Institución Universitaria

Diseño de una arquitectura de Security Service Edge basada en SASE para ambientes de Cloud AWS.

Luis Alberto Martínez Salgado

Andrés Felipe Ramírez Restrepo

Instituto Tecnológico Metropolitano

Facultad de Ingeniería

Medellín, Colombia

2026

Diseño de una arquitectura de Security Service Edge basada en SASE para ambientes de Cloud AWS.

Luis Alberto Martínez Salgado

Andrés Felipe Ramírez Restrepo

Tesis o trabajo de investigación presentada(o) como requisito parcial para optar al título de:

Magister en Seguridad informática

Director (a):

Título (Mg.,) Javier Mauricio Duran Vásquez

Línea de Investigación: Ciencias Computacionales

Instituto Tecnológico Metropolitano

Facultad de Ingeniería

Medellín, Colombia

Año 2026

Dedicatoria

Este trabajo de investigación está dedicado con todo nuestro agradecimiento a nuestras familias, por su amor, paciencia y el apoyo incondicional que nos brindaron en cada momento de este recorrido. A nuestros amigos y compañeros, por ser nuestra guía, fuente de aprendizaje y lealtad, acompañándonos en cada desafío. Finalmente, a nuestros profesores y director de grado, quienes nos ofrecieron su confianza, amistad y sabiduría, dándonos siempre el impulso necesario para seguir adelante.

Agradecimientos

En primer lugar, damos gracias a Dios, por darnos la fortaleza, sabiduría y perseverancia para superar los desafíos de este proceso. Sin su guía y bendiciones, este logro no hubiera sido posible.

A nuestro director de proyecto, Javier Mauricio Durán Vásquez, le agradecemos profundamente por su orientación, paciencia y compromiso con el desarrollo de este trabajo. Su conocimiento, apoyo constante y valiosos consejos fueron fundamentales para la culminación exitosa de este proyecto.

A nuestras familias, por su amor incondicional, paciencia y comprensión a lo largo de todo este camino. Gracias por su apoyo inquebrantable, por estar siempre a nuestro lado y por los sacrificios que hicieron para que pudiéramos alcanzar esta meta.

A nuestros amigos y compañeros, por su ánimo y por ser siempre una fuente de inspiración y apoyo en cada etapa de este proyecto.

Finalmente, agradecemos a la Institución Tecnológica Metropolitano (ITM), al cuerpo de docentes que de alguna manera hicieron parte del proceso, por brindarnos las bases necesarias para la realización de este trabajo. Su apoyo institucional fue clave en nuestro desarrollo académico.

RESUMEN DEL PROYECTO

La creciente migración de entidades financieras hacia la nube pública de Amazon Web Services (AWS) ha traído consigo una serie de beneficios, como la escalabilidad y la reducción de costos. Sin embargo, esta transición también ha expuesto a estas organizaciones a importantes desafíos en materia de seguridad de la información. La falta de un diseño específico para mitigar los riesgos asociados con la navegación en este entorno compartido ha generado vulnerabilidades críticas, como fugas de información y accesos no autorizados a datos sensibles. Para afrontar este reto, se hace crucial desarrollar una solución que ayude a mitigar la pérdida de la confidencialidad, integridad y disponibilidad de la información. Así, el objetivo general de este trabajo de profundización es proponer un diseño para una solución de Security Service Edge (SSE) en AWS basada en la arquitectura Secure Access Service Edge (SASE), utilizando controles como Secure Web Gateway (SWG) y Zero Trust Network Access (ZTNA) para establecer políticas de seguridad.

Para abordar estos desafíos, se han establecido objetivos claros que guiarán el desarrollo de esta solución. En primer lugar, se caracterizarán los criterios de aceptación necesarios para la solución SSE, enfocándose en mitigar los riesgos de fuga de información mediante controles como SWG y ZTNA. Luego, se identificarán las tecnologías más adecuadas que cumplan con estos criterios. Posteriormente, se integrará las tecnologías para SWG y ZTNA, permitiendo la generación del diseño SSE. Finalmente, se evaluará el cumplimiento de estos criterios mediante el desarrollo de una prueba de concepto (PoC) en AWS. A través de este enfoque metodológico, se pretende contribuir significativamente a la mejora de la seguridad en la nube, fortaleciendo así la confianza en las operaciones digitales del sector financiero y avalando la protección de sus activos.

El presente trabajo de profundización pretende ser un referente en el acople de tecnologías de seguridad en ambientes de nube pública en AWS. Así, se espera que los resultados obtenidos puedan ser aplicados en diferentes contextos, desde pequeñas y medianas empresas hasta grandes corporaciones, adaptándose a las necesidades específicas del entorno de seguridad. Además, este trabajo de profundización servirá como base para futuras investigaciones y desarrollos en el campo de la ciberseguridad, contribuyendo a crear entornos digitales seguros y resilientes.

Palabras Claves: Amazon Web Services (AWS), diseño Security Service Edge (SSE), filtrado de contenido web (WCF), Controles, Secure Access Service Edge (SASE), seguridad en la nube, Zero Trust Network Access (ZTNA).

ABSTRACT

The increasing migration of financial institutions to the Amazon Web Services (AWS) public cloud has brought with it a number of benefits, such as scalability and cost reduction. However, this transition has also exposed these organizations to significant information security challenges. The lack of a specific design to mitigate the risks associated with browsing this shared environment has led to critical vulnerabilities, such as information leaks and unauthorized access to sensitive data. To address this challenge, it is crucial to develop a solution that helps mitigate the loss of confidentiality, integrity, and availability of information. Thus, the overall objective of this in-depth study is to propose a design for a Security Service Edge (SSE) solution on AWS based on the Secure Access Service Edge (SASE) architecture, using controls such as Secure Web Gateway (SWG) and Zero Trust Network Access (ZTNA) to establish security policies.

To address these challenges, clear objectives have been established to guide the development of this solution. First, the acceptance criteria required for the SSE solution will be characterized, focusing on mitigating information leakage risks through controls such as SWG and ZTNA. Next, the most appropriate technologies that meet these criteria will be identified. Subsequently, the technologies for SWG and ZTNA will be integrated, enabling the generation of the SSE design. Finally, compliance with these criteria will be assessed through the development of a proof of concept (PoC) on AWS. Through this methodological approach, the aim is to significantly contribute to improving cloud security, thus strengthening confidence in the digital operations of the financial sector and ensuring the protection of its assets.

This in-depth work aims to serve as a benchmark for the integration of security technologies in public cloud environments on AWS. Thus, the results obtained are expected to be applicable in different contexts, from small and medium-sized businesses to large corporations, adapting to the specific needs of the security environment. Furthermore, this in-depth work will serve as a foundation for future research and development in the field of cybersecurity, contributing to the creation of secure and resilient digital environments..

Keywords: Amazon Web Services (AWS), Security Service Edge (SSE) Design, Web Content Filtering (WCF), Controls, Secure Access Service Edge (SASE), Cloud Security, Zero Trust Network Access (ZTNA).

Tabla de Contenido

Índice de Figuras

Índice de Tablas

Abreviaturas

Abreviatura	Término
AWS	Amazon Web Services (Servicios Web de Amazon).
SSE	Security Service Edge (Borde de Servicio de Seguridad).
SASE	Secure Access Service Edge (Borde de Servicio de Acceso Seguro).
SWG	Secure Web Gateway (Puerta de Enlace Web Segura).
ZTNA	Zero Trust Network Access (Acceso a Red de Confianza Cero).
VPC	Virtual Private Cloud (Nube Privada Virtual).
IAM	Identity and Access Management (Gestión de Identidades y Accesos).
KMS	Key Management Service (Servicio de Gestión de llaves).
TLS	Transport Layer Security (Seguridad en la Capa de Transporte).
SSL	Secure Sockets Layer (Capa de Conexión Segura).
VLAN	Virtual Local Area Network (Red de Área Local Virtual).
WAF	Web Application Firewall.
Azure AD	Azure Active Directory (Directorio Activo de Azure)
GCP	Google Cloud Platform (Nube Publica Google Cloud Platform).
IAP	Identity Aware Proxy.
SSO	Single Sign-On (Inicio de sesión unificado).
POC	Prueba de concepto.
MFA	Autenticación Multifactor
NGFW	Next Generation Firewall
XSS	Cross-site scripting

INTRODUCCIÓN

En la actualidad, muchas entidades financieras están adoptando la nube pública, especialmente plataformas como AWS, para mejorar la escalabilidad, flexibilidad y reducir costos operativos. Ejemplos como Itaú, Unibanco en Brasil y Bancolombia en Colombia muestran cómo estas organizaciones están migrando parte de su infraestructura hacia la nube con el fin de mantenerse competitivas en un mercado que exige constante innovación tecnológica. Sin embargo, esta migración también plantea desafíos significativos en términos de seguridad de la información. A medida que los datos y las operaciones se trasladan a la nube, proteger la confidencialidad, integridad y disponibilidad de la información se vuelve aún más importante [1]. A continuación, en la Fig. 1 se observa la proyección del cambio de nube vs los esquemas tradicionales, según Gartner, en todo el mundo, 2019 – 2025 [2].

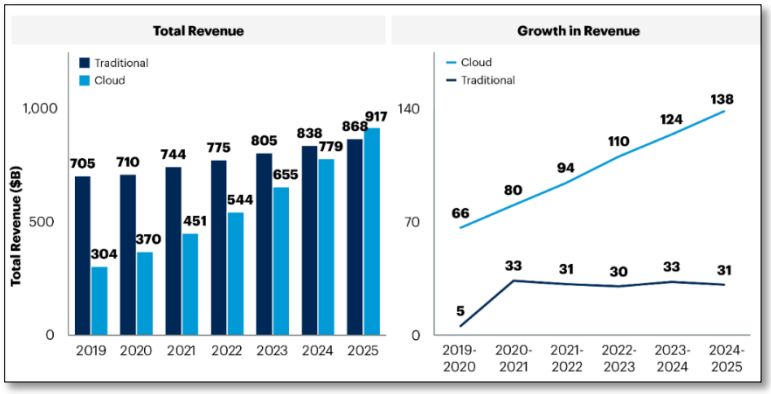

Fig. 1 Proyección de cambios de la nube, tomado de *[2]*.

El uso de infraestructuras compartidas en la nube incrementa la exposición a riesgos de seguridad como fugas de información, accesos no autorizados y configuraciones incorrectas. Un informe de [3] señala que el 81% de las empresas que utilizan la nube pública han experimentado al menos un incidente de seguridad, lo que subraya la necesidad de contar con estrategias robustas de mitigación de riesgos. Aunque AWS ofrece múltiples herramientas de seguridad, como cifrado de datos, control de accesos y firewalls (Security Groups) [4], no proporciona una guía estandarizada para gestionar riesgos específicos asociados con la navegación desde la nube hacia Internet. Esto deja a las entidades financieras expuestas a amenazas como la exfiltración de datos, el malware y accesos indebidos, afectando el cumplimiento de regulaciones como la Ley General de Protección de Datos Personales. En la Fig. 2 se muestran los desafíos en la gestión de las operaciones diarias de seguridad en la nube [5].

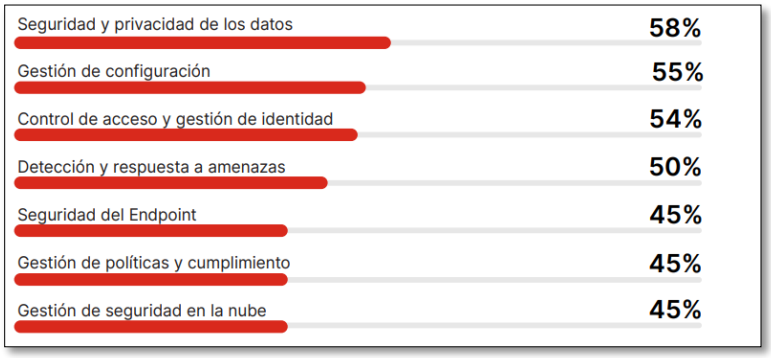

Fig. 2 Retos en las operaciones diarias en nube, tomado de *[5]*.

Para abordar este desafío, se propone un diseño de SSE basado en la arquitectura SASE, mediante la utilización de herramientas basadas en ZTNA. Lo cual permite establecer políticas de seguridad en el perímetro de la red, minimizando el riesgo de accesos no autorizados y la protección continua de los activos. Diversos estudios evidencian que la adopción de arquitecturas SSE y SASE contribuye a la reducción de incidentes de seguridad en entornos de nube. En particular, organizaciones que han implementado estos modelos reportan una disminución aproximada entre el 20% y 30 % en incidentes de seguridad, lo que demuestra la efectividad de estas soluciones para proteger infraestructuras modernas [6], [7].

La migración hacia la nube no solo afecta a las empresas, sino que también se ha convertido en un problema de seguridad a nivel global. En Colombia, por ejemplo, el país registró 20,000 millones de intentos de ciberataques en 2022, lo que representa un aumento del 80% respecto al año anterior [8], [9]. Adicionalmente, un informe de riesgos [10], destaca que el error humano sigue siendo un factor clave en la inseguridad de la nube: el 60% de las cargas de trabajo de contenedores carecen de configuraciones de seguridad adecuadas, y más del 36% presentan configuraciones predeterminadas inseguras del proveedor. Este problema se agrava cuando la navegación desde la nube hacia Internet se realiza sin controles adecuados, facilitando el acceso de actores malintencionados a los sistemas corporativos [10].

La importancia de este trabajo de grado radica en la necesidad de proteger la infraestructura en la nube pública del sector financiero, implementando controles para la navegación en Internet. En este contexto, SSE se posiciona como una solución clave para mitigar riesgos como la fuga de información, el malware y accesos no autorizados. Este estudio propone un marco práctico para el diseño de SSE en entornos de AWS, aplicando tecnologías de SWG para inspección de tráfico TLS/SSL, filtrado de contenido web y control

de aplicaciones, y ZTNA para brindar acceso basado en el principio de mínimo privilegio [11], [11]. Casos de éxito respaldan estas soluciones. Empresas del sector financiero como el Banco Internacional Raiffeisen han logrado consolidar la seguridad en la nube mediante la adopción de tecnologías SSE. De manera similar, CARE Ratings, al implementar soluciones de SWG, CASB y ZTNA, mejoró la visibilidad del uso de la nube y fortaleció el control de accesos no autorizados [12] [13].

OBJETIVO GENERAL

Proponer el diseño de una solución para SSE en AWS basada en la arquitectura SASE, a través de la utilización de controles como SWG y ZTNA, estableciendo políticas de seguridad en el perímetro de la red, mitigando fugas de información y accesos no autorizados, a los recursos de nube de entidades financieras.

OBJETIVOS ESPECÍFICOS

- Caracterizar un conjunto criterios de aceptación para la solución de SSE en la nube de AWS que contribuyan a la mitigación de los riesgos de fuga de información y accesos no autorizados, a través de SWG y ZTNA.

- Seleccionar las tecnologías que mejor cumplan los criterios de aceptación, para los controles de seguridad SWG y ZTNA en la solución de nube SSE AWS.

- Integrar las tecnologías seleccionadas a un diseño de arquitectura SSE para la implementación de los controles SWG y ZTNA en la nube de AWS.

- Evaluar el cumplimiento de los criterios de aceptación de la solución SSE a través del desarrollo de una prueba de concepto PoC en la nube de AWS que integre los controles SWG y ZTNA.

1. MARCO TEÓRICO Y ESTADO DEL ARTE

En este capítulo se describen los conceptos necesarios para abordar y comprender el desarrollo de esta propuesta, dichos temas se agrupan dentro de las siguientes áreas: Amazon Web Services (AWS), Zero Trust Network Access (ZTNA), Diseño Security Service Edge (SSE), Filtrado de contenido web (WCF), Secure Access Service Edge (SASE), Seguridad en la nube. Además, se exponen trabajos e investigaciones previas que abordaron objetivos similares a este. Estos estudios previos sientan las bases para el desarrollo de esta propuesta, proporcionando un punto de partida para abordar los desafíos de la seguridad en la navegación web en entornos de nube pública.

1.1. Marco teórico

La seguridad en la nube pública se ha vuelto crucial para proteger los datos en entornos digitales, su crecimiento acelerado [14], [15]; ha generado la necesidad de medidas necesarias que combatan amenazas cibernéticas y gestionen los servicios de la nube [16], [17], [18]. En este contexto, la arquitectura Secure Access Service Edge (SASE) surge como respuesta, agrupando la seguridad de red y servicios de acceso, donde la protección de los datos es primordial [19], [20], [21]. Además, el filtrado web y la clasificación de sitios se vuelven importantes para defender amenazas y promover un uso de la red. Explorar estos aspectos revela la importancia del filtrado de contenido y la clasificación de sitios. La prevención de fuga de información Data Lost Prevención (DLP) completa el panorama, abordando conceptos y técnicas clave para evitar la divulgación no autorizada de datos [22], [23].

Partiendo de lo expresado, es relevante considerar cómo AWS se ha consolidado como un líder en el ámbito de la computación en la nube, lo cual se evidencia en el primer trimestre de 2024, donde AWS controlaba aproximadamente el 31% del mercado mundial de servicios de infraestructura en la nube, mientras que su principal competidor, Microsoft Azure, tenía una participación del 25% y Google Cloud ocupaba el 11% [24], [25]. AWS ofrece una variedad de servicios que incluyen almacenamiento, computación, bases de datos y herramientas de análisis, todos diseñados para facilitar la escalabilidad y la flexibilidad. Un aspecto clave de la infraestructura de AWS es su diseño global, que abarca 108 zonas de disponibilidad en 34 regiones geográficas, lo que ofrece una alta disponibilidad y resiliencia. En la Fig. 3, se observa cómo el mapa de infraestructura no solo muestra la distribución de los centros de datos, sino que también resalta cómo AWS puede ofrecer servicios con baja latencia y alto rendimiento a nivel mundial [26].

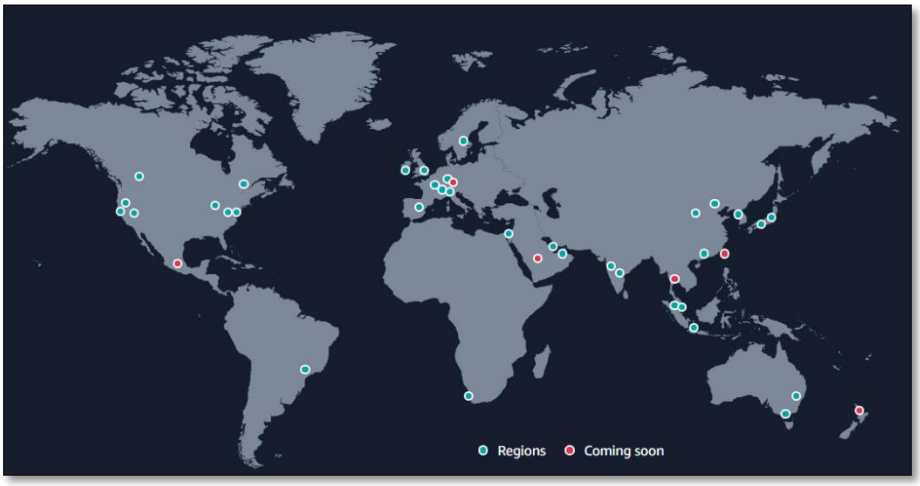

Fig. 3 Infraestructura global de AWS por regiones, tomando de *[26]*.

Este mapa es fundamental para entender la capacidad de AWS para proporcionar servicios rápidos a sus clientes en todo el mundo [26]. Uno de los aspectos más destacados de AWS es su enfoque en la seguridad, que se basa en un modelo de responsabilidad compartida. Esto significa que, aunque AWS protege su infraestructura, los usuarios también son responsables de asegurar sus datos y aplicaciones. La plataforma incluye características de seguridad integradas, como el cifrado de datos, la gestión de identidades y accesos, y herramientas de monitoreo continuo, que ayudan a las organizaciones a mantener un entorno seguro. Además, AWS cumple con numerosas certificaciones de cumplimiento, lo que proporciona a los clientes la confianza necesaria para operar en la nube [27], [28] y [29].

En este sentido, el diseño SSE se muestra como un complemento importante para la seguridad en la nube. SSE se centra en la integración de soluciones de seguridad en un marco adherente que opera en la nube, permitiendo a las organizaciones gestionar de manera integral sus políticas de seguridad. Este enfoque facilita la implementación y el mantenimiento de medidas de protección adicionales, combinando funciones como el filtrado de contenido web, la prevención de pérdida de datos y el acceso seguro a aplicaciones [30].

Al ofrecer un enfoque integral la seguridad en la nube, las empresas pueden contener a las amenazas emergentes, con una defensa robusta y proactiva. Además, una de las características claves de SSE es su enfoque en el borde de la red (Edge) [31], lo que indica que la seguridad se centra más del lado del usuario final. También, SSE brinda trazabilidad en tiempo real de las actividades de la red, lo que resulta

importante para la detección anticipada de incidentes de seguridad. La implementación de SSE fortalece la postura de seguridad de la empresa, creando así un entorno seguro para las operaciones en la nube y obteniendo visibilidad en tiempo real de las actividades en la red, lo que es crucial para la detección temprana de incidentes de seguridad [30] , [32].

El filtrado de contenido web (WCF) es una herramienta esencial en la estrategia de seguridad de las organizaciones, protegiendo a los usuarios y sistemas de amenazas en línea. Esta solución permite analizar y controlar el tráfico web, bloqueando accesos no autorizados a sitios peligrosos. Al implementar WCF, las empresas pueden prevenir la descarga de malware, el phishing y otros ataques cibernéticos que comprometen la integridad de sus datos. Asimismo, el filtrado de contenido ayuda a cumplir con políticas de cumplimiento normativo, para que los empleados no accedan a contenido perjudicial. La personalización de las políticas de filtrado según las necesidades específicas de la empresa permite un enfoque detallado en la gestión de riesgos. En un entorno donde la navegación web es crucial, el WCF se convierte en un componente clave para mantener un entorno seguro en la nube, complementando estrategias de seguridad como SASE y SSE. En la Fig. 4 se observa el concepto de WCF, lo que resalta su importancia en la infraestructura de seguridad. Al integrar WCF, las organizaciones mejoran su capacidad de respuesta ante amenazas y la postura de seguridad general [33], [34] y [35].

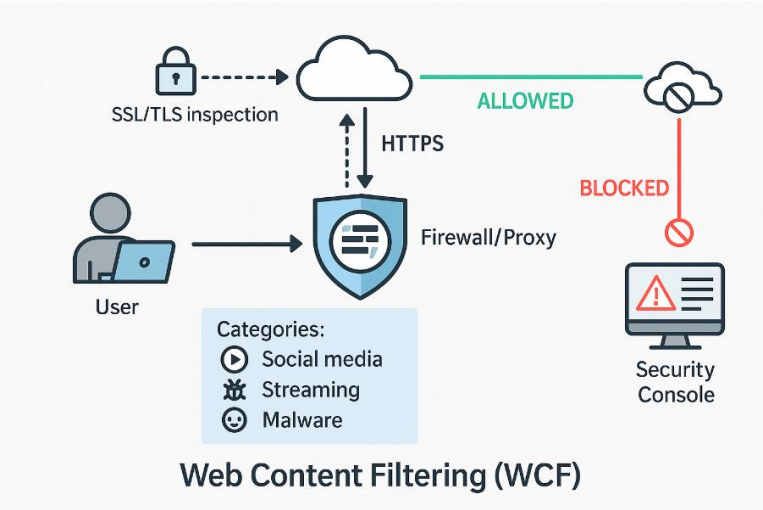

Fig. 4 Arquitectura técnica de filtrado de contenido web, creación propia, adaptado con IA.

La arquitectura SASE ha surgido como un enfoque innovador para la seguridad y conectividad en la nube, integrando funciones de red y seguridad en una solución unificada. Este modelo es particularmente relevante en un entorno laboral remoto, ya que permite a las organizaciones ofrecer acceso seguro a aplicaciones y datos desde cualquier ubicación. Al combinar capacidades como el acceso seguro a la red, el filtrado de contenido y la prevención de pérdida de datos, SASE proporciona una defensa sólida contra las amenazas cibernéticas. Además, mejora la experiencia del usuario al reducir la latencia y aumentar la velocidad de acceso. Al complementarse con las soluciones de AWS y el filtrado de contenido web (WCF), SASE fortalece la postura de seguridad de las organizaciones, permitiendo un entorno seguro para las operaciones en la nube. En un panorama digital lleno de amenazas, SASE se presenta como una solución para enfrentar los desafíos de seguridad actuales [19], [20]; en la Fig. 5 se muestra como se integra SASE en la seguridad y la red [21].

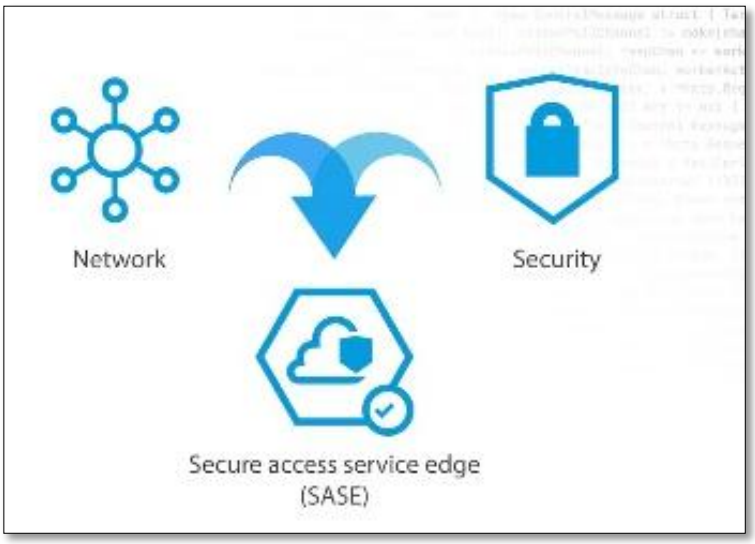

Fig. 5 Integración del concepto de SASE en la seguridad y en la red, tomado de *[21]*.

A continuación, en la TABLA 1 se muestran los principales beneficios que trae la implementación de SASE:

TABLA 1.
Beneficios que trae abordar SASE.

Beneficio	Aporte para el proyecto
Refuerza la seguridad	Ubica las capacidades de seguridad lo más cerca posible del usuario final, lo que refuerza la postura de seguridad general y dificulta la explotación de vulnerabilidades, así como la realización de ataques exitosos.
Mejora la resiliencia	Proporciona conectividad y seguridad con baja latencia para usuarios, dispositivos y servicios. Una red global de puntos de presencia (PoP) ofrece controles de red y seguridad sin comprometer el rendimiento.
Minimice el costo y la complejidad	Simplifica el trabajo para los equipos de TI y seguridad, mientras aumenta la visibilidad y reduce los costos de administración.
Admite Zero Trust	Emplea diversas señales contextuales y de amenazas para salvaguardar el acceso a los recursos internos y a Internet. Solo usuarios y dispositivos autorizados son de confianza y de tal manera han sido autenticados pueden acceder a la red.
Habilite escenarios de negocio	Facilita nuevos escenarios empresariales digitales al proporcionar controles de seguridad en el perímetro, donde son más necesarios para proteger a los usuarios, dispositivos y recursos que se encuentran fuera de la red y más allá del alcance de una infraestructura de seguridad local.
Aumenta la efectividad	Al ofrecer una plataforma única para desarrollar la estrategia de seguridad empresarial, SASE alinea las soluciones de seguridad y los equipos de TI, facilitando su colaboración.

Fuente: tomado de *[21]*.

