Control de acceso unificado para la gestión de la identidad en un sistema de administración institucional

por

Sydney Javier Domínguez Domínguez

Tesis sometida como requisito parcial para obtener el grado de

MAESTRO EN CIENCIAS Y TECNOLOGÍAS DE SEGURIDAD

Instituto Nacional de Astrofísica, Óptica y Electrónica
Agosto 2022
Tonantzintla, Puebla

Supervisada por:

Dr. José Roberto Pérez Cruz
Dr. Lázaro Bustio Martínez - IBERO

Resumen

Las malas prácticas en la implementación de servicios de TI son comunes en organizaciones públicas y privadas, debido principalmente a la falta de planificación y alineación con los objetivos estratégicos. Estas prácticas fomentan la incompatibilidad y la redundancia, características que pueden convertirse en amenazas de ciberseguridad, como la elevación de privilegios y la suplantación de identidad. Para solucionar estos problemas, en esta tesis se propone un esquema de unificación del control de acceso basado en el principio *single-sign-on*, implementado a través de un gestor de identidades y accesos. Con este desarrollo se logra que los usuarios accedan a varias aplicaciones y servicios con un solo conjunto de credenciales mientras se garantiza la concesión del mínimo privilegio. La factibilidad técnica del esquema propuesto se demuestra mediante un modelo de despliegue, considerando como caso de estudio a los sistemas de TI de la Universidad de Montemorelos. Para el modelo de despliegue se consideró el enclave de recursos descrito en la arquitectura *Zero Trust* (NIST SP 800-207). Finalmente, se desarrolló un modelo de amenazas para evaluar la seguridad de la propuesta y proporcionar información detallada para su implementación.

Abstract

The development of institutional computer systems that is not based on proper design or the use of independent access paradigms, platforms, and policies promotes high heterogeneity and lack of control in unified access to such systems. This, coupled with inadequate maintenance of these systems, can create security gaps and, consequently, losses to the organization. This research proposes a solution to the aforementioned problems through the design of a unified access control scheme for identity management in an institutional computer system.

Índice general

1. Introducción **1**

1.1. Motivación 1

1.2. Descripción del problema 2

1.3. Descripción de la solución propuesta 3

1.4. Objetivos de la investigación 3

1.4.1. Objetivo general 3

1.4.2. Objetivos específicos 4

1.5. Metodología 4

1.6. Organización del documento 5

2. Materiales y métodos **6**

2.1. Redes de confianza cero 6

2.1.1. Arquitectura de Confianza Cero 6

2.1.1.1. Control de acceso 7

2.1.1.2. Sujeto 7

2.1.1.3. Recurso 7

2.1.1.4. Objeto 7

2.1.1.5. Atributos 8

2.1.1.6. Rol 8

2.1.1.7. Reglas 8

2.1.1.8. Políticas 8

2.1.1.9. Punto de Decisión de Políticas 9

2.1.1.10. Motor de políticas 9

2.1.1.11. Administrador de Políticas 9
2.1.1.12. Punto de Aplicación de Políticas 9
2.1.1.13. Listas de acceso 10
2.1.1.14. Control de acceso basado en roles 10
2.1.1.15. Control de acceso basado en atributos 11
2.1.2. Modelos para la implementación de una ZTA 11
2.1.2.1. Modelo de Despliegue basado en Recursos 11
2.1.2.2. Modelo de Despliegue Basado en Enclave 12
2.1.2.3. Modelo de Despliegue Basado en Microsegmentación . . 12
2.1.2.4. Modelo de Despliegue en la Nube con Enrutamiento . . 13
2.2. Migración al modelo de Confianza Cero 14
2.2.1. Evaluación 14
2.2.2. Inventario de datos, aplicaciones, activos y servicios 15
2.2.3. Evaluación y priorización de riesgos 15
2.2.4. Implementación y revisión 15
2.2.5. Modelo de Inicio de Sesión Único 16
2.2.6. Definición de Políticas de Seguridad 16

3. Revisión del estado de la tecnología 18
3.1. Adopción de la ZTA en redes empresariales 18
3.2. Soluciones enfocadas en la autenticación 19
3.3. Control de acceso 20
3.4. Discusión 22

4. Esquema de control de acceso unificado 24
4.1. Caracterización de los sistemas de TI de la UM 25
4.2. Análisis de riesgos y amenazas 30
4.3. Propuesta de políticas de control de acceso 30
4.3.1. Jerarquía de tipos de usuarios y privilegios 31
4.3.2. Políticas de control de acceso 33
4.3.3. Mecanismos de otorgamiento y revocación de privilegios 35

4.4. Modelado del control de acceso unificado 37
4.4.1. Diseño del esquema de unificación de usuarios, permisos y privilegios 38
4.4.2. Esquema de unificación 40
4.4.3. Entorno de pruebas 45
4.4.4. Discusión 45

5. Conclusiones **50**
5.1. Resumen 50
5.2. Contribuciones 51
5.3. Principales limitaciones 52
5.4. Trabajo futuro 53

Bibliografía **55**

Capítulo 1

Introducción

1.1. Motivación

En organizaciones públicas y privadas, la falta de planificación y alineación con los objetivos estratégicos son las principales causas de las malas prácticas en la implementación de servicios de TI [MLDR18]. En muchos casos, se incorporan tecnologías con el único propósito de cumplir funciones específicas, sin establecer un horizonte de proyecto coherente. Estas malas prácticas a menudo desencadenan fallas, relacionadas con incompatibilidades o redundancia, que a menudo se convierten en amenazas de ciberseguridad como la elevación de privilegios y la suplantación de identidad [Lop22].

Un caso concreto de esta problemática se presenta en los sistemas de TI de la Universidad de Montemorelos[1] (UM). Esta Universidad, fundada en 1942, comenzó a implementar servicios de TI a partir de 1990, poniendo en marcha varios desarrollos e innovaciones. No obstante, para la consecución de estos proyectos no se consideró la interacción ni la escalabilidad de los procesos o los sistemas.

Actualmente, en la UM existen tres sistemas para la gestión de los procesos universitarios: 1) un sistema con el material de cursos educativos y seguimiento de clases alumno-maestro llamado *e42*, 2) un sistema para la gestión de documentación académica oficial llamado *Virtual UM* y 3) un sistema de gestión de registros financieros llamado *Financiero*. Además, se han implementado tres subsistemas para facilitar la interconexión de los tres sistemas. La figura 1.1 muestra la estructura actual de los sistemas antes mencionados.

[1] https://www.um.edu.mx/

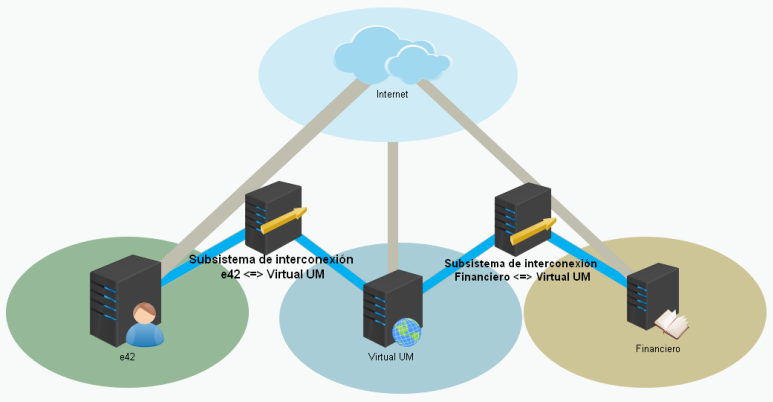

Figura 1.1: Sistemas para la gestión de los procesos universitarios de la UM

Los sistemas de la UM tienen una heterogeneidad elevada debido a que fueron creados para ofrecer funcionalidades puntuales. Por otra parte, fueron desarrollados por diferentes especialistas, empleando diversos paradigmas y plataformas, con políticas de seguridad casi nulas. Esta particularidad ha propiciado que cada uno de los sistemas se gestione independientemente, empleando usuarios y privilegios para cada sistema, promoviendo la multiplicidad de identidades y la colección de privilegios.

1.2. Descripción del problema

Actualmente, cada uno de los sistemas de la UM cuenta con un mecanismo de *login* independiente. Estos mecanismos fueron diseñados para controlar el acceso mediante la validación de tuplas usuario-contraseña. Cada tupla está asociada a cierto nivel de privilegios, establecidos incrementalmente por los administradores. Sin embargo, estos mecanismos de control de acceso presentan diversas vulnerabilidades de seguridad, la mayoría relacionadas con su diseño. Por una parte, estos sistemas carecen de políticas y mecanismos de modificación y revocación de cuentas y permisos, promoviendo la colección de privilegios y la acumulación de cuentas en desuso. Por otra parte, como resultado de la alta heterogeneidad de plataformas y de controles de acceso, existen numerosos usuarios que poseen varias identidades (tuplas usuario-contraseña) con privilegios diversificados.

Para resolver los problemas de multiplicidad de identidades y colección de privilegios, este trabajo de investigación propone un esquema de unificación del control de acceso

que permite a los usuarios iniciar sesión en los diferentes servicios con un conjunto único de credenciales. La unificación del control de acceso centraliza la autenticación, lo que mejora la gestión de usuarios, permisos y privilegios.

1.3. Descripción de la solución propuesta

La unificación del control de acceso propuesta se basa en la adopción del esquema *single-sign-on* (SSO) [Bha23] . El SSO es un esquema de autenticación que permite a los usuarios de una organización acceder a varios sistemas independientes con un único inicio de sesión y un conjunto único de credenciales. Con el objetivo de garantizar una gestión segura de las credenciales de acceso, se implantó un gestor de identidad y acceso (Identity and Access Management, IAM) para centralizar la administración de los accesos y las credenciales [clo23] . La implantación del IAM también permite supeditar y controlar los accesos a los servicios, garantizando la concesión del mínimo privilegio.

Se planteó un modelo de despliegue para describir la integración del esquema de unificación y el IAM con la infraestructura actual de los sistemas de la UM. El modelo de despliegue se basa en el enclave de recursos definido en la arquitectura *Zero Trust* del NIST [NIS20]. El enclave de recursos tiene el propósito de agrupar los recursos (sistemas E42, Virtual UM y Financiero) dentro de un perímetro de confianza cuyo acceso es gestionado por el IAM. Finalmente, la seguridad del esquema propuesto se analizó mediante un modelo de amenazas guiado por el marco de referencia STRIDE [Sho14].

1.4. Objetivos de la investigación

1.4.1. Objetivo general

El objetivo general de este trabajo de investigación es:

> Diseñar un esquema de control de acceso unificado para la gestión de la identidad en un sistema de administración institucional que permita garan-

tizar la concesión del mínimo privilegio y mitigar amenazas asociadas a la suplantación de identidad.

1.4.2. Objetivos específicos

Para dar cumplimiento al objetivo general se proponen los siguientes objetivos específicos:

- Caracterizar la red UM mediante la identificación de sus activos, servicios y vulnerabilidades.
- Diseñar un conjunto de políticas de control de acceso unificado para mitigar efectos de heterogeneidad.
- Diseñar un esquema para la gestión de identidad, basado en las políticas de control de acceso unificado, para garantizar la concesión del mínimo privilegio y evitar al multiplicidad de identidades.

1.5. Metodología

A continuación se presenta la metodología que encausó la investigación para alcanzar los objetivos.

1. **Integración de un inventario de datos, aplicaciones, activos y servicios (DAAS).** Se realizaron entrevistas con los administradores de los sistemas para recopilar información sobre la arquitectura institucional e identificar y caracterizar los elementos del sistema, flujos de datos y las relaciones entre éstos. Con la información recopilada se realizó una clasificación de aplicaciones, servicios y usuarios del sistema.
2. **Ejecución de pruebas de penetración.** Para complementar el DAAS con información sobre vulnerabilidades y posibles vectores de ataque, se realizaron pruebas exploratorias con sistemas automatizados como *Nmap*, *Nessus scanner* y *Acunetix web vulnerability scanner*. Con el resultado, se jerarquizaron las amenazas según su prioridad y sus interacciones con los DAAS.

3. **Definición de políticas de control de acceso.** Basándose en el inventario DAAS, se definió una jerarquía de tipos de usuarios. Consecuentemente, se estableció una jerarquía de privilegios alineada a la jerarquía de usuarios. Por último, se definieron políticas y mecanismos de otorgamiento y revocación selectiva de privilegios.

4. **Definición de los mecanismos de control de acceso unificado.** Mediante el despliegue del sistema IAM WSO2 [referencia requerida]; se estableció un enclave o dominio aislado, que actúa como un perímetro de confianza, para albergar a los sistemas E42, Virtual UM y Financiero. Se implementó un módulo de inicio de sesión, supeditado y controlado por el IAM, para controlar acceso a los sistemas del enclave con un conjunto único de credenciales, generadas dinámicamente a partir de cada *login*.

5. Análisis de la seguridad del esquema propuesto. La seguridad del esquema de unificación del control de acceso se analizó mediante un modelo de amenazas, tomando como referencia el marco STRIDE.

1.6. Organización del documento

Este documento está organizado de la siguiente manera. En el Capítulo 2 se introducen los principales conceptos relacionados con la gestión de la identidad de usuarios, el control de acceso y la arquitectura de red de confianza cero. En el Capítulo 3 se hace una revisión del estado de las tecnologías enfocadas al control de acceso en redes corporativas. El Capítulo 4 presenta el esquema de unificación propuesto así como su análisis de seguridad. Finalmente, las conclusiones y el trabajo futuro se presenta en el Capítulo 5.

