Institución Universitaria

Modelo de ciberseguridad aplicado a la infraestructura como servicio IaaS usada en la nube híbrida para pymes, con base en gestión de riesgos.

Andrey Fabian Moncada Garcia

Instituto Tecnológico Metropolitano

Facultad

Ciudad, Colombia

2025

Modelo de ciberseguridad aplicado a la infraestructura como servicio IaaS usada en la nube híbrida para pymes, con base en gestión de riesgos.

Andrey Fabian Moncada Garcia

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

Magister en Seguridad informática

Director (a):

Magister Juan Fernando Hurtado

Instituto Tecnológico Metropolitano

Facultad

Ciudad, Colombia

2025

Dedicatoria

A mis padres, quienes con su amor, esfuerzo y ejemplo han sido la guía en mi camino.

A mi madre, por su inquebrantable fortaleza y comprensión, por enseñarme que los sueños se construyen con disciplina y dedicación.

A mi padre, por su sabiduría y valentía, por demostrarme que la perseverancia es la clave para superar cualquier desafío.

A mi hermano, por su fortaleza y siempre estar en cualquier situación que lo he necesitado.

A mi novia, por su cariño, paciencia y comprensión, por estar a mi lado en cada desafío y por creer en mí incluso cuando yo mismo dudé.

A cada uno de ustedes, gracias por su apoyo incondicional, por ser parte de esta historia y por inspirarme a seguir adelante. Este logro es tan suyo como mío.

Agradecimientos

Este trabajo no hubiera sido posible sin el apoyo, orientación, paciencia y aporte de mi asesor, profesores de las asignaturas y el director de la maestría. A todos ellos, mi más sincero agradecimiento, ya que su guía fue fundamental para llevar este proyecto adelante, adicional le doy un agradecimiento especial a Jonathan Emir, cuyo valioso aporte en la evaluación del modelo fue clave para su desarrollo y validación, su colaboración y disposición fueron fundamentales para alcanzar los objetivos de este estudio.

Resumen

El presente trabajo de grado está orientado al diseño de un modelo de ciberseguridad aplicado a la infraestructura como servicio (IaaS) en entornos de nube híbrida para pymes, basado en la gestión de riesgos y buenas prácticas internacionales, dado el crecimiento en la adopción de servicios en la nube por parte de las pymes, se han generado nuevos desafíos en materia de seguridad, debido a limitaciones presupuestarias, conocimiento y falta de procesos estructurados para la protección de sus infraestructuras. El objetivo principal de este trabajo es proporcionar un modelo que permita reducir la exposición a riesgos en entornos híbridos, asegurando la confidencialidad, integridad y disponibilidad de los activos digitales. El modelo propuesto se fundamenta en estándares reconocidos como ISO/IEC 27001, NIST SP 800-53 y el marco de seguridad de la Cloud Security Alliance (CSA), abordando aspectos clave como la gestión de accesos, la protección de datos y la respuesta a incidentes. El trabajo se desarrolla en varias fases dadas por la caracterización de los servicios IaaS utilizados por pymes, el análisis de estándares de seguridad aplicables, la clasificación de los principales riesgos en la nube híbrida y la evaluación del modelo en un caso de estudio real. La validación del modelo permitió evidenciar su efectividad en la identificación de controles para ayudar a la mitigación de riesgos y su adaptabilidad a diferentes tipos de pymes, se identificaron amenazas críticas como accesos no autorizados, vulnerabilidades en la infraestructura, fuga de datos y ataques de denegación de servicio (DDoS), y se proporcionan lineamientos específicos para su mitigación.

La principal contribución de este trabajo radica en la creación de un modelo práctico y escalable, que proporciona una guía integral para la protección de infraestructuras IaaS, diseñado específicamente para el contexto de las pymes que operan en la nube híbrida, el cual les permitirá evaluar y fortalecer su seguridad mediante un enfoque estructurado de gestión de riesgos, asegurando el cumplimiento de estándares internacionales y reduciendo su vulnerabilidad ante amenazas cibernéticas.

Palabras clave: Buenas prácticas, gestión de riesgos, infraestructura como Servicio (IaaS), modelo, normas internacionales, nube híbrida, pymes.

Abstract

This thesis is focused on designing a cybersecurity model applied to Infrastructure as a Service (IaaS) in hybrid cloud environments for small and medium-sized enterprises (SMEs), based on risk management and international best practices. Given the increasing adoption of cloud services by SMEs, new security challenges have emerged due to budget constraints, lack of knowledge, and the absence of structured processes for protecting their infrastructures. The main objective of this study is to provide a model that reduces risk exposure in hybrid environments while ensuring the confidentiality, integrity, and availability of digital assets. The proposed model is based on recognized standards such as ISO/IEC 27001, NIST SP 800-53, and the Cloud Security Alliance (CSA) security framework, addressing key aspects such as access management, data protection, and incident response. The research is structured into several phases, including the characterization of IaaS services used by SMEs, the analysis of applicable security standards, the classification of major risks in hybrid cloud environments, and the evaluation of the model through a real-world case study. The validation of the model demonstrated its effectiveness in identifying controls to help mitigate risks and its adaptability to different types of SMEs. Critical threats such as unauthorized access, infrastructure vulnerabilities, data breaches, and denial-of-service (DDoS) attacks were identified, and specific guidelines for their mitigation were provided.

