentran dispersas a no más de 0.32 de desvió a cada lado de la media. En la Figura 33, se observa una distribución homogénea no simétrica.

Tabla 11 *Descripción de datos sobre la intención de uso*

Variable	Mínimo	Máximo	Media	Desv. típ.
Intención de uso (FUP)	2,67	5,00	4,33	0,65

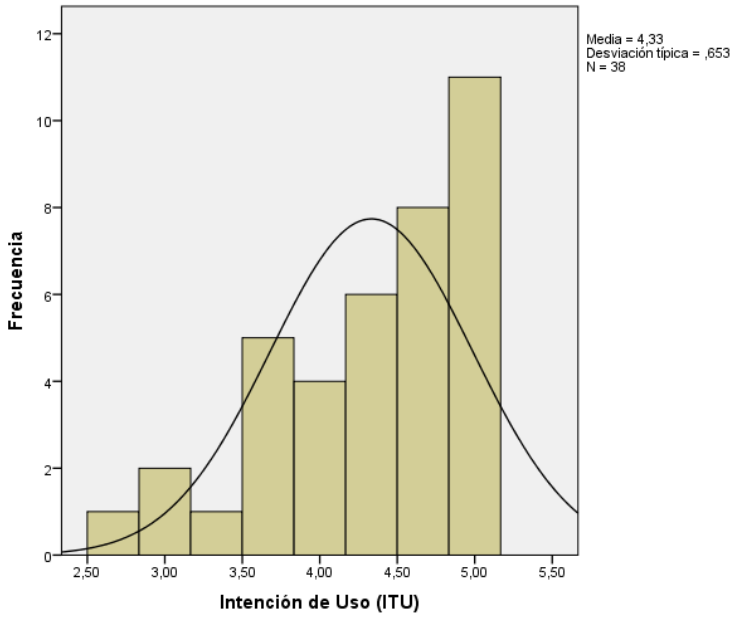

Figura 33. Diagrama de Frecuencias para la intención de uso.

Por consiguiente, los datos descriptivos presentan una actitud positiva sobre la intención de uso del modelo de identidad digital. Sin embargo, para generalizar estos resultados es necesario realizar la prueba de hipótesis especifica formulada de la siguiente manera:

H3: *Los usuarios tienen la intención de usar el modelo de identidad digital, basado en el programa TIER de internet2, para gestionar el acceso a servicios informáticos en la universidad pública de la región Cusco.*

$$H3_0: \mu \leq 3, \quad \propto = 0.05$$

$$H3_a: \mu > 3$$

Los datos que corresponden a la intención de uso presentan una distribución normal según la Figura 34, donde los puntos caen aproximadamente sobre X=Y.

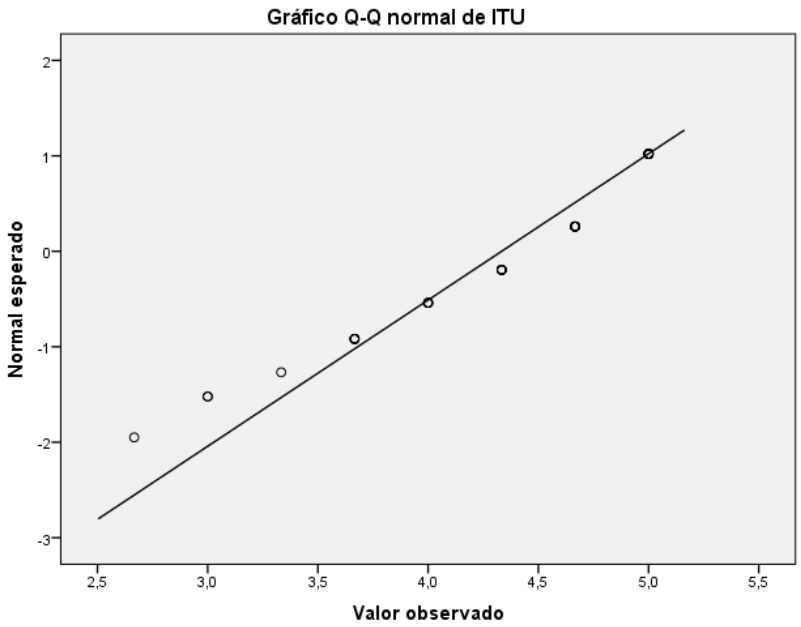

Figura 34. Dispersión de datos de la facilidad de uso percibida.

Finalmente, la prueba de t-student fue utilizada para verificar $H3_0$: $\mu \leq 3$. Así mismo, los resultados obtenidos en la Tabla 12, permiten rechazar la hipótesis nula $H3_0$, puesto que el valor del estadístico t-student está fuera del intervalo de confianza, siendo el nivel de significancia alto ($p < 0.05$). Entonces, podemos afirmar con el 95% de confianza que el modelo de identidad digital tiene la intención de ser utilizado para la gestión del acceso a los servicios informáticos de la Universidad, de tal forma, que la hipótesis especifica es contrastada.

Tabla 12 *Prueba de T-Student para la Intención de uso (ITU)*

	Prueba para una muestra					
	Valor de prueba = 0					
	t	gl	Sig. (bilateral)	Diferencia de medias	95% Intervalo de confianza para la diferencia	
					Inferior	Superior
ITU	40,91	37	,000	4,33	4,19	4,55

4.6.4. Relación entre las variables según el modelo MAM

Según lo planteado por el Modelo de Adopción de Métodos (MAM) la facilidad de uso percibida (FUP) y la utilidad percibida (UP) influye en la intención de uso (ITU). para comprobar está situación en el caso de la adopción del modelo de identidad digital TIER de Internet2 nos planteamos la siguiente hipótesis:

H4: *La facilidad de uso percibida y la utilidad percibida influye en la intención de uso del modelo de identidad digital basado en TIER de Internet2 para la*

gestión del acceso a sistemas informáticos de la Universidad Pública de la Región del Cusco.

$$H4\text{: } FUP + UP \rightarrow ITU$$

Donde la Facilidad de Uso Percibida (FUP) y la Utilidad Percibida (UP) fueron utilizadas como variables independientes y la intención de uso (ITU) como variable dependiente. Entonces, la ecuación de regresión múltiple resultante del análisis es:

$$ITU = 2{,}05 + 0{,}5 * UP + 0{,}1 * FUP$$

Los detalles del análisis de regresión múltiple se presentan en la Tabla 13 donde se rechaza la hipótesis nula $H4_0$ entonces se acepta el modelo de regresión lineal múltiple.