De igual manera, la seguridad en la nube se define como una rama de la ciberseguridad que se dedica a proteger los sistemas informáticos en entornos de nube. Esto significa que los datos permanezcan protegidos y confidenciales en toda la infraestructura, las aplicaciones y los servicios en línea. La responsabilidad de proteger estos sistemas corresponde tanto a los proveedores de servicios en la nube como a los usuarios, que pueden incluir desde individuos, pequeñas y medianas empresas hasta grandes organizaciones. La seguridad en la nube abarca una variedad de tecnologías, protocolos y mejores prácticas que protegen los entornos informáticos, las aplicaciones que en ellos se ejecutan y los datos almacenados [16], [17], [18].

Es así como, el acceso a la red con confianza cero (ZTNA) se presenta como un enfoque de seguridad que se fundamenta en el principio de que no se debe confiar inmediatamente en usuarios y dispositivos, sin importar si están dentro o fuera del perímetro de la red de una organización. Cada solicitud de acceso, sin importar su origen, debe ser verificada y autenticada de manera rigurosa y continua para otorgar

o conservar el acceso a los recursos. Este enfoque de "nunca confiar, siempre verificar" ha demostrado ser efectivo que las defensas tradicionales se basan en el perímetro y la segmentación de la red. De esta manera, ZTNA se adapta a las necesidades de las empresas modernas, proporcionando protección en entornos de nube híbrida, redes locales, así como para trabajadores remotos y dispositivos, aplicaciones, datos e infraestructuras que utilizan, sin importar su ubicación [36], [37], [38] y [39] .

La confianza cero implica que cada usuario, dispositivo y aplicación deben ser verificados de manera constante. Una estrategia de seguridad basada en este modelo autentica y autoriza cada conexión y flujo de red, y se apoya en una amplia gama de datos para una visibilidad completa. La gran mayoría de los ataques involucran normalmente el uso o mal uso de credenciales comprometidas dentro de una red. Una vez que los actores malintencionados acceden al perímetro de una red, pueden generar daños en todos los sistemas. Con el rápido incremento de la migración a la nube y el trabajo remoto, la confianza cero emerge como una evolución de un modelo de seguridad que presenta limitaciones frente a la exposición asociada con las VPN de acceso remoto tradicionales. [37], [39].

La adopción de un modelo de confianza cero implica utilizar tecnologías y técnicas como la autenticación multifactor (MFA), el control de acceso basado en identidad, la microsegmentación, la seguridad de los puntos finales y la supervisión continua del comportamiento del usuario y del estado del dispositivo. Al combinar estos elementos, la confianza cero otorga el acceso únicamente según una evaluación de confianza en tiempo real, en lugar de basarse en la autenticidad de credenciales fijas o la posición en la red. Este modelo se fundamenta en la premisa de que ya ha ocurrido una filtración o que es probable que suceda, por lo que ningún usuario debe tener acceso a información sensible solo por haber pasado una verificación en el perímetro de la empresa [37], [38], [39].

Con el crecimiento de las diversas modalidades de trabajo remoto en las empresas, ZTNA se presenta como una solución segura para acceder a aplicaciones y datos sin depender de las redes privadas virtuales (VPN). Al integrarse con otras capacidades del Security Service Edge (SSE), como el filtrado de contenido web (SWG), ZTNA ofrece una protección integral contra amenazas, así como una revisión y control en tiempo real del acceso de los usuarios y de los flujos de datos en toda la red. Esta combinación mejora la seguridad y la experiencia del usuario al facilitar un acceso

más rápido y seguro a los recursos necesarios [37]; a continuación, en la Fig. 6, se ilustra las funcionalidades de ZTNA.

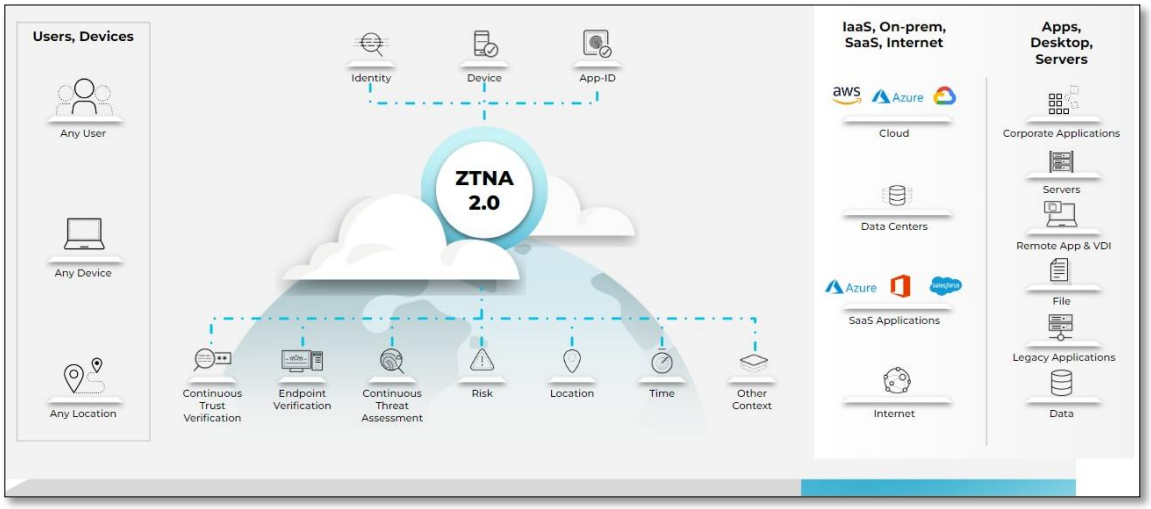

Fig. 6 Funcionalidad ZTNA, tomado de *[39]*.

En la Fig. 6, se observan las funcionalidades de ZTNA, destacando cómo cada uno de estos componentes se integra para proporcionar un acceso seguro y controlado a los recursos de la empresa. Adicional se puede mirar cómo ZTNA combina la autenticación continua, el monitoreo del comportamiento del usuario y la segmentación de red para crear un entorno seguro que se adapta a las necesidades cambiantes de las empresas. Esta visualización ayuda a comprender mejor cómo ZTNA implementa el enfoque de confianza cero en la práctica [39].

En este contexto, la prueba de concepto (POC) representa una fase del proyecto que permite comprobar si la integración entre los controles SWG y ZTNA puede funcionar dentro de un entorno controlado en AWS. Este tipo de prueba se utiliza para evaluar de manera limitada y experimental la viabilidad técnica y funcional del diseño propuesto, antes de llevarla a una implementación completa. Cabe resaltar que una POC no siempre garantiza el éxito del proyecto, ya que sus resultados pueden demostrar tanto la factibilidad del diseño como la necesidad de replantear o mejorar ciertos aspectos [40].

1.2. Estado del arte

La protección de la navegación desde la nube pública de AWS es un desafío crítico de la ciberseguridad, según un informe, publicado por [41], el 81% de las empresas han reportado haber experimentado al menos un incidente de seguridad relacionado con la nube en el último año, y casi la mitad (45%) ha sufrido al menos cuatro incidentes durante el mismo período. Además, se destaca que 95% de los profesionales de ciberseguridad están extremadamente preocupados por la seguridad en la nube pública, lo que ha generado un aumento del 4% en comparación con el año anterior [42]. Esta preocupación se traduce en un aumento significativo en los presupuestos destinados a la seguridad en la nube, con un 65% de las organizaciones aumentando sus inversiones en este ámbito, con un promedio del 36% de incremento [42]. Por otro lado, el 20% de los datos financieros almacenados en la nube están expuestos públicamente, lo que resalta la vulnerabilidad de los datos sensibles y la necesidad de endurecer las medidas de seguridad [41]. Estos datos reflejan un crecimiento del uso de servicios en la nube, adicional los riesgos asociados que se deben gestionar para proteger la información.

En los últimos años, la adopción de modelos de seguridad como SSE dentro de la arquitectura SASE han ganado importancia para proteger los entornos de nube pública, incluidos los basados en AWS. Jones y Silver [43], proponen que SSE es una solución que ofrece un enfoque completo para asegurar el acceso y el tráfico dentro de la nube. Este modelo, al integrar diversas tecnologías de seguridad como SWG y ZTNA, permite a las empresas crear una defensa fuerte contra amenazas externas. De manera similar, Sharma y Kumar [44], realizan un análisis comparativo de diferentes arquitecturas de seguridad, destacando cómo SASE y SSE pueden ser implementados en AWS para mejorar la protección de las infraestructuras en la nube, enfrentando tanto desafíos operacionales como técnicos, como la complejidad en la gestión de políticas de acceso y la escalabilidad. Por otro lado, Kumar y Gupta [45], proporcionan una revisión de cómo estas arquitecturas se aplican a servicios de nube, integrando SSE para asegurar la infraestructura en la nube pública. En conjunto, estos estudios destacan la importancia de implementar arquitecturas de seguridad basadas en SASE y SSE como una solución para abordar los riesgos de seguridad en la nube y asegurar la protección de datos y aplicaciones en AWS.

Por otra parte, autores como Forrester Research, y Palo Alto Networks, también han abordado este problema, proponiendo soluciones que integran tecnologías como

SSE, SWG y ZTNA. Estas soluciones permiten a las empresas adoptar un enfoque de seguridad robusto, diseñado para reducir los riesgos asociados con la migración a la nube y la vulnerabilidad ante amenazas externas en plataformas como AWS. SSE, en particular, se presenta como un enfoque crucial para las empresas que buscan asegurar sus datos y aplicaciones en la nube, dado que permite un control completo sobre el acceso, monitoreo de tráfico y protección de recursos alojados en entornos compartidos como AWS. Según [46] a adopción de SSE es esencial para las empresas que desean establecer una infraestructura de seguridad completa. Este enfoque no solo gestiona el acceso a la red de manera eficiente, sino que también optimiza la experiencia del usuario, al permitir una implementación dinámica de políticas de seguridad que se adaptan a las necesidades de las empresas.

InterVisio [47] resalta como la integración de tecnologías como ZTNA, SWG, CASB y Firewall as a Service (FWaaS) dentro de una arquitectura SSE, puede crear una defensa fuerte contra amenazas externas. Al integrar estas soluciones, las empresas logran un modelo de seguridad de Confianza Cero (Zero Trust), que permite que solo los usuarios y dispositivos autorizados puedan acceder a recursos críticos, lo que refuerza la protección de aplicaciones en la nube. Este modelo no solo reduce las vulnerabilidades, sino que también proporciona una mayor visibilidad y control de las actividades de red dentro de la infraestructura de AWS. En este sentido, tanto Gartner como InterVision coinciden en que una arquitectura SSE bien implementada es crucial para proteger los entornos de nube, especialmente aquellos que operan en entornos como AWS, donde la escalabilidad y la flexibilidad de los servicios deben estar acompañadas de medidas de seguridad para la protección continua frente a ciberamenazas y accesos no autorizados.

Partiendo de lo anterior, lo expuesto por AWS en su artículo, destaca que la seguridad es una prioridad fundamental en la nube, enfatizando el modelo de responsabilidad compartida que define las obligaciones de seguridad tanto para AWS como para sus clientes [48], [49]. Este modelo establece que, mientras AWS se encarga de la seguridad de la infraestructura, los clientes son responsables de la seguridad de sus datos y aplicaciones en la nube. Esto implica que las organizaciones deben implementar controles de acceso, cifrado de datos y monitoreo continuo para proteger sus activos. Por otro lado, el fabricante Zscaler subraya que la adopción de un enfoque de SSE es crucial para abordar estos desafíos, integrando tecnologías como SWG y ZTNA para proporcionar una defensa robusta contra amenazas cibernéticas [50].

La adopción de un modelo de SSE es fundamental para enfrentar estos retos de seguridad. [50] enfatiza que la arquitectura de SSE permite a las organizaciones proteger sus aplicaciones y datos sin comprometer la experiencia del usuario [50]. Al adoptar un enfoque de confianza cero, las organizaciones pueden asegurarse de que solo los usuarios autorizados tengan acceso a los recursos críticos, lo que minimiza el riesgo de fugas de información y accesos no autorizados. [51], arquitecta de soluciones en AWS también destaca la relevancia de emplear servicios de seguridad en la nube para salvaguardar aplicaciones web, tanto en entornos en la nube como en instalaciones locales [51], [52]. En su trabajo, [52] destaca cómo los servicios de AWS pueden ser utilizados para implementar medidas de seguridad, como la detección de amenazas y la protección perimetral. Complementando esta perspectiva, [52], enfatiza la necesidad de integrar soluciones de seguridad que permitan a las organizaciones gestionar los riesgos de sus aplicaciones y datos [52].

El modelo de responsabilidad compartida también se extiende a la gestión de datos y la seguridad de la red. Según un informe de CloudSecurity Ninja, los clientes son responsables de la configuración de políticas de seguridad, la gestión de accesos y la protección de datos en tránsito y reposo [53]. Esto implica que las organizaciones deben implementar controles de acceso, como la autenticación multifactor y la gestión de identidades, para que solo los usuarios autorizados puedan acceder a la información. Además, la configuración de reglas de firewall y grupos de seguridad es esencial para controlar el tráfico hacia y desde los recursos en la nube, lo que ayuda a prevenir ataques y vulneraciones de seguridad. Complementando esta perspectiva, Netskope enfatiza que la implementación de políticas de seguridad es fundamental para mitigar los riesgos asociados con la navegación en la nube [11]. La integración de SWG y ZTNA permite a las organizaciones no solo proteger sus datos, sino también cumplir con las regulaciones del sector financiero, lo que es crucial en un entorno donde la seguridad de la información es primordial [54].

Por otro lado, el estudio de [55] sobre la seguridad en la nube para AWS subraya la importancia de las integraciones de seguridad que facilitan la gestión y la visibilidad en todos los entornos [55]. Adicionalmente, [55] proporciona soluciones de firewall de próxima generación que son esenciales para proteger aplicaciones y datos en la nube, permitiendo que las organizaciones mantengan un alto nivel de seguridad en sus operaciones. Además, [48], [56] menciona que AWS sigue innovando en el ámbito de la seguridad, desarrollando nuevos servicios que permiten a las organizaciones gestionar sus riesgos de manera más proactiva y automatizada.

Se vienen investigando casos de estudio para entidades financieras, en este caso, la empresa estadounidense Ascensus se esforzó por comprender el riesgo de seguridad en su diversa infraestructura en la nube y cómo priorizar los esfuerzos de seguridad en función del riesgo para el negocio. Allí acompañó la empresa Netskope a ofrecer las soluciones de Next Gen Secure Web Gateway (SWG) y Cloud Access Security Broker (CASB), Ascensus resolvió estos desafíos y se dio cuenta de una reducción del tiempo necesario del personal, visibilidad del uso de las soluciones en la nube y DLP mejorado [57], [58].

Otro caso de estudio que se brinda en las entidades financieras se dio con Raiffeisen Bank International, una entidad financiera australiana, en donde consolida las tecnologías en una única plataforma y desbloquea la seguridad en la nube como un acelerador de negocios. Para esto, RIS acudió a Netskope para que les apoyara en su transición a las aplicaciones y servicios en la nube, lo que les permitió consolidar las tecnologías existentes en una única plataforma, proteger su uso de las aplicaciones en la nube y desbloquear la seguridad en la nube como acelerador de negocios [59], [60].

Investigaciones académicas refuerzan la navegación segura con SWG en Zero Trust. Según [61] valida arquitecturas híbridas donde SWG integra DLP granular, demostrando una reducción del 35% en exfiltración de datos sensibles vía navegación web comprometida, mediante inspección profunda de tráfico HTTPS. Según [62] implementa SWG como proxy inverso para tráfico web hacia aplicaciones AWS EC2/ALB, asegurando visibilidad completa en entornos multicloud y validando políticas de acceso contextuales alineadas al modelo de responsabilidad compartida de AWS. Complementariamente, [63] confirma SWG como control primario contra navegación maliciosa en almacenamiento distribuido, bloqueando el 92% de amenazas zero-day identificadas en sesiones HTTP/3 cifradas. Estos estudios académicos demuestran que SWG no solo complementa ZTNA, sino que se convierte en componente crítico para proteger la navegación hacia recursos críticos en AWS.

Según [64], realiza revisión sistemática de arquitecturas Zero Trust, cuantificando 40% reducción brechas mediante microsegmentación y verificación continua. Además [61], sistematiza 15 modelos IAM Zero Trust para nube híbrida, integrando análisis comportamental que reduce 35% accesos no autorizados. De acuerdo a [65], implementa la tesis de maestría en ZTNA automatizando AWS EC2/S3, demostrando Zero Trust con IaC (AES256, KMS, MFA) que supera VPN tradicional en latencia/throughput para ALB/Keycloak. Estos artículos confirman ZTNA como

evolución obligatoria del acceso tradicional, especialmente para entidades financieras donde la granularidad de políticas es regulatoria.

Continuando con la investigación, acerca de las entidades financieras a nivel mundial, se ha presentado el caso de CARE Ratings, la cual necesitaba mejorar la experiencia de usuario en la compañía para el entorno de TI híbrido y además se enfrentaba a la falta de visibilidad del uso de la nube y la navegación Web. Para este caso, con las soluciones de Secure Web Gateway (SWG), Cloud Access Security Broker (CASB) y ZTNA, CARE Ratings mejoró el conocimiento de la pérdida de datos, las políticas de acceso con información granular sobre el comportamiento del usuario y la visibilidad de los dispositivos no gestionados [66].

Finalmente, es importante señalar que Colombia enfrenta retos en el área de la ciberseguridad, particularmente en lo que respecta a la protección de datos en la nube pública. En 2023, el país sufrió un ciberataque masivo que afectó a más de 20 entidades públicas y 78 privadas, evidenciando la vulnerabilidad de sus sistemas digitales [67], [68]. En el primer semestre del año, se contabilizaron aproximadamente 5,000 millones de intentos de ciberataques, lo que coloca a Colombia como el cuarto país más atacado en América Latina, con un incremento del 79% en comparación con el año anterior. A pesar de estas preocupaciones, el gobierno colombiano ha tomado medidas proactivas para fortalecer la ciberseguridad, estableciendo la Dirección de Ciberseguridad del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), con el objetivo de desarrollar políticas y programas que mejoren la seguridad digital. Sin embargo, las entidades financieras siguen siendo los principales objetivos de los ciberdelincuentes debido a su acceso a información sensible, lo que resalta la necesidad urgente de implementar controles hardenizados para proteger los datos y la integridad de la infraestructura digital del país [69], [70].

2. METODOLOGÍA Y RESULTADOS

En este trabajo de profundización se empleó un enfoque mixto que combino métodos deductivos y experimentales. El enfoque deductivo se utilizó en las primeras fases, en las cuales se comenzó con la revisión de la literatura sobre la arquitectura SSE y las tecnologías de SWG y ZTNA. Se exploraron los conceptos claves y los principios que resaltaban estas tecnologías que desarrollaron un marco teórico desde el cual se derivaron criterios de aceptación específicos. Este enfoque se llevó a cabo realizando consultas en portales web, repositorios institucionales como el del ITM, artículos académico y bases de datos

científicas como Scopus o IEEE. Estos recursos permitieron analizar, categorizar y organizar la información disponible sobre la seguridad en la nube. Proporciono una base que valido los conceptos existentes en la mitigación de riesgos, como la protección contra fuga de información.

El enfoque experimental se aplicó en la fase final del estudio, cuando se desarrolló una prueba de concepto (PoC) en la infraestructura de AWS. Para esta fase, se utilizaron diversas herramientas y servicios de AWS, incluyendo Amazon VPC (Virtual Private Cloud), AWS Identity and Access Management (IAM) para la gestión de identidades y accesos, entre otras. Además, un componente importante de esta fase fue incorporar herramientas de código abierto que integraron tecnologías como ZTNA (Zero Trust Network Access) y SWG (Secure Web Gateway) dentro de la arquitectura de seguridad en la nube. La elección de estas herramientas nativas y de código abierto no solo respondieron a la necesidad de proporcionar una capa adicional de seguridad, sino que también aportaron un enfoque innovador al proyecto, dada la escasa documentación existente en fuentes oficiales o abiertas sobre este tipo de propuestas. Adicionalmente, se consideraron el uso de algunas herramientas nativas de la nube, con el objetivo de complementar y reforzar la solución de seguridad que se adoptó. Este enfoque resalto el carácter experimental e innovador del proyecto, posicionándose como un posible referente para futuros estudios y propuestas en seguridad en la nube.

Finalmente, se realizó la validación de políticas de acceso y evaluación de la seguridad en la navegación web, donde se verifico el cumplimiento de los criterios de aceptación previamente establecidos. Para la parte experimental, también se utilizaron herramientas de monitoreo y análisis como AWS CloudWatch y AWS CloudTrail que recopilo logs que permitieron evaluar las políticas de seguridad implementadas. A continuación, la Fig. 7 se presenta la metodología en cuatro fases, cada una diseñada para abordar el objetivo general y los objetivos específicos planteados.

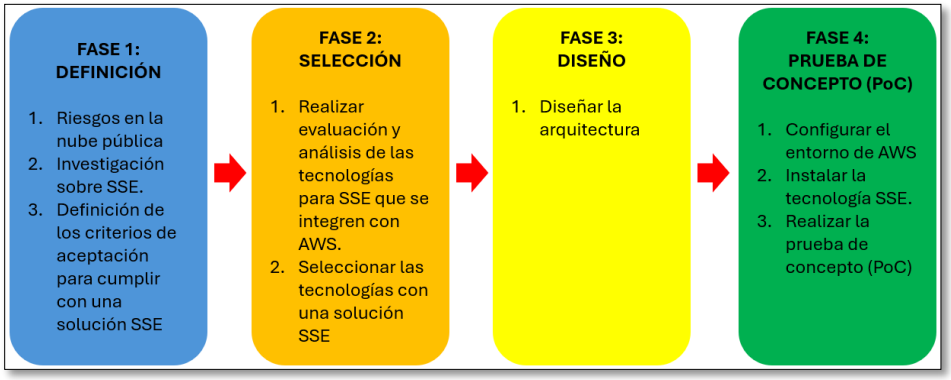

Fig. 7 Fases y actividades por objetivo, elaboración propia.

2.1 Fase 1 Definición.

2.1.1 Arquitecturas tradicionales vs modelo SSE

Las arquitecturas tradicionales basadas en el perímetro han sido ampliamente utilizadas para proteger los recursos organizacionales. Este enfoque se fundamenta en la idea de establecer un límite claro entre la red interna y el entorno externo, utilizando mecanismos como firewalls, VPN y sistemas de detección de intrusos. Sin embargo, con la adopción de la computación en la nube, el trabajo remoto y la descentralización de los recursos, este modelo ha evidenciado limitaciones significativas en términos de escalabilidad, visibilidad y control de accesos. A diferencia de este enfoque, las arquitecturas modernas como SSE, enmarcadas dentro del modelo SASE, proponen un esquema basado en identidad, contexto y principios de confianza cero. Este modelo elimina la dependencia del perímetro tradicional, permitiendo aplicar controles de seguridad directamente sobre los usuarios, dispositivos y aplicaciones, sin importar su ubicación [71]. A continuación, se muestra en la TABLA 2 un análisis comparativo orientado entre arquitecturas tradicionales de Filtrado de Navegación y el modelo SSE con SWG.

TABLA 2.
Comparación entre Filtrado tradicional Web y SWG.

Criterio	Filtrado Web Tradicional (Web 2.0)	SWG
Enfoque de seguridad	Basado en perímetro de red	Basado en identidad y contexto
Ubicación del control	Dentro de la red corporativa (on-premise)	En la nube (cloud-based)
Mecanismo principal	Listas negras/blancas de URLs	Análisis dinámico y políticas granulares
Capacidad frente a amenazas	Limitada a amenazas conocidas	Detección de amenazas avanzadas (malware, phishing, zero-day)
Inspección de tráfico HTTPS	Limitada o inexistente	Inspección SSL/TLS completa
Adaptación a entornos cloud	Deficiente	Nativa para SaaS, IaaS y trabajo remoto
Visibilidad del tráfico	Parcial	Alta visibilidad en tiempo real
Protección fuera de la red corporativa	No disponible o limitada	Protección continua sin importar la ubicación
Actualización de políticas	Manual o periódica	Automática y en tiempo real
Prevención de fuga de datos	No integrada	Integración con DLP (Data Loss Prevention)
Escalabilidad	Limitada (infraestructura física)	Alta (modelo cloud escalable)
Eficiencia frente a amenazas modernas	Baja	Alta

Fuente: Elaboración propia.

Por otra parte, en el contexto de la evolución de los modelos de acceso remoto, las redes privadas virtuales (VPN) han sido tradicionalmente utilizadas para permitir la conexión segura a recursos internos. Sin embargo, este enfoque presenta limitaciones en términos de seguridad y escalabilidad en entornos modernos. De acuerdo con [72], los modelos basados en confianza implícita, como las VPN, no son adecuados en arquitecturas distribuidas, lo que ha impulsado la adopción de enfoques como ZTNA. A continuación, se muestra en la TABLA 3 un análisis comparativo orientado entre arquitecturas tradicionales de VPN y el modelo SSE con ZTNA.

TABLA 3.
Comparación VPN Tradicional y ZTNA.

Criterio	VPN Tradicional	ZTNA
Enfoque de seguridad	Basado en perímetro	Basado en identidad y confianza cero
Modelo de acceso	Acceso a la red completa	Acceso solo a aplicaciones específicas
Nivel de confianza	Implícita tras autenticación inicial	Verificación continua ("never trust, always verify")
Exposición de la red	Alta (el usuario entra a la red)	Mínima (no se expone la red)
Superficie de ataque	Amplia	Reducida
Segmentación	Limitada o manual	Granular y dinámica
Experiencia del usuario	Puede ser lenta (backhauling)	Optimizada (acceso directo a la app)
Escalabilidad	Limitada por infraestructura	Alta (cloud-native)
Acceso remoto	Diseñado para acceso remoto tradicional	Diseñado para entornos híbridos y cloud
Visibilidad y control	Limitados	Alta visibilidad y control por sesión
Protección contra amenazas internas	Baja	Alta (microsegmentación)
Integración con nube	Compleja	Nativa
Autenticación	Generalmente única (login inicial)	Continua + contexto (dispositivo, ubicación, riesgo)

Fuente: Elaboración propia.

2.1.2 Riesgos en nube publica

Se inició con la revisión de fuentes, catálogos de amenazas y vulnerabilidades reconocidas internacionalmente [73], [74] también informes especializados como él (DBIR) 2024 [75], con el objetivo de identificar algunos de los riesgos y evaluar los controles de seguridad SWG y ZTNA, de esta manera se observó que ellos pueden mitigar algunos de los riesgos más recurrentes. Esta fase permitió conocer que el 68% de los incidentes de seguridad en la nube están relacionados con errores humanos [75], destacándose configuraciones incorrectas como una de las principales causas de las

brechas de seguridad. También se identificó que una parte significativa de las fugas de información ocurrieron debido a configuraciones erróneas de servicios en la nube, como permisos excesivos en AWS S3 o políticas mal definidas en Identity and Access Management (IAM).

Además, el acceso no autorizado y el uso indebido de credenciales representaron un riesgo [75], con el phishing siendo el método más común utilizado por actores maliciosos para obtener credenciales, involucrado al 51% de las empresas y en más del 25% de los ataques en la nube en los últimos cinco años [76], por otra parte de acuerdo al reporte de ciberseguridad realizado por [77] publicado en el presente año 2025 se ha registrado un aumento del 61% de los reportes de seguridad en la nube durante los últimos 12 meses, lo cual representó un aumento significativo en comparación con el 24% del año anterior, teniendo como tendencias claves en cuanto a amenazas a la nube las siguientes: aprovechamiento de vulnerabilidades, ataques de ingeniería social, movimiento lateral, exfiltración de datos, aumento de la velocidad. Así mismo dentro del top 3 de Vulnerabilidades más explotadas durante el año 2024 se encontró: brechas de seguridad de datos, uso indebido de los servicios en la nube, errores de configuración y administración [77].