The main contribution of this study lies in the creation of a practical and scalable model that offers a comprehensive guide for protecting IaaS infrastructures. It is specifically designed for SMEs operating in hybrid cloud environments, enabling them to assess and strengthen their security through a structured risk management approach, ensuring compliance with international standards, and reducing their vulnerability to cyber threats.

Keywords: Best practices, hybrid cloud, infrastructure as a service (IaaS), international standards, model, risk management, small and medium-sized enterprises (SMEs).

Contenido

Lista de figuras

Pág.

Lista de tablas

Pág.

Lista de Símbolos y abreviaturas

Abreviaturas

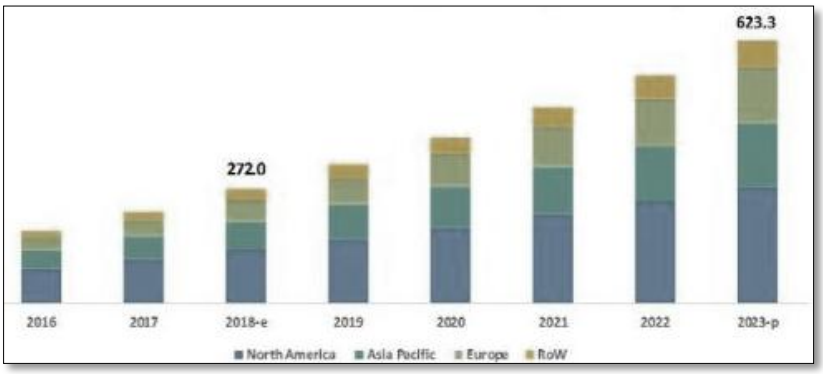
Abreviatura	Término
ALB	Application load balancer
API	Application programming interface
AWS	Amazon Web Services
CC	cumple completamente
CRM	Customer relationship management
CP	Cumple parcialmente
CSP	Cloud service provider
CSA	Cloud security alliance
DBaaS	Database as a Service
DDoS	Distributed denial of service
DLP	Data loss prevention
DNS	Domain name system
DRP	Disaster Recovery Plan
EC2	Elastic compute cloud
ELB	Elastic load balancer
ERP	Enterprise resource planning
GCP	Google cloud plataform
IaaS	Infrastructure as a service
IaC	Infrastructure as code
IAM	Identity and access management
IEC	International electrotechnical commission
IPS	Intrusion prevention system
ISO	International organization for standardization
KMS	Key management service
MFA	Multi-factor authentication
NA	No aplica
NC	No cumple

Introducción

El crecimiento de los servicios alojados en la nube está aumentando de manera exponencial, y dadas las circunstancias actuales donde el modelo de estudio, de trabajo y en general del estilo de vida han cambiado a un entorno virtual, está promoviendo que el crecimiento sea aún más acelerado, adicional el tener los servicios alojados en la nube brindan la oportunidad de reducir los costos de mantenimiento de infraestructura propia; así mismo los ataques a los entornos de nube han ido en crecimiento, toda vez que son servicios que están expuestos en internet, resguardados en infraestructura de terceros que pueden ser alcanzados con más facilidad [1]. En ese sentido, los servicios de IaaS en la nube híbrida tiene diferentes funciones de seguridad que un usuario u organización puede utilizar para mantener la confidencialidad, integridad y disponibilidad de la información, pero no son lo suficientemente óptimos cuando se busca hacer todo un proceso de detección, análisis y mejora del esquema de seguridad, dado que diferentes parámetros dependen del proveedor y las organizaciones carecen de modelos de seguridad en el entorno local, adicional los modelos de seguridad aplicados a la nube híbrida existentes, son individuales o para una plataforma específica y no se ajusta a la necesidad de una pyme.

La evolución tecnológica avanza de manera acelerada, y para las empresas es crucial mantenerse a la vanguardia para garantizar su sostenibilidad y competitividad en el mercado. En este contexto, la adopción de servicios en la nube ha experimentado un crecimiento exponencial, consolidándose como un pilar fundamental en la transformación digital de las organizaciones. De acuerdo con Datacenter Dynamics, se estima que el gasto global de los usuarios finales en servicios de nube pública alcanzará los 723.400 millones de dólares en 2025, lo que refleja un incremento significativo desde los 595.700 millones de dólares estimados para 2024 [2]. Así mismo, el mercado de la nube híbrida sigue expandiéndose a gran velocidad, con una tasa de crecimiento anual compuesta del 21,91 %, proyectándose que alcanzará un valor de 348.530 millones de dólares en 2028, en comparación con los 129.430 millones de dólares registrados en 2023 [3]. Estas cifras evidencian cómo la migración a entornos híbridos se ha convertido en una tendencia clave para las empresas que buscan optimizar costos y mejorar la eficiencia operativa a través de la flexibilidad que brinda la computación en la nube.