Tabla 13 *Modelo de regresión lineal múltiple para FUP, UP e ITU*

R	**R cuadrado**	**R cuadrado corregida**	**Error típ. de la estimación**	**F**	**Sig.**
0,54	0,29	0,25	0,56	7.30	0,002

Tal como se observa en la Tabla 14, el resultado de la regresión permite el rechazo de la hipótesis nula $H4_0$ lo que significa que empíricamente podemos afirmar con un 95% de confianza que la intención de uso es influenciada por la facilidad de uso percibida y la utilidad percibida.

Tabla 14. *Coeficientes del Modelo de regresión lineal múltiple para FUP, UP e ITU*

Coeficientes[a]						
Modelo		**Coeficientes no estandarizados**		**Coeficientes tipificados**	**t**	**Sig.**
		B	Error típ.	Beta		
1	(Constante)	2,046	,618		3,310	,002
	FUP	,085	,111	,115	,774	,444
	UP	,493	,148	,497	3,340	,002

a. Variable dependiente: ITU

El coeficiente de determinación R^2 del análisis de regresión indica que el 29% de la diversificación en la intención de uso (ITU) puede ser explicada por la diversificación que ocurre tanto en la facilidad de uso percibida (FUP), como en la utilidad percibida (UP) al momento de acceder a los sistemas utilizando el modelo de identidad digital TIER de Internet2.

V. DISCUSIÓN DE RESULTADOS

La gestión de identidades digitales centralizadas que contempla operaciones de identificación, autenticación y autorización de usuarios a un conjunto de sistemas informáticos en una organización tiene vital importancia para la seguridad de los datos y productividad de los usuarios. Por lo tanto, en una universidad también es de vital importancia tomar en cuenta aspectos de identidad digital, En este sentido, muchas investigaciones resaltan algunas soluciones popularidad en la implementación de sistemas de identificación digital única como es el caso de Keycloak, WSO2 Identity Server, Gluu CAS, OpenAM y Shibboleth IdP (Uddin & Preston, 2015). Sin embargo, la plataforma por excelencia para gestión de identidades digitales en universidades es Shibboleth del programa TIER (Internet2, 2019).

En el caso de las universidades del interior del Perú en especial la universidad pública de la Región del Cusco requiere de manera inmediata una solución para la gestión de identidades digitales para evitar problemas en la gestión del acceso a los sistemas informáticos de la universidad. En este sentido, la gestión inadecuad de la identidad digital en la universidad generan problemas de inconsistencia y duplicidad de datos de usuarios provocando incomodidad en los mismos usuarios y problema de seguridad de la información (Monedero et al., s. f.).

Entonces, el diseño de un modelo de identidad digital basado en el programa TIER de Internet2 es la base para la implementación de un sistema de autenticación único en la Universidad Pública de la Región del Cusco. Por

lo tanto, el diseño de un repositorio de datos de usuarios efectivo y adecuado para procesos de autenticación corresponde al servicio de directorio LDAP. Así mismo, las principales ventajas de LDAP es poder unificar datos de usuarios que se encuentra dispersos y repetidos en muchas bases de datos propias de cada sistema informático. También, LDAP permite hacer público los datos de los usuarios como directorios de contactos que son útiles para la autenticación de usuarios.

Por otro lado, los procesos de autenticación y autorización son abordados como un problema aparte puesto que los sistemas informáticos están desarrollas en diferentes plataformas de Hardware y Software entonces querer integrarlos en una sola solución no es posible puesto que no se tiene acceso a muchos softwares, porque no se dispone de un código fuente adecuado o los sistemas son servicios de la nube. Entonces, es necesario mantener independiente a cada software con su propia tecnología, pero, podemos hacer que los sistemas informáticos puedan manejar una federación de identidades de tal forma que el usuario pueda utilizar una sola credencial para acceder a muchos sistemas informáticos.

Para la gestión de autenticación y autorización se plantea el diseño de una arquitectura de software cuyos componentes principales son el Portal Web de Autenticación centralizada e inicio de sesión único, el Sistema de Información de Identidades y el Agente de Sistemas Informáticos de la Universidad. En este sentido, estos componentes logran satisfacer las

necesidades de la organización que corresponde al acceso a una aplicación y recursos digitales de la universidad.

Para evaluar la influencia de la gestión de acceso a los sistemas informáticos de la universidad utilizando el modelo de identidad digital basado en TIER se realizó un análisis estadístico de chi-cuadrado para evaluar diferencias significativas en las etapas de pre-test y post-test. La etapa del pre-test corresponde a la encuesta realizada antes de utilizar el nuevo modelo de identidad digital y la etapa del post-test permite observar los resultados después de utilizar el modelo de identidad digital. Los resultados muestran que si existen mejoras en la gestión particularmente en proporcionar seguridad de los datos, adecuada gestión de usuarios y contraseñas y recuperación de contraseñas ante perdidas.