Capítulo 2

Materiales y métodos

En esta sección se presentan los elementos teóricos que sustentan esta investigación y que son necesarios para entenderla de manera adecuada. También se explican cómo estos elementos teóricos son empleados en la propuesta y se revisan críticamente sus fortalezas y debilidades.

2.1. Redes de confianza cero

El modelo de red de confianza cero (Zero Trust Network o ZTN) es un modelo de seguridad que requiere una estricta verificación de la identidad de dispositivos y usuarios, independientemente de su ubicación en relación con el perímetro de la red [Fit20]. Al limitar qué partes tienen acceso privilegiado a cada segmento de una red, o cada máquina en una organización segura, el número de oportunidades para que un atacante obtenga acceso a contenido seguro se reduce considerablemente. Una red que implementa el modelo de Confianza Cero se denomina Red de Confianza Cero [Mic23].

2.1.1. Arquitectura de Confianza Cero

La arquitectura de Confianza Cero (ZTA por sus siglas en ingles) adopta un enfoque en el que todos los sujetos se consideran implícitamente no confiables sin importar dónde se encuentren (ya sea interno o externo), que es lo opuesto a cómo funciona la seguridad perimetral. La ZTA obliga a cumplir con el proceso de autenticación y autorización en cada solicitud/transacción, brindando al sistema la capacidad de controlar y ajustar

granularmente el nivel de seguridad requerido para acceder a un recurso en particular [TUI21].

2.1.1.1. Control de acceso

En el contexto de una ZTA, el control de acceso (Access Control, AC) emerge como un componente de vital importancia, ya que constituye el punto de entrada a la red. El control de acceso habilita a los administradores de la organización para registrar, supervisar y limitar el acceso a recursos, interfaces de programación de aplicaciones (API) y sistemas, asegurando que los usuarios adecuados obtengan acceso en el momento oportuno. Este enfoque se sustenta en roles, atributos y en las decisiones discrecionales de los administradores, todo ello adaptado a la necesidad de acceso, ya sea de manera voluntaria u obligatoria.[WSO22a]

2.1.1.2. Sujeto

El término *sujeto* se utiliza para denotar a un ser humano o una entidad no personal (o Non-Personal entity, NPE por su siglas en inglés) que solicita acceso a un objeto o recurso. El sujeto representa la entidad que solicita realizar una operación sobre el objeto o recurso [NF20].

2.1.1.3. Recurso

Un *recurso* abarca cualquier objeto, entidad o información salvaguardada mediante el sistema de control de acceso. Se trata de elementos tangibles o físicos, como archivos de datos, bases de datos, dispositivos de hardware, aplicaciones de software, redes, sitios web, entre otros [NF20].

2.1.1.4. Objeto

Un *objeto*, a veces conocido como *objeto lógico*, constituye una entidad que requiere salvaguardarse contra el uso no autorizado. Al igual que los sujetos, cada objeto posee un conjunto de atributos destinados a describirlo e identificarlo. Este término abarca aspectos más abstractos o conceptuales, como funciones, procesos o datos lógicos. Y

pueden englobar elementos de naturaleza más abstracta, como funciones, procesos o datos lógicos [NF20].

2.1.1.5. Atributos

Hay características o atributos de un sujeto, como el nombre, la fecha de nacimiento y la dirección del hogar, pueden formar una identidad única que distingue a esa persona. Estas características, conocidas como atributos de sujeto u objeto, son igualmente relevantes para cada recurso. Cada recurso cuenta con un conjunto de atributos que se emplean para gestionar su acceso, abarcando aspectos como el propietario del recurso, los permisos de acceso y su ubicación. Estos atributos desempeñan un papel esencial en el establecimiento de políticas de seguridad que definen quiénes tienen acceso al recurso y en qué circunstancias [NF20].

2.1.1.6. Rol

El *rol* se define por medio de una función laboral o puesto de trabajo al que se pueden asignar personas u otras entidades del sistema en un sistema [NF20].

2.1.1.7. Reglas

En el contexto de control de acceso y seguridad de la información, las *reglas* son directrices específicas y detalladas que complementan las políticas de seguridad en una organización. Mientras que las políticas establecen los principios generales y las normas de alto nivel, las reglas proporcionan instrucciones más específicas sobre cómo se deben implementar esas políticas en situaciones prácticas [NF20].

2.1.1.8. Políticas

Las políticas, las reglas y las relaciones, rigen el comportamiento permitido dentro de una organización según los privilegios de los sujetos y cómo se protegerán los recursos u objetos bajo qué condiciones ambientales. Las políticas generalmente se escriben desde la perspectiva del objeto que necesita protección y los privilegios disponibles para los sujetos [NF20].

2.1.1.9. Punto de Decisión de Políticas

En términos generales, un Punto de Decisión de Política (Policy Decision Point, PDP por sus siglas en inglés) es el módulo que toma decisiones sobre si un sujeto (usuario, proceso, aplicación, dispositivo, etc.) está autorizado para acceder a un objeto (recurso, archivo, base de datos, red, etc.) en un sistema de información. El PDP utiliza una serie de reglas y políticas de seguridad predefinidas para determinar si un sujeto puede o no acceder a un objeto. El PDP esta dividido en dos componentes lógicos el motor de políticas y el administrador de políticas [NIS20], en la figura 2.1 se muestra la relación básica entre los componentes lógicos y sus interacciones.

2.1.1.10. Motor de políticas

En el contexto de control de acceso, el Motor de políticas (PE, por sus siglas en inglés), como parte del PDP, toma la decisión final sobre si otorgar acceso a un recurso para un sujeto dado. Utiliza políticas empresariales y entrada externa como parámetros para un algoritmo de confianza, decidiendo aprobar, denegar o revocar el acceso. Es la entidad central en la toma de decisiones, evaluando políticas y factores externos para determinar el acceso [NIS14].

2.1.1.11. Administrador de Políticas

El Administrador de políticas (PA, por sus siglas en inglés) es el componente encargado de la administración de políticas. Es responsable de definir, gestionar y mantener las políticas de control de acceso que se aplican en el PDP. Este componente determina qué acciones están permitidas o prohibidas en función de las políticas de seguridad establecidas por la organización. El PA depende de las decisiones tomadas por el PE. Si el PE aprueba una sesión, el PA configura los PEP para permitir que comience. [NIS14].

2.1.1.12. Punto de Aplicación de Políticas

Los PEP son componentes que ejecutan las decisiones tomadas por el PDP. Son responsables de hacer cumplir las políticas de control de acceso. Se colocan en varios puntos de un sistema para controlar el acceso. Interceptan solicitudes y hacen cumplir

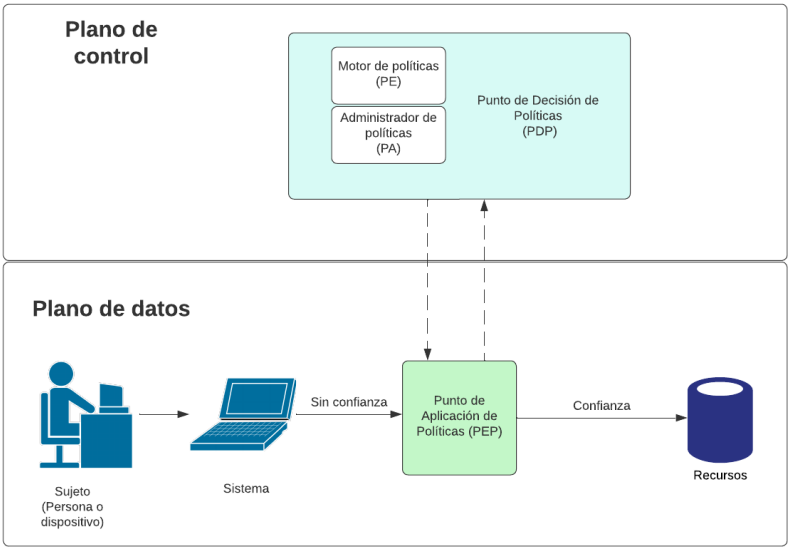

Figura 2.1: Componentes lógicos de Zero Trust Architecture

decisiones basadas en políticas definidas por el PDP. Los PEP se comunican con el PDP, enviando solicitudes para la toma de decisiones y, una vez que se toma una decisión, la hacen cumplir[NIS14].

2.1.1.13. Listas de acceso

Una estrategia para llevar acabo el control de acceso es mediante el uso de las listas de acceso (Access Control Lists, o ACL por sus siglas en inglés). Las ACL controlan el acceso permitiéndolo y/o denegándolo a través de reglas configuradas previamente. Las reglas comúnmente usan las direcciones IP de los clientes, pero también pueden configurarse para filtrar puertos o servicios [HFK+13].

2.1.1.14. Control de acceso basado en roles

El control de acceso se basa en varios aspectos entre ellos los roles. El modelo de control de acceso basado en roles (Roles Based Access Control, o RBAC por su siglas en inglés) trabaja con el atributo de rol. Emplea roles predefinidos que llevan un conjunto específico de privilegios asociados a ellos y a los que se asignan sujetos. En el momento de una solicitud de acceso, el mecanismo de control de acceso evalúa el rol asignado al

sujeto que solicita el acceso y el conjunto de operaciones que este rol está autorizado a realizar en el objeto antes de presentar y hacer cumplir una decisión de acceso [HFK+13].

2.1.1.15. Control de acceso basado en atributos

Otro elemento clave en la implementación del control de acceso es el *atributo*. Este término se relaciona con el Modelo de Autorización basado en Atributos (Atributes Based Access Control, o ABAC por sus siglas en inglés), que es una metodología de control de acceso que se centra en la evaluación de atributos o características específicas en lugar de roles predefinidos para determinar si un usuario debe tener acceso a ciertos recursos [NIS14]. El propósito fundamental de ABAC es garantizar la protección de objetos (como datos, dispositivos de red y otros recursos de tecnología de la información) de acciones y usuarios no autorizados. Esto se logra al considerar si los atributos del usuario y las características del recurso cumplen con las políticas de seguridad definidas por la organización. En otras palabras, el ABAC se enfoca en verificar si un usuario tiene las características *aprobadas* que se ajustan a las políticas de seguridad de la organización antes de permitir el acceso [Cas20].

2.1.2. Modelos para la implementación de una ZTA

Siguiendo el modelo Zero Trust, a continuación se muestran modelos de despliegue, los cuáles se refieren a diferentes opciones en como se puede desplegar una arquitectura Zero Trust.

2.1.2.1. Modelo de Despliegue basado en Recursos

El modelo de despliegue basado en recursos es el más sencillo de implementar y el menos complejo. Este modelo se compone de un agente de usuario (PEP) incorporado en el sistema del sujeto. Además, se incluye un PEP que se implementa directamente frente al recurso. Por último, se encuentra un PDP encargado de gestionar el control de acceso desde el momento en que el usuario solicita acceder al recurso. Este modelo garantiza que todas las comunicaciones de red entre los dispositivos de los usuarios y

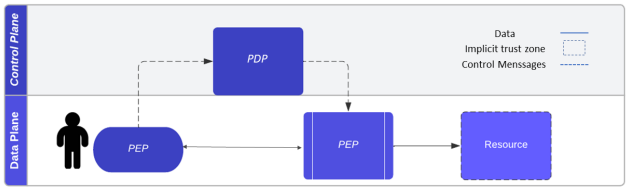

Figura 2.2: Modelo de despliegue basado en recursos

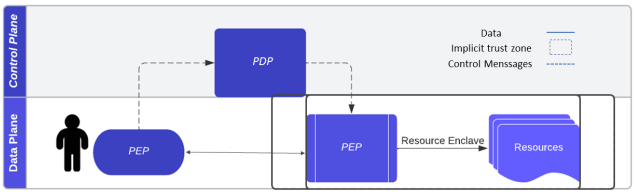

Figura 2.3: Modelo de despliegue basado en enclave

el recurso de destino estén cifradas y que se apliquen las políticas de control de acceso [GC21]. La Figura 2.2 describe este modelo.

2.1.2.2. Modelo de Despliegue Basado en Enclave

El siguiente modelo se centra en unificar el acceso a múltiples recursos por medio de un PEP. El PEP está frente a múltiples recursos, denominado *enclave de recursos*. Este modelo es útil cuando la zona de confianza implícita contiene múltiples recursos en red que se comunican entre sí. La Figura 2.3 describe este modelo.

Es fundamental que en este modelo el enclave de recursos se ejecute únicamente en una red privada que esté bajo el control de la empresa. Además, una ventaja de este modelo es que no necesita implementar ningún software adicional en los recursos, simplificando su administración y también evita la mayoría de los conflictos técnicos y/o políticos con las aplicaciones y los propietarios de las aplicaciones [GC21].

2.1.2.3. Modelo de Despliegue Basado en Microsegmentación

Este modelo se centra en el caso de uso de servidor a servidor, denominado *microsegmentación*. Los recursos se consideran los sujetos principales en torno a los cuales se deben crear y hacer cumplir las políticas. Este modelo es similar al modelo basado en recursos, con la diferencia de que los recursos son también sujetos (identidades auten-

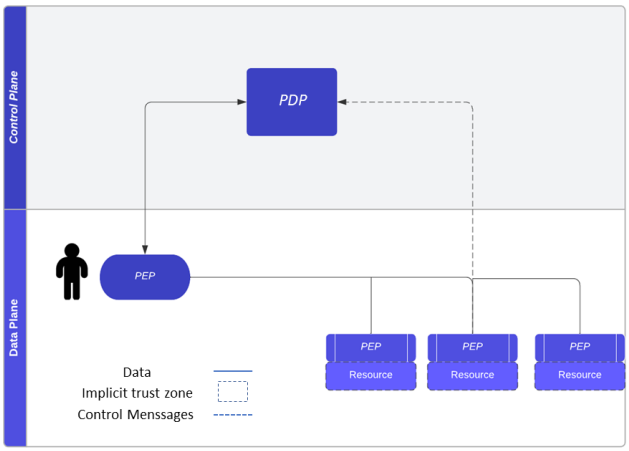

Figura 2.4: Modelo de despliegue basado en Microsegmentación

ticadas). Esto implica que la forma en que el PEP y PDP autenticaban únicamente al usuario se usa para autenticar al servidor. Esto tiene implicaciones significativas en el modelo de políticas y las capacidades de aplicación de PEP, así como en las capacidades de descubrimiento y visualización de recursos que las implementaciones comerciales suelen proporcionar [GC21]. La Figura 2.4 representa este modelo.