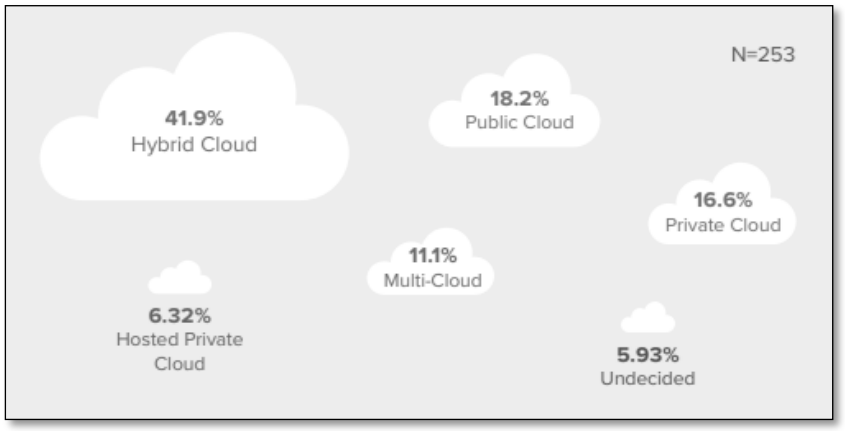
Figura 1: Gastos en recursos de nube pública por región (billones de dólares)



Nota. Esta figura representa el crecimiento del gasto en el uso de servicios de nube. Fuente: [4]**.**

Por otro lado, en la figura 1, se muestra un gráfico de barras apiladas que representa el crecimiento del gasto en servicios de nube pública por región desde 2016 hasta 2023, lo cual respalda la afirmación de que el mercado de la computación en la nube ha venido creciendo significativamente. En una encuesta realizada por la empresa Denodo, la cual realizó un sondeo sobre el estado de la adopción de la nube para algo más de 250 organizaciones en la que participaron usuarios de diversos orígenes, roles y regiones, se logra apreciar que las arquitecturas híbridas y Multi-Cloud se han convertido en los estándar de mayor implementación, con más de la mitad (53%) siendo la forma más común de despliegue, adicional en la figura 2 se aprecia con más detalle las estadísticas de los diferentes tipos infraestructuras usadas por las organizaciones evaluadas, en la cual la nube híbrida constituye el despliegue mayoritario (42%); seguido de las nubes públicas (18%) y privadas (17%), por otro lado según los encuestados, las ventajas de las configuraciones de nube híbrida y Multi-Cloud incluyen la capacidad para diversificar su gasto, sus capacidades, potenciar su resiliencia y elegir características dependiendo de las fortalezas particulares de cada proveedor de servicio en la nube, además evitar indisponibilidad del servicio por bloqueo del proveedor [4].

Figura 2. Estadísticas de adopción de la nube

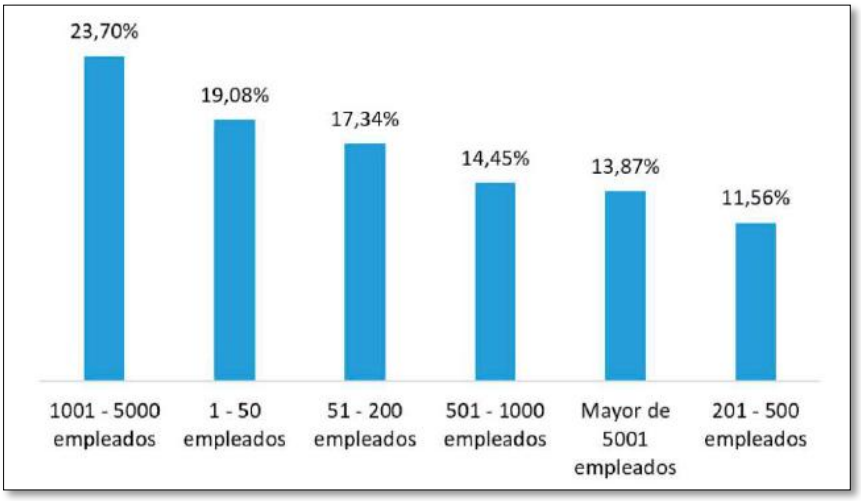


Nota. Esta figura representa las estadísticas de adopción en cuanto al tipo de nube de acuerdo a una encuesta. Fuente: [4]**.**

En los últimos años, América Latina ha experimentado un aumento significativo en los ciberataques. Según un informe de Fortinet, en 2023 se registraron aproximadamente 200.000 millones de intentos de ciberataques en la región, lo cual representa el 14,5% del total global. México fue el país más afectado, con 94.000 millones de intentos, seguido de Brasil y Colombia [5]. Este incremento se atribuye, a la creciente migración de datos hacia plataformas en la nube, lo que las convierte en objetivos atractivos para los ciberdelincuentes. Además, la adopción acelerada de tecnologías en la nube, a veces sin una implementación adecuada de medidas de seguridad, ha expuesto vulnerabilidades que pueden ser explotadas [6].

Asimismo, según el estudio realizado por la revista Resiliencia digital de la asociación Colombiana de Ingenieros de Sistemas (ACIS), da a conocer los datos sobre una encuesta realizada entre abril y junio del 2021, acerca del estado de la seguridad informática en las empresas Colombianas, en esta se contó con la participación de 173 empresas encuestadas, de diferentes tamaños y sectores económicos, como se observa en la figura 3, en la cual se muestra el promedio de empleados de las empresas encuestadas, y se puede analizar que el 47.98% tienen menos de 500 empleados, y se constituyen como empresa tipo pyme, que para la proyecto actual es el foco de investigación [7].

Figura 3. Tamaño de las empresas según el número de empleados



Nota. Esta figura representa el porcentaje de empresas de acuerdo a la cantidad de empleado. Fuente: [7].