Por otro lado, con la finalidad de evaluar la adopción del modelo por los usuarios se realizó un análisis de percepción de facilidad de uso, percepción de utilidad e intensión de uso del modelo. En general, del análisis descriptivo para la percepción de facilidad de uso, percepción de utilidad e intensión de uso presenta una media superior a 3 de la escala de Likert con puntaje mínimo 1 y puntaje máximo 5. Por ejemplo, la media más alta corresponde a la intención de uso con un puntaje de 4.33. Sin embargo, en ninguna de las variables el valor mínimo supero a 3 y en el caso de la variable facilidad de uso percibida el valor mínimo es cercano a 1 y también una desviación cercana a 1. Entonces, podemos afirmar que para algunos casos la facilidad de uso del modelo de identidad digital TIER de Internet2 no es fácil de usar en el proceso

de acceder a los sistemas informáticos de la universidad. Así mismo, en el caso de la utilidad percibida e intención de uso tienen poca variabilidad con respecto a la media. En la Tabla 15, se muestra la comparación de medias.

Tabla 15 *Comparación de datos descriptivos de las variables FUP, UP e ITU*

Variables	**Mínimo**	**Máximo**	**Media**	**Desv. típ.**
Facilidad de uso percibida (FUP)	1,40	5,00	3,79	0,88
Utilidad percibida (UP)	2,50	5,00	3,98	0,66
Intención de uso (ITU)	2,67	5,00	4,33	0,64

Para poder generalizar la actitud positiva de los usuarios con respecto al uso del modelo fue necesario la prueba de las hipótesis especificas H1, H2 y H3. En primer lugar, la prueba de Kolmogorov-Smirnov fue llevada a cabo para comprobar la normalidad de los datos. Así mismo, como la distribución de estos datos fue normal, la prueba de t-student fue utilizada para comprobar la diferencia de medias logrando que todas las hipótesis nulas sean rechazadas y por lo tanto se acepten con un alto nivel de significancia las hipótesis especificas formuladas en la investigación. En la Tabla 16, se ilustra la comparación de las pruebas t-student.

Tabla 16 *Comparación de la prueba t-student de las hipótesis especificas*

Estadística	**Facilidad de Uso Percibida**	**Utilidad Percibida**	**Intención de uso**
Diferencia de Medias	3,79	3,98	4,33
95% Intervalo de confianza	3,51 (Inferior) 4,08 (Superior)	3,76 (Inferior) 4,19 (Superior)	4,12 (Inferior) 4,55 (Superior)
T	26,61	37,28	40,91

p-valor	,000	,000	,000

Finalmente, para completar el estudio fue necesario comprobar la relación de las variables planteada por el Modelo de Adopción del Método MAM que considera una influencia en la intención de uso por la facilidad de uso percibida y la utilidad percibida. Entonces, para dicho fin fue necesario formular un modelo de regresión lineal múltiple donde la variable dependiente es la intención de uso (ITU) y las variables independientes la facilidad de uso percibida (FUP) y la utilidad percibida (UP). El resultado del modelo expresa que es posible predecir que la facilidad de uso percibido (FUP) y la utilidad percibida (UP) determinan la intención de uso (ITU) del modelo de identidad digital. Sin embargo, el modelo muestra una mínima incidencia de la facilidad de uso percibida, y con respecto a la utilidad percibida es mayor, pero con una tasa de cambio de 0.5 lo cual no es muy significativo.

Así mismo, en base al modelo de regresión lineal múltiple podemos interpretar lo siguiente: Por cada unidad de facilidad de uso percibida (FUP), manteniendo constante la variable de utilidad percibida (UP), se incrementará la intención de uso en 0.1 unidades. Por otro lado, por cada unidad de la utilidad percibida (UP), manteniendo constante la variable de facilidad de uso percibida (FUP), se incrementará la intención de uso en 0.5 unidades.

Por otro lado, el Modelo de Adopción del Método MAM expresa también diversas relaciones entre las variables la única que se cumple es la relación entre la variable utilidad percibida (UP) e intención de uso (ITU). En la Tabla 17 y Figura 35, se ilustra la correlación entre las variables. Los estudios

de (Fernandez, 2007), (Pow Sang Portillo, 2012) y (Cohn Muroy, s. f.) también afirman no cumplir las correlaciones entre las variables de MAM sin embargo manifiestan que esto no invalida los estudios realizados.

Tabla 17 *Correlaciones de las variables de estudio*

Correlaciones

		FUP	UP	ITU
FUP	Correlación de Pearson	1	,299	,264
	Sig. (bilateral)		,068	,110
	N	38	38	38
UP	Correlación de Pearson	,299	1	,531**
	Sig. (bilateral)	,068		,001
	N	38	38	38
ITU	Correlación de Pearson	,264	,531**	1
	Sig. (bilateral)	,110	,001	
	N	38	38	38