Adicionalmente, un informe de [78] sobre el costo de las brechas de datos 2024 señaló que el costo promedio de una filtración de datos en nubes públicas alcanzó los 5,17 millones de dólares, siendo así el valor más alto registrado en comparación con otros entornos de almacenamiento. Este incremento resaltó la importancia de tomar medidas de seguridad, particularmente aquellas enfocadas en el acceso seguro y la mitigación de riesgos asociados a configuraciones incorrectas y accesos no autorizados [78]. A partir de lo anterior, en la Fig. 8 se presentan algunos de los riesgos más comunes en la infraestructura de la nube, identificados por [79]

Fig. 8 Los 6 principales riesgos de seguridad en la nube, tomado de *[79]*.

Por otro lado, para definir los criterios de aceptación de SSE en AWS, fue fundamental conocer los riesgos críticos relacionados con la fuga de información y los accesos no autorizados. Estos riesgos han sido identificados a partir de fuentes de referencia como: [75], [76], [78] , [80], [81], [82], [83].

Partiendo de las fuentes de referencia consultadas se documentan los siguientes riesgos que han sido destacados por su frecuencia en incidentes de seguridad en la nube, como se muestra en la TABLA 4.

TABLA 4.

Riesgos con mayor frecuencia en incidentes de seguridad en la nube.

Riesgo	Descripción	Cifras/Relevancia	Ejemplos
Acceso no autorizado a datos sensibles.	Usuarios no autorizados acceden a información confidencial.	El 43% de las filtraciones involucran credenciales robadas [84].	Un atacante accede a bases de datos sin permisos adecuados.

Fugas de información.	Configuraciones incorrectas exponen datos críticos. Empleados o socios roban o filtran datos confidenciales. Configuraciones erradas, extracción no autorizada de datos por parte empleados, infostealers. Actores maliciosos intentan comprometer credenciales o sistemas.	El 60% de los ataques provienen de amenazas internas [85]. Según la publicación de [79], el costo promedio de una filtración de datos alcanzó los 4,45 millones de dólares en 2023. De acuerdo al estudio de seguridad en la nube edition global 2024 publicado por [86], el 44% de las organizaciones ha sufrido una vulneración de datos en la nube, y el 14% declaró haber tenido un incidente en los últimos 12 meses. El error humano y la configuración incorrecta continuaron siendo la principal causa de estas infracciones (31%), seguidos por la explotación de vulnerabilidades conocidas (28%) y la falta de uso de la autenticación multifactor (17%). Con base en la publicación realizada por [87] alrededor de un 25% de las incidencias de seguridad implica la presencia de infiltrados.	Un correo falso engaña a un usuario para robar sus credenciales [88]. Un empleado descarga datos críticos antes de renunciar. Repositorios o buckets públicos (como S3 en AWS) expuestos sin autenticación. Permisos excesivos en identidades (IAM), que permiten a usuarios o servicios hacer más de lo necesario (principio de menor privilegio no aplicado). Controles de cifrado desactivados o mal implementados. Captura sesiones activas o tokens de acceso.
Pérdida de la confidencialidad de datos no cifrados.	Datos en tránsito o en reposo sin cifrado pueden ser interceptados.	El 45% de los ataques a datos se deben a falta de cifrado [89].	Un atacante intercepta credenciales en texto plano [90].
Acceso no autorizado a recursos expuestos de Cloud.	Recursos mal protegidos que permiten accesos no autorizados.	El 30% de las empresas tienen servidores expuestos públicamente [91].	Un servidor mal configurado es accesible desde Internet.

		90% de los ciberataques inician con phishing [92].	
Daño reputacional y legal	Dominios comprometidos utilizados para distribuir malware o fraudes.	70% de las campañas de phishing usan dominios recién creados [93].	Un atacante usa un dominio similar a una empresa para estafas.
Indisponibilidad del servicio.	Sobrecarga de recursos en la nube, afectando la disponibilidad.	Los ataques que DDoS aumentaron un 200% en los últimos años [94]. Los datos del portal [95] Los ataques DDoS y la distribución de malware están en alza en la dark web. Un ciberdelincuente puede comprar la instalación de 1.000 amenazas por 1.800 dólares.	Un ataque DDoS deja inaccesible un servicio en la nube [96].

Fuente: Elaboración propia.

En este contexto, se estableció un conjunto de criterios de aceptación, para orientar la implementación de soluciones SSE. Para ello, el uso de tecnologías como SWG y ZTNA resultó clave, ya que permitió reducir la superficie de ataque, previniendo accesos no autorizados y ayudando a la seguridad en entornos de nube pública, mitigando así los riesgos previamente identificados. El primer paso para desarrollar los criterios de aceptación fue comprender los riesgos relacionados con la fuga de información y los accesos no autorizados en las nubes públicas como AWS, Microsoft Azure y Google Cloud Platform.

2.1.3 Investigación del modelo SSE y sus controles SWG y ZTNA en SASE.

Se realizó una investigación sobre el modelo SSE de los controles SWG y ZTNA en el marco de SASE, enfocado en nubes distintas a la de AWS. Luego se caracterizaron los riesgos más comunes de fuga de información en nubes públicas como Microsoft Azure y Google Cloud Platform (GCP), y se analizaron cómo los controles propuestos (SWG, ZTNA) ayudaron a mitigan estos riesgos.

En este contexto, se destacó SSE como un modelo de seguridad dentro de la arquitectura SASE, diseñado para proteger la red y los datos en la nube sin depender de soluciones de seguridad tradicionales en las instalaciones. Dentro de SSE, los controles SWG y ZTNA desempeñaron un papel clave en la protección de los entornos de nube pública [97]. Por otro lado, SASE combina servicios de red y

seguridad en la nube para crear una infraestructura flexible y escalable. Dentro de este marco, SSE fue la capa de seguridad encargada de gestionar el acceso seguro, protegiendo contra amenazas web, autenticación a los usuarios y salvaguardar los datos [98].
Dentro de los componentes claves de SSE en el marco SASE nos centraremos en:

- **SWG:** Protege el tráfico web de amenazas como malware y phishing, asegurando que los usuarios y aplicaciones en la nube solo interactúen con contenido seguro.

- **ZTNA**: Implementa el principio de "nunca confiar, siempre verificar", asegurando que cada usuario y dispositivo sean validados antes de acceder a los recursos en la nube [98].

Partiendo de lo anterior, tomamos como referencia los principales proveedores de nubes públicas, como: Microsoft Azure, Google Cloud Platform (GCP) y AWS, los cuales ofrecieron servicios que cubren el modelo SSE mediante los controles SWG y ZTNA. Aunque estos servicios no siempre vienen en un solo paquete de SSE, cada plataforma tuvo opciones que permitieron implementar estas funcionalidades. A continuación, se registran los controles SWG y ZTNA en el marco de SASE para cada una de las nubes públicas de referencia.

2.1.3.1 Nube Pública Microsoft Azure.

Microsoft Azure proporciona servicios que permitieron implementar controles SWG y ZTNA, facilitando la adopción del modelo SSE:

- **Servicios SWG en Azure:**

  Azure Web Application Firewall (WAF): Protege las aplicaciones web al filtrar y monitorear el tráfico HTTP/HTTPS entrante. Aunque no es un SWG convencional, cumple funciones parecidas al bloquear tráfico malicioso y proteger las aplicaciones de vulnerabilidades como inyecciones de SQL, ataques XSS, entre otros [99].

  Microsoft Defender for Identity: Ayuda a detectar y mitigar ataques a identidades, complementando la protección del tráfico web. Aunque no

cubre todas las características de un SWG tradicional, puede complementar la protección del tráfico web [99].

- **Servicios ZTNA en Azure:**

Azure Active Directory (Azure AD): Azure AD es un servicio centralizado de gestión de identidades y accesos, que implementa un enfoque de cero confianzas. A través de políticas de acceso condicional, se puede asegurar que solo los usuarios y dispositivos verificados accedan a los recursos de la nube [100].

Azure AD Conditional Access: Permite establecer reglas estrictas sobre qué dispositivos y usuarios pueden acceder a los recursos, integrando principios de Zero Trust en el acceso a aplicaciones y servicios.

Microsoft Defender for Identity: Complementa el enfoque Zero Trust, ya que monitorea el comportamiento de las identidades y detecta actividades sospechosas o no autorizadas [101].

En Azure, los controles de seguridad como Azure AD para ZTNA y Azure WAF para SWG crean una capa de protección que ayuda a implementar el modelo SSE, aunque Azure no tiene un servicio específico con la etiqueta SSE. Aun así, sus herramientas se pueden combinar para ofrecer las funcionalidades que proporciona SSE.

2.1.3.2 Nube Pública Google Cloud Platform (GCP).

GCP también tiene servicios propios que cubren los controles de SWG y ZTNA en un enfoque SSE, dentro de ellos se encuentran:

- **Servicios SWG en GCP:**

Google Cloud Armor: Protege las aplicaciones web y los servicios con un firewall que filtro el tráfico HTTP/HTTPS, funciona de manera parecida a un SWG. Ayuda a mitigar ataques como DDoS, XSS y otras amenazas basadas en la web [102].

Threat Intelligence: GCP ofrece inteligencia de amenazas a través de servicios como Chronicle Security protegiendo amenazas web y filtrar el tráfico malicioso. Aunque no es un SWG tradicional, sus funciones son bastante similares [103].

- **Servicios ZTNA en GCP:**

Google BeyondCorp: Es una solución de Google para Zero Trust la cual permite un acceso seguro basado en la identidad del usuario, el estado del dispositivo y otros factores. En lugar de confiar en la red, asegura que cada solicitud de acceso es verificada de manera independiente, siguiendo los principios de Zero Trust [104].

Identity-Aware Proxy (IAP): Permite que las aplicaciones y servicios de GCP se accedan bajo el enfoque de Zero Trust, asegurando que los usuarios solo puedan acceder a los recursos si cumplen con las políticas definidas, sin importar dónde se encuentren. Este servicio controla el acceso a las aplicaciones y ayuda a implementar Zero Trust [105].

En GCP, BeyondCorp y Google Cloud Armor son servicios que ayudan a implementar el modelo SSE, abarcando tanto SWG como ZTNA. BeyondCorp es un modelo de Zero Trust creado por Google, y es perfecto para empresas que necesitan una arquitectura basada en cero confianzas.

2.1.3.3 Nube Pública AWS.

AWS cuenta con varios servicios propios que implementan los controles SWG y ZTNA dentro de su infraestructura de seguridad, a continuación, los relacionamos:

- **Servicios SWG en AWS:**

AWS Network Firewall: aunque no es un SWG tradicional, permite inspeccionar y filtrar el tráfico de red, detectar amenazas y aplicar reglas de control sobre el tráfico web saliente. Ofrece protección frente a malware, exfiltración de datos y conexiones no autorizadas, actuando como componente dentro de una arquitectura SWG [106].

AWS Private NAT Gateway: facilita el control del tráfico saliente desde subredes privadas hacia Internet, permitiendo enrutar dicho tráfico a través del Network Firewall para su inspección y registro [107].

DNS Firewall Route 53: no es un SWG tradicional, puede desempeñar un papel complementario dentro de este control al actuar como un punto inicial de filtrado y control del tráfico DNS en el entorno de AWS. A través de sus capacidades de resolución personalizada y su integración con DNS Firewall, Route 53 permite aplicar políticas de seguridad que restringen las consultas DNS hacia dominios no autorizados o maliciosos, funcionando como un mecanismo preventivo antes de que se establezca una conexión hacia Internet. Por otra parte, DNS Firewall actúa como un punto de inspección temprana, ya que analiza las solicitudes DNS antes de que se establezcan las conexiones hacia Internet. Esta capacidad permite detener intentos de conexión hacia destinos potencialmente peligrosos, evitando la descarga de contenido malicioso o la exfiltración de información sensible**.** [108].

En conjunto, estos cuatro servicios (Private NAT + Network Firewall + DNS Firewall Route 53) permiten construir una capa de seguridad que ofrece funciones similares a las de un SWG tradicional en el entorno de AWS. AWS Private NAT Gateway controla el tráfico saliente desde las subredes privadas, AWS Network Firewall inspecciona y filtra las conexiones hacia Internet aplicando políticas de seguridad, y Amazon Route 53 junto con DNS Firewall gestionan y restringen las consultas de nombres de dominio según listas definidas por la organización. Al integrarse, estos servicios permiten supervisar, filtrar y proteger el tráfico web saliente conforme a las políticas internas

AWS Macie: Aunque no es un SWG tradicional, protege los datos sensibles en buckets S3 que podrían filtrarse a través del tráfico web, lo cual lo realiza detectando y clasificando información mediante aprendizaje automático (ML) [109].

AWS GuardDuty: Funciona como complemento de SWG, porque analiza logs de red y detecta tráfico malicioso o no autorizado hacia y desde Internet [110].

- **Servicios ZTNA en AWS:**

AWS Identity and Access Management (IAM): Es un servicio clave para implementar Zero Trust, ya que permite a los administradores controlar quién podía acceder a qué recursos en AWS. A través de políticas de acceso basadas en roles (RBAC) y autenticación multifactor (MFA), se gestiona el acceso de acuerdo con el modelo de Zero Trust. No obstante, para poder tener un enfoque alineado con los principios de Zero Trust, es bueno incorporar políticas basadas en atributos ABAC, las cuales permiten tomar decisiones de acceso en función de múltiples factores como la identidad del usuario, el tipo de dispositivo, la ubicación geográfica y el estado de seguridad del endpoint. [111].

Cuando IAM se integra con servicios como AWS Verified Access, esta capacidad se amplía, ya que el acceso a las aplicaciones o recursos se evalúa según el contexto del usuario y las condiciones de seguridad. En conjunto, estos mecanismos establecen un esquema de autorización contextual y adaptativa, que ayuda a la confianza mínima requerida en el modelo Zero Trust [111].

AWS Detective: es un servicio que apoya la implementación del modelo ZTNA al proporcionar capacidades de análisis y correlación de eventos dentro del entorno de AWS. Su función principal consiste en recopilar y relacionar de forma automática datos provenientes de servicios como CloudTrail, VPC Flow Logs y GuardDuty, con el fin de identificar comportamientos anómalos y posibles violaciones a las políticas de acceso [112].

AWS Control Tower: es un servicio que facilita la creación y el gobierno de entornos multi-cuenta en AWS bajo un esquema seguro y estandarizado. Su propósito es automatizar la implementación de buenas prácticas de seguridad, cumplimiento y administración, permitiendo que las organizaciones establezcan una base de control (landing zone) con políticas predefinidas, cuentas segregadas y monitoreo centralizado [113].

AWS PrivateLink: Permite acceder a los servicios de AWS de manera segura a través de redes privadas, asegurando que el acceso a los recursos se realice de forma segura sin tener que usar Internet público. Ayuda a crear arquitecturas basadas en Zero Trust [114]**.**

AWS Single Sign-On (SSO): Ofrecie autenticación y autorización para acceder a varias aplicaciones en la nube, y se puede combinar con MFA para aplicar el enfoque de Zero Trust [115].

AWS IAM Access Analyzer: Ayuda a aplicar principios de Zero Trust, revisando políticas de acceso y evitando exposición de recursos [116].

AWS Config: Ayuda que las configuraciones de acceso y seguridad estén alineadas con políticas de Zero Trust [117].

AWS GuardDuty: Refuerza ZTNA con detección de accesos anómalos o uso indebido de credenciales, ayudando que usuarios autenticados no puedan abusar de accesos [110].

AWS Security Hub: Evalúa el cumplimiento contra estándares de seguridad (incluido CIS), lo cual es parte de una estrategia de gobernanza Zero Trust [118].

En AWS, servicios como IAM y IAM Access Analyzer ayuda a aplicar el modelo ZTNA al gestionar el acceso de forma granular y detectar permisos excesivos o configuraciones que puedan exponer recursos. La integración de IAM con AWS Verified Access amplía este enfoque, ya que el acceso se evalúa según el contexto del usuario, su dispositivo y condiciones de seguridad. A su vez, AWS PrivateLink cubre la conectividad privada a los servicios de AWS sin depender del Internet público, mientras que SSO ayuda a la autenticación centralizada y el uso de multifactor. Complementariamente, AWS Detective facilita la validación de eventos y comportamientos anómalos, y AWS Control Tower ayuda a tener una administración y gobernada de entornos multi-cuenta. Finalmente, AWS Config y AWS Security Hub ofrecen visibilidad y cumplimiento, Amazon GuardDuty la detección de accesos o actividades sospechosas. En conjunto, estos servicios conforman una arquitectura SSE orientada al principio de Zero Trust, ayudando a la identidad, la visibilidad y la protección dentro del entorno cloud de AWS.

Para identificar los riesgos en entornos de nube pública y definir criterios de aceptación, se llevó a cabo un análisis basado en diversas fuentes de referencia, incluyendo informes de seguridad [75], [76], [78] , marcos de seguridad reconocidos [80], [81], y estudios de mejores prácticas [82]. Este proceso

investigativo permitió no solo reconocer los principales riesgos, sino también comprender cómo cada proveedor (AWS, Microsoft Azure y Google Cloud Platform) los enfrenta y mitiga a través de sus propios servicios y herramientas de seguridad.

Con base en el párrafo anterior, se desarrolló un cuadro comparativo que resumió la información clave. En este cuadro, los riesgos de seguridad se presentaron en cada plataforma y los controles de mitigación aplicados en cada caso. Las columnas correspondientes a AWS, Microsoft Azure y Google Cloud Platform (GCP) contienen los servicios específicos de cada nube asociados a los riesgos identificados. Es importante destacar que, aunque ciertos riesgos parecen exclusivos de una plataforma, esto se debe a que cada proveedor maneja configuraciones y herramientas distintas, lo que puede hacer que un riesgo sea más o menos relevante en su entorno.

Por ejemplo, la falta de cifrado de datos es un riesgo potencial en todas las nubes, pero se manifiesta de diferentes formas: en AWS, se menciona S3 sin encriptación; en Azure, Blob Storage sin encriptación; y en GCP, Cloud Storage sin encriptación. Asimismo, el acceso no autorizado a datos sensibles puede ocurrir en cualquier nube, pero los servicios afectados varían: en AWS, los principales involucrados son IAM y S3; en Azure, Azure AD y Storage; y en GCP, IAM y Storage. Además, es importante considerar que no todos los servicios existen en todas las nubes con el mismo nombre. Por ejemplo, mientras AWS tiene IAM como su servicio de gestión de identidades, Azure usa Azure Active Directory y GCP emplea IAM de Google Cloud.

En la TABLA 5 se presentó la estructura del Anexo 1: “Mitigación de Riesgos en las Plataformas”, en el cual se detallaron los riesgos identificados y las respectivas estrategias de mitigación asociadas a cada una de las plataformas evaluadas.

2.1.4 Definición de criterios para cumplir una solución SSE

Teniendo como punto de partida la información recopilada en el anterior numeral relacionada con la investigación sobre los riesgos, se procedió a definir los criterios que debieron cumplirse para que el modelo SSE contribuya en la mitigación de dichos riesgos, particularmente los relacionados en los controles SWG y ZTNA.

Para definir los criterios de análisis, nos basamos en el estudio de la documentación oficial de AWS, GCP y Azure, así como en informes de riesgos [75], [76], [78] , [80], [81] y [82] que abordaron aspectos claves de la seguridad en la nube. Como parte de este proceso, se elaboró un cuadro comparativo ver Anexo 2, en el cual se examinaron los principales riesgos de seguridad en la nube y las estrategias de mitigación implementadas por cada proveedor. A continuación, en la TABLA 5 se presenta la estructura del cuadro utilizado en este análisis, sin los datos detallados, con el fin de ilustrar los elementos evaluados. El cuadro completo, con la información detallada sobre cada plataforma y sus respectivas estrategias de mitigación, se encuentra disponible en el Anexo 1.

TABLA 5.
Mitigación de Riesgos en las Plataformas.

Riesgo	Descripción	AWS	Microsoft Azure	Google Cloud Platform (GCP)	Mitigación con SWG y ZTNA	Nube	Riesgo Común a Todas las Nubes	Soluciones Nativas en Nube SWG/ZTNA	Observaciones
(Ejemplo de riesgo)	(Breve descripción)	(Medidas en AWS)	(Medidas en Azure)	(Medidas en GCP)	(Estrategias de mitigación)	(Nube específica o general)	(Sí/No)	(Soluciones específicas)	(Notas adicionales)

Fuente: Elaboración propia.

A partir de esta revisión, se identificaron los riesgos en cada plataforma y se contrastaron entre sí. Es importante destacar que, aunque ciertos riesgos parecieron estar presentes en una nube que, en otra, esto no significo que sean exclusivos de esa plataforma. Más bien, la variabilidad en la documentación y en los enfoques de seguridad de cada proveedor influyo en cómo estos riesgos se manifiestan.

Además, el análisis exploratorio indicado en el cuadro comparativo permitió identificar las vulnerabilidades de seguridad en las nubes públicas, los cuales incluyen:

- **Falta de integración con otras soluciones de seguridad**: La seguridad en las nubes publicas requieren interoperabilidad con herramientas como Security Information and Event Management (SIEM) y Security Orchestration, Automation, and Response (SOAR) para una gestión de incidentes.

- **Escalabilidad y flexibilidad limitadas:** A medida que las organizaciones crecen, se requieren que las soluciones de seguridad sean capaces de adaptarse sin afectar el rendimiento o generar brechas de seguridad.

- **Políticas de seguridad inconsistentes en entornos multicloud**: La heterogeneidad en la configuración de seguridad en diferentes nubes pudo generar vulnerabilidades y dificultar la aplicación de controles uniformes.

- **Falta de visibilidad y monitoreo en tiempo real**: La detección de amenazas dependieron de la capacidad de monitoreo del tráfico y el comportamiento de los usuarios.

- **Deficiencias en la autenticación y autorización**: La ausencia de políticas de autenticación robustas y de un enfoque Zero Trust pudo facilitar accesos no autorizados a los recursos.

Estas vulnerabilidades fueron analizadas en cada proveedor de nube, evidenciando diferencias en la implementación de sus medidas de seguridad y en la documentación disponible sobre mitigación de amenazas.

La revisión de las amenazas permitió establecer criterios para la implementación de un modelo SSE adecuado para las nubes públicas, en donde las soluciones de seguridad integraron capacidades de monitoreo, control de acceso y escalabilidad. Además, la aplicación de estos criterios contribuyo a la protección de los activos en las nubes públicas y a una respuesta oportuna ante incidentes de seguridad. Estos criterios fueron establecidos en función de controles específicos diseñados para la mitigación de riesgos. Su implementación permitió reducir la superficie de exposición, ayudando a los mecanismos de defensa a una mayor resiliencia ante eventos de seguridad.

A continuación, relacionamos los criterios para los controles SWG y ZTNA dentro del modelo SSE:

2.1.4.1 Criterios de aceptación (Controles) para SWG.

Los criterios de aceptación fueron presentados como controles de seguridad, ya que estos permitieron evaluar de manera concreta la capacidad de cada herramienta para así, ayudar a mitigar riesgos, y vulnerabilidades específicas

identificadas en entornos de nube pública. Este enfoque basado en controles apoyo al cumplimiento de inspección de tráfico Web, y protección contra amenazas, contribuyendo a obtener una navegación segura. Esta estructura permitió alinear cada criterio con un objetivo de control técnico u organizacional, facilitando su implementación, medición y auditoría. En la TABLA 6 se mencionarán los criterios de aceptación (controles) para SWG.

TABLA 6.
Criterios de aceptación (Controles) para SWG.

Control	Criterio de aceptación	Justificación	Vulnerabilidad mitigada
Inspección Web de tráfico SSL/TLS.	Permite detectar y bloquear exfiltración de datos en tráfico cifrado.	Identifica amenazas ocultas en tráfico cifrado, evitando pérdida de datos y comandos maliciosos.	Exfiltración de datos en tráfico cifrado / Falta de visibilidad y monitoreo en tiempo real.
Autenticación y autorización robusta basada en identidad.	Asegura el control de acceso basado en la identidad del usuario y dispositivo.	Permite aplicar políticas individualizadas, reduciendo accesos no autorizados.	Debilidades en la autenticación y autorización.
Filtrado de tráfico y contenido en tiempo real.	Bloquea sitios maliciosos y amenazas como malware, phishing y ransomware.	Previene ataques al detener el tráfico malicioso antes de que llegue a los usuarios o sistemas.	Falta de visibilidad y monitoreo / Ausencia de filtrado de URLs maliciosas.
Visibilidad y control granular sobre el tráfico web.	Proporciona visibilidad total del tráfico web y permite políticas por tipo de contenido.	Segmenta el acceso web y reduce el riesgo de visitas a sitios inseguros.	Falta de visibilidad y monitoreo / Políticas de seguridad inconsistentes en entornos de nube.
Integración con herramientas de SOAR, monitoreo y correlación.	Debe integrarse con soluciones como SIEM o MFA para respuestas automáticas ante incidentes.	Facilita la automatización en la gestión de eventos de seguridad.	Falta de integración con herramientas de SOAR, monitoreo y correlación.
Capacidades de protección avanzada contra malware.	Incluye análisis de archivos y URLs en busca de amenazas.	Mitiga infecciones por malware en etapas tempranas, evitando compromisos de seguridad.	Ausencia de antivirus

Fuente: Elaboración propia.

2.1.4.2 Criterios de aceptación (Controles) ZTNA.

En el contexto del modelo de ZTNA, los criterios de aceptación fueron estructurados como controles de seguridad específicos con el objetivo de ayudar con la protección de los recursos frente a accesos no autorizados, movimientos laterales y amenazas internas o externas. Este enfoque basado en controles permitió evaluar el cumplimiento de los principios de confianza mínima, verificación continua y segmentación. Cada control se justificó desde su capacidad para mitigar vulnerabilidades, como deficiencias en autenticación, falta de visibilidad, políticas inconsistentes y ausencia de integración entre soluciones de seguridad. La implementación adecuada de estos controles contribuyó a fortalecer el acceso seguro en entornos de nube pública y a reducir la superficie de ataque expuesta a actores maliciosos. En la TABLA 7 se mencionarán los criterios de aceptación (controles) para ZTNA.

TABLA 7.
Criterios de aceptación (controles) ZTNA.

Control	Criterio de aceptación	Justificación	Vulnerabilidad mitigada
Autenticación y autorización robusta basada en identidad.	Asegura control de acceso sin depender de red perimetral.	Impide accesos no autorizados incluso si se compromete un nodo interno.	Debilidades en la autenticación y autorización.
Autenticación multifactor.	Requiere MFA incluso dentro de la red.	Protege contra robo de credenciales, aumentando la seguridad del proceso de inicio de sesión.	Suplantación de identidad.
Acceso condicional basado en contexto.	Aplica políticas según ubicación, dispositivo y comportamiento.	Permite acceso solo si se cumplen condiciones seguras, reduciendo riesgos contextuales.	Falta de visibilidad / Accesos desde ubicaciones geográficas sospechosas.
Segmentación de red y recursos.	Controla el acceso a recursos según permisos definidos.	Impide movimientos laterales dentro de la red en caso de compromiso.	Políticas inconsistentes de autenticación / Superficie de ataque ampliada.
Monitoreo y análisis de comportamientos anómalos.	Identifica patrones inusuales de uso que puedan indicar amenazas.	Detecta amenazas internas o externas mediante análisis del comportamiento de usuarios y dispositivos.	Actividad maliciosa no detectada.

Integración con herramientas de SOAR, monitoreo y correlación.	Compatible con SIEM, MFA, etc., para respuesta coordinada ante incidentes.	Permite una gestión centralizada de eventos de seguridad.	Falta de integración con herramientas de SOAR, monitoreo y correlación.
Acceso basado en el principio de menor privilegio.	Otorga acceso solo a recursos estrictamente necesarios.	Minimiza la exposición de datos sensibles y limita el impacto de accesos no autorizados.	Acceso no autorizado a recursos sensibles.

Fuente: Elaboración propia.