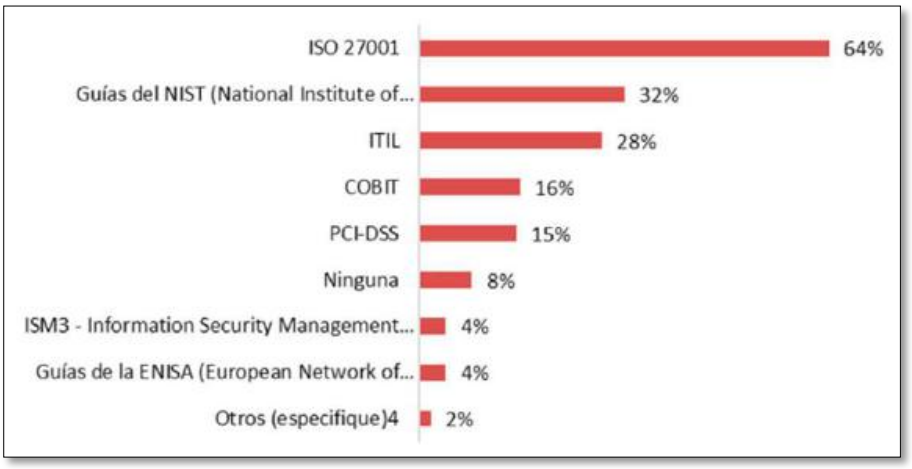
Esta misma encuesta realizó un análisis sobre las razones para no realizar una evaluación de riesgos en las empresas, y como se ve en la figura 4, el 58% es por falta de no contar con una buena documentación con unos modelos bien definidos que permitan realizar esta evaluación.

Figura 4. Motivo para no realizar evaluación de riesgos

Nota. Esta figura representa en porcentajes los motivos por los cuales no realizan evaluación de riesgo según los encuestados. Fuente: [7]

Otro análisis interesante se da con la encuesta sobre los estándares y buenas prácticas de seguridad que usan las empresas encuestadas, y se observa según la figura 5, que el 8% no aplica ninguno, y la ISO27001 se constituye como la más implementada con un 64%.

Figura 5. Estándares y buenas prácticas de seguridad



Nota. Esta figura representa el porcentaje de implementación para cada uno de los estándares. Fuente: [7].

De acuerdo a la información, datos, y estadísticas presentados en este ítem se logra identificar que el futuro cercano está en la migración de los servicios a la nube, ya que presenta diferentes beneficios para las empresas, pero esta evolución trae consigo diferentes retos a nivel de seguridad, y si se da una mirada sobre cómo están siendo afrontados hoy en día en las empresas colombianas, se carece de modelos de ciberseguridad, ya sea porque no se encuentran bien documentados o porque no se le está dando la importancia que se requiere en las diferentes empresas, de aquí surge la necesidad de tener un modelo de ciberseguridad para la nube híbrida que pueda ser adaptado e implementado para las empresas tipo pyme en sus despliegues de infraestructura como servicio (IaaS), dado que estas empresas representan un gran porcentaje de la economía colombiana; esta investigación busca atacar esta necesidad teniendo como:

Objetivo general

Proponer un modelo de ciberseguridad para la infraestructura como servicio (IaaS) en una nube híbrida, a través de normas o modelos internacionales, que permita la reducción de niveles de exposición a los riesgos e impactos en empresas pymes.

Para lograr el cumplimiento de este objetivo se desarrollaron los siguientes objetivos específicos:

- Caracterizar los servicios IaaS que puede tener una empresa pyme para su nube híbrida.

- Realizar un análisis de los estándares, normas y buenas prácticas de seguridad que se aplican para los servicios en la nube híbrida, para tener unas bases en el modelo de ciberseguridad que se busca implementar.
- Clasificar los principales riesgos que se pueden presentar en la nube híbrida con el fin de establecer un plan de tratamiento, con base en la norma ISO27005.
- Aplicar el modelo de ciberseguridad a la nube híbrida que permita la reducción de niveles de exposición en empresas pymes, mediante una simulación o estudio de caso.

1. Marco Teórico y Estado del Arte

1.1 Marco teórico

Para el desarrollo de esta investigación es de gran importancia tener claro los diferentes conceptos que se van a tratar, por eso a continuación se presenta las explicaciones, y características de cada uno de estos conceptos.

1.1.1 Modelo de ciberseguridad

Un modelo de ciberseguridad es un marco estructurado que permite a una organización identificar riesgos, anticipar amenazas, prevenir incidentes mediante controles proactivos, resistir ataques o fallas, detectar comportamientos anómalos, recuperarse de incidentes de manera rápida y efectiva, y adaptarse a nuevas condiciones para fortalecer continuamente su postura de seguridad. A diferencia del enfoque tradicional de la seguridad de la información el cual se centra únicamente en la protección y aseguramiento, el concepto moderno de ciberseguridad, conforme al NIST Cybersecurity Framework, el NIST SP 800-160 y el Ministerio TIC de Colombia, incorpora prácticas de defensa activa, anticipación de amenazas, prevención estratégica y ciberresiliencia organizacional. Estos modelos deben estar dirigidos a identificar los niveles de riesgo presentes y las acciones que se deben implementar para reducirlos [8], [9], [10].

1.1.2 Riesgo vs Ciberriesgo

El riesgo, en términos generales, se refiere a la probabilidad de que un evento ocurra y cause un impacto negativo en los objetivos de una organización. En el contexto de la seguridad de la información, este se relaciona con la pérdida de confidencialidad, integridad o disponibilidad de los activos.