**. La correlación es significativa al nivel 0,01 (bilateral).

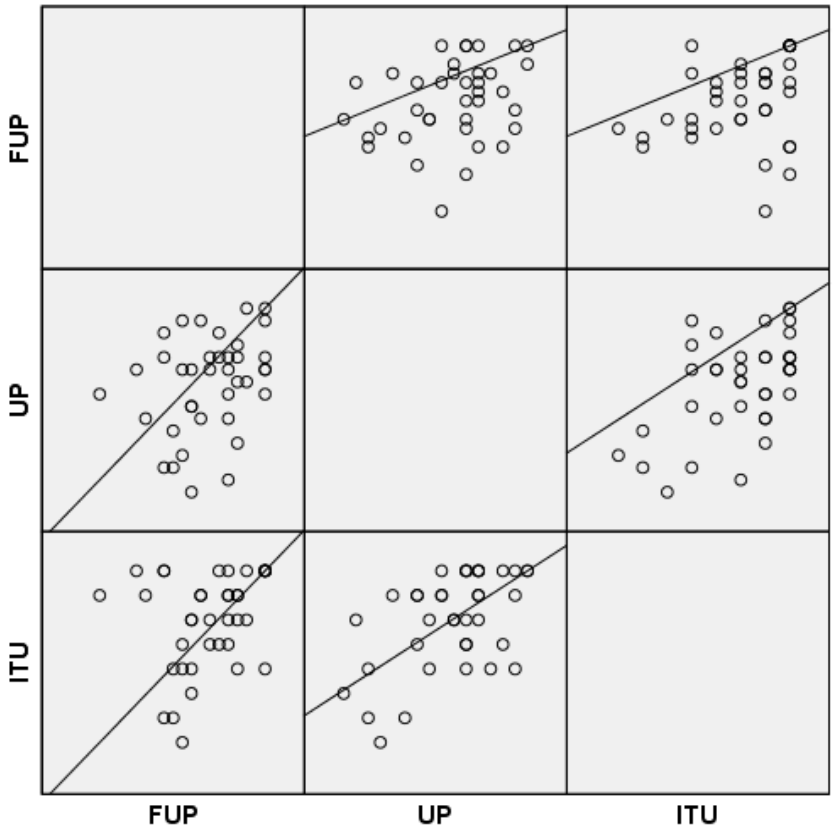

Figura 35. Dispersión de datos de correlación de variables.

VI. CONCLUSIONES

Conclusión principal:

El diseño del modelo de identidad digital que extiende las funcionalidades y buenas prácticas de la suite de aplicaciones de Trust and Identity in Education and Research (TIER) de Internet2 influye de manera positiva en la gestión del acceso a sistemas informáticos de la Universidad Pública de la Región Cusco. En primer lugar, la inconsistencia y duplicidad de datos de identificación de usuarios es organizada de mejor manera en un esquema de directorio o repositorio de datos LDAP (Lightweight Directory Access Protocol). En segundo lugar, el proceso de autenticación y autorización se ha simplificado a un sistema de autenticación unificado y de simple inicio de sesión gracias al diseño de componentes como el portal web de autenticación única, sistema de información de identidades, agente de autenticación de sistemas informáticos. En tercer lugar, los resultados de la gestión de acceso y la evaluación de adopción de modelo son favorable puesto que los usuarios entrevistados perciben que el modelo es fácil de usar, es útil y tienen la intención de utilizarlo en el futuro.

Conclusiones específicas:

1) Considerando la hipótesis especifica donde se plantea que el diseño del modelo de identidad digital basado en el programa TIER de Internet2, influye en la gestión del repositorio de datos para acceder a los servicios informáticos en universidades públicas de la región Cusco, dicha hipótesis es demostrada puesto que el repositorio de datos basado en

LDAP proporciona un esquema de datos adecuado para la autenticación de usuarios sin necesidad de utilizar un gestor de base de datos que no es conveniente utilizarlo en el proceso de autenticación de usuarios.

2) Para el diseño de componentes de autenticación y autorización fue necesario diseñar la arquitectura del Software y Hardware del Modelo para que pueda cumplir el propósito del modelo que corresponde. Los componentes diseñados fueron el Portal Web de Autenticación Unificada y el Agente de Autenticación de Sistemas Informáticos que fueron basados en el Proveedor de Servicios y Proveedor de Identidades del Shibboleth de el Programa TIER de Internet2.
3) Considerando el modelo de regresión lineal múltiple que determina la influencia de la intención de uso en función de la facilidad de uso percibida y la utilidad percibida, se encuentra evidencia suficiente para afirmar que los usuarios adoptaran el modelo de identidad digital basado en el programa TIER de Internet2 para gestionar el acceso a los sistemas informáticos de la Universidad. Entonces, con ello podemos afirmar que se logró el objetivo específico que es determinar en qué medida los usuarios adoptaran el modelo de identidad digital TIER de Internet2, en consecuencia, se ha resuelto el problema específico.

VII. RECOMENDACIONES

1) Según los resultados obtenidos es necesario mejorar la propiedad de usabilidad del modelo de Identidad Digital basado en el Programa TIER de Internet2, considerando que el problema de la gestión de identidades de manera centralizada es complejo por ello es necesario hacer que los procedimientos de acceso a los diferentes sistemas sean fáciles de usar. Además, es necesario considerar que muchos de los usuarios de la universidad pública desconocen algunos sistemas informáticos.
2) Para incrementar la intención de uso del modelo de identidad digital basado en el programa TIER de Internet2 se recomienda capacitar a los Profesores, Administrativos y Estudiantes. Dichas capacitaciones deben ser realizadas por especialidad.
3) Para hacer que el modelo de identidad digital basado en el programa TIER de Internet2, sea una herramienta útil en el futuro es necesario que las nuevas aplicaciones implementen servicios para un acoplamiento optimo entre el modelo y otros Sistemas. Esto significa, que en lo sucesivo los sistemas que se adquieran o se desarrollen en la Universidad deben cumplir ciertos requisitos para el intercambio de datos y perfiles de usuarios.
4) Para realizar un estudio sin considerar percepciones que corresponden a variables psicológicas es necesario analizar los datos registrados por el administrador del modelo de identidad digital TIER. Luego, debemos realizar una correlación entre los datos obtenidos y la percepción de los usuarios.

VIII. REFERENCIAS

Abrahao, S. M. (2004). *On the functional size measurement of object-oriented conceptual schemas: Design and evaluation issues*. Universidad Politecnica de Valencia (Spain).

Apéstegui Culli, G. P. (2018). *Identidad digital y el gobierno electrónico en el registro nacional de identificación y estado civil-2017*. http://repositorio.ucv.edu.pe/handle/UCV/14435

Campbell, D. T., & Fiske, D. W. (1959). Convergent and discriminant validation by the multitrait-multimethod matrix. *Psychological bulletin*, *56*(2), 81.