Partiendo de lo anterior, el análisis realizado en la sección anterior ha permitido identificar una serie de riesgos asociados a la seguridad en nubes públicas y la necesidad de implementar medidas de protección de los activos y la integridad de la información. En este contexto, el modelo de seguridad SSE, a través de sus controles SWG y ZTNA, proporciono un enfoque para mitigar estos riesgos. A continuación, la TABLA 8, establece la relación entre los riesgos identificados y los criterios definidos para los controles SWG y ZTNA, justificando cómo cada criterio contribuye a la mitigación de dichos riesgos.

TABLA 8.

Relación entre riesgo y criterios definidos.

Riesgo Identificado	Control	Criterios de aceptación	Relación / Justificación
Acceso no autorizado a datos sensibles	-Acceso basado en el principio de menor privilegio. -Control de acceso basado en roles. -Autenticación Multifactor.	Asegura el control de acceso basado en la identidad del usuario.	Permite aplicar políticas individualizadas, reduciendo accesos no autorizados.
Fuga de información	-Inspección web de tráfico TLS/SSL. -Monitoreo. -Aislamiento de navegador.	Permite detectar y bloquear exfiltración de datos en tráfico cifrado.	Identifica amenazas ocultas en tráfico cifrado, evitando pérdida de datos y comandos maliciosos.
Exposición no intencionada de datos sensibles.	-Visibilidad y control granular sobre el tráfico web. -Capacitación constante del personal. - Política de uso aceptable de internet y servicios en la nube. - Integración con sistemas de proxy inverso.	Proporciona visibilidad total del tráfico web y permite políticas por tipo de contenido.	Segmenta el acceso web y reduce el riesgo de visitas a sitios inseguros.

Descarga o ejecución de archivos maliciosos a través de canales no controlados (Infección por malware).	-Filtrado de tráfico y contenido en tiempo real. -Bloqueo de tráfico cifrado sospechoso. -Capacitación en phishing y descargas seguras. -Monitoreo de tráfico web en tiempo real.	Bloquea sitios maliciosos y amenazas como malware, phishing y ransomware.	Un Secure Web Gateway filtra tráfico malicioso y analiza archivos sospechosos antes de permitir su descarga.
Posibilidad de que atacantes obtengan credenciales de acceso mediante campañas de phishing o técnicas de ingeniería social, lo cual podría permitir accesos no autorizados a recursos críticos.	-Autenticación multifactor. -Capacitación contra phishing e ingeniería social. -Monitoreo.	Requiere MFA incluso dentro de la red.	Protege contra robo de credenciales, aumentando la seguridad del proceso de inicio de sesión.
Retraso en la detección y respuesta oportuna ante eventos.	-Integración con herramientas de SOAR, monitoreo y correlación. - Detección basada en comportamiento.	Compatible con SIEM, MFA, etc., para respuesta coordinada ante incidentes.	Permite una gestión centralizada y automatizada de incidentes, asegurando una respuesta rápida y coordinada ante amenazas.
Afectaciones a la disponibilidad por limitaciones en la escalabilidad y rendimiento	-Acceso condicional basado en contexto. - Capacitación.	Aplica políticas según ubicación, dispositivo y comportamiento.	Permite acceso solo si se cumplen condiciones seguras, reduciendo riesgos contextuales
Brechas de seguridad debido a configuraciones incorrectas	-Visibilidad y control granular sobre el tráfico web. -Políticas de inspección TLS. -Validación de configuración de accesos.	Proporciona visibilidad total del tráfico web y permite políticas por tipo de contenido.	Segmenta el acceso web y reduce el riesgo de visitas a sitios inseguros.
La organización no cuenta con visibilidad ni monitoreo en tiempo real del comportamiento de usuarios, dispositivos y tráfico de red, lo que podría impedir la detección oportuna de actividades anómalas o maliciosas.	-Monitoreo y análisis de comportamientos anómalos. -Configuración de política para inspección de descargas maliciosas en la navegación web.	Identifica patrones inusuales de uso que puedan indicar amenazas.	Detecta amenazas internas o externas mediante análisis del comportamiento de usuarios y dispositivos.
Que los mecanismos de autenticación y autorización implementados no sean	-Autenticación y autorización robusta basada en identidad.	-Asegura control de acceso sin depender de red perimetral.	Refuerza la verificación de identidad y evita accesos no autorizados.

suficientemente robustos o consistentes, lo que podría permitir accesos indebidos a recursos críticos por parte de usuarios no autorizados.	-Autenticación multifactor. -Acceso condicional basado en contexto. -Acceso basado en el principio de menor privilegio.	-Requiere MFA incluso dentro de la red. -Aplica políticas según ubicación, dispositivo y comportamiento. -Otorga acceso solo a recursos estrictamente necesarios.	
Daño reputacional y legal	-Monitoreo y análisis de comportamientos anómalos. -Monitoreo. -Auditoria de log.	Identifica patrones inusuales de uso que puedan indicar amenazas.	Detecta amenazas internas o externas mediante análisis del comportamiento de usuarios y dispositivos.
Exfiltración de información, escalada de privilegios y abuso de acceso	- Acceso basado en el principio de menor privilegio. - Segmentación de red y recursos. - Monitoreo y análisis de comportamientos anómalos.	- Otorga acceso solo a recursos estrictamente necesarios. -Controla el acceso a recursos según permisos definidos. -Identifica patrones inusuales de uso que puedan indicar amenazas.	Asegura que los usuarios solo tengan acceso a los recursos necesarios, limitando el impacto de un acceso comprometido.

Fuente: Elaboración propia.

2.2 Fase 2 Selección de tecnologías.

Partiendo de los criterios de aceptación definidos en la fase 1, se realizó una evaluación de las tecnologías disponibles que permitieron implementar controles SWG y ZTNA en AWS, con el objetivo de ayudar a mitigar riesgos como fugas de información, accesos no autorizados y errores de configuración. Esta evaluación no se limitó únicamente a soluciones comerciales presentadas en fuentes como el Cuadrante Mágico de Gartner o Forrester Wave, sino que también incluyo tecnologías individuales tanto nativas de AWS como de código abierto, que, al ser integradas, pudo conformar un esquema SSE. Este enfoque busco aportar flexibilidad y valor a la tesis, al considerar arquitecturas personalizadas que no dependieron exclusivamente de soluciones propias integradas de fabricantes.

2.2.1 Fuentes.

Para identificar las tecnologías que permitieron implementar controles SWG y ZTNA en un entorno SSE dentro de AWS, el análisis partió del estudio de soluciones individuales, iniciando en aquellas nativas de AWS. Continuando luego con las herramientas de código abierto, las cuales al integrarse construyeron una

arquitectura de seguridad, escalable y alineada con los controles de ZTNA y SWG. Con este análisis se buscó mostrar que es posible conformar un esquema sin depender exclusivamente de soluciones comerciales. Este análisis se complementó con el estudio de fuentes especializadas del sector, como el Cuadrante Mágico de Gartner y el Forrester Wave, que clasificaron y compararon los fabricantes según su liderazgo, desempeño y capacidades técnicas. Estas fuentes permitieron entender cómo las soluciones integradas de los principales proveedores se posicionaron en el mercado y qué funcionalidades ofrecieron en términos de integración, seguridad. A continuación, en los siguientes numerales se abarcarán las herramientas nativas, código abierto y comerciales respecto a los controles ZTNA y SWG en el marco SASE.

2.2.1.1 Herramientas nativas de AWS útiles para SWG.

AWS ofreció varios servicios que ayudaron a conectar los recursos en la nube con Internet de forma sencilla. Sin embargo, estas herramientas por sí solas no cubrieron toda la seguridad que se necesitó para proteger tanto el entorno en la nube como la información almacenada. Por eso, es importante revisar estas soluciones y combinarlas con otras opciones para lograr una protección. A continuación, se mencionarán algunas herramientas nativas de AWS que se pudieron utilizar para crear una arquitectura SWG, junto con una breve descripción de lo que hace cada una.

- **AWS Network Firewall.**

Es un servicio gestionado de firewall de red y detección y prevención de intrusiones (IDPS) que se implementa en el perímetro de una VPC. Permite inspeccionar profundamente los paquetes, bloquear URLs, dominios o direcciones IP, controlar el tráfico saliente y establecer reglas de contenido para proteger los recursos en la nube. Utiliza reglas compatibles con Suricata para realizar inspección con estado y puede integrarse de forma centralizada usando AWS Firewall Manager [119], [120].

- **AWS Route 53 Resolver DNS Firewall.**

Este servicio permite filtrar consultas DNS que salen de una VPC, bloqueando o permitiendo dominios específicos para evitar el acceso a sitios maliciosos o no autorizados. Se basa en la definición de reglas y grupos de reglas asociadas a las VPCs, permitiendo acciones como bloquear,

permitir o alertar sobre consultas DNS según el dominio solicitado. Solo filtra tráfico DNS, no otros protocolos de capa de aplicación [121].

- **Amazon VPC Flow Logs.**

Permite capturar y registrar información sobre el tráfico de red que entra y sale de las interfaces de red en una VPC. Esta herramienta es esencial para monitorear, analizar y auditar las comunicaciones entre recursos dentro de la nube, ya que proporciona visibilidad detallada del comportamiento del tráfico en tiempo real o casi en tiempo real. Es especialmente útil en una arquitectura SSE porque permite detectar patrones anómalos, identificar posibles accesos no autorizados o mal configuraciones, y reforzar las políticas de segmentación y monitoreo continuo. Al combinarse con servicios como GuardDuty o CloudWatch, los VPC Flow Logs fortalecen la capacidad de respuesta ante incidentes y ayudan a mantener un entorno Cloud más seguro y controlado [122], [123].

- **Amazon Eventbridge.**

Es un servicio de orquestación de eventos que permite automatizar, coordinar y responder de manera dinámica a actividades relacionadas con los controles ZTNA y SWG. En este contexto, EventBridge recibe eventos generados por servicios de seguridad, como autenticación ó filtrado y ejecuta acciones basadas en políticas de Zero Trust. A través de reglas de eventos, EventBridge facilita la aplicación automática de controles, como actualizar políticas de acceso, iniciar flujos de verificación adicional, bloquear tráfico no autorizado, aislar recursos o generar alertas. Esto permite que tanto el acceso a aplicaciones internas (ZTNA) como la navegación segura hacia internet (SWG) operen bajo un modelo contextual, adaptable y en tiempo real, fortaleciendo la postura de seguridad y el cumplimiento continuo [124].

- **AWS CloudTrail + GuardDuty + Security Hub.**

Estos servicios trabajan juntos para monitorear el comportamiento, detectar amenazas y generar alertas sobre accesos no autorizados o actividades anómalas en el entorno AWS. CloudTrail registra eventos y acciones, GuardDuty analiza continuamente registros y fuentes de datos

para identificar actividades sospechosas usando inteligencia de amenazas y machine learning, y Security Hub centraliza la gestión y visualización de alertas de seguridad [125], [126], [118].

- **AWS S3 Access Points + IAM Policies.**

  Los Access Points de S3 permiten definir puntos de acceso específicos con políticas de IAM asociadas para controlar y limitar el tráfico hacia recursos de S3. Esto facilita restringir qué usuarios o aplicaciones pueden acceder a ciertos datos, aplicando condiciones y restricciones detalladas en las políticas, y así evitar que instancias accedan a recursos externos no necesarios [127].

Adicionalmente, existen servicios nativos de AWS orientados al cumplimiento, auditoría y gestión de riesgos que, aunque no forman parte directa del control SWG, fortalecen la postura de seguridad de la arquitectura. Entre estos se encuentran:

- **AWS Artifact.**

  Permite proporcionar acceso bajo demanda a los documentos de cumplimiento, seguridad y auditoría de Amazon Web Services, tales como certificaciones ISO, informes SOC y PCI. Actúa como un portal centralizado para revisar, descargar y gestionar acuerdos legales y cumplimiento normativo [128].

- **AWS Audit Manager.**

  Facilita la evaluación continua de controles mediante la recolección automatizada de evidencias, ayudando a mapear recursos de AWS con estándares regulatorios (como PCI, HIPAA, NIST), reduciendo el trabajo manual y simplificando la demostración de conformidad [129].

2.2.1.2 Herramientas de Código abierto útiles para SWG.

Además de las soluciones nativas que ofrece AWS, también se pudo utilizar herramientas de código abierto para implementar un control SWG en la nube. Estas herramientas permitieron aplicar políticas de filtrado web, monitoreo de

tráfico y control de acceso a Internet desde las instancias en AWS, ofreciendo flexibilidad y personalización según las necesidades del entorno. A continuación, se presentan algunas de las opciones que podrían ser utilizadas.

- **Squid Proxy.**

  Es un servidor proxy de código abierto que actúa como intermediario para tráfico HTTP/HTTPS. Ofrece funciones como filtrado de URLs, almacenamiento en caché para acelerar solicitudes repetidas, autenticación de usuarios y gestión del ancho de banda. Su flexibilidad permite integrarlo con herramientas de seguridad adicionales para análisis de contenido [130].

- **OPNsense.**

  Es plataforma de firewall y enrutamiento de código abierto que prioriza una interfaz intuitiva y funciones avanzadas de seguridad, como prevención de intrusiones en línea (IPS), VPN y filtrado de contenido. Es ideal para implementar políticas de red granularmente, incluyendo autenticación de dos factores y análisis de tráfico mediante herramientas integradas [131].

- **pfSense.**

  Es una herramienta de código abierto basada en FreeBSD, Su diseño modular permite implementar funciones de filtrado de tráfico, autenticación, balanceo de carga y detección de intrusos, facilitando el control y monitoreo del tráfico saliente desde instancias en la nube. Además, pfSense se administra mediante una interfaz web intuitiva, lo que simplifica la gestión de políticas de acceso y la integración con otras herramientas de inspección de tráfico, ofreciendo así una solución flexible y personalizable para la protección y segmentación de redes en arquitecturas SSE. [132].

- **ICAP con C-ICAP + ClamAV.**

  Esta combinación permite escanear archivos en tiempo real a través del protocolo ICAP. C-ICAP actúa como servidor intermediario que recibe

solicitudes del proxy (como Squid) y las redirige a ClamAV, un motor antimalware de código abierto. Juntos, detectan virus o contenido peligroso en tráfico web, bloqueándolo antes de que llegue al usuario final [130], [133], [134], [135].

- **E2guardian.**

  Es un filtro de contenido web de código abierto que se utiliza para analizar y controlar el acceso a páginas web en una red. Puede funcionar tanto de manera independiente como junto a proxies de caché como Squid, permitiendo aplicar políticas de filtrado basadas en coincidencia de frases, encabezados de solicitud, URLs y más. Ofrece funcionalidades avanzadas como listas blancas y negras, bloqueo por expresiones regulares, escaneo profundo de URLs, bloqueo de anuncios, limitación de tamaño de carga y filtrado SSL. Es una herramienta flexible y eficiente para implementar un control granular del tráfico web, ideal para entornos que requieren un alto nivel de filtrado de contenidos [136], [137].

2.2.1.3 Herramientas nativas de AWS útiles para ZTNA.

AWS ofreció varias herramientas nativas que ayudaron a controlar el acceso a los recursos de manera segura y detallada. A continuación, se relacionan las herramientas que se pudieron usar en AWS para construir una arquitectura ZTNA, describiendo para qué sirve cada una.

- **AWS Identity and Access Management y IAM Identity Center.**

  AWS Identity and Access Management (IAM) y el IAM Identity Center (antes conocido como AWS SSO) son los servicios que se utilizan para manejar quién puede entrar y qué puede hacer cada usuario o servicio dentro de AWS. IAM permite crear usuarios, roles y políticas de acceso, mientras que el Identity Center facilita la integración con otros sistemas de identidad como Active Directory u Okta. Usar estos servicios es clave para aplicar el principio de “menor privilegio” y asegurarse de que solo las personas autorizadas tengan acceso a los recursos necesarios [138].

- **Amazon Cognito.**

Está pensado para gestionar los usuarios finales de aplicaciones web o móviles. Permite que los usuarios se registren, inicien sesión y accedan a las aplicaciones de forma segura. Es muy útil cuando se crean aplicaciones y se necesita escalar la gestión de usuarios sin complicaciones [139].

- **AWS PrivateLink.**

Permite que los servicios internos se conecten de forma privada, sin exponer direcciones IP públicas ni pasar por Internet. Así, se reduce la posibilidad de ataques externos y se mantienen los servicios más protegidos dentro de la VPC [140].

- **Amazon VPC Flow Logs.**

Permite capturar y registrar información sobre el tráfico de red que entra y sale de las interfaces de red en una VPC. Esta herramienta es esencial para monitorear, analizar y auditar las comunicaciones entre recursos dentro de la nube, ya que proporciona visibilidad detallada del comportamiento del tráfico en tiempo real o casi en tiempo real. Es especialmente útil en una arquitectura ZTNA porque permite detectar patrones anómalos, identificar posibles accesos no autorizados o mal configuraciones, y reforzar las políticas de segmentación y monitoreo continuo. Al combinarse con servicios como GuardDuty o CloudWatch Logs, los VPC Flow Logs fortalecen la capacidad de respuesta ante incidentes y ayudan a mantener un entorno Cloud más seguro y controlado [122], [123].

- **Amazon VPC (subredes privadas y NAT Gateway).**

Se puede dividir la red en subredes privadas y públicas, lo que ayuda a aislar los recursos. Usando un NAT Gateway, las instancias en subredes privadas pueden salir a Internet (por ejemplo, para actualizaciones), pero no se exponen a conexiones entrantes no deseadas [141].

- **AWS CloudTrail, Amazon GuardDuty y AWS Config.**

  - ✓ **CloudTrail:** graba todas las acciones que se hacen en la cuenta de AWS, lo que es muy útil para auditoría y cumplimiento [126].

- ✓ **GuardDuty:** detecta amenazas y comportamientos sospechosos analizando los logs y el tráfico [142].

- ✓ **AWS Config:** revisa la configuración de los recursos para ver si cumplen con las políticas definidas y avisa si algo cambia [143].

- ➢ **AWS Verified Access**

Es un servicio de AWS que permite dar acceso seguro a aplicaciones y recursos corporativos sin necesidad de usar una VPN. Lo que hace es evaluar cada solicitud de acceso en tiempo real, comprobando que el usuario y su dispositivo cumplan con los requisitos de seguridad que se hayan definido. Esto significa que, en vez de confiar automáticamente en alguien solo por estar dentro de la red, se revisa cada intento de acceso y solo se permite si cumple con las políticas establecidas. Además, Verified Access se integra con sistemas de identidad y de gestión de dispositivos, registra todos los intentos de acceso para facilitar auditorías y permite administrar las políticas de acceso desde una sola interfaz, lo que ayuda a simplificar la gestión y mejorar la seguridad siguiendo el enfoque de confianza cero [144].

- ➢ **AWS Detective**

Es un servicio que apoya la implementación del modelo ZTNA al proporcionar capacidades de análisis y correlación de eventos dentro del entorno de AWS. Su función principal consiste en recopilar y relacionar de forma automática datos provenientes de servicios como CloudTrail, VPC Flow Logs y GuardDuty, con el fin de identificar comportamientos anómalos y posibles violaciones a las políticas de acceso [112].

- ➢ **AWS Control Tower**

Facilita la creación y el gobierno de entornos multi-cuenta en AWS de forma segura y estandarizada. Su objetivo es automatizar la adopción de buenas prácticas de seguridad, cumplimiento y administración, ayudando a las organizaciones a establecer una landing zone con políticas definidas, separación clara de cuentas y un monitoreo centralizado. En este esquema, las Service Control Policies (SCPs) juegan un rol clave desde un enfoque Zero

Trust, ya que establecen los límites de lo que cada cuenta puede o no puede hacer, sin asumir confianza previa. Estas políticas funcionan como una capa de control que bloquea acciones no autorizadas incluso para usuarios o roles con permisos elevados, evitando configuraciones riesgosas o el uso de servicios no aprobados. Gracias a ello, se mantiene un control coherente y consistente en todo el entorno multi-cuenta [113], [145], [146].

2.2.1.4 Herramientas de Código abierto útiles para control ZTNA.

Es importante considerar no solo las herramientas nativas, sino también las opciones de código abierto. Las herramientas de código abierto ofrecieron flexibilidad y suelen adaptarse fácilmente a diferentes necesidades, permitiendo personalizar la seguridad y el control de acceso según los requerimientos de cada proyecto. Además, muchas de estas soluciones cuentan con comunidades activas que ayudan a mantenerlas actualizadas y seguras. Usar herramientas de código abierto en AWS puede ser una buena manera de complementar los servicios de la nube y reforzar la estrategia de confianza cero, aprovechando tanto la innovación de la comunidad como la integración con la infraestructura existente.

A continuación, se presentaron algunas de las herramientas de código abierto que pudieron utilizarse para implementar ZTNA en AWS, junto con una breve descripción de sus características y el rol que cumplen dentro de una arquitectura de confianza cero.

- **Pomerium.**

Es un proxy reverso de código abierto que actúa como un proxy de identidad, permitiendo controlar el acceso a aplicaciones privadas a través de HTTPS de manera granular y centralizada. Es ideal para exponer aplicaciones internas sin abrirlas directamente a Internet, ya que verifica la identidad y el contexto de cada usuario antes de permitir el acceso [147].

- **Teleport.**

Es una plataforma código abierto que facilita el acceso seguro y basado en Zero Trust a servidores, clústeres de Kubernetes, bases de datos y aplicaciones internas. Ofrece autenticación sin contraseñas, control de

acceso detallado y registro completo de auditoría, lo que ayuda a cumplir con los principios de ZTNA [148].

- **OpenZiti.**

Es una plataforma de red Zero Trust que permite crear túneles cifrados para acceder a aplicaciones de manera segura sin exponer puertos públicos. Utiliza autenticación fuerte y segmentación de red, lo que ayuda a reducir la superficie de ataque [149].

- **ZITADEL.**

Es una plataforma de gestión de identidades de código abierto que soporta OIDC, SAML y MFA, funcionando como alternativa a servicios como Auth0 o Cognito. Permite implementar autenticación federada y control de acceso en aplicaciones ZTNA [150].

- **Keycloak.**

Es una solución open source para la gestión de identidades, autenticación federada y SSO/MFA. Es muy útil como proveedor de identidad (IdP) para otras herramientas de ZTNA como Pomerium o Teleport [151].

- **OAuth2-Proxy.**

Es una solución open source que implementa un proxy de autenticación compatible con los estándares OAuth 2.0 y OpenID Connect (OIDC), diseñada para proteger aplicaciones web mediante el control de acceso basado en identidad. Su función principal es interceptar las solicitudes entrantes, autenticar al usuario y generar cabeceras seguras que permiten aplicar políticas de autorización en cada sesión [152].

- **OPA (Open Policy Agent).**

Es una herramienta de código abierto que permite crear y aplicar políticas de acceso granulares y personalizadas, asegurando que solo los usuarios y dispositivos autorizados obtengan el mínimo privilegio necesario para acceder a aplicaciones y datos, implementando el principio de "nunca confiar, siempre verificar" en cada solicitud de acceso, más allá del perímetro tradicional [153].

2.2.1.5 Herramientas Comerciales para controles SWG y ZTNA.

Antes de mencionar herramientas específicas, es importante contextualizar el marco de referencia para evaluar soluciones comerciales. Gartner y Forrester se posicionaron como los estándares más reconocidos en análisis tecnológico estratégico, cuyas metodologías permitieron contrastar las herramientas con los criterios de aceptación definidos en la Fase 1. Gartner es una empresa líder en investigación y consultoría tecnológica que proporciona análisis estratégicos para ayudar a las organizaciones a tomar decisiones informadas y mejorar su desempeño [154]. Entre sus metodologías más reconocidas se encuentra el Cuadrante Mágico, una evaluación detallada de las principales soluciones tecnológicas que clasifica a los fabricantes según su capacidad de ejecución y visión panorámica del mercado. Gracias a su representación gráfica y un conjunto uniforme de criterios de evaluación, este modelo permitió identificar rápidamente cómo los distintos fabricantes están desarrollando sus estrategias y qué tan bien se están desempeñando en relación con la visión de mercado establecida por Gartner.

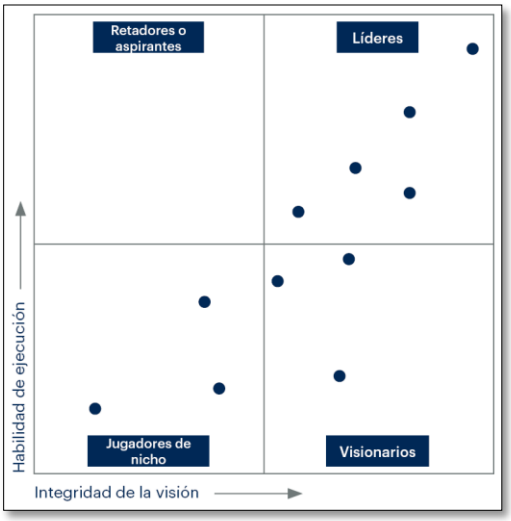

Fig. 9 Cuadrante de Gartner, tomado de *[155]*.

El Cuadrante Mágico de Gartner se construye a partir de un gráfico con dos ejes:

- **Eje vertical:** Evalúa el conocimiento de mercado de cada proveedor.
- **Eje horizontal**: Mide la visión estratégica y su alineación con las tendencias del mercado.

Según estos criterios, Gartner clasifica a los proveedores en cuatro grupos:

- **Líderes**: Sobresalen tanto en desempeño como en visión estratégica.
- **Visionarios**: Proponen innovaciones relevantes, pero aún presentan limitaciones en su implementación.
- **Retadores**: Muestran un alto rendimiento actual, aunque sin una estrategia clara a futuro.
- **Jugadores de nicho:** Se especializan en segmentos específicos sin destacar en innovación o alcance de mercado [155].

Se tomó como referencia el cuadrante mágico de Gartner publicado en el sitio de Netskope en el año 2025 [156], con énfasis en el cuadrante lideres. Esta decisión se basó en su capacidad de ejecución, visión estratégica y adopción del mercado, obteniendo así una solución acorde, escalable y alineada con los criterios de aceptación definidos previamente en la fase 1.

Fig. 10 Cuadrante mágico de Gartner SSE 2025, tomado de [156].

Por otra parte, Forrester Research es una empresa líder en investigación y consultoría tecnológica que ofrece evaluaciones detalladas sobre soluciones de seguridad emergentes y su impacto en el sector empresarial. Una de sus metodologías más reconocidas es el Forrester Wave, el cual proporciona una evaluación comparativa de los principales proveedores en diferentes áreas tecnológicas. Este informe permite a las organizaciones tomar decisiones informadas con base en criterios de funcionalidad, desempeño y alineación estratégica con las necesidades del mercado [157].

Fig. 11 The Forrester Wave 2025, tomado de *[157]*.

La metodología de Forrester Wave se basa en una matriz de puntuaciones que evalúa las soluciones tecnológicas en función de tres dimensiones principales:

- **Oferta actual:** Examina las capacidades técnicas de la solución, incluyendo su rendimiento, nivel de integración y funcionalidad específica.
- **Estrategia**: Analiza la visión a futuro del proveedor, su enfoque en innovación y la alineación de su producto con las tendencias del mercado.
- **Presencia en el mercado:** Evalúa la adopción de la tecnología, el tamaño de su base de clientes y la estabilidad financiera del proveedor.

El resultado de la evaluación se representa gráficamente en un cuadrante que categoriza a los proveedores en cuatro grupos:

- **Líderes:** Empresas que destacan por ofrecer soluciones sólidas, con una visión estratégica clara y una presencia consolidada en el mercado.
- **Fuertes competidores:** Proveedores con productos avanzados, aunque con oportunidades de mejora en términos de estrategia o alcance.
- **Contendientes:** Fabricantes con soluciones viables, pero con ciertas limitaciones en funcionalidad, escalabilidad o adopción.
- **Participantes de nicho:** Empresas con un alcance reducido o con productos especializados en segmentos específicos.