Por su parte, el ciberriesgo es una categoría específica de riesgo que se refiere a la posibilidad de que una amenaza explote una vulnerabilidad en un sistema digital como redes, plataformas en la nube, o infraestructuras tecnológicas, y provoquen un daño a los activos de información, a la operación o incluso a la reputación de la organización. A diferencia del riesgo tradicional, el ciberriesgo está asociado al entorno digital y suele evolucionar rápidamente debido a cambios tecnológicos, nuevas amenazas y vulnerabilidades emergentes.

De acuerdo con la norma ISO/IEC 27005:2022 y el enfoque del NIST Risk Management Framework, una adecuada gestión del ciberriesgo debe considerar las relaciones entre activos, amenazas, vulnerabilidades, impactos y probabilidades, en entornos tan dinámicos como la nube híbrida. En

el caso de las pymes, entender esta distinción es clave para implementar controles proporcionales a los riesgos cibernéticos reales que enfrentan sus infraestructuras IaaS [11].

1.1.3 Gestión del riesgo

La gestión del riesgo consiste en el análisis y la evaluación del riesgo lo cual busca describir cuantitativamente o cualitativamente los riesgos, para facilitar la gestión de la seguridad de la información mediante la implementación efectiva de controles y toma de decisiones. El análisis y la evaluación del riesgo contempla tres actividades, la primera es identificar los riesgos, en el cual se colecta información con el fin de identificar posibles escenarios que puedan causar impacto negativo en la organización; la segunda actividad es la estimación del nivel de riesgo, aquí se calcula el riesgo de acuerdo al impacto versus la probabilidad de ocurrencia; por último se tiene la actividad de evaluación del riesgo, proceso en el cual se revisan los controles existentes además se identifican, estiman y evalúan los activos, las amenazas y las vulnerabilidades existentes, para así poder determinar el nivel de importancia con el que deben ser implementados los controles, buscando minimizar los riesgos [12].

Adicional para este proceso es esencial definir el apetito de riesgo, entendido como el nivel y tipo de riesgo que una organización está dispuesta a aceptar en la consecución de sus objetivos. Esta declaración del apetito, ya sea cualitativa (por ejemplo, “aceptamos un riesgo moderado en proyectos de innovación”) o cuantitativa (como un límite del 5 % en desviación presupuestal) permite ayudar a la organización con la priorización de riesgos dentro de sus parámetros estratégicos[13].

1.1.4 Cloud computing

La Nist define Cloud Computing como “La computación en la nube es un modelo para permitir el acceso ubicuo, conveniente y bajo demanda a un conjunto compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que pueden aprovisionarse y liberarse rápidamente con un mínimo esfuerzo de gestión o Interacción del proveedor de servicios.” [3]. también se pueden identificar los tres modelos básicos de servicios de nube, dados dependiendo del tipo de servicio o capa de servicio que se virtualice en la nube, los cuales son infraestructura, plataforma o software [14].

Cuando se habla de software hace referencia al SaaS que por sus siglas en ingles indica software as a service (software como servicio), es un servicio en el cual el proveedor de la nube brinda tanto el software como el hardware de la aplicación o necesidad de la organización, uno de los usos más comunes en este tipo de servicios es el correo electrónico. Los servicios tipo SaaS permiten además libera al usuario final de hacer mantenimiento y actualizaciones periódicas del software [15].

Por otro lado, se tiene la plataforma como servicio, abreviada como PaaS (plataforma as a service), este servicio hace referencia a el uso de infraestructura informática remota para el desarrollo, las prueba y el uso de las aplicaciones, lo cual quiere decir que los usuarios u organizaciones pueden desplegar sus aplicaciones en la infraestructura de un CSP (cloud service provider) y no se tendrán que preocupar infraestructura, sistemas operativos o aprovisionamiento de recursos [14].

Otro de los servicios es el de infraestructura como servicio, conocida como IaaS, en el cual los usuarios pueden hacer uso de las capacidades para desplegar recursos de procesamiento, almacenamiento y redes virtuales, todo esto en la infraestructura del proveedor de servicios de nube, en estos servicios el cliente establece las características

de necesita configurar de acuerdo a sus necesidades, como por ejemplo definir la capacidad y cantidad de procesadores, el tamaño de la memoria, el tipo de sistema operativo, las reglas de seguridad de la red, entre otros. Por otro lado, los CSP permiten a sus clientes visualizar los servicios de forma similar a como son vistos en infraestructuras en tierra. Algunos de los servicios que actualmente existen en el mercado y hacen uso de IaaS son los servicios de computación (Compute Service), Servicios de almacenamiento (Storage Service) y Servicios de copia de seguridad (Backup Service) [14].

1.1.3.1. Modelos de despliegue de cloud computing

Existe una clasificación de los tipos de nubes, relacionada con la propiedad, la cobertura y el acceso a los servicios, la cual esta clasificación así:

- **Nube Pública**

Una nube pública es un servicio administrado por un CSP dueño de una infraestructura tecnológica importante y muy sofisticada, el cual los clientes utilizan para desplegar sus servicios, y puede tener varios clientes haciendo uso de su infraestructura, sin embargo, los distintos clientes no tienen la posibilidad de saber si otro cliente está haciendo uso de los mismos servicios, tampoco se puede acceder física o lógicamente a los ficheros de los servicios desplegados por otros clientes. Uno de los mayores beneficios de la nube pública está dados por la facilidad, rapidez y menores costos en el momento de configurar y administrar, ofreciendo a sus clientes una gran cantidad de métodos para escalar y flexibilizar sus recursos de acuerdo a sus requerimientos [16].