2.1.2.4. Modelo de Despliegue en la Nube con Enrutamiento

Este modelo de despliegue se ofrece comúnmente como servicio de proveedores comerciales. Se implementan PEPs en los enclaves de recursos empresariales. Estos PEPs locales funcionan como conectores hacia PEPs en la nube, que actúan como el punto de entrada a la red empresarial. Cuando un sujeto busca comunicarse con un recurso, primero se autentica con el PDP, luego su tráfico se dirige a uno de los PEPs basados en la nube. Desde aquí, el tráfico fluye a través de los PEPs dentro de la nube hasta alcanzar el PEP conectado al enclave de recursos de destino. Este enfoque proporciona un acceso seguro y eficiente a los recursos empresariales a través de una infraestructura en la nube bien gestionada y altamente disponible [GC21]. La Figura 2.5 describe este modelo.

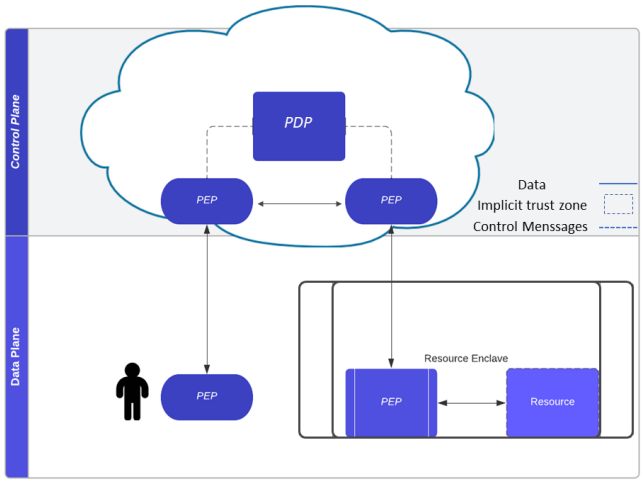

Figura 2.5: Modelo de despliegue en la nube con enrutamiento

2.2. Migración al modelo de Confianza Cero

Ya habiendo explicado los conceptos de Zero Trust y la importancia que tiene este modelo a los problemas de red en las organizaciones es importante saber por dónde comenzar a trabajar para adoptar este modelo.

La migración a Zero Trust es un proceso continuo y de múltiples pasos que no se puede lograr reemplazando todas las herramientas y equipos por otros nuevos. Para realizar la migración basada en el perímetro existente, hay varios pasos y factores a tener en cuenta [TUI21]:

2.2.1. Evaluación

El primer paso para llevar acabo la migración hacia un enfoque Zero Trust es la evaluación (o *assessment*). Este paso implica la identificación de los actores y los activos de la empresa, incluidas las entidades humanas y no personales. Debe ser capaz de identificar y monitorear tanto los activos de propiedad de la empresa como los que no lo son, incluidos el hardware y los artefactos digitales (por ejemplo, software y certificados digitales). Deben descubrirse las relaciones entre las cargas de trabajo, las redes, los dispositivos y los usuarios. La finalidad de este paso es identificar datos sobre la actividad de acceso y autorización dentro de la arquitectura [TUI21].

2.2.2. Inventario de datos, aplicaciones, activos y servicios

Parte fundamental de la etapa de evaluación es la integración de un inventario de datos, aplicaciones, activos y servicios (DAAS). Para el DAAS se deben contemplar todos aquellos elementos que forman parte del sistema en cuanto al hardware (tales como equipos de cómputo: servidores, computadores de escritorio, portátiles, clúster, etc.), equipos de comunicaciones, equipos eléctricos y periféricos (tales como: impresoras, escáneres, plotters, etc.) También se deben considerar los bienes inmateriales que proporcionan los datos, instrucciones, etc. En resumen, el DAAS incluye todos los componentes de la infraestructura de una organización. Realizar un inventario DAAS permite tener en cuenta cada elemento de la red al definir una superficie de protección [Joi22].

2.2.3. Evaluación y priorización de riesgos

Una vez concluida la etapa de evaluación y el inventario DAAS, la organización debe proceder a la evaluación y priorización de riesgos. Esto implica realizar una jerarquización por prioridad. La organización puede decidir comenzar a migrar su primer proceso comercial que tiene un riesgo relativamente bajo a Zero Trust y más tarde con el proceso comercial más crítico. Una vez que se ha seleccionado el proceso de negocio candidato, entonces es el momento de crear políticas para este proceso candidato. En este paso se deben identificar todos los recursos utilizados o afectados por el proceso del candidato. Esto permite que la empresa sepa con precisión qué recursos están involucrados en el proceso de migración [TUI21].

2.2.4. Implementación y revisión

Una vez que se han identificado los recursos involucrados en el proceso de migración, llega el momento de la implementación. Diseñado el conjunto de políticas e identificado qué recursos están involucrados en el proceso de migración, resta la implementación de un nuevo flujo de trabajo empresarial. Este, basado en Zero Trust Architecture (ZTA), debe seguir las políticas de seguridad desarrolladas en las fases anteriores. Esta etapa se asocia con el proceso de registro y monitoreo. El análisis del resultado permite a

la organización asegurarse de que el nuevo proceso comercial basado en ZTA funcione de manera efectiva. se recopilan los resultados, incluidos los errores durante las fases anteriores. Con cada migración, la empresa/organización gana más confianza y puede elegir un flujo de trabajo más desafiante para su próximo ciclo de migración [TUI21].

2.2.5. Modelo de Inicio de Sesión Único

El inicio de sesión único (Single Sign-On,SSO por sus siglas en inglés) ocurre cuando un usuario ingresa sus credenciales para iniciar sesión en una aplicación y, al mismo tiempo, se inicia sesión en otras aplicaciones conectadas sin tener que ingresar sus credenciales nuevamente. Esto también elimina la necesidad de tener y recordar diferentes credenciales para aplicaciones diferentes. Esto minimiza las superficies de ataque y se aplica un enfoque de *Zero Trust* para todos los usuarios [WSO22b].

2.2.6. Definición de Políticas de Seguridad

Las políticas de seguridad son un conjunto de reglas que definen cómo se debe proteger la información y los sistemas informáticos. Estas políticas deben ser claras y concisas, además de ser fáciles de entender para una aplicación consistente.

El lenguaje SAML (Security Assertion Markup Language) es un estándar de código abierto basado en XML para el intercambio de datos de autenticación y autorización. SAML se puede utilizar para implementar políticas de seguridad, como el inicio de sesión único (SSO), la autorización basada en roles y la administración de identidades [WSO22b]. La especificación de SAML define tres roles principales:

- El principal: normalmente, este es el usuario que intenta acceder a un recurso o servicio protegido por un proveedor de servicios.
- El proveedor de identidad (identity provider): un proveedor de identidad (IdP) es responsable de autenticar a los usuarios y emitir afirmaciones que incluyen decisiones de autenticación/autorización y atributos de usuario.
- El proveedor de servicios(service provider): un proveedor de servicios (SP) consume las afirmaciones emitidas por el proveedor de identidad y proporciona servicios

a los principales. El escenario de uso principal cubierto por SAML es cuando el principal (el usuario) solicita acceso a un recurso o servicio del proveedor de servicios. Luego, el proveedor de servicios utiliza SAML para comunicarse con el proveedor de identidad y obtener una afirmación de identidad. El proveedor de servicios toma la decisión de control de acceso en función de esta afirmación.

Capítulo 3

Revisión del estado de la tecnología

En este capítulo se revisan algunos trabajos publicados, relacionados con la implementación de redes de confianza cero. Las temáticas de estos trabajos son: Modelo ZTA y la migración empresarial, autenticación y el control de acceso.

3.1. Adopción de la ZTA en redes empresariales

Las arquitecturas basadas en el modelo de Confianza Cero brindan un nivel de protección elevado a las organizaciones, pues desde su concepción y diseño consideran a todo usuario como malicioso. Este enfoque, si se maneja de una manera adecuada, reduce los problemas de seguridad que se pudieran presentar. Sin embargo, su implementación requiere de un trabajo de diseño fuerte y de conocimiento previo de todas las situaciones que pudieran ocurrir.

En un estudio publicado por Teerakanok et al. [TUI21] se destacan los puntos fuertes y beneficios que trae a las organizaciones adoptar la ZTA y se enfoca cuando una empresa quiere adoptar este modelo y se plantea la migración.

De los puntos esenciales e importantes presentado por Teerakanok et al. esta el cómo realizar la migración a un esquema de seguridad basado en ZT, comenzando con la evaluación y priorización de riesgos. Lo anterior se traduce en elegir el proceso con el cual se comenzará la migración. Posteriormente se deberán crear las políticas e implementarlas, lo cual conlleva a las revisiones de los resultados parciales que se van obteniendo. Además de atender y desarrollar los pasos para realizar la migración. También, se abordan aspectos cruciales para la migración, como los procedimientos de cambios, la gestión de

riesgos, la gestión de identidad, las leyes y regulaciones, entre otros. también los puntos a considerar para la migración como los procedimiento de cambios, gestión de riesgos, gestión de identidad, leyes y regulaciones entre otros.

3.2. Soluciones enfocadas en la autenticación

Yuanjun y Hongrui [YH19] proponen un sistema de control de acceso que permite la autenticación de usuarios que comprende 3 módulos. El primer módulo permite al usuario identificarse ante el servidor de autenticación. El segundo módulo implementa un terminal móvil que detecta al usuario y genera un token de acceso después de autenticarse. El tercer módulo, implementado en un servidor de autorización, proporciona un token y otros identificadores usados para seleccionar el recurso al que se accederá. Siguiendo el enfoque planteado, se logra una gestión concentrada para diferentes recursos de control de acceso y demandas de autenticación.

Zhixian et al. [ZGS+20] desarrollaron un sistema para la autenticación basada en un esquema ZT. El sistema comprende un punto de servicio (interface front-end), un modulo central de autenticación, un motor de verificación y un módulo de gestión de registros. En el modulo frontal el usuario se autentica y genera una solicitud de servicio, la solicitud pasa a un modulo de verificación para comprobar su validez, que si es válida entonces pasa al modulo de gestión de registros para recibir y cifrar la información, y luego traspasarla al módulo de servicio que el usuario desea acceder.

Siguiendo un enfoque más teórico, Ethan et al. [ELS+22] describieron sistemas y métodos para gestionar la autenticación siguiendo el modelo de ZT. Dentro de los métodos que analizaron, se incluyen aquellos basados en funciones hash para crear e intercambiar llaves públicas y privadas además, para generar un token que permita autorizar y autenticar los mensajes. En este contexto se debe entender por mensajes a las solicitudes de autenticación y acceso.

3.3. Control de acceso

En [SSAV19] se describe un control de acceso basado en atributos (ABAC). Esta propuesta captura esos requisitos como una política y modelo administrativo basado en roles y luego presenta una metodología que utiliza un enfoque basado en puntos fijos para verificar las propiedades de seguridad (como la seguridad y la vida) de esas políticas en presencia del modelo administrativo. Por último, se analiza el impacto de ciertos mecanismos de seguridad del modelo administrativo. Los resultados experimentales demuestran que el enfoque propuesto es escalable y eficaz.

En la patente presentada en [ROSS22] se discute un método para el acceso sin inicio de sesión por medio de credenciales de confianza (cookies, certificados y otros conjuntos de datos). Este tipo de datos pueden ser almacenados en un dispositivo para acceder a los servicios y adaptarse a ciertos requerimientos de seguridad.

Un trabajo muy similar es Passkeys de Google [Goo23], un sistema de inicio de sesión sin contraseña que ofrece una alternativa más segura y fácil. Los usuarios pueden acceder a aplicaciones y sitios web mediante un sensor biométrico o un PIN, cumpliendo con los requisitos de autenticación multifactor en un solo paso. Los Passkeys reemplazan tanto las contraseñas como los códigos OTP, proporcionando una protección robusta contra ataques de phishing. Además, al ser estandarizados, ofrecen una experiencia sin contraseña en todos los dispositivos del usuario y en diferentes navegadores y sistemas operativos. Estos passkeys se gestionan a través de la infraestructura del sistema operativo, permitiendo la creación, copia de seguridad y disponibilidad para las aplicaciones del sistema. En Android, se almacenan en el Administrador de contraseñas de Google, sincronizándose entre los dispositivos del usuario. Los passkeys se cifran de manera segura y solo el usuario puede acceder y utilizar estos secretos, protegiéndolos contra accesos no autorizados.

Considerando los desafíos relacionados con el desarrollo y la seguridad en dispositivos de IoT, el artículo [RCPLC+15] sugiere la implementación de un sistema de acceso administrado por el usuario. Este sistema busca ofrecer un enfoque unificado para el control de acceso en una arquitectura heterogénea que involucra dispositivos IoT y agentes inteligentes.