Castro Velarde, K. E., & Guzmán Salgado, J. del R. (2010). *Implementación del sistema de administración de accesos e identidades en el proceso de control de accesos en el Banco de la Nación* [San Martín de Porres]. http://www.repositorioacademico.usmp.edu.pe/bitstream/usmp/331/1/castro_ke.pdf

Ccosi, Z., & Martin, E. (2018). *Diseño e implementación de un servidor con el protocolo de acceso a directorio LDAP para la seguridad y control de los trabajadores en el uso de dispositivos y computadoras de la empresa Claro en la región Puno*. http://repositorio.unap.edu.pe/bitstream/handle/UNAP/9435/Zavalaga_Ccosi_Edwin_Martin.pdf?sequence=1&isAllowed=y

Cohn Muroy, D. S. (s. f.). *Análisis de la transparencia en la elicitación de requerimientos al combinar historias de usuario y casos de uso*.

Conklin, Wm. A., & Shoemaker, D. (2019). *CSSLP Certification All-in-One Exam Guide, Second Edition* (second edition). McGraw-Hill. https://acm.skillport.com/skillportfe/main.action?assetid=144453

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, 319–340.

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*. https://documentos.redclara.net/bitstream/10786/1003/1/130-Shibboleth-DIA-PUCP.pdf

El Maliki, T., & Seigneur, J.-M. (2007). A survey of user-centric identity management technologies. *The International Conference on Emerging Security Information, Systems, and Technologies (SECUREWARE 2007)*, 12–17. https://www.computer.org/csdl/proceedings/secureware/2007/2989/00/04385303.pdf

Fernandez, O. N. C. (2007). *Un procedimiento de medición de tamaño funcional para especificaciones de requisitos* [PhD Thesis]. Universitat Politècnica de València.

Internet2. (2019). *Trust and Identity in Education and Research (TIER)*. https://www.internet2.edu/vision-initiatives/initiatives/trust-identity-education-research/

Mendieta, H. D., Andrade Navarro, F., & others. (2015). *Sistema centralizado de gestión de usuarios para la Universidad del Tolima*.

https://repository.unad.edu.co/bitstream/10596/3623/1/13992720_14398493.pdf

Monedero, J. S., Aganzo, L. M., & Soto, S. V. (s. f.). *Implantación de LDAP como sistema de autenticación centralizada*. https://www.researchgate.net/profile/Javier_Sanchez-Monedero/publication/265172629_Implantacion_de_LDAP_como_sistema_de_autenticacion_centralizada/links/540990290cf2187a6a6f6cf1/Implantacion-de-LDAP-como-sistema-de-autenticacion-centralizada.pdf

Moody, D. L. (2003). The method evaluation model: A theoretical model for validating information systems design methods. *ECIS*.

Nina, H., Enciso, L., & Chavez, W. A. (s. f.). *Software as a Service Google Apps in the Internal Communication of the National University of San Antonio Abad del Cusco*.

Penna, E., De León, M., & others. (2016). *Implementación de un servicio de autenticación centralizado y gestión de identidades en la Universidad de la República*. http://dspace.redclara.net:8080/bitstream/10786/1077/1/Implementaci%C3%B3n%20de%20un%20servicio%20de%20autenticaci%C3%B3n%20centralizado%20y%20gesti%C3%B3n%20de%20identidades%20en%20la%20Universidad%20de%20la%20Rep%C3%BAblica.pdf

Pow Sang Portillo, J. A. (2012). *Técnicas para la Estimación y Planificación de Proyectos de Software con Ciclos de Vida Incremental y Paradigma Orientado a Objetos* [PhD Thesis]. Informatica.

Presidencia República Perú. (2018). *Decreto legislativo Nro. 1412 que aprueba la ley de gobierno digital*. El Peruano.

Ramírez, S. (1999). *Teoría general de sistemas de Ludwig von Bertalanffy* (Vol. 3). UNAM.

Shapiro, S. S., & Wilk, M. B. (1965). An analysis of variance test for normality (complete samples). *Biometrika*, *52*(3/4), 591–611.

Telefónica, F. (2013). Identidad Digital: El nuevo usuario en el mundo digital. *Barcelona: Editorial Ariel. Recuperado de http://www. educando. edu. do/files/9513/9281/6433/identidad_digital. pdf*. http://boletines.prisadigital.com/identidad_digital.pdf

Torres, M. J., de los Reyes, A., Espinoza, L., Saquicela, V., & others. (2017). *Plataforma de Gestión de Identidad y Acceso Federado para la Universidad de Cuenca*. http://dspace.redclara.net:8080/bitstream/10786/1261/1/30-3-4Plataforma%20de%20Gesti%C3%B3n%20de%20Identidad%20y%20Acceso%20Federado%20para%20la%20Universidad%20de%20Cuenca.pdf

Uddin, M., & Preston, D. (2015). Systematic Review of Identity Access Management in Information Security. *Journal of Advances in Computer Networks*, *3*(2). http://www.jacn.net/vol3/158-IS009.pdf

Veliz, F. (2015). La identidad digital para la inclusión digital en el gobierno electrónico y los derechos fundamentales de cuarta generación. *XX Congreso Internacional del CLAD sobre la Reforma del Estado y de la Administración Pública*.

http://www2.congreso.gob.pe/sicr/cendocbib/con4_uibd.nsf/304E32FE0C
B00E8E05257F31007A81F1/$FILE/velifaz.pdf

IX. ANEXOS

ANEXO 1. MATRIZ DE CONSISTENCIA

TITULO: MODELO DE IDENTIDAD DIGITAL BASADO EN EL PROGRAMA TIER DE INTERNET2 PARA GESTIONAR EL ACCESO A LOS SERVICIOS INFORMÁTICOS EN UNIVERSIDADES PÚBLICAS DE LA REGIÓN CUSCO