La selección de los fabricantes dentro del marco SSE, se consideraron en el informe Forrester Wave: Security Service Edge Solutions, Q3 2025, enfocándonos en la categoría de líderes. Esta elección se basó en el análisis de su desempeño actual, estrategia de mercado y nivel de adopción, lo que permite identificar soluciones tecnológicas con un alto grado de innovación, escalabilidad y compatibilidad con los criterios establecidos en la fase 1.

Fig. 12 Forrester Wave: Security Service Edge Solutions, Q3 2025, tomado de *[158]*.

- **Fabricantes para SSE con SWG y ZTNA.**

Con lo identificado en los puntos anteriores se realizó una selección de tecnologías dentro del marco SSE en AWS, para ello, se llevó a cabo un análisis basado en los fabricantes identificados como líderes en los informes más recientes de Forrester Wave: Security Service Edge Solutions, Q3 2025 y el Cuadrante Mágico de Gartner 2025. Al comparar ambas evaluaciones, se identificaron los fabricantes que coinciden en la categoría de líderes, ya que estos destacan por su capacidad de ejecución, innovación estratégica y adopción en el mercado.

Los fabricantes que aparecen como líderes en ambos análisis (Forrester y Gartner) son:

- **Zscaler**.

Fue uno de los primeros innovadores en gran parte de la tecnología que ahora se denomina SSE, incluida la SWG entregada en la nube y la gestión de la experiencia digital. Zscaler ya es un fabricante importante en Zero Trust, que proporciona acceso a aplicaciones privadas. La visión de este fabricante para el futuro es llevar la conectividad Zero Trust a todo lo demás (como aplicaciones públicas e IoT/OT). Zscaler utiliza un único cliente integrado para su funcionalidad SWG y ZTNA en el endpoint [158].

- **Netskope**.

Netskope llega a SSE con una herencia CASB. El fabricante tiene una visión vívida que hace de la protección de datos el propósito al que deben servir sus tecnologías SSE. Netskope ha demostrado innovación en toda su pila técnica, incluidas importantes inversiones en una nueva e impresionante red privada global (NewEdge), inteligencia artificial (docenas de modelos en ejecución) y seguridad de IA generativa (genAI) [158].

- **Palo Alto Networks.**

El gigante de la seguridad Palo Alto Networks ofrece una solución SSE con énfasis en la seguridad de la red, la identidad y Zero Trust. La solución Prisma Access SSE del fabricante cuenta con excelentes capacidades ZTNA, accesibles desde el agente VPN GlobalProtect que sus clientes de seguridad de red ya tienen implementado. La seguridad de salida de Internet se aplica mediante el SWG renovado del fabricante, que ahora aplica la inspección de seguridad en tiempo real incluso durante 0-days. El fabricante innova constantemente en investigación y desarrollo y adquiere nuevas empresas innovadoras: construyó puntajes de riesgo CASB en torno a su AppID, creó AIOps para SSE y recientemente adquirió el startup de navegadores empresariales Talón [158].

2.2.2 Elección de herramienta para la arquitectura SSE basada en SASE.

Se procedió a realizar una evaluación tanto de las herramientas nativas, como de las herramientas de código abierto, que al implementarse cumplan con los controles SWG y ZTNA en AWS, para ello se llevó a cabo una comparación entre ellas de acuerdo con los criterios establecidos en la fase 1. Es de recalcar que las herramientas comerciales solo se referencian para dar contexto de que existen como soluciones y abarcan los controles SWG y ZTNA. A continuación, la TABLA 9, se presenta la estructura del cuadro comparativo de las herramientas en función de los criterios de aceptación definidos previamente en la Fase 1. Esta versión se muestra sin los datos detallados, con el objetivo de ilustrar los elementos evaluados. El cuadro completo, con la información completa y desglosada, se encuentra disponible en el Anexo 3.

TABLA 9.
Estructura del Anexo 3 "Comparación de herramientas".

Herramienta	Autenticación y autorización robusta basada en identidad	Autenticación multifactor	Acceso condicional basado en contexto	Segmentación de red y recursos	Monitoreo y análisis de comportamientos anómalos	Integración con otros controles de seguridad	Menor privilegio	Inspección Web de tráfico SSL/TLS	Filtrado de tráfico y contenido en tiempo real	Visibilidad y control granular sobre el tráfico web	Capacidades de protección avanzada contra malware.
AWS Identity and Access Mgmt	☑	☑	✗	☑	✗	☑	☑	✗	✗	✗	✗

Fuente: Elaboración propia.

A partir de este análisis, se identificaron las fortalezas y las limitaciones de cada herramienta evaluada frente a los criterios de aceptación establecidos para una solución SSE. Es importante señalar que, si bien algunas herramientas parecen sobresalir o quedarse cortas en determinados aspectos, esto no implica que sus debilidades sean exclusivas de esa solución. En realidad, las diferencias observadas responden en gran medida a la orientación funcional de cada herramienta (nativa o de código abierto). Esta variabilidad influye directamente en cómo cada herramienta aborda los controles como autenticación, segmentación, inspección de tráfico y protección contra amenazas.

Por otra parte, para dar mayor objetividad al análisis, se calculó un nivel de cumplimiento cuantitativo (%) para cada herramienta. Este valor se obtuvo de la TABLA 9 convirtiendo cada criterio evaluado en una escala: se asignó un 1 si la herramienta cumplía con el criterio (☑), un 0.5 si cumplía de manera parcial (◐) y un 0 si no lo cumplía (✗). Luego, se sumaron los criterios cumplidos por cada herramienta y se dividió entre el total de criterios evaluados, multiplicando por 100 para obtener el porcentaje. Esta metodología permitió comparar fácilmente el

desempeño de las distintas herramientas frente a los controles esperados en una solución SSE, facilitando la toma de decisiones basada en evidencia. A continuación, en la TABLA 10 se relaciona el nivel de cumplimiento cuantitativo (%) calculado para cada herramienta, basado en los criterios (Controles) definidos previamente.

TABLA 10.

Nivel de Cumplimiento de Herramientas Según Criterios (controles).

Herramienta	Porcentaje de Cumplimiento (%)
SCPs (Service Control Policies)	63,6%
OPNsense (Squid + SquidGuard + ClamAV)	63,6%
pfSense (Squid + SquidGuard + ClamAV)	63,6%
AWS Vierified Access	59,1%
AWS Network Firewall	59,1%
Keycloak	54,5%
OPA (Open Policy Agent)	54,5%
Teleport	54,5%
OpenZiti	54,5%
OAuth2-Proxy	54,5%
IAM Identity Center	50,0%
AWS Systems Manager Session Manager	50,0%
AWS Control Tower	50,0%
Pomerium	45,5%
AWS Identity and Access Mgmt (IAM)	40,9%
Amazon Cognito	40,9%
AWS Route 53 Resolver DNS Firewall	40,9%
AWS IAM Access Analyzer	36,4%
Amazon GuardDuty	36,4%
ZITADEL	36,4%
AWS Config	31,8%
Amazon Detective	31,8%
Amazon Macie	27,3%
AWS CloudTrail	27,3%
AWS Security Hub	22,7%
AWS PrivateLink	18,2%
Amazon VPC	18,2%
VPC Flow Logs	18,2%
Network ACL (NACL)	18,2%
Amazon EventBridge	13,6%
NAT Gateways	4,5%
AWS Internet Gateway	4,5%
Private NAT Gateway	4,5%

Fuente: Elaboración propia.

En la TABLA 10 se aplicó un método de evaluación multicriterio ponderado, donde cada herramienta fue valorada según su nivel de cumplimiento frente a los criterios de aceptación definidos para SWG y ZTNA. Cada criterio tuvo igual peso porcentual, y la puntuación final representa el porcentaje de cumplimiento. Partiendo de la tabla anterior, el diseño SSE que propone esta tesis, pretende cubrir la mayor parte de controles definidos como criterios y es por tal razón que se decide realizar una integración de herramientas que permita identificar los componentes arquitectónicos necesarios.

A continuación, en la TABLA 11 y TABLA 12 presentamos los resultados obtenidos de la integración de las herramientas con respecto a los criterios definidos en la fase 1. Las herramientas que aparecen separadas por comas dentro de cada celda representan opciones independientes que pueden cumplir el mismo criterio, pero que no necesariamente deben utilizarse todas al mismo tiempo. Es decir, la coma indica que esas herramientas son válidas para resolver el control evaluado, y se puede seleccionar una o varias según la arquitectura final. Por otro lado, cuando se utiliza el símbolo "/", esto sí representa alternativas equivalentes, donde cada herramienta puede reemplazar a la otra dependiendo del entorno. Finalmente, el símbolo "+" indica que las herramientas deben emplearse de manera conjunta porque se complementan para cubrir completamente un criterio. (Para más detalle, ver anexo 3).

TABLA 11.
Ranking de herramientas SWG

Solución	Herramientas Integradas	Porcentaje de Cumplimiento (%)	Justificación frente a criterios
1	PfSense/OPNsense + Keycloak / IAM Identity Center / OAuth2-Proxy + VPC Flow Logs, CloudTrail, GuardDuty, Security Hub + Security Hub + EventBridge	100%	Al incorporar inspección SSL/TLS, filtrado avanzado y protección antimalware. Es una solución SWG completa y flexible, adaptable a múltiples entornos. Se consolida como la alternativa más robusta, completa y alineada con los requerimientos técnicos del modelo SWG.
2	AWS Network Firewall, Route53 DNS Firewall + IAM Identity Center, IAM, Verified Access +	83%	Se destaca por su integración nativa, mínima complejidad operativa y capacidades sólidas de identidad, filtrado, monitoreo y correlación. Aunque no incluye antimalware,

	VPC Flow Logs, CloudTrail, GuardDuty, Security Hub + Security Hub + EventBridge		ofrece una solución SWG estable, escalable y administrada, ideal para entornos en nube donde se busca simplicidad y visibilidad centralizada.

Fuente: Elaboración propia.

En la TABLA 11, seleccionamos la Solución 1 dado que combina herramientas como pfSense/OPNsense, Squid Proxy, SquidGuard y ClamAV, que juntas permiten cumplir el 100 % de los criterios del modelo SWG. En esta solución, “pfSense/OPNsense” actúan como la plataforma central por donde pasa e inspecciona el tráfico web; Squid Proxy y SquidGuard se encargan del filtrado granular, la inspección SSL/TLS y la aplicación de políticas por usuario; y ClamAV aporta la capacidad de análisis antimalware sobre el tráfico HTTP/HTTPS. Paralelamente, las herramientas de identidad como “Keycloak / IAM Identity Center / OAuth2-Proxy” permiten controlar el acceso basado en usuarios o grupos, mientras que los servicios de visibilidad “VPC Flow Logs, CloudTrail, GuardDuty, Security Hub” fortalecen la detección y el monitoreo continuo. Finalmente, “Security Hub + EventBridge” soportan la automatización y respuesta a eventos de seguridad. En conjunto, esta integración ofrece una solución SWG completa, flexible y altamente alineada con las necesidades del proyecto. Por otra parte, en la TABLA 12 observamos el ranking de herramientas para el control ZTNA.

TABLA 12.

Ranking de herramientas ZTNA

Solución	Herramientas Integradas	Porcentaje de Cumplimiento (%)	Justificación frente a criterios
1	Keycloak, ZITADEL + OPA + RBAC Keycloak + Pomerium, OpenZiti, Aoth2-proxy + VPC, Security Groups, Network ACL, PrivateLink + GuardDuty, Detective, CloudTrail + Security Hub + EventBridge	93%	Integra de manera complementaria herramientas como Keycloak o ZITADEL para la gestión de identidades, OPA para la definición de políticas basadas en atributos y Pomerium/Aouth2-proxy como proxies de acceso Zero Trust, logrando una arquitectura más completa y flexible sobre AWS. Esta combinación permite aplicar autenticación multifactor, segmentación detallada por aplicación, políticas dinámicas basadas en contexto, y control de acceso granular por rol, atributo y comportamiento del usuario. Además, facilita un análisis continuo y contextual de decisiones de acceso, alineándose completamente con los principios de verificación continua, mínimo privilegio y reducción de superficie de ataque característicos de ZTNA. Gracias a su capacidad para extender el modelo Zero Trust más allá de las capacidades nativas de AWS, esta solución logra cumplir casi la totalidad los criterios establecidos, consolidándose como una alternativa más robusta y adaptable para entornos híbridos, multicloud.
2	IAM, IAM Identity Center, Verified Access + IAM Identity Center, Cognito + Verified Access (Policies + Device Trust Providers) + VPC, Security Groups, Network ACL, PrivateLink + GuardDuty, Detective, CloudTrail + Security Hub + EventBridge + Control Tower + SCPs + IAM Access Analyzer	86%	Basada exclusivamente en servicios nativos de AWS como IAM Identity Center, IAM, Verified Access, GuardDuty, Detective y Security Hub, proporciona una arquitectura con capacidades sólidas de autenticación, MFA, monitoreo y control de acceso por identidad. Sin embargo, al centrarse únicamente en mecanismos internos de AWS, presenta limitaciones frente a los requerimientos completos de un modelo ZTNA. Aunque Verified Access habilita acceso seguro a aplicaciones, no ofrece segmentación granular basada en identidad a nivel de aplicación, ni decisiones dinámicas basadas en contexto comparable a motores de políticas como OPA. De igual forma, los servicios de monitoreo de AWS detectan amenazas a nivel de infraestructura, pero no realizan análisis profundo del comportamiento del usuario ni evaluaciones continuas de riesgo propias de Zero Trust. Estas brechas reducen su nivel de cumplimiento frente a los criterios definidos, posicionándola como una solución efectiva en entornos AWS tradicionales, pero menos madura para satisfacer la totalidad de los criterios establecidos para ZTNA.

Fuente: Elaboración propia.

En la Tabla 12 seleccionamos la solución 1 ya que contiene un conjunto de herramientas open source que permiten expresar el mejor cumplimiento en porcentajes (%). Keycloak o ZITADEL cumplen el papel de proveedor de identidad, gestionando usuarios, roles, autenticación y MFA para asegurar que solo identidades verificadas puedan iniciar el proceso de acceso. OPA, junto con el RBAC de Keycloak, se encarga de definir y evaluar políticas avanzadas basadas en atributos y contexto, permitiendo decisiones de autorización más precisas y alineadas con el principio de mínimo privilegio. Por su parte, herramientas como Pomerium, OpenZiti u OAuth2-Proxy funcionan como el componente de acceso seguro, actuando como un proxy que valida la identidad del usuario y aplica las políticas antes de permitir el ingreso a las aplicaciones. En conjunto, estas herramientas nos permiten construir una arquitectura ZTNA funcional, capaz de aplicar autenticación, autorización basada en políticas y control granular del acceso, utilizando soluciones abiertas, accesibles y adecuadas para un entorno académico y de prueba.

2.3 Fase 3 Diseño.

Como resultado de lo realizado en las fases anteriores, donde se identificaron los riesgos en la nube pública y se seleccionaron las herramientas para ayudar en su mitigación, se procedió a integrarlos en un diseño de arquitectura SSE desplegado sobre AWS. Este diseño tuvo como propósito implementar los controles de SWG y ZTNA, de acuerdo con los criterios de aceptación definidos en la fase 1. La arquitectura resultante busca ayudar a entregar un acceso seguro a las aplicaciones internas mediante autenticación y control de privilegios mínimos (ZTNA), y a su vez inspeccionar y filtrar el tráfico saliente hacia Internet para prevenir fugas de información y amenazas web (SWG). El diseño propuesto busca ayudar a tener un acceso seguro y controlado a los recursos corporativos, tanto internos como en la nube pública de AWS, a través de mecanismos de autenticación, segmentación, filtrado de tráfico y monitoreo. Esto permite ayudar a proteger la organización frente a amenazas externas, prevenir la exfiltración de información y la gobernanza del entorno.

El diseño de arquitectura propuesto en esta tesis se basa en un caso de uso híbrido, que puede combinar escenarios relevantes de adopción de controles SWG y ZTNA bajo un modelo SSE, lo cual permite a las organizaciones del sector financiero gestionar de forma centralizada la seguridad de usuarios, aplicaciones y datos, tanto en la red local como en la nube. Esto facilita una protección consistente, adaptable y compatible con

los principios de Zero Trust. En este contexto, la arquitectura podría adaptarse a los siguientes escenarios:

- Seguridad del tráfico de las aplicaciones cloud (EC2): los recursos desplegados

- en instancias EC2 dentro de AWS operan bajo controles SWG dedicados, que filtran y registran el tráfico saliente generado por las aplicaciones, previniendo conexiones a dominios o destinos maliciosos y reduciendo el riesgo de fuga de datos.

- Acceso seguro para administradores y desarrolladores: los usuarios con privilegios administrativos o de desarrollo acceden a los recursos que gestionan mediante controles ZTNA, apoyándose así a una autenticación contextual, control de privilegios mínimos y trazabilidad de las sesiones.

Por otra parte, el diseño de la arquitectura propuesta cumple con un enfoque por capas alineado con el modelo de seguridad en la nube de AWS, lo cual permite organizar los controles implementados y apoyar una defensa en profundidad. Este enfoque facilita la identificación de responsabilidades de seguridad en cada nivel, así como la integración de mecanismos de protección que operan de forma complementaria para mitigar riesgos asociados al acceso y consumo de servicios en la nube.

En la capa de identidad, se establecen los mecanismos de autenticación y autorización que permiten validar la identidad de los usuarios y definir sus niveles de acceso. En esta capa se integran soluciones como IAM Identity Center y Keycloak, las cuales permiten implementar esquemas de Single Sign-On (SSO), autenticación multifactor (MFA) y control de acceso basado en roles (RBAC), garantizando el cumplimiento del principio de mínimo privilegio. Esta capa constituye el primer punto de control dentro del modelo Zero Trust, donde ningún usuario o dispositivo es considerado confiable por defecto.

La capa de red se encarga de la segmentación y protección del tráfico dentro de la infraestructura, mediante el uso de componentes como VPC, subredes, Security Groups y soluciones como pfSense. Estos elementos permiten definir perímetros lógicos, controlar el tráfico entrante y saliente, y aislar recursos críticos, reduciendo la superficie de ataque. Asimismo, esta capa facilita la implementación de políticas de acceso granular basadas en direcciones IP, puertos y protocolos.

En la capa de aplicación, se materializan los controles de acceso seguro mediante la integración de tecnologías como OAuth2-Proxy, Pomerium y Open Policy Agent (OPA), las cuales permiten aplicar políticas dinámicas de autorización basadas en atributos contextuales. Adicionalmente, se incorporan mecanismos de Secure Web Gateway (SWG) mediante herramientas como Squid, que permiten inspeccionar y filtrar el tráfico web, bloqueando contenido malicioso y controlando el acceso a recursos externos. Esta capa es fundamental para garantizar que el acceso a las aplicaciones esté condicionado no solo por la identidad, sino también por el contexto de la solicitud.

Complementariamente, se incluye una capa de inspección y filtrado, donde se integran herramientas como SquidGuard, ClamAV y C-ICAP, las cuales permiten realizar análisis de contenido, detección de malware y filtrado de URLs. Esta capa fortalece la capacidad de prevención frente a amenazas avanzadas, asegurando que el tráfico que ingresa o sale del entorno sea validado antes de ser procesado por las aplicaciones. Finalmente, la capa de monitoreo y auditoría centraliza la recolección de eventos y registros de seguridad mediante servicios como CloudWatch, CloudTrail y EventBridge. Esta capa permite garantizar la trazabilidad de las acciones realizadas dentro del sistema, así como la detección temprana de incidentes de seguridad. La integración de estos servicios facilita la implementación de estrategias de respuesta ante incidentes y el cumplimiento de requisitos de auditoría y gobernanza.

En conjunto, la arquitectura propuesta no solo implementa controles de seguridad aislados, sino que los organiza de manera estructurada en múltiples capas interdependientes, lo cual permite mejorar la resiliencia del sistema, optimizar la gestión de políticas de seguridad y garantizar una protección integral de los recursos en la nube bajo un enfoque de Zero Trust. A continuación, Fig. 13 se presenta la propuesta del diseño de la arquitectura que integra estos controles y herramientas seleccionadas, alineándose con los principios del modelo SASE y contribuyendo a la seguridad en ambientes Cloud del sector financiero.

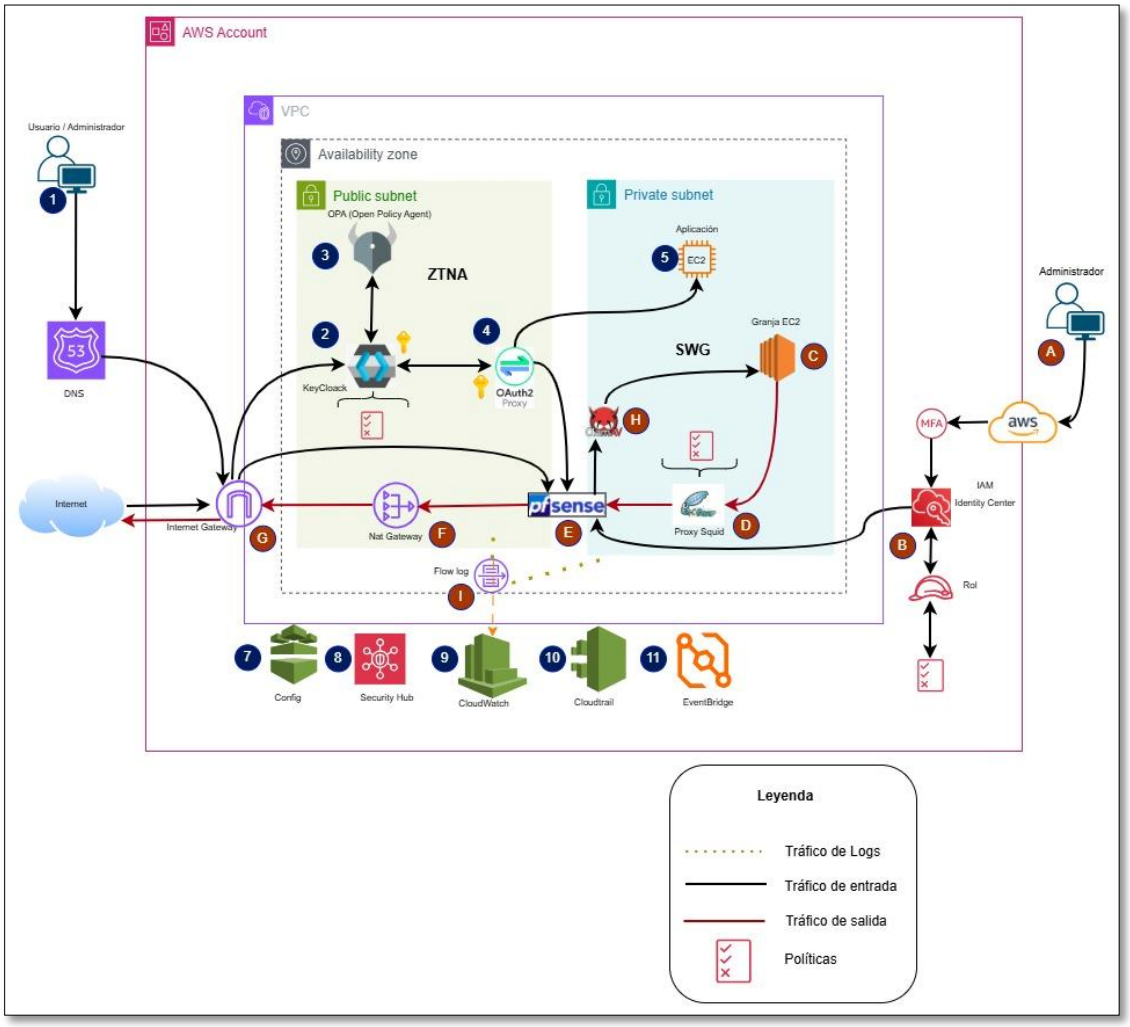

Fig. 13 Diseño de la arquitectura SSE integrando los controles ZTNA y SWG en AWS.

- **Flujo SWG.**

El análisis inicia desde la perspectiva del control SWG, cuya función principal es inspeccionar y filtrar el tráfico saliente (outbound) generado por las instancias EC2 dentro de la subred privada, antes de que alcance Internet. Este flujo se orienta a prevenir exfiltraciones de información, accesos no autorizados o navegación hacia dominios maliciosos. El tráfico comienza en la granja EC2 (C), donde las aplicaciones internas envían solicitudes hacia el exterior. Dicho tráfico atraviesa el Proxy Squid independiente (D), desplegado sobre una instancia dedicada, que actúa como SWG. Este proxy ejecuta la inspección HTTP/HTTPS y aplica políticas de navegación definidas por el administrador (A) desde la consola que tenga un rol específico en IAM Identity

Center, el cual debe ser el mismo que pueda autenticarse usando SSO que actúa como puente (IdP) que entrega esa identidad a pfSense y de esta manera ejecutar tareas administrativas, estableciendo políticas de control y filtrado que se sincronizan con pfSense (E).

El pfSense (E), instalado con dos interfaces NIC, cumple un rol de firewall perimetral y Gateway. La interfaz WAN se ubica en la subred pública, y la interfaz LAN en la subred privada, permitiendo enrutar el tráfico entre ambas zonas de manera controlada y segura. Esta solución se incorpora dentro de la capa de inspección profunda, SquidGuard y ClamAV (G) amplían las funciones del SWG: SquidGuard aplica políticas de filtrado por categorías, usuarios y tipo de contenido. ClamAV (G), mediante C-ICAP, realiza análisis antimalware sobre archivos y URLs. El internet Gateway (F) canaliza el tráfico saliente de pfSense hacia Internet, permitiendo que las instancias privadas permanezcan sin exposición directa. En esta arquitectura, pfSense utiliza su módulo nativo de filtrado y NAT, el cual opera para la inspección de contenido y control outbound. Así, todo el tráfico hacia Internet pasa primero por el control SWG, donde se inspecciona, valida y registra, reforzando la postura de seguridad perimetral y reduciendo el riesgo de fugas de información.

- **Flujo ZTNA.**

En cuanto al control ZTNA, este proporciona la capa de acceso basada en Zero Trust, centrada en el tráfico entrante (inbound) desde los usuarios hacia las aplicaciones privadas. El tráfico que proviene del usuario (1) primero lo resuelve Route53 y luego debe entrar a la VPC por medio del IGW (G). La validación de identidad se realiza mediante OAuth2-Proxy (4) y Keycloak (2): OPA (3) evalúa las políticas de acceso según identidad, postura del dispositivo, ubicación y nivel de cumplimiento. Keycloak actúa como proveedor de identidad (IdP), ofreciendo autenticación federada, inicio de sesión único (SSO) y MFA. Las políticas se implementan bajo un modelo ABAC (Attribute-Based Access Control), donde OPA interpreta los atributos de usuario y contexto provenientes de Keycloak para autorizar o denegar solicitudes.

Por otra parte, OAuth2-Proxy (4) actúa como proxy de identidad dentro del control ZTNA, validando los tokens emitidos por Keycloak antes de redirigir las solicitudes hacia las aplicaciones internas. Finalmente, la aplicación protegida (5) o (E), alojada en una instancia EC2 privada, recibe únicamente tráfico previamente autenticado y autorizado por las políticas de OPA, OAuth2-Proxy y Keycloak.