En el artículo [YBJ+22], se describe un dispositivo diseñado conforme al modelo ZT. Este dispositivo sirve como punto de entrada y salida, incorporando una arquitectura de seguridad de doble aislamiento a nivel de hardware. A través de políticas de control de acceso basadas en listas blancas, el filtrado de protocolos y la implementación de un canal dedicado, se refuerza la seguridad de ZT para resistir ataques externos. Lo anterior contribuye a mejorar la seguridad general del sistema ZT.

En [TY12] se presenta un dispositivo de control de acceso que incluye una unidad que genera una relación entre usuarios y el recurso al que el usuario desea acceder y una unidad que evalúa el acceso solicitado.

En el ámbito de la gestión de identidad y control de acceso, WSO2 Identity Server [WSO22a] destaca como una solución de código abierto fundamental. Funcionando como proveedor de identidad y servicios, desempeña un papel integral en la autenticación y autorización de usuarios. Su capacidad para unificar los mecanismos de control de acceso garantiza coherencia en toda la infraestructura, mientras que su flexibilidad permite la definición de políticas basadas en roles, atributos y otros criterios. La integración con sistemas institucionales y la emisión segura de tokens de acceso aseguran la consistencia y la seguridad, haciendo de WSO2 Identity Server una pieza clave en la implementación de modelos de seguridad avanzados, como el enfoque Zero Trust, en entornos institucionales.

Existen varias alternativas al que pueden utilizarse como herramientas de control de acceso. A continuación, se describen algunas de estas alternativas, junto con sus pros y contras.

Keycloak [Key21]: Keycloak es una herramienta de código abierto que se utiliza para gestionar la autenticación y la autorización de usuarios en aplicaciones web y servicios. Algunos de los pros de Keycloak son que es fácil de instalar y configurar, tiene una interfaz de usuario intuitiva y se integra bien con otras herramientas de código abierto como Docker y Kubernetes. Uno de los contras de Keycloak es que puede ser menos escalable que otras soluciones comerciales.

Okta [Okt23b]: Okta es una solución comercial de gestión de identidades que se utiliza para la autenticación y autorización de usuarios en aplicaciones web y servicios. Algunos de los pros de Okta son que tiene una interfaz de usuario intuitiva, es fácil de

usar y es muy escalable. Uno de los contras de Okta es que puede ser más costoso que algunas soluciones de código abierto.

Auth0 [Okt23a]: Auth0 es una solución comercial de gestión de identidades que se utiliza para la autenticación y autorización de usuarios en aplicaciones web y servicios. Algunos de los pros de Auth0 son que tiene una interfaz de usuario intuitiva, es fácil de usar y se integra bien con otras herramientas de código abierto como Docker y Kubernetes. Uno de los contras de Auth0 es que puede ser más costoso que algunas soluciones de código abierto.

Gluu [Inc23]: Gluu es una herramienta de código abierto que se utiliza para la gestión de identidades y el control de acceso. Algunos de los pros de Gluu son que es fácil de instalar y configurar, es altamente escalable y es muy personalizable. Uno de los contras de Gluu es que puede ser menos intuitivo que otras soluciones comerciales.

WSO2 Identity Server [WSO22a]: es una buena herramienta de código abierto para la gestión de identidades y el control de acceso, para la migración a un modelo de Zero Trust, Algunos de los pros es que como solución se somete a pruebas rigurosas de seguridad y se actualiza regularmente para proteger contra vulnerabilidades conocidas, es altamente escalable e integrable con sistemas existentes. Además es altamente configurable y se integra fácilmente con sistemas existentes. Algunos de sus contras es que como es altamente configurable su configuración se vuelve compleja, lo mismo en su curva de aprendizaje, además que es una plataforma que requiere una cantidad significativa de recursos de hardware.

3.4. Discusión

En general, luego de la revisión del estado de la técnica realizada, se aprecia la relevancia del tema de investigación propuesto en esta tesis al tomar estos documentos sobre la autenticación y el acceso como parte esencial en la seguridad hoy en día, de los puntos resaltantes en estos trabajos son: 1) como realizar una migración exitosa al modelo de seguridad ZT, 2) que métodos y estrategias se han desarrollado hoy en día para realizar autenticación segura en sistemas donde no era un punto prioritario

inicialmente, y por ultimo, 3) los mecanismos existentes para dar acceso correcto a los clientes.

Capítulo 4

Esquema de control de acceso unificado

En esta sección se abordan los diversos aspectos relacionados con el control de acceso en los sistemas de Tecnologías de la Información (TI) de la Universidad de Montemorelos (UM). Se busca establecer un enfoque coherente y eficiente para gestionar el acceso a los recursos y servicios de la universidad, garantizando la seguridad y protección adecuada de la información y los activos digitales.

En primer lugar, se presenta una caracterización exhaustiva de los sistemas de TI de la UM. Esta caracterización incluye una descripción detallada de la arquitectura de TI, la infraestructura de red, los sistemas de información, las aplicaciones, y los diferentes servicios digitales utilizados en la institución. Este análisis permite identificar los activos digitales críticos y los puntos de acceso que deben ser protegidos de manera más rigurosa.

En un segundo apartado se presentan los resultados del análisis de riesgos y amenazas. En ese análisis se evaluaron los posibles escenarios de riesgo y se identificaron las amenazas potenciales que podrían afectar la seguridad de los sistemas de la UM.

Basándose en los resultados del análisis de riesgos y amenazas, se diseñaron políticas y mecanismos de control de acceso adecuados para mitigar los riesgos identificados. Se definieron un conjunto de normativas y directrices para regular el acceso a los recursos de TI de acuerdo con las necesidades y roles de los usuarios. Estas políticas buscan equilibrar la accesibilidad y la seguridad, asegurando que solo los usuarios autorizados puedan acceder a la información y realizar las operaciones pertinentes.

Por último se describe el esquema de unificación del control de acceso, mediante el cual se establecen los mecanismos para centralizar la administración de los usuarios,

sus permisos y privilegios. Este enfoque unificado garantiza la protección de los activos digitales y la concesión del mínimo privilegio, lo que se verifica mediante un modelo de amenazas.

4.1. Caracterización de los sistemas de TI de la UM

Para caracterizar los sistemas de TI de la UM se levantó un inventario de datos, aplicaciones, activos y servicios (DAAS en ingles Data, Assets, Applications and Services) [Pal19]. Este inventario permitió identificar las relaciones usuarios-aplicaciones, usuarios-servicios y aplicaciones-activos. Además permite establecer un modelo sobre la topología actual del sistema.

El inventario DAAS de la institución está constituido de la siguiente manera:

- Datos: son datos generales de alumnos, egresados, docentes y empleados (equipo del campus, etc.) Cada tipo de datos puede incluir información personal, ID institucional (matrícula), datos académicos, documentos oficiales digitalizados, firmas, contabilidad, cálculos de cobro, presupuestos, información financiera (estados de cuenta, entidades, proveedores, facturas), etc.

- La institución posee activos que incluyen servidores como Apache-Ubuntu y un Gestor de servidores, así como dispositivos finales IP, como impresoras, teléfonos IP, y equipos de interconexión, como Switches (Brocade, Cisco, Aruba), controladora AP (Aruba controller), y Software de gestión de servidores (iLO). En la tabla 4.1 se presenta un inventario detallado de las aplicaciones.

  En general, la red de la Universidad de Montemorelos se puede dividir en 2 secciones: 1)- dispositivos de distribución y acceso al usuario, y 2)- sistemas UM (los servidores que alojan las aplicaciones más importantes de la institución). En la Figura 4.1 se muestra la configuración actual de la red.

  La red de la UM en la sección de distribución y acceso contiene cerca de 11 interconexiones saliendo del backbone a los edificios principales de la UM. De los

Tabla 4.1: Inventario de aplicaciones

No. de dispositivos	Tipo de dispositivo	Descripción
17	Páginas Web	Sistemas web e42, Financiero, UM Virtual, efectividad institucional, Emprendum, DPI (nutrición), repositorio institucional, etc.
22	Servidores	Apache2 Ubuntu, Gestionador de servidores (hiperv-isor VMWare, ESX, vCenter Server), Windows Server, nginx, etc.
10	Dispositivos finales IP	Impresoras, teléfonos IP (Enterprise IP phone), etc.
13	Dispositivos de conexión	Switches (Brocade, Cisco, Aruba), controladora AP (Aruba controller), Software de gestión de servidores (iLO), etc.

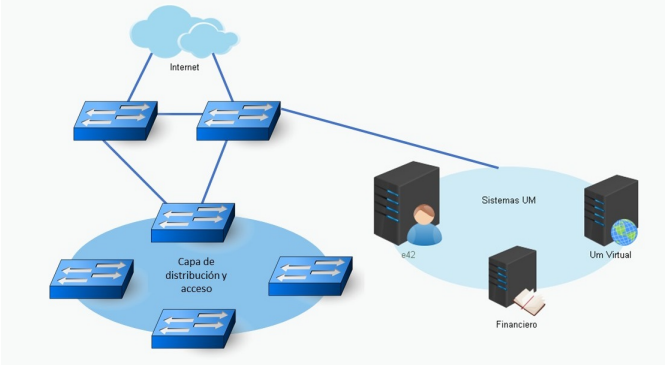

Figura 4.1: Diagrama de la estructura de la red

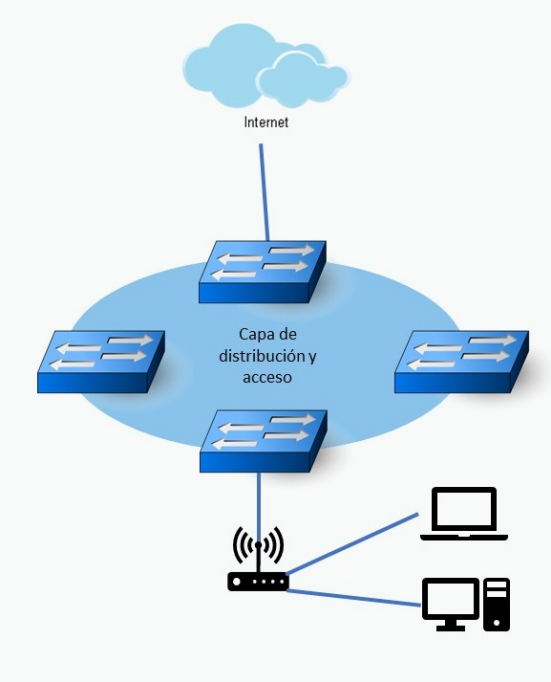

Figura 4.2: Diagrama de la estructura de la capa de distribución y acceso UM

switches en los edificios se interconectan a puntos de acceso (Access Points, AP, por sus siglas en inglés) inalámbrico para que el usuario final tenga acceso a la red institucional. Lo anterior se muestra en la Figura 4.2.

En la Figura 4.3 se presentan los sistemas UM, cada uno acompañado de un subsistema de interconexión. Para establecer la conexión con el Virtual UM, tanto el sistema E42 como el financiero requieren la integración de un subsistema adicional denominado ”traductor”. Este componente facilita la comunicación y la interoperabilidad entre los diversos sistemas, asegurando una integración fluida y eficiente.

A continuación se describen las Aplicaciones y servicios que emplean la red de la UM:

- Sistema E42: este sistema es una solución institucional diseñada para facilitar la interacción entre clases, alumnos y maestros, ofreciendo funcionalidades que abarcan el seguimiento de calificaciones, comunicación con los docentes, un calendario virtual y la posibilidad de participar en foros. Asimismo, este sistema habilita la realización de preguntas y respuestas, y se integra con el

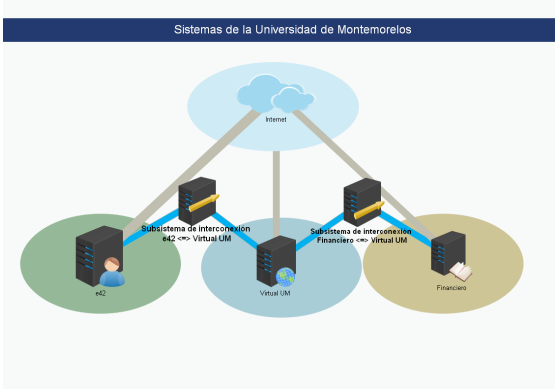

Figura 4.3: Diagrama de la estructura de los sistemas UM

sistema UM Virtual para mantener actualizado el registro de calificaciones. Los detalles de las principales aplicaciones se encuentran detalladas en la Tabla 4.2.

- UM Virtual: este sistema representa una solución institucional creada con el propósito de rastrear y gestionar a los alumnos inscritos, incluyendo su información personal y documentos académicos. Esta plataforma habilita el seguimiento detallado de las materias y calificaciones, además de mantener registros financieros, como estados de cuenta. La interfaz del sistema proporciona acceso a datos personales y documentos oficiales, así como la capacidad de solicitar trámites, como constancias o permisos. Algunos detalles del sistema UN Virtual se muestran en la Tabla 4.3.
- Financiero: representa una plataforma de gestión de registros financieros, siendo principalmente utilizada por el personal empleado de la institución. Esta plataforma abarca cálculos relacionados con el cobro, presupuestos, trámites de recursos humanos, interacción con proveedores, contabilidad y seguimiento de facturas. La Tabla 4.4 resume los detalles más importantes del sistema Financiero.