PROBLEMAS	OBJETIVO	HIPOTESIS	VARIABLES E INDICADORES	METODOLOGIA
GENERAL ¿De qué manera el diseño del modelo de identidad digital basado en el programa TIER de internet2 influye en la gestión de acceso a servicios informáticos en universidades públicas de la región Cusco? **PROBLEMAS ESPECIFICOS** a) ¿De qué manera el diseño del modelo de identidad digital basado en el programa TIER de internet2 influye en la gestión del repositorio de datos para acceder a los servicios informáticos en universidades públicas de la región Cusco? b) ¿De qué manera el diseño del modelo de identidad digital basado en el programa TIER de internet2 influye en la gestión de la autenticación y autorización de usuarios para el acceso a servicios informáticos de las universidades públicas de la región Cusco? c) ¿Es posible que los usuarios adopten el modelo de identidad digital, basado en el programa TIER de internet2, para gestionar el acceso a servicios informáticos en la universidad pública de la región Cusco?	**GENERAL** Determinar si el diseño del modelo de identidad digital basado en el programa TIER de internet2 influye en la gestión de acceso a servicios informáticos en universidades públicas de la región Cusco. **OBJETIVOS ESPECIFICOS** a) Determinar si el diseño del modelo de identidad digital basado en el programa TIER de internet2 influye en la gestión del repositorio de datos para acceder a los servicios informáticos en universidades públicas de la región Cusco. b) Determinar si el diseño del modelo de identidad digital basado en el programa TIER de internet2 influye en la gestión de la autenticación y autorización de usuarios para el acceso a servicios informáticos de las universidades públicas de la región Cusco. c) Determinar en qué medida los usuarios adoptan el modelo de identidad digital, basado en el programa TIER de internet2, para gestionar el acceso a servicios informáticos en la universidad pública de la región Cusco.	**GENERAL** El diseño del modelo de identidad digital basado en el programa TIER de internet2, influye positivamente en la gestión de acceso a servicios informáticos en universidades públicas de la región Cusco. **HIPOTESIS ESPECIFICAS** a) El diseño del modelo de identidad digital basado en el programa TIER de internet2, permitirá una gestión eficiente del repositorio de datos para acceder a los servicios informáticos en universidades públicas de la región Cusco. b) El diseño del modelo de identidad digital basado en el programa TIER de internet2, influye significativamente en la gestión de la autenticación y autorización de usuarios para el acceso a servicios informáticos de las universidades públicas de la región Cusco. c) El modelo de identidad digital, basado en el programa TIER de internet2, es factible de ser adoptado por los usuarios para gestionar el acceso a servicios informáticos en la universidad pública de la región Cusco.	**MODELO DE IDENTIDAD DIGITAL BASADO EN EL PROGRAMA TIER DE INTERNET2** - Capacidad de inicio de sesión unificado - Capacidad de soporte del protocolo SSO y SAML - Capacidad de disponer funciones de proveedor de identidad - Capacidad de disponer funciones de proveedor de servicios - Capacidad de disponer de funciones de un servicio de descubrimiento - Capacidad para mantener automáticamente grupos - Capacidad para almacenar datos de grupos. **ACCESO A LOS SERVICIOS INFORMÁTICOS** - Proporción de tiempo requerido para el acceso a los sistemas informáticos - Disponibilidad de seguridad y confiabilidad de los datos al acceder a los sistemas informáticos - Proporción de la cantidad de cuentas de usuario para acceder a los sistemas informáticos - Disponibilidad del servicio de recuperación de contraseñas - Existencia de un procedimiento para reportar el seguimiento y control de acceso	**Enfoque:** Cuantitativo **Tipo:** Aplicada **nivel:** Correlacional Cuasi experimental **Diseño** No Experimental con pre-test y post-test de un solo grupo **Técnicas** Encuesta **Instrumento** cuestionario **Población:** Directores de las Escuelas Profesionales de la UNSAAC **Muestra:** Probabilística cuyo resultado es 38 personas.

ANEXO 2. ENCUESTA

UNIVERSIDAD NACIONAL FEDERICO VILLAREAL
ESCUELA UNIVERSITARIA DE POSGRADO

"MODELO DE IDENTIDAD DIGITAL BASADO EN EL PROGRAMA TIER DE INTERNET2 PARA GESTIONAR EL ACCESO A LOS SERVICIOS INFORMÁTICOS EN UNIVERSIDADES PÚBLICAS DE LA REGIÓN CUSCO

ENCUESTA

Objetivo. - Evaluar la adopción del modelo de identidad digital basado en el programa TIER de Internet2 para el acceso a los servicios informáticos de la Universidad.