El modelo se complementa con una capa de monitoreo y cumplimiento continuo, sustentada por servicios nativos de AWS. AWS Config (7) evalúa constantemente las configuraciones de los recursos frente a las políticas definidas. AWS Security Hub (8) y EventBridge (11) centraliza los hallazgos de seguridad provenientes de Config, CloudTrail, Flow Logs (6) y las herramientas open source (pfSense, Squid, SquidGuard, ClamAV, OAuth2-Proxy). Los logs de las herramientas open source se envían hacia CloudWatch Log Groups mediante agentes syslog o CloudWatch Agent. Una función Lambda intermedia transforma los eventos al formato JSON compatible con la API de Security Hub, y el EventBridge permitiendo su ingesta y correlación automática. CloudWatch (9) recopila métricas operativas y genera alarmas ante eventos críticos, pudiendo ejecutar respuestas automáticas, como revocar accesos o aplicar nuevas políticas. Por su parte, CloudTrail (10) registra todas las acciones administrativas, cambios de roles o políticas, habilitando auditorías completas y análisis forense, consolidando un ciclo de monitoreo y verificación continua que refuerza la seguridad y trazabilidad de la arquitectura SWG y ZTNA.

2.4 Fase 4 PoC.

2.4.1 PoC SWG

La presente Prueba de Concepto se desarrolló con el propósito de validar la implementación del control Secure Web Gateway (SWG) dentro de la nube pública de AWS, mediante una arquitectura basada en pfSense y el uso de herramientas de inspección y filtrado como Squid, ClamAV y SquidGuardian. Esta demostración técnica busca evidenciar la capacidad del modelo propuesto para inspeccionar tráfico web saliente desde recursos alojados en una subred privada, previniendo fugas de información, mitigando amenazas web y asegurando un tráfico controlado y monitoreado conforme a los criterios establecidos en la fase 2 de definición.

A continuación, en la Fig. 14 se ilustra en esta PoC, el flujo en donde el pfSense se implementó con una arquitectura de doble interfaz: Una interfaz WAN ubicada en la subred pública, responsable de enrutar el tráfico hacia Internet mediante el Internet Gateway. Una interfaz LAN ubicada en la subred privada, actuando como puerta de enlace para todo el tráfico generado por los recursos internos. Adicionalmente, se desplegó una instancia Amazon EC2 dentro de la red privada, utilizada como host de validación para realizar pruebas de navegación, inspección de tráfico y verificación de políticas. Esta instancia no dispone de acceso público,

garantizando que toda la navegación debe atravesar el SWG implementado sobre pfSense.

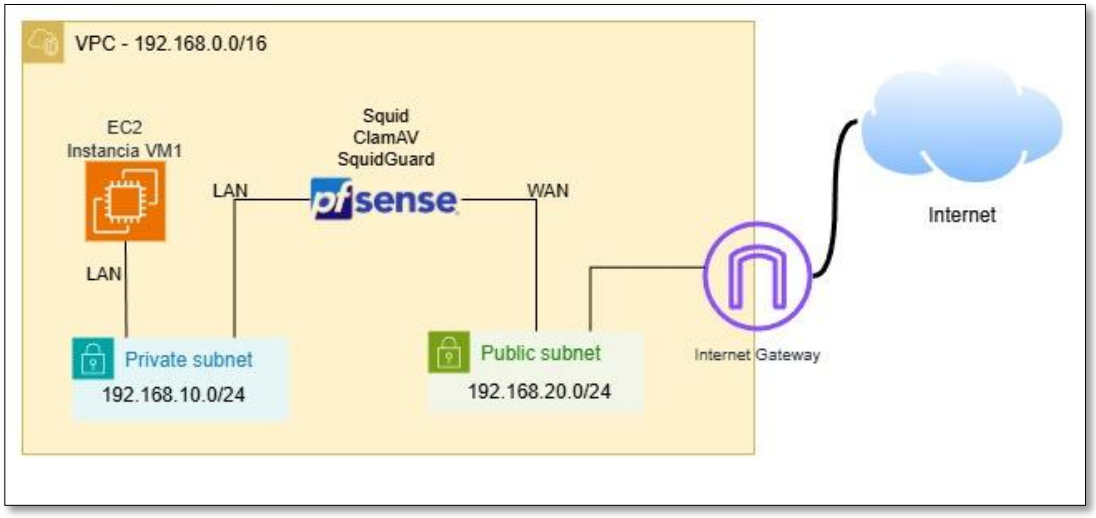

Fig. 14 Flujo PoC SWG en AWS, elaboración propia.

Partiendo de la Fig. 14, en la TABLA 13 se observa el mapeo de los Criteros (Controles) de herramientas para el control SWG en donde se detalla la correspondencia directa entre los controles SWG de la TABLA 6 y su implementación concreta mediante las herramientas seleccionadas en la fase 3, conforme al flujo ilustrado en la Fig. 14.

Tabla 13.
Implementación de controles SWG en AWS.

Criterio "Control" SWG	Criterio de Aceptación	Herramienta	Implementación en la POC
Inspección Web de tráfico SSL/TLS.	Permite detectar y bloquear exfiltración de datos en tráfico cifrado	Squid	CA Autofirmado Interno en pfSense
Filtrado de tráfico y contenido en tiempo real.	Bloquea sitios maliciosos.	SquidGuard	Conjunto de sitios Web agrupados por categorías.
Capacidades de protección avanzada contra malware.	Incluye análisis de archivos y URLs en busca de amenazas.	ClamAV	Firma de Virus para Web y aplicaciones.

Fuente: Elaboración propia.

A continuación, se presentan los casos de prueba diseñados para validar cada control, verificando su cumplimiento frente a algunos de los riesgos identificados en la TABLA 8.

2.4.1.1. Casos de Pruebas.

En el contexto del modelo SWG, se escogieron tres criterios de aceptación de los definidos en la fase 1, los cuales guían esta PoC y permiten validar el cumplimiento del diseño:

- **CT-SWG-01: Inspección de tráfico cifrado mediante técnica MITM (SSL/TLS Interception):** Para cumplir este criterio, Squid se configuró para operar en modo SSL Bump, permitiendo descifrar, analizar y volver a cifrar el tráfico HTTPS. Esta capacidad ofrece visibilidad profunda sobre conexiones cifradas, posibilitando la detección de intentos de exfiltración, acceso a dominios maliciosos y amenazas ocultas dentro de túneles SSL.

  Prueba: Sobre una instancia EC2 en la subred privada y cubierta con el Proxy Squid, se ingresa al sitio Web https://www.youtube.com y se detecta una alerta sobre la conexión no segura (Puerto https). Ver Fig. 15.

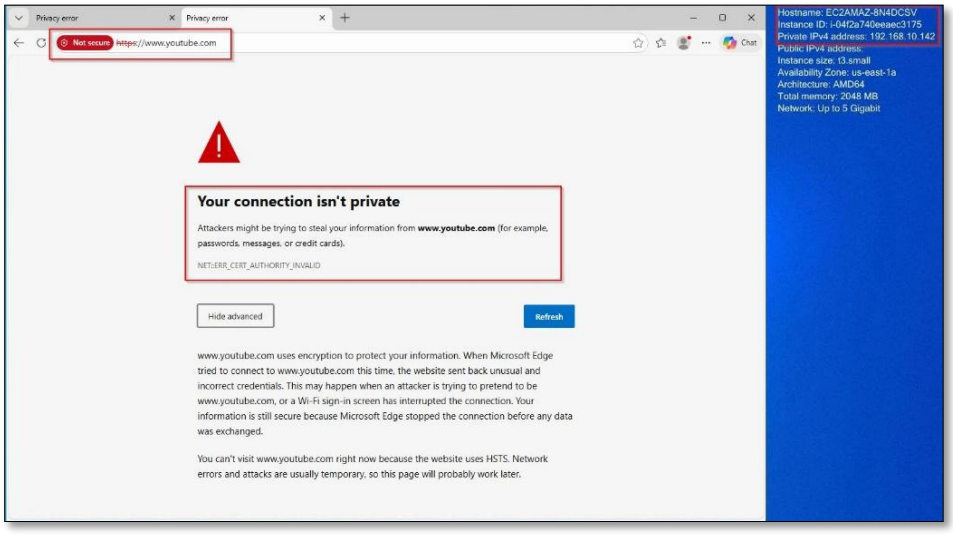

Fig. 15 Sitio Web con conexión no segura, elaboración propia.

Se instala el certificado digital generado por Squid en la instancia EC2 privada, agregándolo al Keystore de “Entidades de certificación raíz de confianza” emitido por pfSense.domain.local. Ver Fig. 16

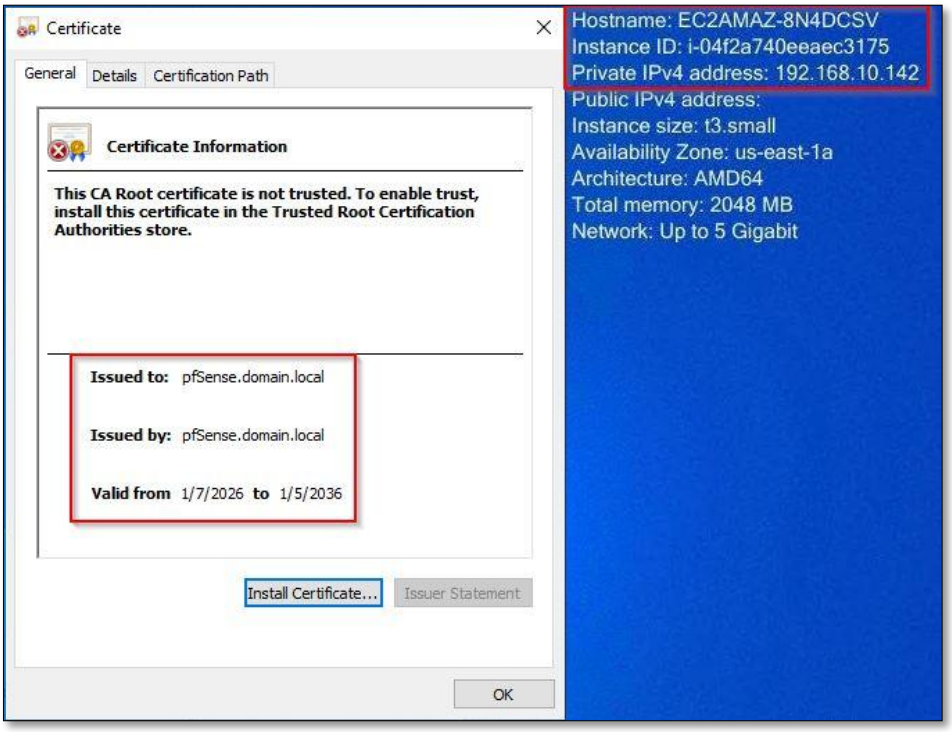

Fig. 16 Certificado digital del Squid para la inspección SSL, elaboración propia.

Una vez instalado el certificado en la instancia, se accede nuevamente a https://www.youtube.com y el sitio carga correctamente. Esto se debe a que no solo el navegador confía en la autoridad certificadora del pfSense/Squid, sino también que la inspección SSL está activa y funcionando. Durante esta inspección, el proxy descifra temporalmente el tráfico HTTPS, permitiendo analizar el contenido real de la sesión, es decir, hace la validación de URL, la verificación de categorías, también la identificación de intentos de exfiltración, el análisis antimalware de archivos y detección de patrones sospechosos en el flujo cifrado. Gracias a esta visibilidad, el control SWG puede aplicar políticas de filtrado, bloqueo y registro que normalmente no serían posibles en tráfico HTTPS cifrado de extremo a extremo. De esta manera, la inspección SSL habilita la capacidad del SWG para proteger contra conexiones maliciosas ocultas en túneles cifrados y reduce el riesgo de fuga de información o descargas peligrosas. Ver Fig. 17.

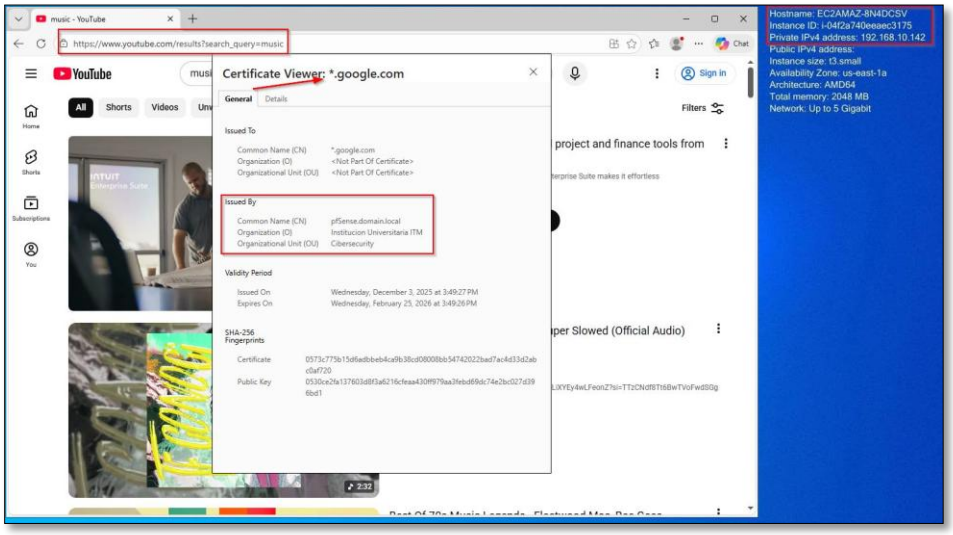

Fig. 17 Sitio Web inspeccionado con Squid, elaboración propia

Resultado: Cumplido, El Squid realiza la inspección SSL de los sitios protegidos por el control que pasen por el HTTPS.

- **CT-SWG-02: Filtrado de tráfico por categorías:** A través de SquidGuardian, integrado a pfSense y Squid, se aplican políticas de acceso basadas en categorías de contenido. Esto permite bloquear navegación hacia sitios considerados riesgosos, improductivos o no autorizados, fortaleciendo las medidas de cumplimiento y reduciendo la superficie de exposición frente a amenazas Web.

  Prueba: Desde el módulo SquidGuard en pfSense se configuró la denegación de las categorías Redes Sociales y Video. Posteriormente, desde la instancia EC2 privada se intentó acceder al sitio web https://www.facebook.com y, al estar clasificado dentro de la categoría de redes sociales, el acceso fue bloqueado conforme a las políticas establecidas en SquidGuard.. Ver Fig. 18.

Fig. 18 Bloqueo de sitio Web por categoría, elaboración propia

En los registros de bloqueo de SquidGuard se puede observar la política aplicada, la fecha y hora del evento, la IP de origen, el sitio solicitado y la acción ejecutada. Ver Fig. 19.

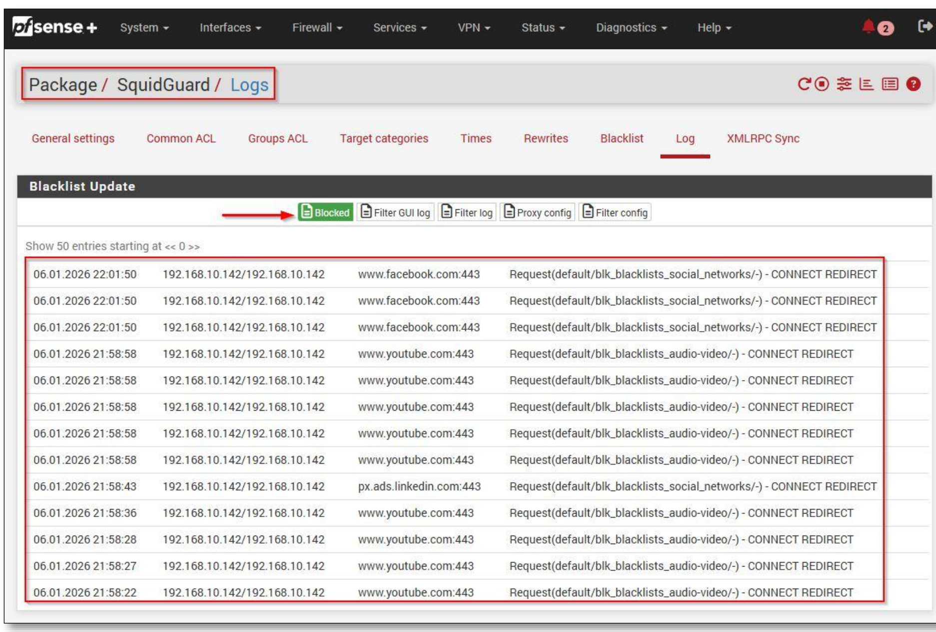

Fig. 19 Logs de SquidGuard, elaboración propia.

Resultado: Cumplido, desde el SquidGuard se configura cada una de las categorías de contenido que se desean aplicar, para este caso solo fue denegado dos categorías.

- **CT-SWG-03: Antivirus Web (AV Web) para validación de descargas y análisis de archivos:** Para este criterio se integró ClamAV mediante ICAP,

permitiendo analizar en tiempo real archivos descargados o transmitidos por HTTP/HTTPS. Esta capa de defensa previene la llegada de malware, troyanos y paquetes sospechosos hacia la EC2 interna, imponiendo un control preventivo sobre el material descargado.

Prueba: Una vez revisado que los servicios de Squid, Clamav y c-icap se encuentran activos en el pfSense, se procede a realizar la prueba de Antimalware. Ver Fig. 20.

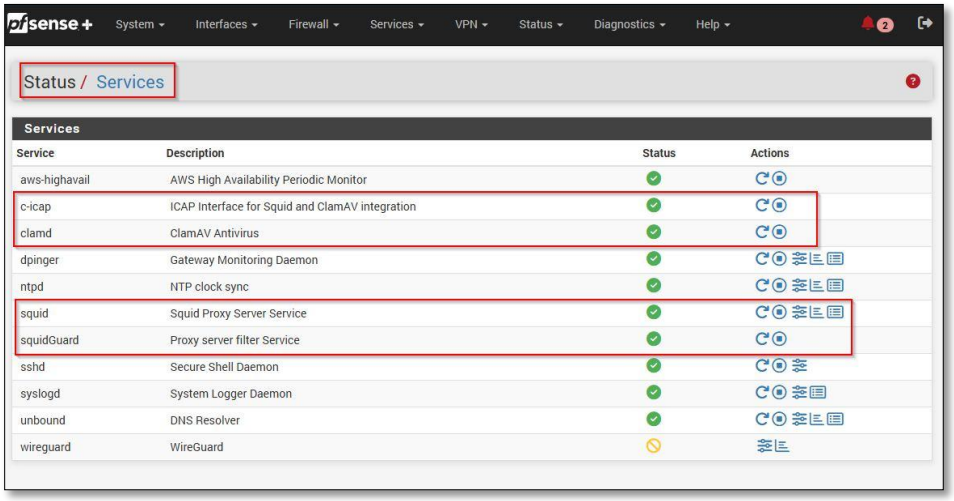

Fig. 20 Servicios activos, elaboración propia.

Se ingresa al sitio Web https://www.eicar.org/download-anti-malware-testfile para realizar pruebas de descargas de virus. Ver Fig. 21.

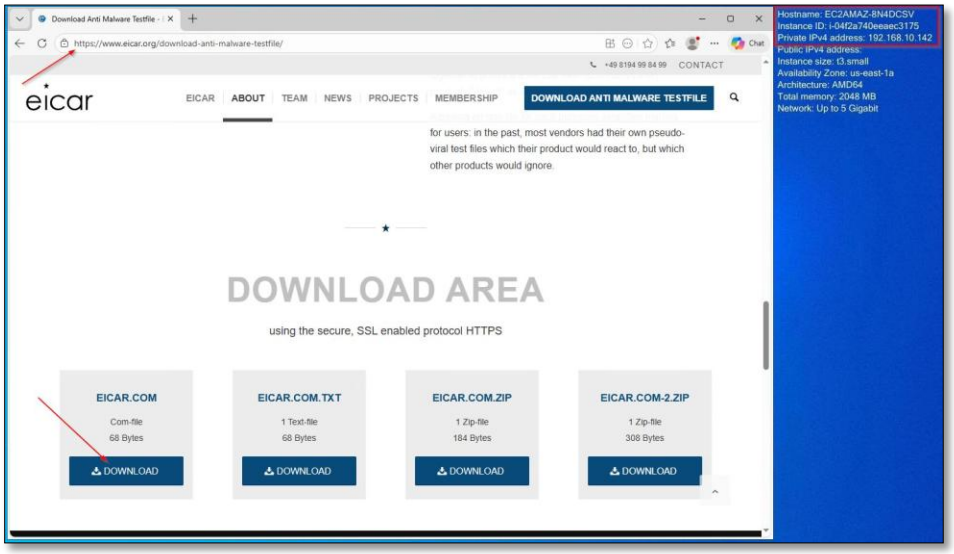

Fig. 21 Sitio Web para prueba de Virus, elaboración propia.

Se identifica que el archivo es detectado como virus por el ClamAV, como lo muestra la URL en la Fig. 22.

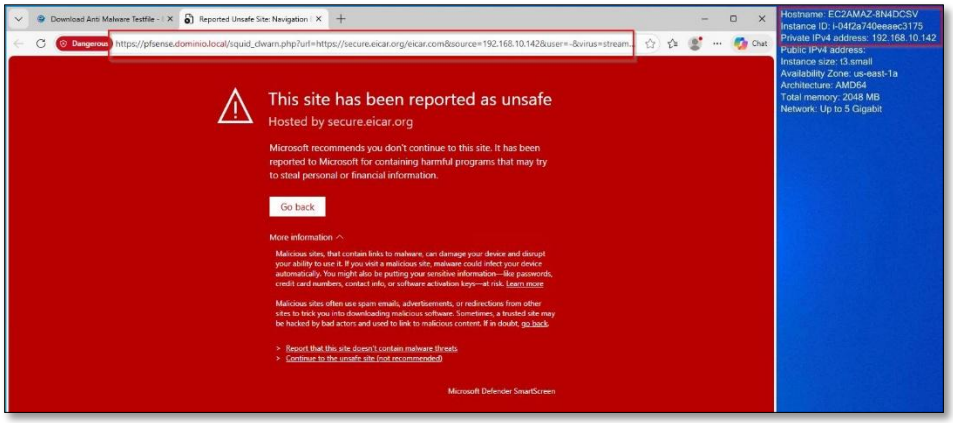

Fig. 22 Detección de virus, elaboración propia.

Resultado: Cumplido, con las descargas de virus se genera el bloqueo por el ClamAV.

2.4.2 PoC ZTNA.

En esta sección se presenta la validación de 3 criterios de aceptación definidos previamente en la fase 2 para el modelo ZTNA, utilizando las herramientas seleccionadas en la fase 3 como capa de acceso basada en confianza cero. Para ello, se desplegaron en AWS las soluciones Keycloak, oauth2-proxy, políticas OPA y una aplicación interna de Node.js, integradas para que la autenticación, la autorización y la evaluación de políticas se ejecuten de forma centralizada sobre el tráfico entrante hacia la aplicación privada. Estos criterios, establecidos previamente como controles de seguridad, se verificaron mediante casos de prueba orientados a comprobar su cumplimiento frente a algunos de los riesgos identificados en la TABLA 5 en el entorno de la nube pública de AWS.

A continuación, en la Fig. 23 se ilustra el flujo que siguen las herramientas dentro del modelo ZTNA propuesto en la fase 3; la solicitud del usuario remoto se autentica en Keycloak mediante OIDC/SAML con MFA y SSO, emitiendo tokens que OAuth2-proxy valida antes de permitir el forwarding. Posteriormente, OPA evalúa políticas ABAC considerando identidad, contexto y atributos del token para autorizar o denegar el acceso a los recursos internos de la aplicación Node.js alojada en VPC privada. Este diseño asegura verificación continua.

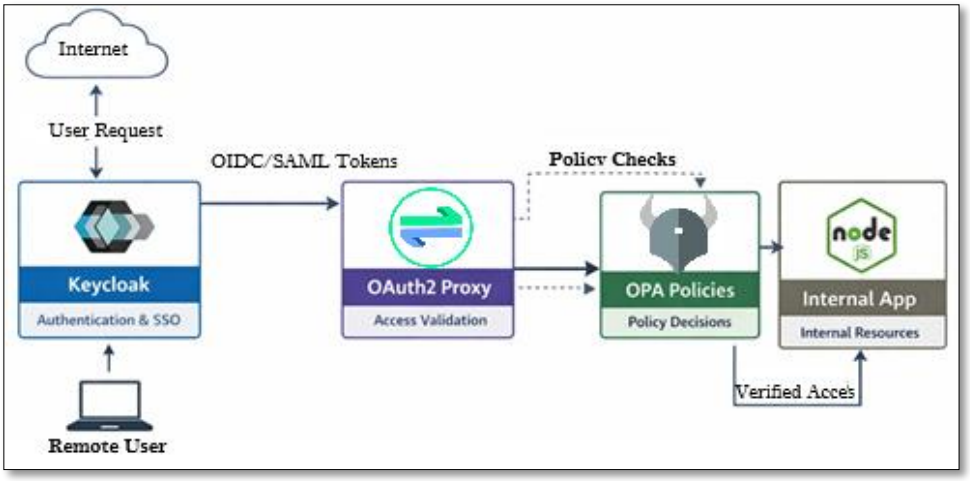

Fig. 23 Flujo Poc ZTNA en AWS, elaboración propia.

Partiendo de la Fig. 23, en la TABLA 14 observamos el mapeo de los Criteros (Controles) de herramientas para el control ZTNA.

TABLA 14.
Implementación de controles ZTNA en AWS.

Criterio "Control" ZTNA	Criterio de Aceptación	Herramienta	Implementación en la POC
Autenticación y autorización robusta basada en identidad	Asegura control de acceso sin depender de red perimetral.	Keycloak + oauth2-proxy	Validación OIDC de tokens JWT.
Autenticación multifactor	Requiere MFA incluso dentro de la red.	Keycloak (realm MFA)	MFA obligatorio configurado en el cliente OIDC para todos los usuarios
Acceso condicional basado en contexto/Menor Privilegio	Aplica políticas según ubicación, dispositivo y comportamiento. /Otorga acceso solo a recursos estrictamente necesarios.	Políticas OPA (.rego) Roles Keycloak + OPA	Validación ABAC con claims Según rol definido en Keycloak. Reglas que limitan recursos por grupo/rol (ej: admin→/api/all, user→/api/read-only)

Fuente: Elaboración propia.

La TABLA 14 detalla la correspondencia directa entre los controles ZTNA de la TABLA 7 y su implementación concreta mediante las herramientas seleccionadas en la fase 3, conforme al flujo ilustrado en la Fig. 23. A continuación, se presentan los casos de prueba diseñados para validar cada control, verificando su cumplimiento frente a algunos de los riesgos identificados en la TABLA 8.

2.4.2.1. Casos de Pruebas.

Para los casos de prueba CT-ZTNA-01, CT-ZTNA-02 y CT-ZTNA-03, a continuación, en la TABLA 15 se presentan los usuarios creados en Keycloak para cada uno de ellos, junto con los códigos de retorno esperados y los resultados obtenidos. Estos casos se detallarán paso a paso en las siguientes secciones "CT-ZTNA-01, CT-ZTNA-02 y CT-ZTNA-03".

TABLA 15
Códigos de retorno por usuario.

Usuario	Keycloak MFA	Roles	OPA Result	Código	Resultado	Justificación
User1	✗ Sin MFA	["user"]	{"result":true}	**N/A**	**MFA requerido**	Keycloak Exige la activación del MFA
Usuario2	☑ MFA OK	["admin"]	{"result":true}	**200 OK**	**Dashboard completo**	MFA + rol válido

Luis	☑ MFA OK	["Rol_No_Valido"]	{"result":false}	**403 Policy**	**ZTNA Denied**	Rol no permitido OPA
User3	☑ MFA OK	[]	{"result":false}	**403 policy**	**Sin rol creado en Keycloak.** **ZTNA Denied.**	Token invalido, oauth2-proxy lo rechaza por no contar con rol. OPA lo rechaza.

Fuente: Elaboración propia.

- **CT-ZTNA-01: Autenticación robusta basada en identidad:** Comprobar que ningún recurso interno es accesible sin token válido de Keycloak.