Tabla 4.2: Inventario de aplicaciones en el sistema E42

Aplicación	**Descripción**
Windows Server1: Windows Internet Information Services	Contiene los datos del sistema web.
Windows Server2: Windows Internet Information Services y Oracle database	Base de datos SQL e información del sistema.
Subsistema de interconexión (Traductor)	Conecta el sistema E42 al virtual – Busca alumnos inscritos.

Tabla 4.3: Inventario de aplicaciones en el UM Virtual

Aplicación	**Descripción**
Oracle database	Mayoría de la información sobre las personas (alumnos,empleados,etc.)
SQL server.	Sistema de contabilidad, información financiera (estados de cuenta, entidades, etc.)
Postgress1	Información de contacto de los postulantes (nuevo ingreso).
Postgress2	Datos personales: Documentos oficiales y firmas.
Postgress3	Imágenes y otros documentos.

Tabla 4.4: Inventario de aplicaciones en el Financiero

Aplicación	**Descripción**
Oracle database	Recursos Humanos, cálculos, cobro.
Postgres	Facturas (informes y proveedores), reembolso.
SQL Server	Información contable, Usuarios.

Tabla 4.5: Resumen de vulnerabilidades en los sistemas institucionales

Tipo de vulnerabilidad	**Descripción**
Cross-site scripting (XXS)	Caja de comentarios dentro de un sistema permite ejecutar código javascritpt.
SQL Injection	En la página principal del servidor de logeo asignamos un payload con cierto formato, el resultado mostró evidencia de poder ser explotable con inyecciones sql.
Old Version of systems	Vulnerabilidades de explotación por falta de un parche o actualización.
TCP Ports	Es posible determinar qué puertos TCP están abiertos al intentar establecer una conexión TCP o envío de un paquete TCP SYN al puerto que se quiera verificar.

4.2. Análisis de riesgos y amenazas

Para completar la Evaluación de Riesgos y Amenazas en el marco del Inventario DAAS, es esencial examinar la seguridad actual de los sistemas prioritarios con el objetivo de identificar posibles vectores de ataque y amenazas. Inicialmente, se llevaron a cabo pruebas exploratorias utilizando herramientas automatizadas como Nmap, Nessus y Acunetix Web Vulnerability Scanner. Posteriormente, las pruebas de penetración se enfocaron en analizar las vulnerabilidades previamente detectadas, abordando aspectos como la ejecución de código fuente, inyecciones SQL y el escalamiento de privilegios, especialmente teniendo en cuenta que los sistemas están en funcionamiento. Se presenta un resumen detallado de los hallazgos de esta fase en la Tabla 4.5.

4.3. Propuesta de políticas de control de acceso

Con el fin de gestionar correctamente el acceso, las políticas de control de acceso son necesarias para garantizar que solo los usuarios autorizados puedan acceder a los recursos y datos de una organización. Estas políticas definen las reglas y procedimientos que deben seguirse para otorgar, negar y administrar el acceso a sistemas y recursos, y prevenir amenazas internas y externas.

4.3.1. Jerarquía de tipos de usuarios y privilegios

Considerando que cada tipo de usuario puede poseer distintos niveles de acceso a los recursos y datos de la organización, la importancia de este aspecto se hace evidente. En este sentido, las políticas de control de acceso deben ajustarse a los diversos roles y responsabilidades de los usuarios para asegurar que accedan únicamente a los recursos necesarios para desempeñar sus funciones. Además, es fundamental reconocer que la formulación de estas políticas está intrínsecamente vinculada a los procesos, directrices y expectativas de la organización, así como a la estructura que se desea implementar.

Crear una jerarquía de usuarios se convierte en un paso fundamental para el desarrollo de una estructura de seguridad eficaz. Este proceso busca equilibrar el acceso a los recursos necesarios para realizar tareas laborales con la imperiosa necesidad de salvaguardar la integridad y seguridad de la organización. En la definición de niveles de acceso para cada tipo de usuario, es esencial tener precaución para evitar otorgar privilegios excesivos, siguiendo la filosofía de "mínimo privilegio" (*least privilege*). Esta filosofía, en plena armonía con la arquitectura Zero Trust abordada en esta tesis, resalta la importancia de restringir los privilegios a lo esencial para evitar posibles amenazas y garantizar la seguridad de la organización. El resultado final de esta sección implica la creación de roles específicos adaptados a la organización de la institución, completando así el marco necesario para una implementación eficiente del control de acceso unificado. Con base en lo expuesto, se delinean los pasos esenciales para establecer una jerarquía de usuarios eficiente:

- Identificar los diferentes tipos de usuarios: La primera tarea es identificar a los diferentes tipos de usuarios que existen en la organización.
- Asignar roles y responsabilidades: Una vez que se han identificado los diferentes tipos de usuarios, se deben asignar roles y responsabilidades específicos a cada tipo de usuario. Esto significa establecer qué recursos de la organización tienen acceso a cada tipo de usuario y qué nivel de permisos tienen para acceder a esos recursos. Esto ayudará a garantizar que cada usuario tenga acceso solo a los recursos necesarios para realizar sus tareas (a continuación se presentan los roles de tipo de usuario asignados).

- **Super Admin (PDP)**: Es el usuario con el máximo nivel de acceso y privilegios en WSO2 Identity Server. Este rol tiene acceso a todas las funcionalidades y recursos del sistema, incluyendo la gestión de usuarios, la configuración de roles, la administración de recursos y la configuración del sistema. En general, solo hay uno o unos pocos Super Admins en una organización, y se les otorga este nivel de acceso solo a individuos de confianza que necesitan este nivel de control.
- **Admin (PDP/PEP)**: Es el usuario responsable de la administración de un sistema específico en WSO2 Identity Server. Este rol tiene acceso a las funcionalidades y recursos específicos del sistema, incluyendo la gestión de usuarios y roles, la configuración de políticas de seguridad y la gestión de aplicaciones. En general, hay uno o varios Admin en una organización, y se les otorga este nivel de acceso para que puedan administrar el sistema de manera efectiva.
- **Internal/ every one**: Se refiere a un grupo de usuarios predefinido en WSO2 Identity Server. Este grupo incluye a todos los usuarios registrados en el sistema, incluyendo los usuarios anónimos y los usuarios autenticados. Los miembros de este grupo tienen acceso a los recursos públicos del sistema, pero su nivel de acceso y privilegios puede estar limitado según las políticas de seguridad configuradas.

- Crear una estructura jerárquica: A continuación, se procede a crear una estructura jerárquica basada en los roles y responsabilidades de cada tipo de usuario, así como en sus niveles de acceso. Esto ayudará a establecer quién tiene autoridad sobre quién y cómo se delegan las responsabilidades. Con base en lo anterior, se propone la siguiente jerarquía para organizar los usuarios y la Figura 4.4 muestra la jerarquía propuesta.

  - **Super Admin:** es un usuario con el máximo nivel de acceso y privilegios en un sistema o aplicación. Tiene control total sobre todas las funciones y

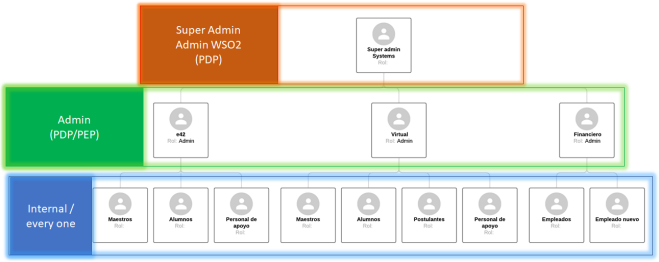

Figura 4.4: Jerarquía de usuarios

recursos del sistema, incluyendo la capacidad de agregar o eliminar usuarios, cambiar configuraciones y acceder a datos confidenciales.

- **Admin:** es un usuario con un nivel intermedio de acceso y privilegios en un sistema o aplicación. Tiene un conjunto específico de responsabilidades y permisos, que pueden incluir la capacidad de crear, editar y eliminar cuentas de usuario, configurar permisos de acceso y supervisar la actividad de los usuarios.
- **Maestro:** es un usuario con un nivel bajo de acceso y privilegios en un sistema o aplicación. Tiene acceso solo a un conjunto limitado de funciones y recursos, que son necesarios para realizar su trabajo. En general, los usuarios con mínimo privilegio no pueden realizar cambios significativos en el sistema y no tienen acceso a datos confidenciales o recursos críticos.
- **Alumno:** es un usuario con el nivel más bajo de acceso y privilegios en un sistema o aplicación.

4.3.2. Políticas de control de acceso

Las políticas de control de acceso son esenciales para garantizar la seguridad y protección de los recursos de una organización. Una vez que se han identificado los recursos y los roles de usuario, se pueden establecer las políticas de control de acceso acordes a los procesos de la institución. En este caso, se utilizará la Guía de referencia XACML 3.0 de Oasis [Ris13] para dar formato a las políticas de control de acceso en WSO2 Identity Server. Esta guía es importante porque describe en detalle los componentes de una po-

lítica XACML, incluyendo los elementos y atributos que se pueden utilizar en las reglas de acceso. El uso del formato XACML garantiza la compatibilidad y conformidad con el estándar XACML, lo que permite la interoperabilidad y portabilidad de las políticas de control de acceso entre diferentes sistemas y plataformas.

Las siguientes políticas se mostrarán en un diagrama de acuerdo con el lenguaje de políticas XACML:

- Política de autenticación: Si el usuario ingresa sus credenciales y éstas no son válidas, se denegará el acceso, según lo visualizado en el diagrama 5. Adicionalmente, se implementará un riguroso control de los intentos de inicio de sesión, registrando cada intento, ya sea válido o no, en un log de seguridad. Esta medida no solo permite mantener un registro detallado de la actividad de autenticación, sino que también contribuye a fortalecer la seguridad del sistema. Además, como medida preventiva ante posibles ataques de *password guessing* u otros intentos maliciosos, se establecerá un límite de intentos fallidos. Una vez que éste límite sea alcanzado, se procederá a bloquear temporalmente la cuenta del usuario, disminuyendo significativamente el riesgo de accesos no autorizados.

- Política de Control de Acceso Basado en Roles: Se muestra en el diagrama 4.6. Esta política establece el acceso al recurso según el rol del usuario. Si el rol del usuario tiene permiso para acceder al recurso, se le concederá el acceso. De lo contrario, se denegará el acceso. Además, se implementará un registro de cada intento de inicio de sesión, ya sea válido o no, en un log de seguridad.

- La política de inicio de sesión único: Se muestra en el diagrama 4.7. La política de inicio de sesión único o Single Sign-On (SSO) permite a los usuarios utilizar las mismas credenciales para acceder a todas las aplicaciones y habilita a un usuario previamente autenticado para acceder a una segunda aplicación sin tener que volver a ingresar sus credenciales.

- La política de revocación selectiva de privilegios: Se muestra en el diagrama 4.8. Esta política cambia los permisos que tenga un usuario al asignarle o revocarle un rol de manera específica y controlada y con ello los permisos con los que cuenta un

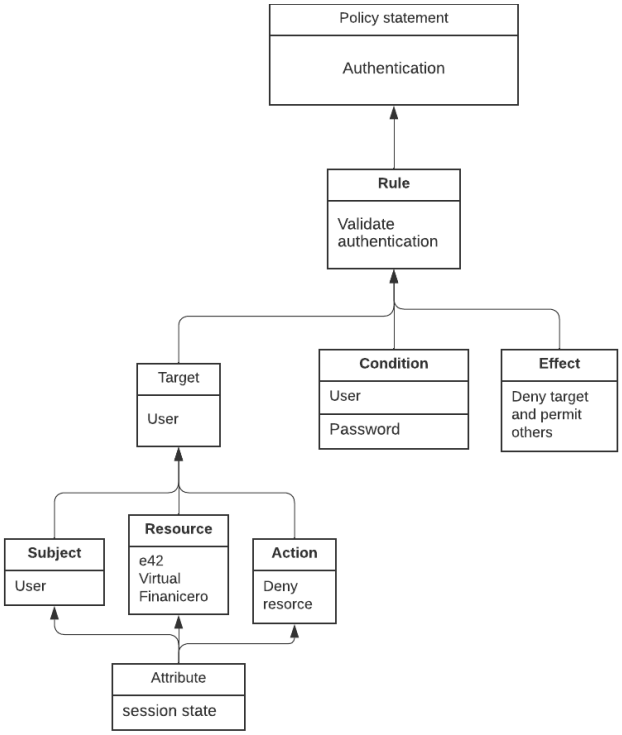

Figura 4.5: Política de autenticación

usuario. Esta política se utiliza en caso de cambios en el rol o responsabilidades de un usuario, o si se detecta un comportamiento inapropiado o violación de políticas de seguridad. Esta política ayuda a reducir los riesgos de seguridad al garantizar que los usuarios tengan solo los privilegios necesarios y adecuados para llevar a cabo sus funciones, al tiempo que se mantienen los niveles adecuados de control y protección de los recursos críticos.