- **Nube Privada**

Hace referencia a una infraestructura de nube dedicada, que es proporcionada por un proveedor de servicios en la nube (CSP) para un único cliente. La empresa que contrata el servicio es dueña de su nube, y es quien decide sobre las políticas y procedimientos de administración y seguridad que se pueden aplicar en ella. En este modelo de computación en la nube, el CSP solo proporciona los servicios de nube y alojamiento mediante una conexión privada entre sus servicios y el cliente. la nube privada permite que su cliente tenga más control y pueda personalizar los servicios para suplir sus requerimientos [16].

- **Nube Híbrida**

La nube híbrida es un modelo de despliegue que utiliza una combinación de varias nubes, nube privada y nube pública, dos nubes privadas o dos nubes públicas, las cuales son independientes entre sí, este tipo de servicios le da la posibilidad a sus clientes de compartir datos, aplicaciones, y servicios entre las distintas nubes, a su vez este tipo de despliegues permite que sus clientes hagan uso de los mejores beneficios de cada una de las nubes y utilizarlos para crear un servicio más adaptado a sus necesidades, sin depender solo de los parámetros o infraestructura disponibles en un proveedor de nube, adicional este tipo de modelos garantiza una mayor disponibilidad, ya que el cliente tiene sus servicios desplegados en diferentes nubes, y dado el caso que una falle puede contar con el respaldo de la otra [17].

1.1.5 Seguridad de la información

La seguridad de la información, está basada en políticas, normas internas y externas de una organización, se encarga de proteger la confidencialidad, la integridad y la privacidad de la información que se encuentra almacenada en un sistema informático, contra cualquier tipo de amenazas, reduciendo los riesgos tanto físicos como lógicos, a los que se encuentra expuesta dicha información. Los principios fundamentales en la seguridad de la información son la Integridad, disponibilidad y confidencialidad, el primero busca que la información que se recibe sea precisa y esté completa (su contenido es el necesario) para los fines que sea requerida, así como con su validez, de acuerdo con los valores y las expectativas de la organización. La disponibilidad hace referencia a que la información requerida para realizar cualquier proceso, se encuentre siempre al alcance y pueda ser utilizada en el momento que sea necesitada en los procesos de la organización. Finalmente, la confidencialidad se refiere a que, en todas las etapas del procesamiento de la información, ésta se encuentre protegida contra accesos no autorizados, los cuales pueden llevar a una alteración o robo de información confidencial [18].

1.2 Estado del arte

Se presentan diferentes investigaciones desde el campo internacional y nacional relacionadas con el problema de investigación, modelo de ciberseguridad aplicado a la nube, con base en gestión de riesgos y el manejo de incidentes de seguridad.

Una de las investigaciones relacionadas es, Aspectos de seguridad informática en la utilización de cloud computing, la cual se enfoca en la identificación de las principales amenazas y vulnerabilidades a las cuales se está expuesto cuando se utiliza Cloud Computing, además de plantear estrategias y recomendaciones de seguridad para la protección y buen uso de los servicios en la nube [19].

Por otro lado según [9], plantea la investigación recomendaciones de seguridad para los servicios de computación en la nube, a partir de los estándares y modelos de seguridad de la información, en el cual analiza e identifica algunos criterios de seguridad en la computación en la nube, mediante el uso de buenas prácticas y algunos modelos de seguridad de la información para la nube, las conclusiones relevantes del trabajo se dieron de cara a la identificación de criterios y recomendaciones de seguridad que ayuden a las organizaciones para lograr una mayor seguridad en la implementación de la computación en la nube, logrando como resultado del trabajo presentar una guía de adquisición de servicios en la nube para las organizaciones [20].

De igual manera se tiene una propuesta en la que plantean un modelo de evaluación de riesgos de seguridad de la información con base a la ISO/IEC 27005 para determinar la viabilidad de obtener un servicio en la nube, con la cual pudieron dar un punto de vista para entender algunos de los riesgos de seguridad de información que asumen actualmente las organización con los controles de seguridad implementados, y los riesgos que se asumirían con la adquisición de un nuevo servicio en la nube, con el fin de que la organización tenga las bases para tomar una decisión sobre que infraestructura utilizar [21].

Otra de las investigaciones es un trabajo llamado Recomendaciones y Estrategias para la Protección de Datos en la Nube, su principal objetivo fue presentar una tendencia de la manera como la Computación en la Nube se fortalece continuamente en los elementos de seguridad informática

necesario, adicional presentan algunas recomendaciones para que las organizaciones hagan un uso apropiado de los recursos disponible en la nube, con el fin de evitar violaciones que pongan en riesgo el manejo de la información [22].

En la investigación Análisis de los componentes de seguridad informática en la implementación de Cloud Computing en pequeñas y medianas empresas colombianas, se da a conocer algunos de los aspectos de seguridad informática que se deben tener en cuenta en la implementación de Cloud Computing en una pequeña o mediana empresa colombiana, teniendo en cuenta aspectos técnicos, regulatorios y riesgos que existen para el Cloud Computing [23].

De acuerdo con el proyecto llamado “Construcción de un modelo de ciberseguridad para empresas de servicios informáticos que fortalezca un adecuado manejo de incidentes de seguridad”, se propone un modelo de ciberseguridad basado en el análisis de riesgos, con el objetivo de fortalecer la gestión de incidentes de seguridad en empresas de servicios informáticos. Con este modelo se busca mejorar la capacidad de respuesta y resiliencia ante amenazas cibernéticas [24].