1	El proceso a seguir para acceder a los servicios informáticos de la universidad es complejo y difícil de seguir.	○	○	○	○	○	El proceso a seguir para acceder a los servicios informáticos de la universidad es simple y fácil de seguir.
2	Creo que este procedimiento reduciría el tiempo requerido para acceder a los servicios informáticos de la universidad	○	○	○	○	○	Creo que este procedimiento aumentara el tiempo requerido para acceder a los servicios informáticos de la universidad
3	En general, el procedimiento de acceso a los servicios informáticos es difícil de usar	○	○	○	○	○	En general, el procedimiento de acceso a los servicios informáticos es fácil de usar
4	Me parecieron claras y fácil de entender las instrucciones para acceder a los servicios informáticos de la universidad	○	○	○	○	○	Me parecieron confusas y difíciles de entender las instrucciones para acceder a los servicios informáticos de la universidad
5	En general, me parece útil el procedimiento para acceder a los servicios informáticos de la universidad	○	○	○	○	○	En general, NO me parece útil el procedimiento para acceder a los servicios informáticos de la universidad
6	Me parece difícil de aprender el procedimiento para acceder a los servicios informáticos de la universidad	○	○	○	○	○	Me parece fácil de aprender el procedimiento para acceder a los servicios informáticos de la universidad
7	Usaré este procedimiento en lo sucesivo para acceder a los servicios informáticos de la universidad	○	○	○	○	○	Definitivamente no usaré este procedimiento en lo sucesivo para acceder a los servicios informáticos de la universidad
8	Me parece que este procedimiento NO es eficiente para acceder a los sistemas informáticos de la universidad	○	○	○	○	○	Me parece que este procedimiento es eficiente para acceder a los sistemas informáticos de la universidad
9	Me resulto difícil en algunos casos seguir el procedimiento de acceso a los servicios informáticos de la universidad	○	○	○	○	○	Me resulto fácil en todos los casos seguir el procedimiento de acceso a los servicios informáticos de la universidad
10	En general pienso que el procedimiento NO es seguro para acceder a los servicios informáticos de la universidad	○	○	○	○	○	En general pienso que el procedimiento es seguro para acceder a los servicios informáticos de la universidad
11	El uso de este procedimiento garantiza un acceso perfecto a los servicios informáticos de la universidad	○	○	○	○	○	El uso de este procedimiento NO garantiza un acceso perfecto a los servicios informáticos de la universidad
12	Será fácil para mí llegar a ser hábil en el uso de este procedimiento para acceder a los servicios informáticos de la universidad	○	○	○	○	○	Será difícil para mí llegar a ser hábil en el uso de este procedimiento para acceder a los servicios informáticos de la universidad
13	En general, considero que este procedimiento simplifica los procesos de acceso a los servicios informáticos de la Universidad	○	○	○	○	○	En general, considero que este procedimiento NO simplifica los procesos de acceso a los servicios informáticos de la Universidad
14	Tengo la intención de utilizar este procedimiento en el futuro para acceder a los recursos digitales de la universidad	○	○	○	○	○	No tengo la intención de utilizar este procedimiento en el futuro para acceder a los recursos digitales de la universidad

ENCUESTA SOBRE GESTIÓN DEL ACCESO A LOS SERVICIOS INFORMÁTICOS

Objetivo. - Evaluar la gestión del acceso a los servicios informáticos de la Universidad por los directores de las escuelas profesionales.

N°	Pregunta	Alternativas
1	El procedimiento actual para acceder a todos los principales sistemas informáticos requiere demasiado tiempo	( ) Si ( ) No
2	Considera que el procedimiento actual para el acceso a los principales sistemas informáticos es seguro y confiable	( ) Si ( ) No
3	¿Utiliza varias cuentas de usuario o contraseñas para el acceso a cada uno de los principales sistemas informáticos?	( ) Si ( ) No
4	Es eficiente el servicio de recuperación de cuentas de usuario y reseteo de contraseñas para el acceso a los principales sistemas informáticos	( ) Si ( ) No
5	El procedimiento actual de acceso a los sistemas informáticos proporciona un reporte de seguimiento o auditoria del control de acceso	( ) Si ( ) No

ANEXO 3. Resultados de la aplicación del instrumento

Sujeto	Percepción de eficiencia del repositorio				Percepción de eficiencia de la Autenticación					Percepción de eficiencia de la Autorización de Permisos				
	P1	P3	P4	P6	P9	P2	P5	P8	P10	P11	P13	P7	P12	P14
1	1	2	1	2	1	4	3	5	3	4	4	5	4	5
2	5	5	5	5	5	4	4	1	4	5	5	5	5	5
3	5	3	2	2	2	3	3	3	3	3	2	3	4	2
4	5	5	5	5	5	5	5	5	5	1	5	5	5	5
5	4	3	5	4	3	5	5	4	4	4	4	5	4	4
6	2	2	3	4	3	5	5	4	3	4	5	5	5	5
7	4	2	4	4	2	5	4	4	3	4	5	5	2	5
8	3	4	3	1	1	4	4	2	2	4	5	5	5	4
9	4	4	5	5	5	4	4	4	4	4	4	4	5	4
10	3	3	2	5	3	5	5	4	5	5	5	3	4	4
11	3	4	4	5	1	5	3	5	2	2	5	3	4	4
12	5	5	5	5	5	5	5	5	5	5	5	5	5	5
13	2	2	2	2	3	5	3	5	2	5	5	5	5	5
14	5	3	5	5	5	5	5	5	5	5	5	5	5	5
15	5	5	4	4	4	5	2	3	5	1	3	5	5	4
16	4	5	3	4	1	4	3	2	5	4	4	3	5	5
17	3	4	5	4	4	5	4	4	5	5	3	5	5	5
18	3	5	1	2	5	2	2	4	5	4	1	3	2	3
19	3	4	4	4	5	4	5	5	5	4	5	4	3	5
20	5	5	2	5	5	5	5	5	2	5	5	1	5	5
21	5	3	4	4	5	4	4	5	3	4	5	5	5	5
22	3	4	4	5	2	4	5	1	2	5	4	5	5	4
23	4	5	5	4	4	5	4	4	3	5	5	4	5	5
24	5	5	4	4	4	5	4	3	4	3	5	4	4	5
25	3	4	3	3	2	4	3	4	2	2	2	4	3	4
26	4	5	4	4	4	5	4	3	4	5	5	4	5	5
27	5	5	5	5	5	5	5	2	5	3	5	1	5	5
28	5	5	5	5	5	5	5	3	2	5	5	5	5	5
29	4	5	5	2	5	4	5	2	3	5	4	4	5	5
30	4	4	4	4	3	5	4	4	4	4	4	4	4	4
31	5	3	5	3	5	2	3	4	3	1	3	4	4	5
32	4	3	3	3	4	2	2	2	3	4	2	4	2	4
33	4	4	4	5	4	5	4	3	3	2	4	3	4	5
34	5	5	5	5	5	5	5	5	4	5	5	5	5	5
35	1	4	2	4	4	4	3	4	2	3	4	2	3	4
36	3	2	4	4	5	5	4	5	5	5	5	5	4	5
37	2	3	3	2	4	5	5	5	4	4	5	5	5	5
38	4	3	2	5	3	2	4	5	4	5	5	4	5	4