Precondiciones:

- ✓ Sin cookies/sesión activa OAuth2-proxy.
- ✓ Acceder a la URL : http://3.148.208.193:4180 (OAuth2-proxy login).

Resultado esperado: Redirección automática a Keycloak → Denegación sin login exitoso.*Ver Fig.24.*

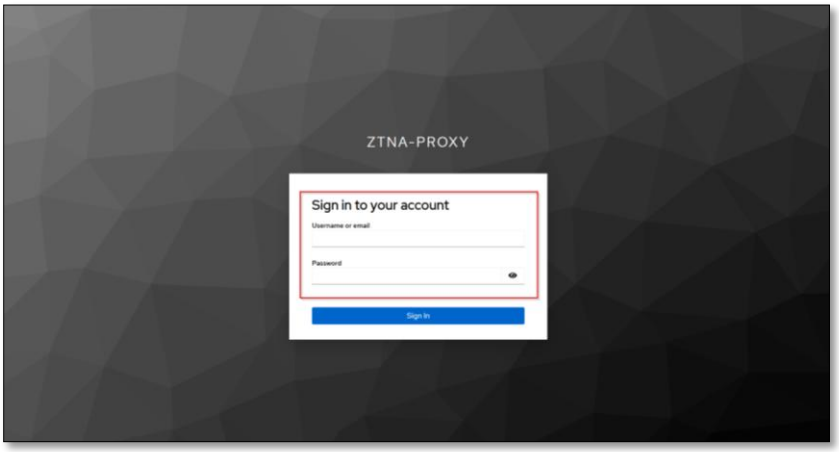

Fig. 24 Pantalla login OAuth2-proxy solicitando credenciales Keycloak, elaboración propia.

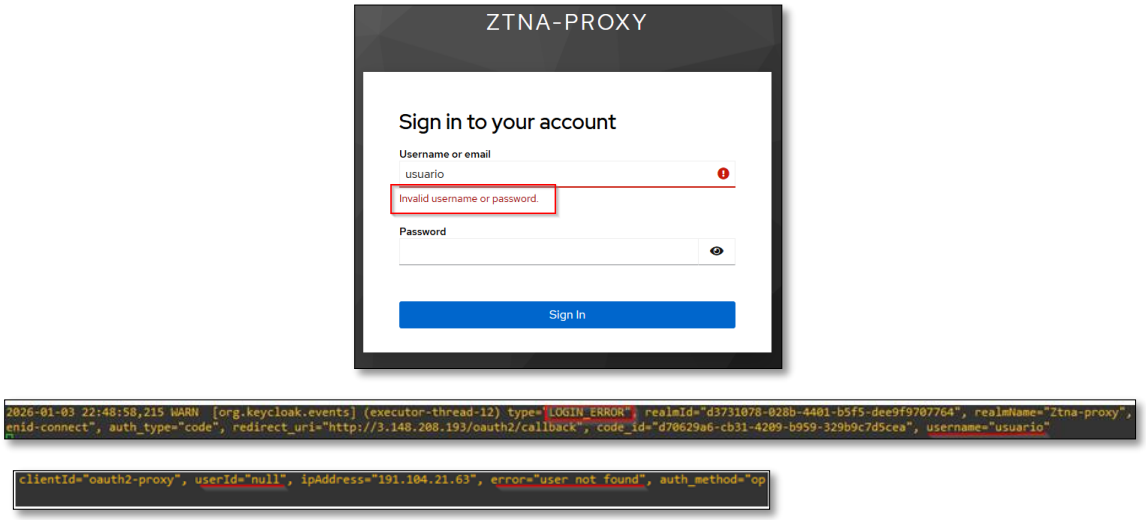

Fig. 25 Redirección a login OAuth2-proxy al intentar acceso no autenticado, elaboración propia.

Log OAuth2-proxy: client_id=ztna-proxy user_ip=... error="user not found" auth method=up.

Resultado: El criterio CT-ZTNA-01 se cumple porque OAuth2-proxy intercepta todo tráfico entrante a la app interna (http://3.148.208.193:4180), actuando como capa de verificación de identidad ante el recurso privado, rechazando accesos sin token OIDC válido de Keycloak, forzando así autenticación explícita.

- **CT-ZTNA-02: Autenticación multifactor:** Verificar MFA obligatorio.

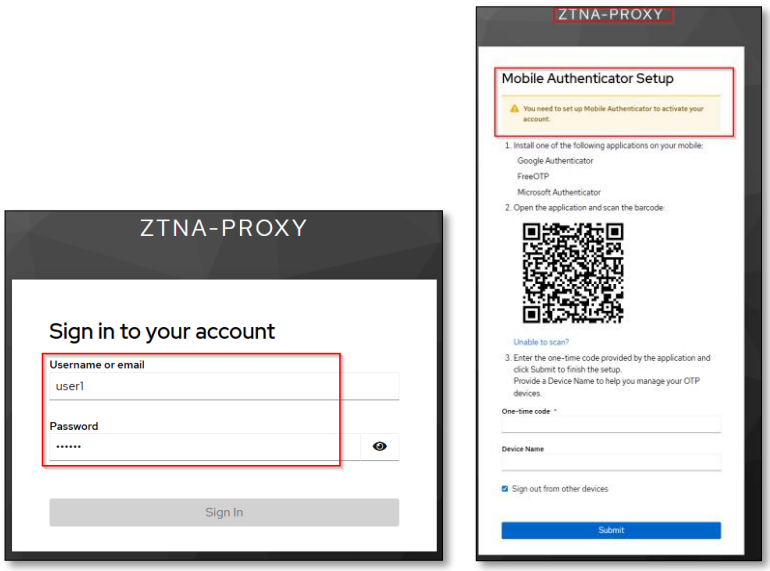

Fig. 26 Obligatoriedad MFA para usuarios, elaboración propia.

El user1 se crea con rol aprobado de acuerdo a las policitas de OPA, pero sin MFA activo para dar trazabilidad del proceso y poder observar que es un paso Obligatorio para poder acceder a la aplicación interna.

Precondiciones:

- ✓ Usuario "usuario2 con credenciales correctas, MFA activado en Keycloak.
- ✓ Acceso inicial vía http://3.148.208.193:4180

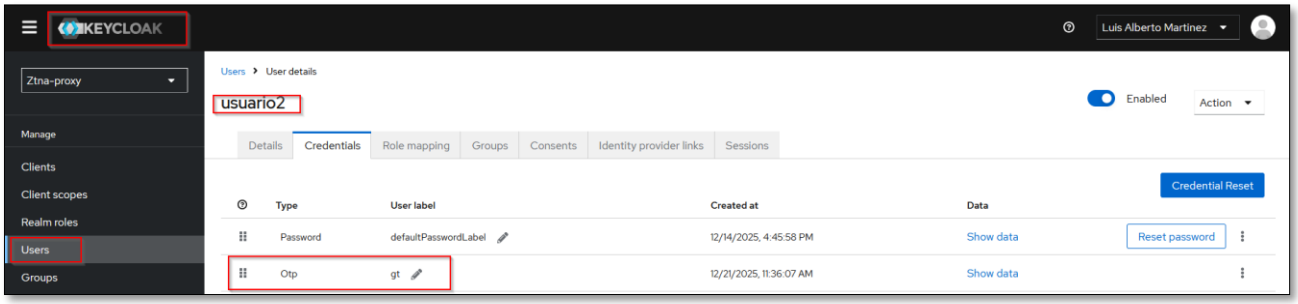

Fig. 27 MFA Obligatorio Keycloak para usuario2, elaboración propia.

Pasos:

- ✓ Acceder a OAuth2-proxy → ingresar usuario/contraseña (usuario2).

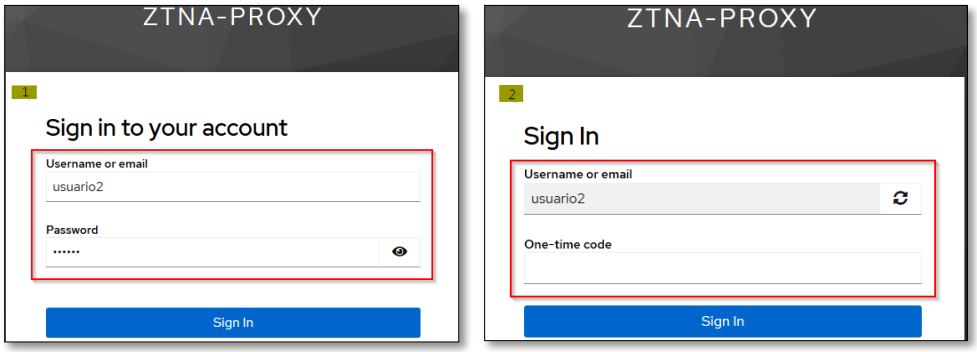

Fig. 28 Login usuario2 con MFA, elaboración propia.

- ✓ Completar código OTP incorrecto (Intento fallido).

Resultado esperado:

- ✓ Sin MFA completo: Denegación con "Invalid authenticator code".

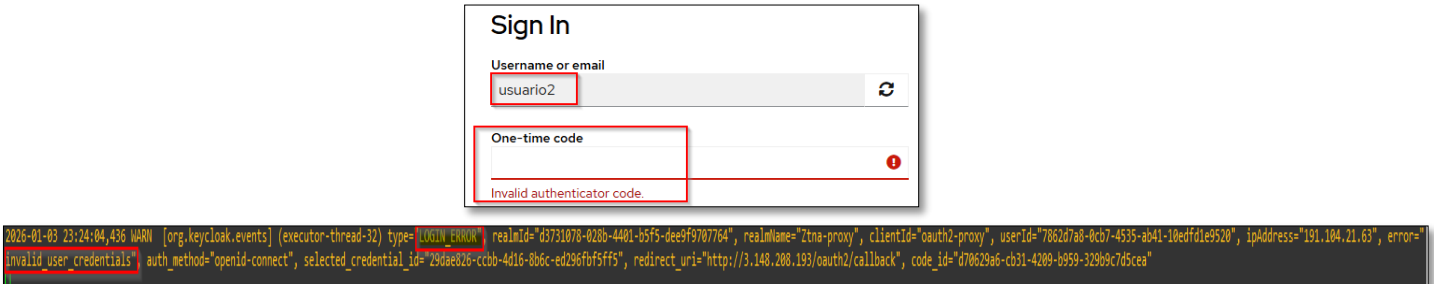

Fig. 29 Login Fallido MFA invalido, elaboración propia.

Resultado: Este criterio CT-ZTNA-02 se cumple porque Keycloak impone MFA (TOTP via app móvil) como paso obligatorio post-username/password, bloqueando accesos con OTP inválido mediante verificación en flujo OIDC.

OAuth2-proxy redirige a Keycloak (OIDC auth_code flow); realm Keycloak configurado con "MFA required" para usuarios como "usuario2", generando challenge OTP dinámico. Fallo en OTP → denegación sin token issuance.

- **CT-ZTNA-03: Acceso condicional basado en rol/Menor privilegio:** Validar políticas ABAC en OPA según rol en Keycloak.

Precondiciones:

- ✓ Usuario "usuario2" (rol: "admin") con MFA completado.
- ✓ Usuario "luis" (sin rol definido en las políticas rego de OPA).
- ✓ Política OPA: permite /api/admin/* solo para rol "admin".

Resultado esperado:

Paso 1: **MFA Ogligatorio (“User1” rol user):**

Usuario autorizado ("usuario2" rol admin):

- ✓ Login + MFA exitoso.
- ✓ Acceder a APP protegido por OPA.

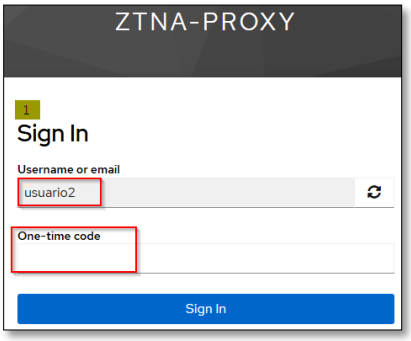

Fig. 30 Login con MFA usuario2, elaboración propia.

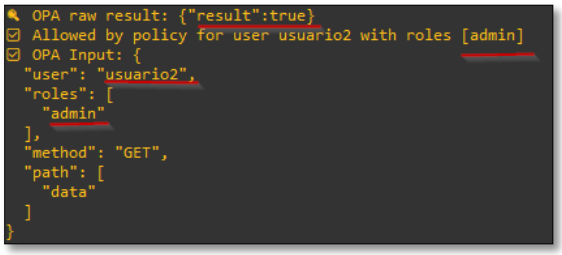

Fig. 31 Política de acceso OPA, elaboración propia.

La app solo devuelve los datos cuando result:true. es decir, acceso Aprobado.

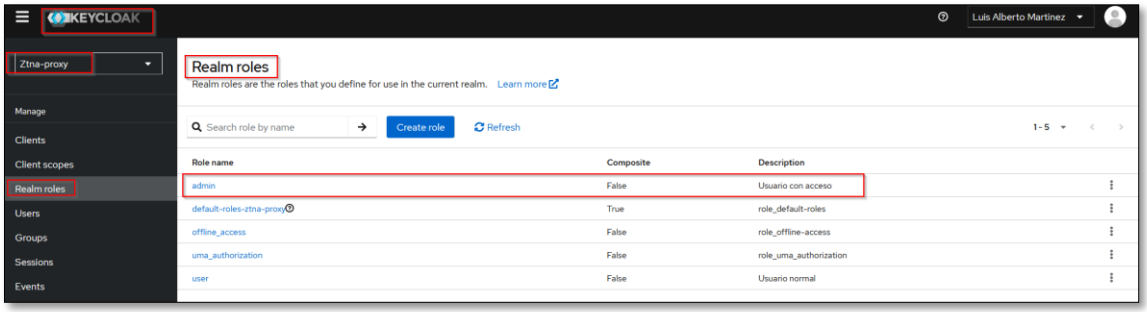

Fig. 32 Roles definidos en Keycloak, elaboración propia.

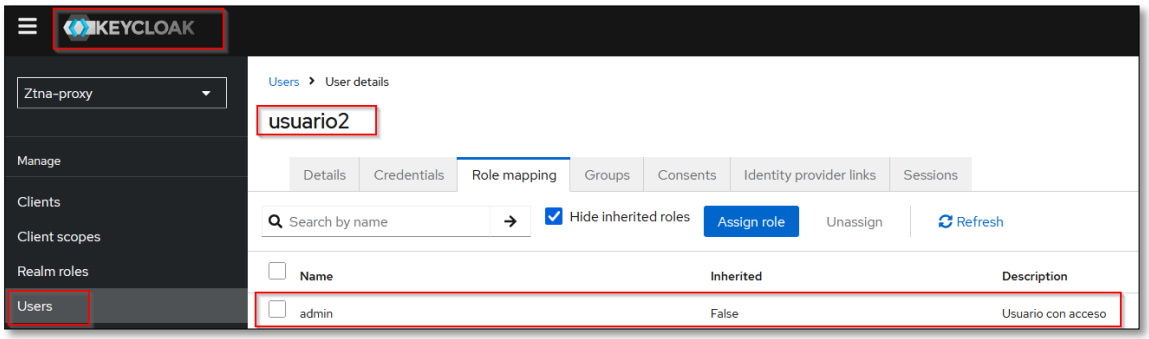

Fig. 33 Roles asignados en Keycloak usuario2, elaboración propia.

Una vez el usuario se autentica, pasa el doble factor de autenticación (MFA), OPA comprueba el rol y permite el acceso, puede ingresar a la APP interna.

Resultado esperado:

- ✓ **Paso 1:** OPA allow → 200 OK, acceso a app interna, ver Fig. 34. La política en authz.rego autoriza correctamente tanto a usuario2 (rol admin).

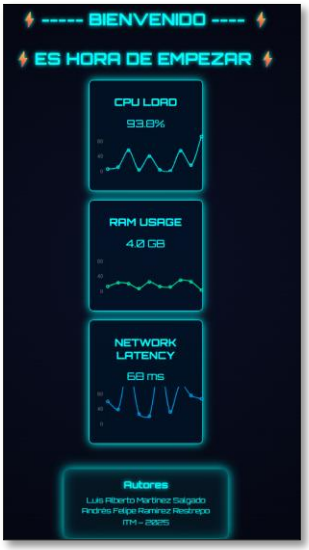

Fig. 34 APP Interna, elaboración propia.

Paso 2: **Usuario no autorizado ("luis" sin rol definido en OPA):**

- ✓ Login + MFA exitoso.
- ✓ Acceder a la misma APP. (OPA deny → OAuth2-proxy 403 Forbidden)

Usuario: "luis" (rol: "Rol_No_Valido"), no permite el ingreso al no contar con un rol definido en las políticas rego de OPA.

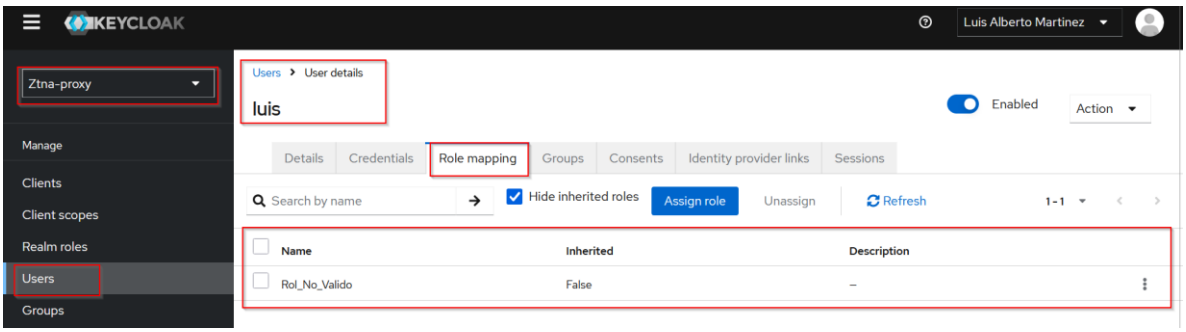

Fig. 35 Rol default Usuario Luis, elaboración propia.

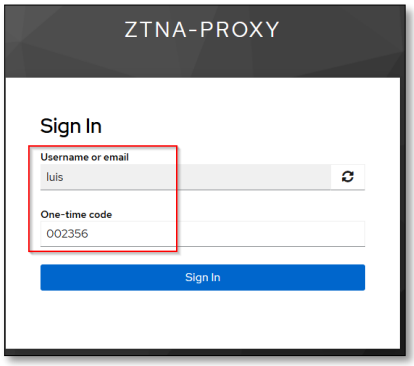

Fig. 36 Login usuario Luis con MFA, elaboración propia.

Resultado esperado:

✓ **Paso 2:** OPA deny → OAuth2-proxy 403 Forbidden.

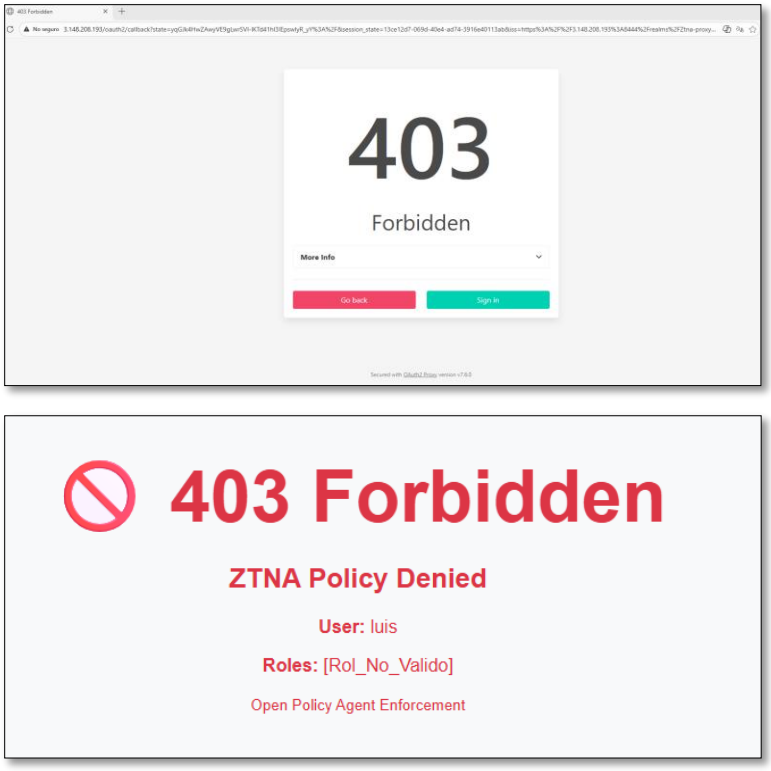

Fig. 37 Acceso denegado política OPA-Rol no Valido, elaboración propia.

Resultado: Este criterio CT-ZTNA-03 se cumple porque OPA evalúa claims JWT de Keycloak (roles) en runtime contra reglas Rego ABAC, permitiendo/denegando granularmente endpoints como /api/admin/* solo para rol "admin".

OAuth2-proxy pasa token a OPA (via header Authorization); authz.rego chequea input.roles contains "admin" para allow. Sin match → deny propagado como 403 Forbidden. Implementa least privilege dinámico.

Paso 3: **Usuario no autorizado ("user3" sin rol definido en Keycloak):**

- ✓ Login + MFA exitoso.
- ✓ Acceder a la misma APP. (oauth2-proxy deny → Keycloak 500 problema **login**)

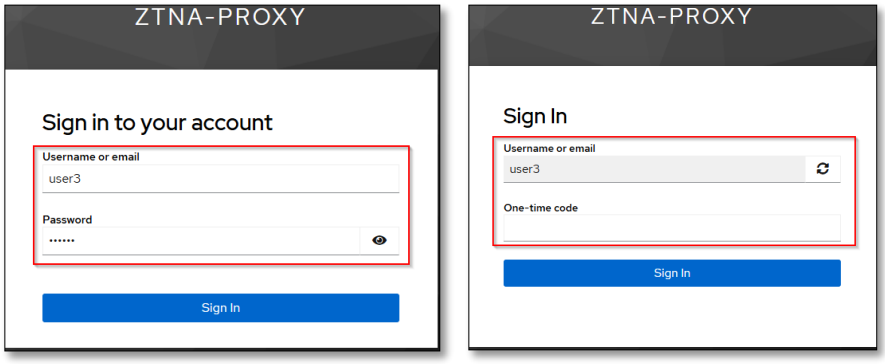

Fig. 38 Fases primarias de autenticación.

Resultado: En este escenario, el usuario “user3” logra completar correctamente las fases de autenticación primaria (credenciales) y autenticación multifactor (MFA), lo que indica que Keycloak valida su identidad y emite de forma correcta un authorization code como parte del flujo OAuth 2.0 / OpenID Connect.

Sin embargo, el usuario no tiene roles asignados en Keycloak ver Fig.39, lo cual es un elemento crítico para la fase de autorización dentro del modelo Zero Trust. Al recibir el authorization code, oauth2-proxy intenta intercambiarlo por un access token ante Keycloak. Durante este proceso, Keycloak evalúa los claims asociados al usuario, incluyendo los roles requeridos por la aplicación cliente.

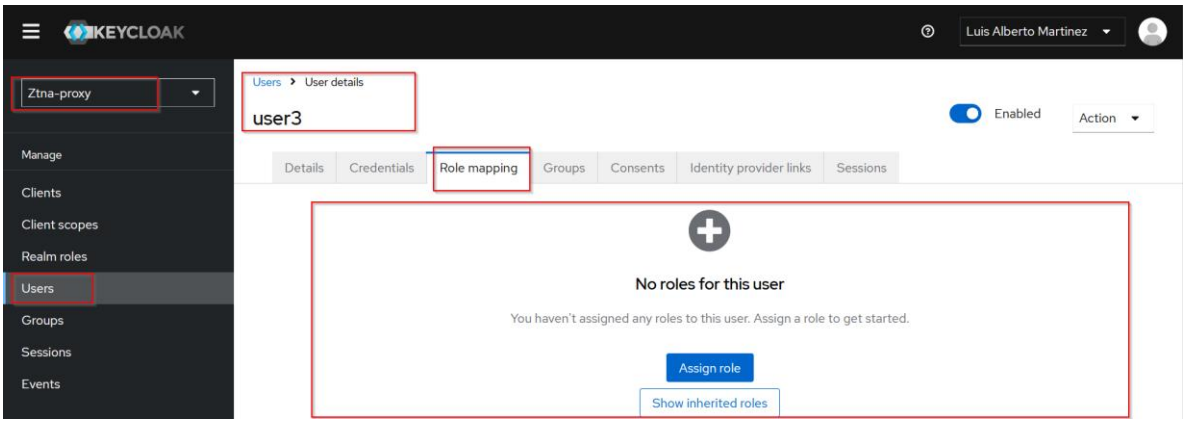

Fig. 39 Validación de Rol User3

Debido a la ausencia de roles válidos, el intercambio de token falla. Este fallo provoca que oauth2-proxy no reciba un token de acceso válido, lo que genera un error interno (HTTP 500) mostrado al usuario final. Este comportamiento evidencia que, aunque la identidad fue verificada, el usuario no cumple las políticas de autorización definidas, por lo que el acceso a la aplicación es correctamente denegado, ver Fig.40.

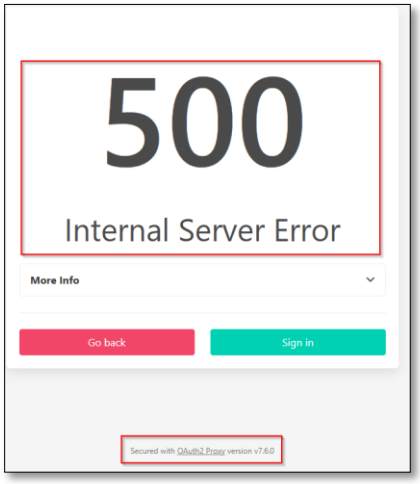

Fig. 40 Acceso Denegado 500 Internal Server Error.

Este resultado demuestra la separación explícita entre autenticación y autorización, principio fundamental del enfoque ZTNA, donde un usuario puede autenticarse exitosamente pero aun así ser bloqueado si no cumple con las políticas de acceso basadas en identidad y contexto.

Conclusiones

- La arquitectura implementada demuestra que es posible construir un control SWG robusto utilizando herramientas de código abierto integradas con componentes nativos de AWS. El uso de pfSense como gateway, junto con Squid, SquidGuardian y ClamAV, permitió obtener una solución flexible, escalable y completamente alineada con los principios de seguridad en la nube basados en SSE. Los resultados de la PoC verifican que esta aproximación no solo cumple los criterios técnicos establecidos, sino que además proporciona una base sólida para escalar hacia ambientes más complejos o integrarse con otros controles de seguridad, como ZTNA, dentro de un marco SASE más amplio.

- La implementación de la POC ZTNA en AWS mediante Keycloak, OAuth2-proxy, políticas OPA y aplicación Node.js valida exitosamente los criterios de aceptación seleccionados para la poc. Los casos de prueba CT-ZTNA-01 al 03 demuestran verificación continua de identidad (autenticación OIDC/MFA), autorización granular basada en roles ABAC (OPA), y aplicación efectiva del principio de menor privilegio, mitigando riesgos identificados en la TABLA 4 como accesos no autorizados, suplantación de identidad y movimientos laterales. La arquitectura desplegada (Fig. 23) elimina confianza perimetral tradicional, reemplazándola por controles dinámicos centrados en identidad y contexto, alineados con NIST SP 800-207 y guías AWS Zero Trust. Cada componente cumple función específica: OAuth2-proxy como PEP, Keycloak como IdP robusto con MFA, OPA como PDP para políticas complejas, evidenciando viabilidad técnica de ZTNA en entornos nube híbridos.