4.3.3. Mecanismos de otorgamiento y revocación de privilegios

Para poder aplicar las políticas en un Service Provider en WSO2, es necesario configurar primero dicho proveedor de servicios en la plataforma de WSO2 Identity Server. Para ello, se deben definir los atributos y requerimientos necesarios para la autenticación y autorización en el Service Provider. Una vez que el Service Provider está configurado se pueden aplicar políticas de autorización y acceso específicas para el Service Provi-

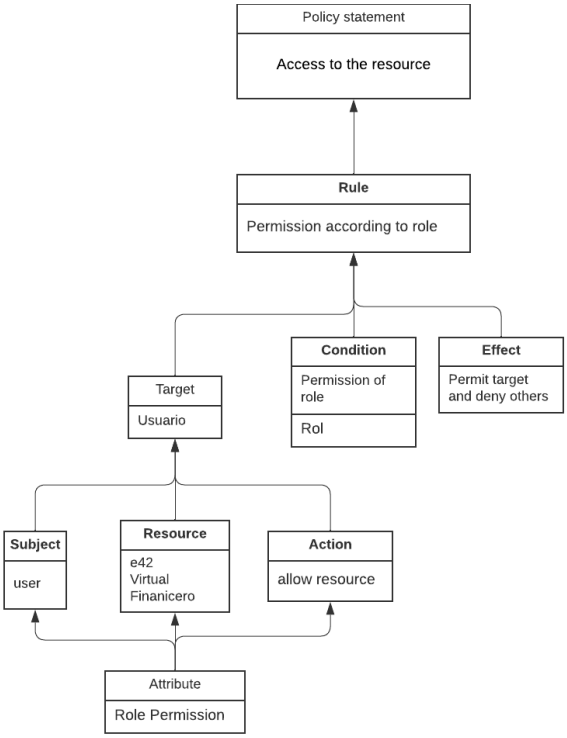

Figura 4.6: Política de acceso al recurso

der, según los roles y permisos necesarios para los usuarios que accedan a la aplicación. Además, se puede aplicar la política de inicio de sesión único (SSO) para permitir que los usuarios accedan al proveedor de servicios sin tener que ingresar sus credenciales de inicio de sesión en cada instancia. Esto se logra mediante la configuración de un flujo de autenticación SSO, que puede ser personalizado según las necesidades del Service Provider y la aplicación en cuestión. En este trabajo se realizó el SSO entre aplicaciones web SAML (Security Assertion Markup Language) [WSO22b].

Una vez que se han definido las políticas de control de acceso utilizando la guía XACML 3.0 de Oasis, es necesario crear la política en WSO2 Identity Server. Para ello, se accede a la consola de administración de WSO2 y se selecciona la opción de "Políticas de Autenticación y Autorización". En esta sección, se puede crear una nueva política utilizando el lenguaje XACML y definir los diferentes atributos y condiciones necesarios para su funcionamiento.

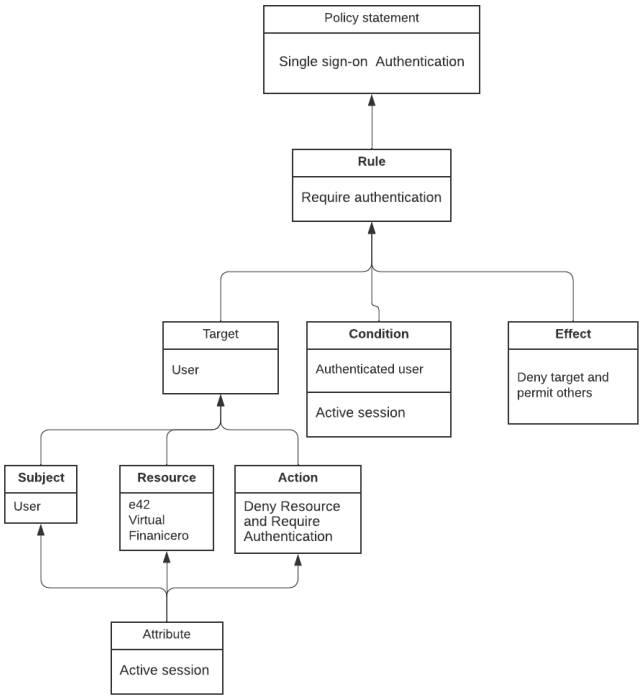

Figura 4.7: Política de inicio de sesión único

Una vez creada la política, es posible aplicarla a un Service Provider específico. Para ello se debe especificar como un parámetro en el formato XACML.

De esta manera, al acceder al Service Provider en cuestión, se evaluará la política de control de acceso definida previamente y se concederá o denegará el acceso de acuerdo con las reglas establecidas en la política.

4.4. Modelado del control de acceso unificado

En esta sección se aborda el proceso de diseño y desarrollo del esquema de unificación de usuarios, permisos y privilegios en los sistemas de TI. El objetivo de esta sección es establecer una estructura coherente y eficiente para gestionar el control de acceso en todas las aplicaciones y servicios de la organización, garantizando una experiencia de usuario consistente y segura.

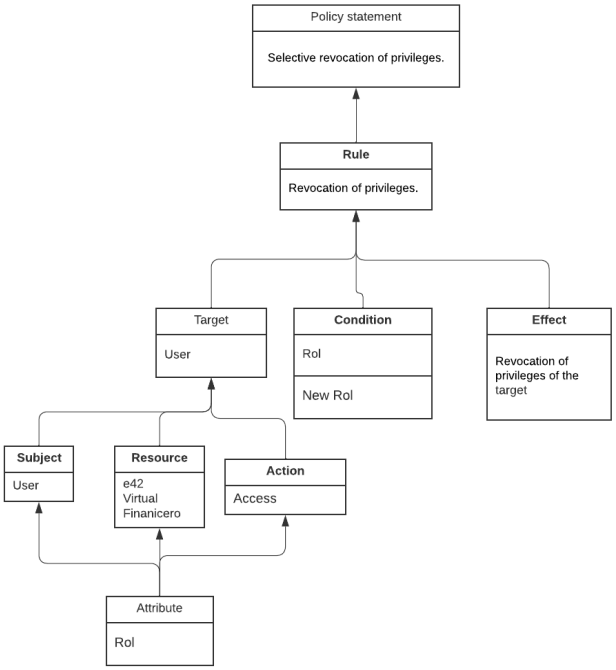

Figura 4.8: Política de revocación selectiva de privilegios

4.4.1. Diseño del esquema de unificación de usuarios, permisos y privilegios

El diseño del esquema de unificación de usuarios, permisos y privilegios es de suma importancia en la gestión de identidad y acceso, ya que permite a las organizaciones administrar de manera eficiente y segura el acceso a los recursos y datos de la organización.

Para la unificación de control de acceso en esta tesis se utiliza la plataforma IAM WSO2 Identity Server [WSO22a]. Dentro de las características que fueron indispensables para este desarrollo son:

- Funcionalidades de control de acceso: autenticación de múltiples factores, autorización basada en roles y políticas, y gestión de sesiones.
- Integración con sistemas existentes: WSO2 Identity Server es altamente configurable y se integra fácilmente con sistemas existentes ya que cuenta con conectores y adaptadores para una amplia variedad de sistemas, lo que lo convierte en una solución ideal para la migración a un modelo de Zero Trust.

- Seguridad: WSO2 Identity Server es una solución de código abierto y cuenta con una comunidad de desarrolladores activa y comprometida. La plataforma se somete a pruebas rigurosas de seguridad y se actualiza regularmente para proteger contra vulnerabilidades conocidas.

- Escalabilidad: WSO2 Identity Server es altamente escalable y puede manejar grandes volúmenes de usuarios y transacciones.

- En el ámbito de la identidad y el acceso, WSO2 Identity Server se destaca por su impresionante capacidad de escalabilidad. Este servidor no solo puede manejar grandes volúmenes de usuarios y transacciones, sino que también se ha ganado el reconocimiento en el panorama de la seguridad.

- Forrester Research [Cse20], una firma de investigación y consultoría, ha desarrollado un modelo de seguridad innovador conocido como Zero Trust. En su informe de 2020, titulado *Customer Identity And Access Management* (IAM), *Q4 2020*, WSO2 Identity Server fue destacado como una de las principales soluciones de gestión de identidades y acceso. El informe subrayó su capacidad para proporcionar seguridad y escalabilidad en entornos empresariales. La fortaleza de WSO2 Identity Server reside en su enfoque centrado en la IAM basada en API y estándares, respaldado por una arquitectura de referencia completa.

Estas funcionalidades y características no solo hacen de WSO2 Identity Server una opción confiable, sino que también aseguran que solo los usuarios autorizados tengan acceso a los recursos protegidos, alineándose perfectamente con el enfoque de seguridad Zero Trust. Actualmente WSO2 Identity Server tiene 2 presentaciones:

- WSO2 Identity Server Community Edition: Es la versión gratuita y de código abierto de WSO2 Identity Server. Proporciona funcionalidades básicas de gestión de identidades y control de acceso, incluyendo autenticación, autorización, y federación de identidades. Esta versión está diseñada para su uso por desarrolladores y empresas pequeñas que buscan una solución de IAM asequible y de fácil acceso.

- WSO2 Identity Server Enterprise Edition: Es la versión comercial y además de ofrecer todas las funcionalidades de la versión Community Edition, ofrece funcionalidades más avanzadas y soporte empresarial, lo que puede ser importante para las empresas que requieren una solución de IAM más completa y personalizada.

Para este trabajo se decidió utilizar WSO2 Identity Server Community Edition. Y el modelo ZT que se apega a nuestro caso de estudio es el modelo de enclave, ya que permite la unificación de diferentes recursos y ayudar a limitar el acceso a los recursos a solo aquellos usuarios y dispositivos autorizados.

4.4.2. Esquema de unificación

Para lograr la unificación coherente del control de acceso, los sistemas E42, VirtualUM y Financiero fueron agrupados en un enclave de recursos. De esta forma, los principales servicios quedan agrupados en un mismo perímetro de confianza, cuyo acceso es controlado por un *Gateway* PEP. El esquema de unificación se describe en la Figura 4.9.

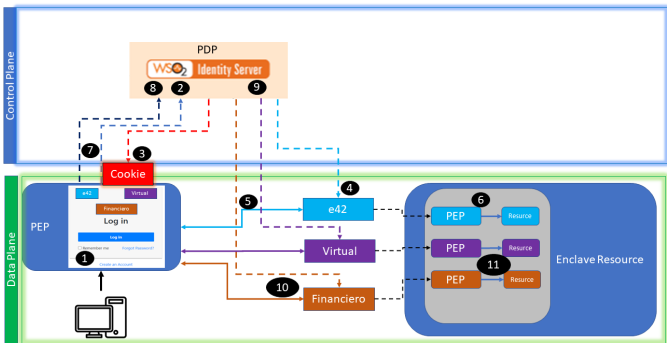

Figura 4.9: Esquema de inicio de sesión único (Single sing-on)

1. El usuario inicia el proceso accediendo a alguna de las 3 plataformas de la institución, que actúan como los primeros PEP (Punto de Enlace de Políticas).

2. Una vez seleccionada la plataforma, se envía una solicitud de login y el WSO2 Identity Server (WSO2 IS), que actúa como PDP (Punto de Decisión de Políticas), solicita las credenciales de autenticación al usuario.

3. Una vez que el usuario ingresa sus credenciales y se autentica exitosamente, el WSO2 IS genera cookies que son almacenadas en el navegador del usuario, y emite un token de acceso que contiene la información de autenticación.

4. El WSO2 IS redirige al usuario al recurso de la aplicación deseada, proporcionando el token de acceso.

5. La aplicación valida el token de acceso con el WSO2 IS y autoriza el acceso del usuario.

6. Finalmente, el usuario accede al recurso de la aplicación.

7. Cuando el usuario intenta acceder a otra plataforma, es redirigido nuevamente al WSO2 IS.

8. El WSO2 IS identifica que el usuario ya ha sido autenticado previamente con una sesión activa, gracias a las cookies almacenadas en el navegador.

9. El sistema WSO2 genera un nuevo token de acceso para la segunda aplicación, evitando la necesidad de que el usuario ingrese sus credenciales nuevamente.

10. El usuario muestra el token de acceso para la segunda aplicación y, al ser validado por el WSO2 IS, la aplicación autoriza el acceso del usuario.

11. Finalmente, el usuario accede al recurso de la segunda aplicación sin requerir autenticación adicional, lo que brinda una experiencia de inicio de sesión único (SSO) para ambas aplicaciones y mejora la comodidad y eficiencia para el usuario.

Para llevar a cabo el esquema planteado en un sistema WSO2 Identity Server Community Edition utilizando SSO es necesario seguir las indicaciones a continuación. Utilizando un *Service Provider (SP)* que es una aplicación o servicio que utiliza WSO2 Identity Server para autenticar y autorizar a sus usuarios. Los *Service Providers* pueden ser implementados mediante aplicaciones web, servicios web, aplicaciones móviles entre otros. En esta propuesta serían los tres sistemas que se pretende unificar (E42, Virtual UM, Financiero).

La gestión de un *Service Provider* en WSO2 Identity Server implica la configuración de varias opciones, como la URL de retorno, el nivel de autenticación requerido, las políticas de autorización y las opciones de inicio de sesión único (SSO). WSO2 Identity Server ofrece varios protocolos de SSO, incluyendo SAML, OAuth y OpenID Connect. En este trabajo se utilizaran sistemas Service Provider con SAML.

Para configurar SSO en un Service Provider en WSO2 Identity Server, se deben seguir los siguientes pasos:

- Configurar un Identity Provider (IDP) en WSO2 Identity Server.
- Configurar un Service Provider en WSO2 Identity Server.
- Configurar la integración de SSO entre el IDP y el SP.
- Prueba y verificación de la integración de SSO.

Una vez que se ha configurado correctamente el SSO entre el IDP y el SP, los usuarios pueden iniciar sesión en el IDP una sola vez y acceder a todos los SP configurados sin tener que volver a iniciar sesión. Esto mejora la experiencia del usuario y aumenta la seguridad del sistema al reducir la necesidad de que los usuarios mantengan múltiples credenciales de inicio de sesión.