Por otro lado, se presenta un Análisis sistémico de riesgos y vulnerabilidades en entornos multi-nube, el cual analiza vectores de ataque en entornos multi-nube, aplicando métodos de modelado de amenazas como STRIDE y DREAD. Se identifican y priorizan amenazas en áreas como arquitectura de la nube, APIs y autenticación, proponiendo estrategias de mitigación [25].

Nota: Para más detalle de los proyectos mencionados, referente a su trabajo, contribución, vacíos y proyecto propuesto, se puede revisar el anexo A.

De acuerdo con las investigaciones anteriormente planteadas, se evidencia que diversos autores han abordado el crecimiento acelerado de los servicios en la nube y la creciente necesidad de establecer mecanismos de seguridad robustos que permitan a las organizaciones reducir los niveles de exposición ante amenazas y vulnerabilidades en estos entornos. La revisión de estas investigaciones muestra que, si bien existen propuestas enfocadas en la gestión de riesgos, la seguridad en la nube y el manejo de incidentes, la mayoría de ellas se centran en aspectos generales

de seguridad, modelos de madurez o estrategias de mitigación de riesgos, sin ofrecer una solución específica y aplicable a Infraestructura como Servicio en entornos de nube híbrida.

Dicho análisis permite identificar la brecha existente en el desarrollo de un modelo integral que no solo considere la identificación y evaluación de riesgos, sino que además ofrezca un enfoque estructurado para la implementación de controles de seguridad en Pymes que utilizan IaaS. A diferencia de los estudios revisados, que abordan la seguridad en la nube desde perspectivas más amplias o centradas en sectores específicos como entidades públicas o grandes empresas, el presente trabajo busca diseñar un modelo de ciberseguridad que sea práctico, escalable y alineado con las necesidades particulares de las pequeñas y medianas empresas en un entorno de nube híbrida.

Por lo tanto, aunque estas investigaciones proporcionan fundamentos clave en términos de gestión de riesgos, metodologías de evaluación y estrategias de mitigación, ninguna ha desarrollado un modelo de ciberseguridad específico para IaaS en la nube híbrida. Esto resalta la relevancia y necesidad de la presente investigación, cuyo objetivo es llenar este vacío mediante la propuesta de un modelo que no solo optimice la seguridad en estos entornos, sino que también facilite su adopción por parte de las pymes, permitiéndoles operar de manera segura y eficiente en infraestructuras de nube híbrida.

2. Metodología

Este trabajo es de carácter experimentación acción donde se propone un modelo de ciberseguridad para la infraestructura como servicio-IaaS en una nube híbrida el cual se podría aplicar a las empresas del sector pyme, para ello el trabajo de grado se dividió en cuatro fases, cada una hace referencia a un objetivo específico, fase 1, caracterización de servicios IaaS, fase 2, análisis de estándares y normas, fase 3, clasificación de riesgos, fase 4, aplicación del modelo.

En la fase 1, la cual se enfocó en la caracterización de los servicios IaaS, buscado identificar los componentes o servicios que a hoy pueden ser los más comúnmente usados por las pymes y que pueden ser llevados a un servicio tipo IaaS, para esto contemplaron las siguientes actividades:

- Se caracterizan las diferentes nubes con el fin de determinar la nube sobre la cual se evaluarán los servicios tipo IaaS prestados.
- se realiza un estudio sobre la infraestructura básica para la operación de empresas pymes, se logró analizando el estado del arte y estadísticas sobre la infraestructura básica para la operación de este tipo de empresas
- Definición de arquitectura básica para la simulación o caso de estudio
- Posterior a las actividades anteriores se procede a identificar las capacidades disponibles en el proveedor de nube para dicha infraestructura
- Como actividad final se determinan los servicios que se pueden implementar en nube y on-premises.

En la fase 2, se realizará un análisis de los estándares normas y buenas prácticas que se aplican para los servicios IaaS en la nube híbrida, para esto será necesario investigar los estándares y normativas a nivel general que existen para implementación de seguridad, tales como la ISO 27001, NIST, Common Criterial, Cobit, SANS y lo recomendado por los mismos proveedores y que pueden ser aplicadas a la IaaS en una nube híbrida, lo cual se realizará mediante un estudio de la documentación y normativas internacionales existentes, esto permitirá la obtención de las ventajas, desventajas, aplicabilidad y características de los estándares y normas encontrados,

adicional se plantea buscar espacios con expertos que hayan realizado alguna implementación de los servicios de IAAS en la nube híbrida, permitiendo hacer un comparativo entre los estándares encontrados y los aplicados por los expertos, esta revisión dará como resultado una lista de normas y buenas prácticas que pueden ser aplicable a la IAAS de la nube híbrida para las pymes.

Para la fase 3, se plantea clasificar los principales riesgos que se pueden presentar en la nube híbrida, para esto será necesario realizar una búsqueda sobre las principales amenazas a las que se encuentra expuesta este tipo de infraestructura, esta búsqueda se realizará revisando la documentación existente en las páginas que se enfocan en dar a conocer a la comunidad este tipo de problemáticas como la CVE, listas de distribución, sitios de hacking, entre otros, después de tener estos riesgos será necesario hacer su respectiva evaluación acorde a la ISO27005:2018 y así determinar su nivel de impacto, después de realizar esta evaluación se podrá entregar la clasificación de los riesgos evaluados.