Recomendaciones

- Fortalecer la gobernanza de seguridad en entornos multicloud. Aunque la arquitectura se implementó sobre AWS, es recomendable extender el modelo SSE basado en SWG y ZTNA a escenarios multicloud y on-premise. Esto permitirá mantener políticas homogéneas, reducir brechas de seguridad y mejorar la trazabilidad de eventos en infraestructuras distribuidas.

- Estandarizar las políticas de acceso e identidad. Dado que el principio Zero Trust depende profundamente de la identidad, se recomienda unificar la gestión mediante un IdP central (Keycloak, ZITADEL o IAM Identity Center). Asimismo, se

debe garantizar que todas las aplicaciones internas consuman roles, atributos y políticas de autorización de forma consistente.

- Automatizar verificaciones de cumplimiento y remediación. Integrar mecanismos automáticos de evaluación y corrección utilizando AWS Config, Security Hub y EventBridge permite que la arquitectura detecte desviaciones o anomalías y ejecute acciones como bloqueo de acceso, aislamiento de instancias o despliegue de políticas correctivas.

- Implementar rotación continua de certificados en SWG. En controles que usan inspección SSL/TLS mediante MITM, como Squid o pfSense, es imprescindible rotar los certificados generados por la CA interna, reforzar su distribución segura y auditar su vigencia para evitar errores de confianza, como el observado en la página “Your connection isn’t private”.

- Profundizar en la integración con SIEM/SOAR corporativos. Para organizaciones financieras, es recomendable enviar todos los logs (pfSense, Squid, ClamAV, Keycloak, OAuth2-Proxy, OPA y servicios AWS) a un SIEM central como Splunk, QRadar o ELK, habilitando correlación avanzada, orquestación y respuesta automatizada ante incidentes.

- Fortalecer la capacitación del personal técnico y de los usuarios. El éxito del modelo SSE depende no solo de la arquitectura, sino del uso correcto por parte de administradores y usuarios. Se recomienda realizar programas de capacitación continua sobre:
    - riesgos de fuga de información.
    - buenas prácticas de navegación.
    - MFA y manejo de identidades.
    - detección de phishing.
    - configuraciones seguras en la nube.

- Escalar la arquitectura hacia ambientes productivos.La PoC demuestra viabilidad, pero para producción deben considerarse elementos adicionales:
    - Alta disponibilidad (HA) para pfSense/OPNsense.
    - Balanceadores de carga (ALB/NLB).
    - Métricas de desempeño y pruebas de estrés del SWG.
    - Endurecimiento adicional del IdP y de los proxies de acceso.

- Gestión de secretos con AWS Secrets Manager o HashiCorp Vault.

- Complementar el modelo SSE con CASB y DLP. Para un control más completo dentro del sector financiero, se recomienda integrar un CASB (nativos, comerciales o de código abierto) que permita inspección profunda de SaaS, así como mecanismos avanzados de DLP que complementen los controles de SWG y ZTNA.

- Monitorear continuamente tendencias de amenazas y actualizaciones. El panorama de amenazas en la nube evoluciona rápidamente. Se recomienda actualizar periódicamente:
  - firmas de ClamAV.
  - listas de filtrado DNS/URL.
  - reglas de OPA.
  - políticas de Keycloak.
  - configuraciones de pfSense y Squid.
  - benchmarks CIS para AWS

- Evaluar la adopción futura de soluciones SSE comerciales. Aunque la arquitectura basada en herramientas open source es viable y robusta, fabricantes como Zscaler, Netskope o Palo Alto ofrecen capacidades avanzadas (IA, sandboxing, DLP dinámico, SD-WAN). Evaluar una posible adopción híbrida o escalada permitirá comparar costos, complejidad operativa y madurez tecnológica.

Bibliografía

[1] T. H. Group, «d1.awsstatic.com,» [En línea]. Available: https://d1.awsstatic.com/psc-digital/2022/gc-mig/business-value-of-migration/Business-Value-of-Migration-eBook-ES-XL.pdf.

[2] gartner, «https://www.gartner.com,» [En línea]. Available: https://www.gartner.com/en/newsroom/press-releases/2022-02-09-gartner-says-more-than-half-of-enterprise-it-spending.

[3] P. Alto, «Palo Alto,» [En línea]. Available: https://www.paloaltonetworks.es/apps/pan/public/downloadResource?pagePath=/content/pan/es_ES/resources/research/cloud-native-security-summary-2023.

[4] aws, «https://aws.amazon.com,» [En línea]. Available: https://aws.amazon.com/es/compliance/data-protection/.

[5] fortinet, «www.fortinet.com,» [En línea]. Available: https://www.fortinet.com/content/dam/fortinet/assets/reports/es_la/cloud-security-report-2024.pdf.

[6] E. S. Group, «SSE Leads the Way to SASE,» [En línea]. Available: https://zerotrust.cio.com/wp-content/uploads/sites/64/2024/08/esg-sse-leads-the-way-to-sase.pdf?utm….

[7] MoldStud, «Moldstud,» [En línea]. Available: https://moldstud.com/articles/p-discover-how-secure-access-service-edge-sase-is-revolutionizing-network-security?.

[8] Forinet, «Fortinet,» [En línea]. Available: https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2023/fortiguard-labs-reports-destructive-wiper-malware-increases-over-50-percent.

[9] R. Semana. [En línea]. Available: https://www.semana.com/tecnologia/articulo/atentos-en-2022-hubo-alarmante-cifra-de-intentos-de-ciberataques-en-colombia/202314/.

[10] crowdstrike, «www.crowdstrike.com,» [En línea]. Available: https://www.crowdstrike.com/cloud-risk-report/.

[11] Netskope, «www.netskope.com,» [En línea]. Available: https://www.netskope.com/solutions/secure-web-gateway.

[12] n.-C. d. Exito, «https://www.netskope.com/resources/case-studies#&&industry=financial-service-insurance&,» [En línea]. Available: https://www.netskope.com/resources/case-studies#&&industry=financial-service-insurance&.

[13] zscaler, «www.zscaler.com,» [En línea]. Available: https://www.zscaler.com/customers#customersListing.

[14] secureframe, «secureframe.com,» [En línea]. Available: https://secureframe.com/es-es/blog/cloud-security-statistics1.

[15] nttdata, «https://mx.nttdata.com,» [En línea]. Available: https://mx.nttdata.com/es/case-studies/multinational-bank-achieves-10x-value-from-aws-migration.

[16] cloudflare, «www.cloudflare.com,» [En línea]. Available: https://www.cloudflare.com/es-es/learning/cloud/what-is-cloud-security/.

[17] Karpersky, «latam.kaspersky.com,» [En línea]. Available: https://latam.kaspersky.com/resource-center/definitions/what-is-cloud-security.

[18] kaspersky, «www.kaspersky.es,» [En línea]. Available: https://www.kaspersky.es/resource-center/definitions/what-is-cloud-security.

[19] cloudflare, «www.cloudflare.com,» [En línea]. Available: https://www.cloudflare.com/es-es/learning/access-management/what-is-sase/.

[20] Paloalto, «www.paloaltonetworks.lat,» [En línea]. Available: https://www.paloaltonetworks.lat/cyberpedia/what-is-sase.

[21] akamai, «https://www.akamai.com,» [En línea]. Available: https://www.akamai.com/glossary/what-is-sase.

[22] microsoft, «www.microsoft.com,» [En línea]. Available: https://www.microsoft.com/es-es/security/business/security-101/what-is-data-loss-prevention-dlp?msockid=3a1a85dca3d362083d449139a27c63ac.

[23] fortinet, «www.fortinet.com,» [En línea]. Available: https://www.fortinet.com/lat/resources/cyberglossary/dlp.

[24] govtechreview, «www.govtechreview.com.au,» [En línea]. Available: https://www.govtechreview.com.au/content/gov-cloud/news/aws-microsoft-have-56-of-cloud-services-market-finbold-767150963.

[25] statista, «https://www.statista.com,» [En línea]. Available: https://www.statista.com/statistics/967365/worldwide-cloud-infrastructure-services-market-share-vendor/.

[26] AWS, «aws.amazon.com,» [En línea]. Available: https://aws.amazon.com/es/about-aws/global-infrastructure/regions_az/.

[27] AWS, «aws.amazon.com,» [En línea]. Available: https://aws.amazon.com/es/what-is-aws/.

[28] D. Guardian, «What is AWS Security? Retrieved from,» 2023. [En línea]. Available: https://www.digitalguardian.com/blog/what-aws-security.

[29] ScalaHosting, «What is AWS Cloud Security? How Does it Work?,» 2023. [En línea]. Available: https://www.scalahosting.com/blog/what-is-aws-cloud-security-how-does-it-work/.

[30] Netskope, «www.netskope.com,» [En línea]. Available: https://www.netskope.com/es/security-defined/security-service-edge-sse.

[31] catonetworks, «https://www.catonetworks.com,» [En línea]. Available: https://www.catonetworks.com/es/security-service-edge/.

[32] checkpoint, «www.checkpoint.com,» [En línea]. Available: https://www.checkpoint.com/es/cyber-hub/network-security/what-is-secure-access-service-edge-sase/what-is-security-service-edge-sse/.

[33] goguardian, «www.goguardian.com,» [En línea]. Available: https://www.goguardian.com/glossary/what-is-content-filtering.

[34] CISCO, «https://www.cisco.com/,» 2023. [En línea]. Available: https://www.cisco.com/site/us/en/products/security/secure-web-appliance/index.html.

[35] checkpoint, «www.checkpoint.com,» [En línea]. Available: https://www.checkpoint.com/es/cyber-hub/threat-prevention/what-is-web-filtering/.

[36] Elastics, «www.elastic.co,» [En línea]. Available: https://www.elastic.co/es/what-is/zero-trust.

[37] Netskope, «www.netskope.com,» [En línea]. Available: https://www.netskope.com/es/security-defined/what-is-zero-trust-network-access.

[38] Cloudflare, «www.cloudflare.com,» [En línea]. Available: https://www.cloudflare.com/es-es/learning/access-management/what-is-ztna/.

[39] P. A. Networks. [En línea]. Available: https://www.paloaltonetworks.es/cyberpedia/what-is-zero-trust-network-access-ztna.

[40] www.asana.com, «asana,» [En línea]. Available: https://asana.com/es/resources/proof-of-concept.

[41] secureframe, «secureframe.com,» [En línea]. Available: https://secureframe.com/es-es/blog/cloud-security-statistics1.

[42] cloudsecurityalliance, «https://cloudsecurityalliance.org,» [En línea]. Available: https://cloudsecurityalliance.org/blog/2020/10/14/aws-cloud-security-report-2020-for-management-managing-the-rapid-shift-to-cloud.

[43] A. &. S. B. Jones, «Security Service Edge: A New Approach to Cloud Security,» de *Journal of Cloud Computing and Security*, 2021, pp. 12(3), 45-67.

[44] R. &. K. P. Sharma, «Comparative Analysis of Security Architectures: SASE and SSE in AWS Environments,» de *International Journal of Cybersecurity and Cloud Computing*, 2022, pp. 5(2), 123-139.

[45] S. &. G. R. Kumar, «Review of Security Architectures for Cloud Services: Focus on SSE Integration,» de *Cloud Security Review*, 2023, pp. 8(1), 78-95..

[46] catonetworks, «www.catonetworks.com,» [En línea]. Available: https://www.catonetworks.com/es/security-service-edge/.

[47] Intervision, «intervision.com,» [En línea]. Available: https://intervision.com/blog-sse-ztna-swg-casb-fwaas/.

[48] Datacenterdynamics, «www.datacenterdynamics.com,» [En línea]. Available: https://www.datacenterdynamics.com/es/noticias/c%C3%B3mo-garantiza-la-seguridad-de-los-datos-de-su-nube-p%C3%BAblica-amazon-web-services/.

[49] AWS, «aws.amazon.com,» [En línea]. Available: https://aws.amazon.com/es/compliance/shared-responsibility-model/.

[50] Zscaler, «www.zscaler.com,» [En línea]. Available: https://www.zscaler.com/es/resources/ebooks/choosing-sse-solution.pdf#:~:text=SSE%20protege%20y%20conecta%20una%20base%20de%20usuarios,moverse%2C%20reubicarse%20y%20transformarse%20sin%20perder%20el%20control..

[51] AWS, «/aws.amazon.com,» [En línea]. Available: https://aws.amazon.com/es/blogs/aws-spanish/seguridad-para-portales-y-aplicaciones-web-on-premises-con-servicios-de-aws/.

[52] AWS, «aws.amazon.com,» [En línea]. Available: https://aws.amazon.com/es/web-application-security/.

[53] cloudsecurityninja.com, «cloudsecurityninja.com,» [En línea]. Available: https://cloudsecurityninja.com/securing-data-in-the-cloud/.

[54] Netskope, «www.netskope.com,» [En línea]. Available: https://www.netskope.com/security-defined/what-is-zero-trust-network-access.

[55] Fortinet, «www.fortinet.com,» [En línea]. Available: https://www.fortinet.com/lat/products/public-cloud-security/aws.

[56] [En línea]. Available: https://www.datacenterdynamics.com/es/opinion/aws-inteligencia-artificial-en-la-base-de-la-seguridad-cloud/.

[57] Netskope, «www.netskope.com,» [En línea]. Available: https://www.netskope.com/resources/case-studies/ascensus.

[58] Ascensus, «www.ascensus.com,» [En línea]. Available: https://www.ascensus.com/.

[59] Netskope, «www.netskope.com,» [En línea]. Available: https://www.netskope.com/resources/case-studies/ris-raiffeisen-information-service.

[60] R. B. International, «www.rbinternational.com,» [En línea]. Available: https://www.rbinternational.com/en/raiffeisen.html.

[61] D. A. Cordova Urbina, S. H. Diaz Sifuentes y A. C. Mendoza de los Santos, «Universidad Privada de Tacna,» 28 11 2025. [En línea]. Available: https://revistas.upt.edu.pe/ojs/index.php/ingenieria/article/view/1342.

[62] S. L. Forero Macabares, «UniPiloto,» 13 09 2024. [En línea]. Available: https://repository.unipiloto.edu.co/handle/20.500.12277/14050.

[63] V. J. Pinargote Bravo, «Innova Science Journal,» 31 01 2025. [En línea]. Available: https://doi.org/10.63618/omd/isj/v3/n1/5.

[64] A. F. Gil Villa, S. A. Espinoza Dávalos y A. C. Mendoza de los Santos, «Universidad Privada de Tacna,» 21 11 2025. [En línea]. Available: https://revistas.upt.edu.pe/ojs/index.php/ingenieria/article/view/1331.

[65] W. Rashid, «National College of Ireland,» 12 12 2024. [En línea]. Available: https://norma.ncirl.ie/8250/.

[66] Netskope, «www.netskope.com,» [En línea]. Available: https://www.netskope.com/customers/care-ratings-case-study.

[67] elpais, «https://elpais.com,» [En línea]. Available: https://elpais.com/america-colombia/2023-09-14/hackeo-masivo-en-colombia-la-informacion-de-millones-de-personas-esta-en-manos-de-delincuentes-en-este-momento.html.

[68] mineryreport, «https://mineryreport.com,» [En línea]. Available: https://mineryreport.com/blog/hackeo-masivo-colombia/.

[69] linktic, «linktic.com,» [En línea]. Available: https://linktic.com/blog/panorama-completo-de-la-ciberseguridad-en-colombia/.

[70] ccce, «https://www.ccce.org.co,» [En línea]. Available: https://www.ccce.org.co/noticias/conozca-los-principales-desafios-de-seguridad-digital-que-tiene-colombia-para-el-2024/.

[71] QMA. [En línea]. Available: https://qma.mx/filtrado-contenido-web-2/.

[72] NIST. [En línea]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

[73] nist, «csrc.nist.gov,» [En línea]. Available: https://csrc.nist.gov/pubs/sp/800/30/r1/final.

[74] mitre, «https://attack.mitre.org/,» [En línea]. Available: https://attack.mitre.org/.

[75] Verizon, «www.verizon.com,» [En línea]. Available: https://www.verizon.com/business/resources/reports/dbir/.

[76] sentinelone, «www.sentinelone.com,» [En línea]. Available: https://www.sentinelone.com/cybersecurity-101/cloud-security/cloud-security-statistics/.

[77] enteldigital, https://enteldigital.cl/, https://enteldigital.cl/hubfs/ebooks/ciberseguridad/2025/Entel_Digital_Reporte_Ciberseguridad_2025_.pdf.

[78] IBM, «www.ibm.com,» [En línea]. Available: https://www.ibm.com/es-es/reports/data-breach.

[79] opswat, «www.opswat.com,» [En línea]. Available: https://www.opswat.com/blog/top-cloud-security-issues-risks-threats-and-challenges.

[80] attack.mitre, «attack.mitre.org,» [En línea]. Available: https://attack.mitre.org/matrices/enterprise/cloud/.

[81] owasp, «https://owasp.org,» [En línea]. Available: https://owasp.org/www-project-cloud-native-application-security-top-10/.

[82] cloudsecurityalliance, «www.cloudsecurityalliance.org,» [En línea]. Available: https://cloudsecurityalliance.org/research/topics/top-threats#.

[83] kaspersky, «www.kaspersky.es/,» [En línea]. Available: https://www.kaspersky.es/resource-center/preemptive-safety/cloud-security-issues-challenges?srsltid=AfmBOooBGyMUsAA6q68YbT8QCGiR_p-ProeM9OQenvHnmzD_o8_WgAuz.

[84] verizon, «www.verizon.com,» [En línea]. Available: https://www.verizon.com/business/resources/reports/dbir/?msockid=3fee3f4f84d7679a1d802ad185786691.

[85] dtexsystems, «www2.dtexsystems.com,» [En línea]. Available: https://www2.dtexsystems.com/insiderriskreport2024?&utm_campaign=2024%20IRIR&utm_medium=Paid%20Search&utm_source=Bing&Latest_Campaign=701Ql00000BnO1N&Latest_Campaign_Status=Convertedhttps://www.dtexsystems.com/resource-insider-risk-investigations-report-2.

[86] thales, «cpl.thalesgroup.com,» [En línea]. Available: https://cpl.thalesgroup.com/cloud-security-research.

[87] G. Caruso, «https://neverofftechnology.com/,» [En línea]. Available: https://neverofftechnology.com/blog/amenazas-internas-quien-se-infiltra-maliciosamente-y-como-gestionar-estos-incidentes-en-la-empresa.

[88] phish.report, «phish.report,» [En línea]. Available: https://phish.report/analysis.

[89] CSA, «cloudsecurityalliance.org,» [En línea]. Available: https://cloudsecurityalliance.org/press-releases/2025/02/27/csa-report-examines-how-organizations-assess-and-manage-cybersecurity-and-data-risks.

[90] owasp, «https://owasp.org,» [En línea]. Available: https://owasp.org/Top10/A02_2021-Cryptographic_Failures/.

[91] censys, «censys.com,» [En línea]. Available: https://censys.com/the-2024-state-of-the-internet-report/.

[92] apwg, «apwg.org,» [En línea]. Available: https://apwg.org/trendsreports/.

[93] Powerdmarc, «https://powerdmarc.com/,» [En línea]. Available: https://powerdmarc.com/es/email-phishing-dmarc-statistics/.

[94] cloudflare, «https://radar.cloudflare.com,» [En línea]. Available: https://radar.cloudflare.com/reports/ddos-2024-q4.

[95] preyproject, «preyproject.com,» [En línea]. Available: https://preyproject.com/es/blog/estadisticas-y-tendencia-dark-web.

[96] desklib, «https://desklib.com,» [En línea]. Available: https://desklib.com/study-documents/ddos-attack-case-study/.

[97] Zscaler, «www.zscaler.com,» [En línea]. Available: https://www.zscaler.com/es/resources/security-terms-glossary/what-is-security-service-edge-sse?utm_source=chatgpt.com.

[98] Zscaler, «www.zscaler.com,» [En línea]. Available: https://www.zscaler.com/resources/security-terms-glossary/what-is-sase.

[99] www.microsoft.com, «learn.microsoft.com,» [En línea]. Available: https://learn.microsoft.com/en-us/azure/web-application-firewall/.

[100] microsoft, «www.microsoft.com,» [En línea]. Available: https://learn.microsoft.com/en-us/security/zero-trust/.

[101] microsoft., «www.microsoft.com,» [En línea]. Available: https://learn.microsoft.com/en-us/azure/defender-for-cloud/.

[102] Google, «cloud.google.com,» [En línea]. Available: https://cloud.google.com/armor/docs?hl=es-419.

[103] Google, «Google,» [En línea]. Available: https://cloud.google.com/blog/products/identity-security/introducing-the-unified-chronicle-security-operations-platform.

[104] Google, «google,» [En línea]. Available: https://cloud.google.com/beyondcorp?hl=es_419.

[105] Google, «Cloud Google,» [En línea]. Available: https://cloud.google.com/iap/docs/concepts-overview?hl=es-419.

[106] AWS, «Amazon,» [En línea]. Available: https://aws.amazon.com/es/network-firewall/.

[107] AWS, «www.aws.com.co,» [En línea]. Available: https://docs.aws.amazon.com/whitepapers/latest/building-scalable-secure-multi-vpc-network-infrastructure/private-nat-gateway.html.

[108] AWS, «www.aws.com.co,» [En línea]. Available: https://docs.aws.amazon.com/es_es/Route53/latest/DeveloperGuide/resolver-dns-firewall-overview.html.

[109] AWS, «https://aws.amazon.com,» [En línea]. Available: https://aws.amazon.com/es/macie/?.

[110] AWS, «https://www.amazonaws.cn,» [En línea]. Available: https://www.amazonaws.cn/en/documentation-overview/guardduty/?.

[111] AWS, «Amazon,» [En línea]. Available: https://aws.amazon.com/es/iam/.

[112] AWS, «www.aws.com,» [En línea]. Available: https://docs.aws.amazon.com/es_es/detective/latest/userguide/what-is-detective.html.

[113] AWS, «www.aws.com,» [En línea]. Available: https://docs.aws.amazon.com/es_es/controltower/latest/userguide/what-is-control-tower.html.

[114] AWS, «Amazon,» [En línea]. Available: https://docs.aws.amazon.com/vpc/latest/privatelink/what-is-privatelink.html.

[115] Aws, «Amazon,» [En línea]. Available: https://aws.amazon.com/what-is/sso/.

[116] AWS, «https://aws.amazon.com,» [En línea]. Available: https://aws.amazon.com/es/iam/access-analyzer/?.

[117] AWS, «https://aws.amazon.com,» [En línea]. Available: https://aws.amazon.com/es/documentation-overview/config/?.

[118] AWS, «https://aws.amazon.com,» [En línea]. Available: https://aws.amazon.com/es/security-hub/?.

[119] AWS, «www.aws.com,» [En línea]. Available: https://aws.amazon.com/es/network-firewall/.

[120] AWS, «WWW.AWS.COM,» [En línea]. Available: https://docs.aws.amazon.com/es_es/vpc/latest/userguide/network-firewall.html.

[121] AWS, «WWW.AWS.COM,» [En línea]. Available: https://docs.aws.amazon.com/es_es/Route53/latest/DeveloperGuide/resolver-dns-firewall-overview.html.

[122] AWS, www.aws.com, https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html.

[123] AWS, «www.aws.com,» [En línea]. Available: https://aws.amazon.com/es/blogs/networking-and-content-delivery/introducing-amazon-vpc-flow-logs-kinesis-data-firehose/.

[124] Amazon, «https://docs.aws.amazon.com,» [En línea]. Available: https://docs.aws.amazon.com/es_es/eventbridge/latest/userguide/eb-what-is.html.

[125] AWS, «www.aws.com,» [En línea]. Available: https://docs.aws.amazon.com/es_es/guardduty/latest/ug/what-is-guardduty.html.

[126] AWS, «www.aws.com,» [En línea]. Available: https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html.

[127] AWS, «www.aws.com,» [En línea]. Available: https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-points-policies.html.

[128] AWS, «docs.aws.amazon.com,» [En línea]. Available: https://docs.aws.amazon.com/es_es/artifact/latest/ug/what-is-aws-artifact.html.

[129] AWS, «AWS,» [En línea]. Available: https://docs.aws.amazon.com/es_es/audit-manager/latest/userguide/what-is.html#:~:text=nota,a%20los%20expertos%20en%20cumplimiento..

[130] squid, «https://www.squid.org,» [En línea]. Available: https://www.squid-cache.org/.

[131] opnsense, «www.shop.opnsense.com,» [En línea]. Available: https://shop.opnsense.com/product/opnsense-on-azure/.

[132] Psense, «https://docs.netgate.com,» [En línea]. Available: https://docs.netgate.com/pfsense/en/latest/general/what-is-pfsense.html.

[133] Squic, «squidclamav.darold.net,» [En línea]. Available: https://squidclamav.darold.net/documentation.html.

[134] c-icap, «https://c-icap.sourceforge.net/,» [En línea]. Available: https://c-icap.sourceforge.net/documentation.html.

[135] clamav, «https://www.clamav.net/,» [En línea]. Available: https://docs.clamav.net/.

[136] e2guardian, «http://e2guardian.org,» [En línea]. Available: http://e2guardian.org/cms/index.php.

[137] linux, «https://www.linux.com,» [En línea]. Available: https://www.linux.com/training-tutorials/filter-content-your-home-network-e2guardian/.

[138] AWS, «www.aws.com,» [En línea]. Available: https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html.

[139] AWS, «www.aws.com,» [En línea]. Available: https://aws.amazon.com/es/cognito/.

[140] aws, «www.aws.com,» [En línea]. Available: https://docs.aws.amazon.com/vpc/latest/privatelink/what-is-privatelink.html.

[141] AWS, «www.aws.com,» [En línea]. Available: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html.

[142] AWS, «www.aws.com,» [En línea]. Available: https://docs.aws.amazon.com/guardduty/latest/ug/what-is-guardduty.html.

[143] AWS, «www.aws.com,» [En línea]. Available: https://aws.amazon.com/es/config/.

[144] AWS, «www.aws.com,» [En línea]. Available: https://aws.amazon.com/es/verified-access/.

[145] AWS, «https://docs.aws.amazon.com,» AWS, [En línea]. Available: https://docs.aws.amazon.com/controltower/latest/userguide/what-is-control-tower.html?.

[146] AWS, «https://docs.aws.amazon.com,» AWS, [En línea]. Available: https://docs.aws.amazon.com/wellarchitected/latest/management-and-governance-guide/controls.html?.

[147] Pomerium, «www.pomerium.com,» [En línea]. Available: https://www.pomerium.com/docs.

[148] goteleport, «www.goteleport.com,» [En línea]. Available: https://goteleport.com/docs/.

[149] openziti, «www.openziti.io,» [En línea]. Available: https://openziti.io/docs/learn/introduction/.

[150] ZITADEL, «www.zitadel.com,» [En línea]. Available: https://zitadel.com/docs.

[151] Keycloak, «https://www.keycloak.org,» [En línea]. Available: https://www.keycloak.org/documentation.

[152] oauth2-proxy, «https://oauth2-proxy.github.io,» [En línea]. Available: https://oauth2-proxy.github.io/oauth2-proxy/.

[153] OPA, «https://www.openpolicyagent.org,» [En línea]. Available: https://www.openpolicyagent.org/docs.

[154] Gartner, «www.gartner.es,» [En línea]. Available: https://www.gartner.es/es?utm_source=chatgpt.com.

[155] Gartner, «www.gartner.es,» [En línea]. Available: https://www.gartner.es/es/metodologias/magic-quadrant.

[156] netskope, «https://www.netskope.com,» [En línea]. Available: https://www.netskope.com/resources/analyst-reports/2025-gartner-magic-quadrant-for-sase-platforms.

[157] Forester, «www.forrester.com,» [En línea]. Available: https://www.forrester.com/policies/forrester-wave-methodology/.

[158] F. Wave, «Forrester Wave SASE,» [En línea]. Available: https://reprint.forrester.com/reports/the-forrester-wave-tm-secure-access-service-edge-solutions-q3-2025-2888fb8f/index.html.