El diagrama 4.10 representa gráficamente el funcionamiento del Single Sign-On (SSO) en la simulación que se ha configurado. A través de esta representación visual, se muestra cómo el proceso de SSO permite a los usuarios autenticarse una sola vez y acceder a varias aplicaciones o servicios protegidos sin la necesidad de proporcionar sus credenciales nuevamente. El diagrama proporciona una visión clara de la interacción entre el usuario, el proveedor de identidad (Identity Provider, IDP) y los proveedores de servicio (Service Providers, SP), resaltando el flujo de autenticación y autorización que se lleva a cabo durante el proceso de inicio de sesión único. Además, el diagrama destaca el papel fundamental del WSO2 Identity Server como el proveedor de identidad central que gestiona y controla el acceso a los recursos protegidos. A través de esta representación visual, se puede comprender de manera más clara y concisa cómo se logra la experiencia de SSO en el entorno implementado. A través de un diagrama de secuencias se muestran todas

las transacciones necesarios para realizar el acceso de un usuario a un recurso a través del IDP WSO2.

En el primer escenario de uso, que se muestra en la Figura 4.10, el usuario busca autenticarse en dos aplicaciones distintas. Inicialmente, el usuario intenta acceder a una de las aplicaciones a través de un PEP. A continuación, el sistema redirige al usuario al WSO2 Identity Server para ingresar sus credenciales de autenticación. Dentro del WSO2 Identity Server, se verifica la validez de las credenciales al contrastarlas con la información almacenada en la tabla de usuarios. En caso de que las credenciales sean incorrectas (Véase en la Figura 4.11), el sistema deniega el acceso y se muestra un mensaje indicando la incorrecta autenticación, solicitando nuevamente la introducción de las credenciales si el conteo de intentos fallidos supera a 2 veces se impide el acceso al usuario durante 15 minutos. En situaciones donde las credenciales resultan ser correctas (Figura 4.10), el WSO2 Identity Server genera una cookie que se almacena en el navegador del usuario, además de crear un token de autenticación. Este token se envía a la aplicación pertinente, donde se lleva a cabo una verificación de autenticidad mediante un proceso de tres pasos. Una vez que se confirma la autenticidad del token, el usuario es autenticado y redirigido exitosamente a la aplicación, otorgándole acceso al recurso deseado.

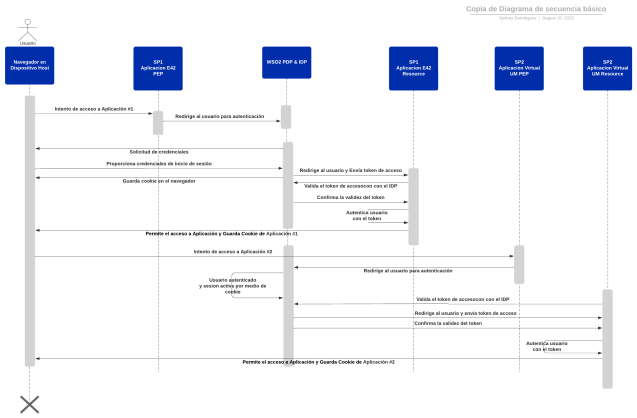

Figura 4.10: Diagrama de secuencia de intercambio de mensajes de un login correcto

En el segundo caso de uso, el sistema implementa una política de seguridad basada en roles de acceso. Cada usuario es asignado a un rol específico, junto con sus respectivos privilegios. Al intentar iniciar sesión, el usuario proporciona sus credenciales en la interfaz de autenticación. El WSO2 Identity Server realiza una doble verificación: primero, se

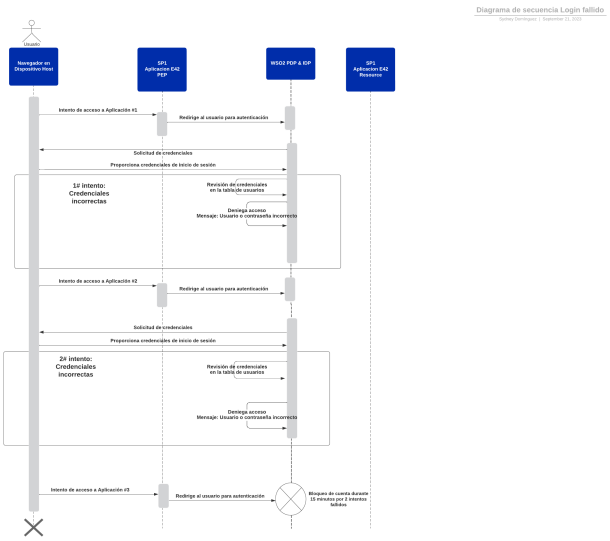

Figura 4.11: Diagrama de secuencia de intercambio de mensajes de un login fallido

confirma si las credenciales son correctas y coinciden con los registros de usuarios; luego, se verifica si el usuario posee el rol adecuado y el privilegio necesario para acceder al sistema objetivo.

Cuando el usuario carece del privilegio necesario (caso de la Figura 4.12), el sistema responde con un mensaje de ”Intento de Autenticación Fallido” y ”Falla de Autorización”. En el caso de intentos fallidos repetidos por parte del mismo usuario, se emite una notificación de ”Intento Sospechoso de Autenticación”. Por el contrario, si el usuario posee el privilegio suficiente, el WSO2 Identity Server genera una cookie y un token de autenticación, enviando este último a la aplicación correspondiente (caso de la figura 4.13). Una vez que el token se somete a una verificación de autenticidad en tres etapas y se confirma su validez, el usuario es autenticado y redirigido exitosamente a la aplicación, concediéndole el acceso al recurso deseado.

En una situación distinta en la que un usuario cambie sus responsabilidades laborales y, por ende, su rol asignado, el administrador se encargará de llevar a cabo un cambio manual en el rol del usuario en el WSO2 Identity Server. Este cambio automático resultará en la modificación correspondiente de los privilegios de acceso del usuario, garantizando así que sus derechos de acceso se ajusten adecuadamente a sus nuevas responsabilidades laborales.

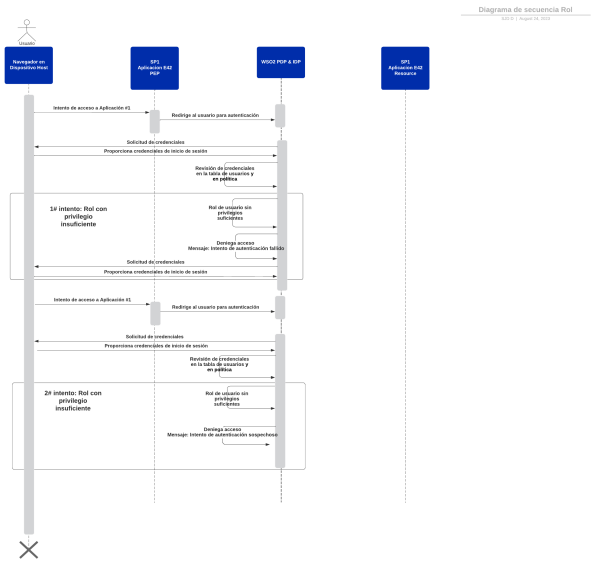

Figura 4.12: Diagrama de secuencia por rol Fallido

4.4.3. Entorno de pruebas

A continuación, se muestra la tabla 4.6 con las diferentes sistemas y versiones utilizados en esta implementación.

4.4.4. Discusión

En esta sección se abordaron diversas consideraciones relacionadas con la seguridad en la implementación del sistema basado en WSO2 con SSO para resolver la multiplicidad de identidades y el control y unificación del acceso.

A continuación, se llevará a cabo un análisis de amenazas utilizando el enfoque STRIDE, que se centra en seis categorías de amenazas: Spoofing (Suplantación), Tampering (Manipulación), Repudiation (Negación), Information Disclosure (Divulgación de Información), Denial of Service (Denegación de Servicio) y Elevation of Privilege (Elevación de Privilegios).

El propósito central de este análisis es comprender a fondo la integración de los componentes en WSO2 Identity Server y la implementación eficaz de políticas de acceso y autenticación a través de SAML. Un papel esencial recae en las aplicaciones de recursos,

Tabla 4.6: Configuración de los sistemas y software del entorno de pruebas

Sistema o software utilizado	**Descripción**
Ubuntu 22.04.2 LTS	Sistema base para las aplicaciones de este trabajo.
WSO2 Identity Server Community Edition wso2is-6.0.0	Sistema principal para gestionar la identidad (PDP/PEP).
Software de javac 11.0.18	Software requisito para WSO2 Identity Server.
Apache Maven 3.6.3	Software para instalar WSO2 Identity Server a partir de la distribución de origen.
Apache/2.4.52 (Ubuntu)	Software usado para la emulación de sistemas institucionales (PEP/SP/Resource).
Apache Tomcat 8.x	Software usado para la emulación de sistemas institucionales (PEP/SP/Resource).
SimpleSAMLphp 2.0	Es una aplicación escrita en PHP nativo que se ocupa de la autenticación.
Dispatch sample	Un ejemplo o muestra de aplicación a base de Tomcat que demuestra el funcionamiento y la configuración en WSO2 Identity Server, en este trabajo se utilizo para simular el UM Virtual.
Manager sample	Un ejemplo o muestra de aplicación a base de Tomcat que demuestra el funcionamiento y la configuración en WSO2 Identity Server, en este trabajo se utilizo para simular el E42.
Travelocity webapp sample	Un ejemplo o muestra de implementación que demuestra el funcionamiento y la configuración en WSO2 Identity Server, en este trabajo se utilizo para simular el Financiero.
PHP 7.4.33	Es un requisito para utilizar los ejemplos de SimpleSAMLphp.
MYSQL 8.0.32-0ubuntu0.22.04.2	Es un requisito para utilizar los ejemplos de SimpleSAMLphp.

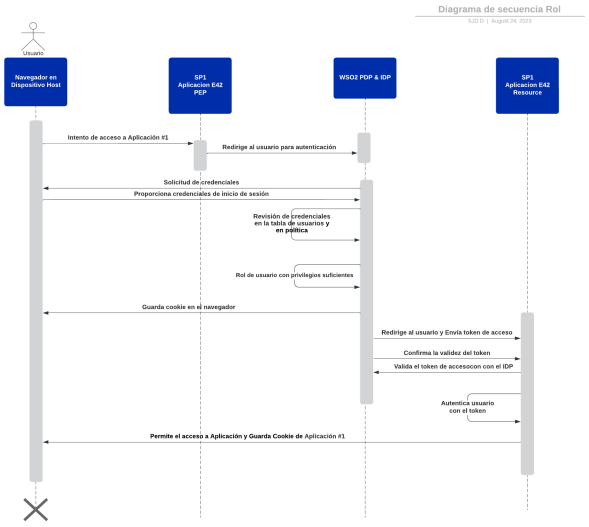

Figura 4.13: Diagrama de secuencia por rol Correcto

que almacenan activos críticos que los usuarios buscan acceder, y desempeñan un papel central en este escenario de seguridad.

Es fundamental enfatizar que la discusión se enfoca exclusivamente en los componentes del servidor. No se profundiza en la exploración de vulnerabilidades en el entorno de red ni en elementos emulados que no representan aplicaciones en producción dentro de este contexto particular.

Estos elementos específicos incluyen el PEP, PDP, IDP y las aplicaciones de recursos, todos ellos constituyentes clave en la infraestructura de seguridad dentro del entorno de WSO2 Identity Server. Sin embargo, es relevante señalar que la discusión detallada sobre vulnerabilidades y vectores de ataque específicos que puedan amenazar la seguridad de estos activos excede el alcance de este trabajo. A continuación, se presenta un diagrama 4.14 que ilustra la disposición de los elementos clave en este entorno.

Con esta introducción, se está adecuadamente preparado para adentrarse en el análisis de vulnerabilidades y vectores de ataque en el ámbito previamente definido, como se presenta en la Tabla 4.7).

Tabla 4.7: Configuración Hardware y Software del entorno de pruebas

Objetivo de amenaza	**Estrategia de mitigación**	**Técnica de mitigación**
Ataque de Fuerza Bruta	El sistema WSO2 bloquea una cuenta de usuario después de un número específico de intentos.	Políticas de Bloqueo de Cuenta.
Ataque de Intercepción de Tráfico no Autenticado	El sistema WSO2 utiliza comunicación mediante medios seguros.	SAML y SSL/TLS y esta deshabilitado la conexión por http.
Ataque de Robo de Credenciales Almacenadas (Gestión de Credenciales Seguras)	WSO2 Identity utiliza el método de almacenamiento de contraseñas con hash y salt.	Hashing (SHA-256 o bcrypt) y Salting.
Ataque de Robo de Credenciales Almacenadas (Firmas Digitales)	SAML utiliza firmas digitales para garantizar la integridad de los mensajes, cualquier alteración de los tokens SAML invalidaría la firma.	Protocolo SAML para autenticar mediante identidades federadas.
Ataque de Contraseña de Administrador por Defecto	El sistema envía recordatorios periódicos sobre el cambio de contraseña.	Política de Cambio de Contraseña Obligatorio.
Repudio	Registros de auditoría y trazabilidad. WSO2 gestiona logs de forma predeterminada.	Carbon logs, Audit logs, HTTP Access o habilitar un servidor Log especifico.
Tampering e information disclosure	Cifrado y firma digital protege la confidencialidad e integridad de los mensajes.	Protocolo SAML.
Elevación de privilegios	Garantizar que los usuarios solo tengan acceso a recursos y funcionalidades correspondientes a sus roles y privilegios.	Políticas de control de acceso y autorización basada en roles.