Resultados de la aplicación del instrumento de gestión del acceso

Tipo (1 Pre-Test; 2 Post-test)	P1	P2	P3	P4	P5
1	0	0	1	0	0
1	0	1	1	0	1
1	0	0	1	1	0
1	0	0	1	0	0
1	0	0	1	1	1
1	0	0	1	1	0
1	0	1	1	0	1
1	0	0	1	0	0
1	0	0	1	1	0
1	0	1	1	0	1
1	0	0	1	1	1
1	0	0	1	0	0
1	0	0	0	0	0
1	0	1	1	0	1
1	0	0	1	0	0
1	1	1	0	0	0
1	0	1	1	0	1
1	0	0	1	1	0
1	0	0	1	0	0
1	0	1	1	0	1
1	1	1	0	0	0
1	0	0	1	0	0
1	0	0	1	1	0
1	0	1	1	0	1
1	0	0	1	0	0
1	0	0	1	1	0
1	0	1	1	0	1
1	0	0	1	1	0
1	0	0	1	0	0
1	1	1	0	0	0
1	0	0	1	0	0
1	1	1	0	0	0
1	0	1	1	0	1
1	0	0	1	0	0
1	0	0	1	1	1
1	0	1	1	0	1
1	0	0	1	0	0
1	0	1	1	0	1
2	0	1	0	1	1
2	0	1	0	1	1
2	1	1	0	1	0
2	0	0	0	0	1

2	0	1	0	1	1
2	0	1	0	1	0
2	1	0	1	0	0
2	0	1	0	1	0
2	0	1	0	1	1
2	0	1	0	0	1
2	1	1	1	1	1
2	0	0	0	0	0
2	0	0	0	0	0
2	0	1	0	1	1
2	0	1	0	1	1
2	1	0	1	0	0
2	1	1	0	0	0
2	0	1	0	1	1
2	0	1	0	1	0
2	0	1	0	1	1
2	0	1	0	1	0
2	0	1	0	1	1
2	0	1	0	1	1
2	0	1	0	0	1
2	1	0	0	0	0
2	0	1	0	1	1
2	0	1	0	0	1
2	0	1	0	1	0
2	0	0	0	0	0
2	0	1	0	1	0
2	0	0	1	0	0
2	1	0	0	0	1
2	0	1	0	1	1
2	0	1	0	0	0
2	1	0	1	0	0
2	0	1	0	1	1
2	0	0	0	0	0
2	0	1	0	1	1

ANEXO 4. Puntaje asignado por cada sujeto a los constructos

Sujeto	Percepción de eficiencia del repositorio (PER)	Percepción de eficiencia de la Autenticación (PEA)	Percepción de eficiencia de la Autorización de Permisos (PEAP)
1	1,4	3,8	4,7
2	5,0	3,8	5,0
3	2,8	2,8	3,0
4	5,0	4,3	5,0
5	3,8	4,3	4,3
6	2,8	4,3	5,0
7	3,2	4,2	4,0
8	2,4	3,5	4,7
9	4,6	4,0	4,3
10	3,2	4,8	3,7
11	3,4	3,7	3,7
12	5,0	5,0	5,0
13	2,2	4,2	5,0
14	4,6	5,0	5,0
15	4,4	3,2	4,7
16	3,4	3,7	4,3
17	4,0	4,3	5,0
18	3,2	3,0	2,7
19	4,0	4,7	4,0
20	4,4	4,5	3,7
21	4,2	4,2	5,0
22	3,6	3,5	4,7
23	4,4	4,3	4,7
24	4,4	4,0	4,3
25	3,0	2,8	3,7
26	4,2	4,3	4,7
27	5,0	4,2	3,7
28	5,0	4,2	5,0
29	4,2	3,8	4,7
30	3,8	4,2	4,0
31	4,2	2,7	4,3
32	3,4	2,5	3,3
33	4,2	3,5	4,0
34	5,0	4,8	5,0
35	3,0	3,3	3,0
36	3,6	4,8	4,7
37	2,8	4,7	5,0
38	3,4	4,2	4,3

ANEXO 5. Datos utilizados en la prueba piloto

Sujeto	Percepción de eficiencia del repositorio				Percepción de eficiencia de la Autenticación					Percepción de eficiencia de la Autorización de Permisos				
	P1	P3	P4	P6	P9	P2	P5	P8	P10	P11	P13	P7	P12	P14
1	4	4	4	4	3	5	4	4	4	4	4	4	4	4
2	4	3	2	4	3	2	4	4	4	5	5	5	5	4
3	2	3	3	2	4	5	5	5	4	4	5	5	5	5
4	5	5	5	5	5	5	5	5	5	4	5	5	5	5
5	1	4	2	4	4	4	3	4	2	2	4	2	3	4
6	3	2	4	4	5	5	4	5	5	5	5	5	4	5
7	4	4	4	5	4	5	4	3	3	2	4	3	4	5
8	4	3	3	3	4	2	2	2	3	4	2	4	2	4
9	5	3	5	3	5	2	3	4	3	1	3	4	4	5

Puntajes de los Constructos

Sujeto	Percepción de eficiencia del repositorio	Percepción de eficiencia de la Autenticación	Percepción de eficiencia de la Autorización de Permisos
1	3,80	4,17	4,00
2	3,20	4,00	4,67
3	2,80	4,67	5,00
4	5,00	4,83	5,00
5	3,00	3,17	3,00
6	3,60	4,83	4,67
7	4,20	3,50	4,00
8	3,40	2,50	3,33
9	4,20	2,67	4,33