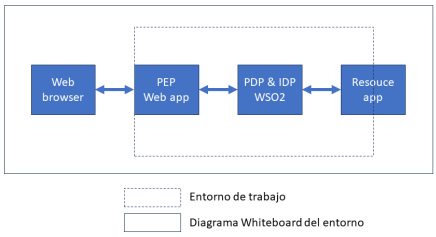

Figura 4.14: Diagrama del entorno

Capítulo 5

Conclusiones

5.1. Resumen

En este proyecto, se ha desarrollado un esquema de control de acceso unificado para sistemas institucionales, adoptando el modelo Zero Trust. Se ha priorizado el modelo de despliegue Resource-Based Deployment, una elección estratégica que subraya la importancia de salvaguardar los recursos como medida prioritaria de seguridad. Este enfoque se ha implementado de manera efectiva mediante la utilización de políticas en formato XACML y el despliegue de sólidos mecanismos de autenticación basados en SSO y SAML, a través de WSO2 como PDP e IDP. La meta central del proyecto ha sido establecer una autenticación segura en tres sistemas distintos, logrando con éxito la emulación de estos entornos de manera integral. El trabajo comenzó con un inventario DAAS y una recopilación de información a través de pruebas de penetración, lo que permitió una clasificación exhaustiva de las amenazas. A partir de esta información, se definieron políticas de acceso que abordan la heterogeneidad de los sistemas.

La implementación se llevó a cabo desplegando WSO2 Identity Server como un gestor de identidad y un PDP/PEP, con características activadas de SSO para lograr un único punto de autenticación. Además, se activaron políticas específicas para garantizar el mínimo privilegio en el acceso.

El proyecto también incluyó la creación de diagramas UML para representar el comportamiento del sistema y el modelado de amenazas utilizando el enfoque STRIDE para evaluar las vulnerabilidades potenciales.

Este trabajo sienta las bases para la gestión segura de la identidad y el control de acceso en sistemas institucionales, contribuyendo al fortalecimiento de la seguridad de la red y el cumplimiento de los objetivos de seguridad.

5.2. Contribuciones

En cuanto a las contribuciones personales, se destacan varios logros significativos. En primer lugar, se realizó un inventario DAAS exhaustivo, incluyendo un análisis de vulnerabilidades y vectores de ataque del sistema. Además, se diseñó un conjunto integral de políticas que regulan el acceso, la autenticación, los permisos, los roles y la revocación de privilegios. También se desarrolló un esquema de unificación que permite la autenticación segura de varios sistemas en un sistema de identidad.

Inventario de Activos y Servicios: Se llevó a cabo una exhaustiva identificación de los activos en la red de la Universidad de Montemorelos (UM), que abarca sistemas, aplicaciones, recursos y datos críticos. Esto proporcionó una visión completa de los activos presentes en la red, contribuyendo a una comprensión más profunda de su infraestructura.

Análisis de Vulnerabilidades: A través de un análisis de vulnerabilidades, se identificaron posibles riesgos en la red. Este paso resultó fundamental para determinar los puntos críticos que requerían una atención especial en términos de seguridad.

Estas dos contribuciones lograron cumplir con el objetivo de caracterizar la red UM mediante la identificación de sus activos, servicios y vulnerabilidades.

Políticas de Control de Acceso Unificado: Se definió un conjunto coherente de políticas de control de acceso unificado que garantizan una uniformidad en los mecanismos de acceso a los tres sistemas institucionales. Estas políticas aseguran que la gestión del acceso sea coherente y eficaz, independientemente del sistema específico en uso. Además, se logró cumplir con el objetivo de crear un conjunto de políticas de control de acceso unificado para mitigar efectos de heterogeneidad que existen en la actualidad en la institucion.

Gestión de Identidad Basada en el ”Mínimo Privilegio”: Se estableció un sistema de gestión de identidad utilizando WSO2 Identity Server en conjunto con las políticas de

control de acceso unificado. Esto aseguró la implementación del principio del ”mínimo privilegio”, lo que significa que los usuarios solo tienen acceso a los recursos y servicios necesarios para sus roles específicos. Esto no solo minimiza riesgos, sino que también fortalece la seguridad del sistema. Esta contribución logró cumplir con el objetivo de diseñar un esquema para la gestión de identidad, basado en las políticas de control de acceso unificado, para garantizar la concesión del mínimo privilegio.

La contribución central de este trabajo radica en el diseño de un enfoque de Control de Acceso Unificado destinado a armonizar sistemas con diseños heterogéneos, empleando diversas tecnologías y paradigmas.

Control de Acceso Unificado: El modelo Zero Trust se enfoca en la unificación de los mecanismos de control de acceso en toda la infraestructura. Utiliza WSO2 Identity Server como un PDP y un IDP para asegurar que la autenticación y la autorización sean consistentes en los tres sistemas institucionales. Esto garantiza un enfoque unificado en la gestión de la identidad en el entorno institucional. Esto cumple con el objetivo general de diseñar un esquema de control de acceso unificado para la gestión de la identidad en un sistema de administración institucional.

Se implementó una estrategia fundamentada en el modelo Zero Trust para consolidar los mecanismos de control de acceso a lo largo de toda la infraestructura. WSO2 Identity Server desempeñó un papel crucial al funcionar como un PD e IDP para garantizar la uniformidad en los procesos de autenticación y autorización en los tres sistemas institucionales. Esta contribución resultó en el exitoso diseño de un esquema de Control de Acceso Unificado, cumpliendo así con el objetivo principal del proyecto.

El resultado es que los usuarios pueden autenticarse una sola vez para acceder a los tres sistemas, lo que no solo mejora la experiencia del usuario sino que también fortalece la seguridad de manera significativa.

5.3. Principales limitaciones

A pesar de las contribuciones presentadas en este trabajo, es crucial reconocer que este es apenas el primer paso en la implementación de un enfoque Zero Trust más completo. El éxito de este proyecto resalta la importancia de la unificación del control

de acceso en sistemas heterogéneos, pero existen desafíos y áreas de desarrollo futuro que merecen consideración.

El desarrollo del proyecto se llevó a cabo dentro de un marco de tiempo definido, lo que limitó la implementación completa.

La identificación y evaluación de vulnerabilidades se vio restringida por las limitaciones de acceso a sistemas, aplicaciones y datos específicos. No se pudo profundizar completamente en la evaluación de vulnerabilidades debido a restricciones en el acceso a ciertos componentes de la red institucional.

Durante la implementación de la solución SSO y SAML, las limitaciones surgieron en el monitoreo del comportamiento real de los usuarios. Factores impredecibles o problemas inesperados pueden haber afectado la evaluación precisa del rendimiento y la seguridad de la implementación.

Es importante recordar que estas limitaciones no deben considerarse como fracasos, sino como áreas de mejora y oportunidades para futuros trabajos en la evolución de tu proyecto.

5.4. Trabajo futuro

Aunque se alcanzaron los objetivos del proyecto, se identificaron oportunidades. Este trabajo representa el primer paso en la implementación de un enfoque Zero Trust más completo. A futuro, se prevé la adición de más características y componentes del modelo Zero Trust para mejorar la seguridad y la gestión de identidades en la institución. Entre las áreas de desarrollo futuro se encuentran:

- Implementación de Políticas de Seguridad Avanzadas: Se deberán implementar políticas de seguridad adicionales para regular el comportamiento de los usuarios una vez que han obtenido acceso a los sistemas. Esto mejorará la supervisión y la mitigación de riesgos en tiempo real.

- Seguimiento y Análisis Avanzado de Registros: Se buscará establecer un seguimiento y análisis de registros más avanzado para detectar y restringir posibles

comportamientos sospechosos. Esto contribuirá a una seguridad más proactiva y a la identificación de amenazas en una etapa temprana.

- Mejoras en la Autenticación: Se investigará la mejora de los métodos de autenticación, como la implementación de la verificación en dos pasos. Esto fortalecerá aún más la seguridad en el acceso a los sistemas institucionales.

- Microsegmentación con Base en Zero Trust: Se planea implementar una estrategia de microsegmentación siguiendo el modelo de Zero Trust. Esta técnica segmenta la red en unidades más pequeñas y controladas, lo que reduce la superficie de ataque y mejora la seguridad global.

- Detección Automatizada de Amenazas: Se considera la integración de sistemas de detección automatizada de amenazas, que permitan identificar y responder rápidamente a posibles incidentes de seguridad. Esto fortalecerá la postura de seguridad global de la institución.

Bibliografía

[Bha23] Rajat Bhargava. ¿en qué consiste el inicio de sesión Único (sso)?, 2023.

[Cas20] Keith Casey. What Is Attribute-Based Access Control (ABAC)?, 2020.

[clo23] cloudflare. ¿qué es la gestión de identidad y acceso?, 2023.

[Cse20] Andras Cser. The forrester wave™: Customer identity and access management, q4 2020 tools and technology: The identity and access management playbook. 10 2020.

[ELS+22] HEILMAN ETHAN, MUGNIER LUCIE, GOLDBERG SHARON, MARCUS YUVAL, and LIPMAN SEBASTIEN. ZERO TRUST AUTHENTICATION, 2022.

[Fit20] Laura Fitzgibbons. Modelo de confianza cero o red de confianza cero (ztn), 11 2020.

[GC21] Jason Garbis and Jerry W Chapman. Zero Trust Architectures, pages 19–51. Apress, 2021.

[Goo23] Google. Passwordless login with passkeys | authentication, 2023. Accessed on November 12, 2023.

[HFK+13] Vincent C Hu, David Ferraiolo, Rick Kuhn, Arthur R Friedman, Alan J Lang, Margaret M Cogdell, Adam Schnitzer, Kenneth Sandlin, Robert Miller, and Karen Scarfone. Guide to attribute based access control (abac) definition and considerations (draft). NIST special publication, 800(162):1–54, 2013.

[Inc23] Gluu Inc. Gluu identity and access management, 2023.

[Joi22] Joint Defense Information Systems Agency (DISA) and National Security Agency (NSA). Department of Defense (DOD) Zero Trust Reference Architecture. DISA Zero Trust Program Lead (ID2), page 104, 2022.

[Key21] Keycloak. Keycloak: Open source identity and access management, 2021.

[Lop22] Anderson Jesús Castillo Lopez. Diseño de un modelo para identificar amenazas no intencionales de ciberseguridad en instituciones públicas generadas por personal interno a partir de su comportamiento sobre la infraestructura de ti. pages 6–142, 20222.

[Mic23] Microsoft. Adoptar una seguridad proactiva con confianza cero, 11 2023.

[MLDR18] Karin Ana Melendez-Llave and Abraham Eliseo Dávila-Ramón. Problemas en la adopción de modelos de gestión de servicios de tecnologías de información. una revisión sistemática de la literatura. Dyna, 85:215–222, 2018.

[NF20] NIST and JOINT TASK FORCE. Special publication 800-53 revision 5: Security controls for information systems and organizations. 11 2020.

[NIS14] NIST. Guide to attribute based access control (abac) definition and considerations, 2014.

[NIS20] NIST. Nist special publication 800-207: Zero trust architecture, 2020.

[Okt23a] Okta. Auth0: Secure access for everyone. but not just anyone., 2023.

[Okt23b] Okta. Okta: Identity for the internet, 2023.

[Pal19] Palo Alto Networks. UNDERSTANDING ZERO TRUST TERMINOLOGY. Palo Alto Networks, page 23, 2019.

[RCPLC+15] Diego Rivera, Luis Cruz-Piris, German Lopez-Civera, Enrique de la Hoz, and Ivan Marsa-Maestre. Applying an unified access control for IoT-based intelligent agent systems. In 2015 IEEE 8th international conference on service-oriented computing and applications (SOCA), pages 247–251. IEEE, 2015.

[Ris13] Erik Rissanen. extensible access control markup language (xacml) version 3.0. Technical report, OASIS Open, January 2013.

[ROSS22] DURBHA SEETHARAMA R, MARCIA OSCAR, HOGGAN STUART, and KRAUSS SIMON. ZERO SIGN-ON AUTHENTICATION, 2022.

[Sho14] A Shostack. Threat Modeling: Designing for Security. Wiley, 2014.

[SSAV19] Mahendra Pratap Singh, Shamik Sural, Vijayalakshmi Atluri, and Jaideep Vaidya. Security analysis of unified access control policies. In International Conference On Secure Knowledge Management In Artificial Intelligence Era, pages 126–146. Springer, 2019.

[TUI21] Songpon Teerakanok, Tetsutaro Uehara, and Atsuo Inomata. Migrating to Zero Trust Architecture: Reviews and Challenges. Security and Communication Networks, 2021:9947347, 2021.

[TY12] MINAMIZAWA TAKEAKI and TOYODA YUKI. ACCESS CONTROL DEVICE, ACCESS CONTROL SYSTEM, ACCESS CONTROL METHOD, AND ACCESS CONTROL PROGRAM, 2012.

[WSO22a] WSO2. Access control with WSO2 Identity Server, 2022.

[WSO22b] WSO2 Identity Server. Identity Server Documentation, 2022.

[YBJ+22] M E I YAN, H U BAOSHENG, X U JIAN, Z H A ZHENGPENG, WANG JIANING, SHENG CHENGHONG, YUAN QIUJIN, W U JUNCHANG, C A O XIN, and L I WEIDONG. Zero-trust model-oriented access control device and implementation method, 2022.

[YH19] L I YUANJUN and CHEN HONGRUI. Uniform authorization center-based access control system and control method, 2019.

[ZGS+20] C A I ZHIXIAN, CHEN GUIMIN, L I N SHAN, HUANG JIAN, F A N LIPENG, C A I LING, and Q I N RUPENG. Zero-trust authentication system, 2020.