Para la fase final, se hará la creación del modelo de ciberseguridad que pueda ser aplicado a la nube híbrida con base en los riesgos encontrados, se evaluará el modelo mediante una simulación o caso de estudio, simulando algunos ataques informáticos (amenazas) e implementando algunos controles, o realizando la validación del modelo y determinando el nivel de cumplimiento que permita establecer la viabilidad del mismo. Así mismo se hará la respectiva documentación de los resultados encontrados con el fin de determinar si el modelo es viable y se puede implementar en la industria. Se hará la construcción de herramientas y/o mecanismos de medición que permitan establecer el nivel de implementación del modelo, estos instrumentos pueden ser, entrevistas, implementaciones técnicas en máquinas virtuales, listas de chequeo, entrevista de expertos, entre otros.

2.1 Caracterización de servicios IaaS para nubes híbridas.

La Infraestructura como Servicio en una nube híbrida combina la flexibilidad y escalabilidad de la nube pública con el control y seguridad de la infraestructura local (on-premises), permitiendo a las pequeñas y medianas empresas optimizar recursos y mejorar su competitividad. Estas infraestructuras ofrecen ventajas claves, como la capacidad de ajustar recursos según la demanda sin necesidad de grandes inversiones en infraestructura física, la optimización de costos al

combinar entornos locales con la nube, pagando únicamente por los recursos utilizados [26]. Por estos motivos toma relevancia para las pymes la elección de una nube pública adecuada, junto con una arquitectura básica que responda a sus necesidades, siendo crucial para optimizar recursos y mejorar su competitividad.

2.1.1 Caracterización de los proveedores de nube

Basados en el estudio realizado por Gartner y analizado por Google Cloud [27], el cual evalúa los proveedores de nube, que prestan servicios IaaS, se puede determinar según la figura 6, que AWS lidera el ranking, seguido por, Google Cloud, y Microsoft, por lo tanto, el estudio es enfocado en los tres primeros proveedores. Esta evaluación Gartner la realiza de acuerdo con unos criterios planteados por ellos y aplicados en las empresas que son sus clientes.

Figura 6. Cuadrante mágico de Gartner.

Nota. Esta figura representa el ranking de proveedores de nube según Gartner. Fuente: [27]

Las características principales, ventas y desventajas de estos proveedores se presentan a continuación:

AMAZON (AWS): Es uno de los proveedores Cloud más conocidos a nivel mundial, ofrece a los usuarios la posibilidad de elegir en que parte del mundo desea desplegar sus servicios. Según Amazon Web Services [28]uno de sus pilares es optimizar los costos en el despliegue de servicios, los costos varían según el tipo de servicio que se va a desplegar, la zona de disponibilidad, y el número de instancias que se deseen iniciar, proporciona también soporte claro para desarrollos en Java, .NET, PHP, NodeJS, Python, Ruby, Go, Docker con servidores como Apache, Nginx, Passenger e IIS, algunas ventajas y desventajas se abordan a continuación [29]:

Ventajas:

- AWS continúa teniendo un liderazgo dominante en muchas de las dimensiones críticas del mercado de CIPS, AWS tiene la mayor participación del mercado mundial en IaaS y ofertas de bases de datos PaaS.
- AWS tiene los recursos que permiten integrar componentes verticalmente y así ofrecer soluciones integrales a los clientes.
- AWS si se emplea de forma correcta permite la reducción de costos, dado que evita la compra de dispositivos físicos, lo cual reduce gastos administrativos, adicional es fácilmente escalable y el costo se genera de acuerdo con lo que se utiliza.

Desventajas:

- AWS tiene una gran variedad de servicios en constante crecimiento, pero algunos con poca integración entre ellos. Su liderazgo en IaaS y PaaS puede generar una percepción errónea de uniformidad en todas sus ofertas. Para aprovechar AWS de manera efectiva, se necesita un conocimiento en desarrollo de aplicaciones, lo que, sumado a algunas complejidades en la integración, puede resultar abrumador para muchas empresas que no cuenten con estas habilidades.
- Los clientes continúan creyendo incorrectamente que AWS reduce los precios en general; sin embargo, las reducciones a menudo no se aplican universalmente en todos los servicios.

Por ejemplo, el almacenamiento aprovisionado con mayor frecuencia para el servicio informático de AWS no ha experimentado una reducción de precio desde 2014, casi la mitad de la vida útil de la empresa, a pesar de la drástica disminución de los precios en el mercado de los componentes sin procesar.

AZURE: Es una propuesta de Microsoft para la Generación de datos en la Nube, "Azure es un conjunto completo y en expansión constante de servicios de informática en la nube que ayudan a su organización a afrontar sus desafíos empresariales". Azure ofrece la flexibilidad de crear, administrar e implementar aplicaciones en una red mundial enorme con las herramientas y las plataformas que prefiera, algunas ventajas y desventajas se abordan a continuación [30]:

Ventajas:

- Microsoft Azure ofrece un conjunto completo de soluciones integrales relacionadas con una amplia gama de cargas de trabajo y aplicaciones. Esto es evidente a partir de las asociaciones de Microsoft Azure con Oracle, SAP y VMware, continúa con las capacidades de Azure con respecto a los contenedores y soluciones atractivas para entornos híbridos.
- Microsoft está haciendo un esfuerzo para servir mejor a los desarrolladores de software, particularmente a través de sus esfuerzos con OSS (Operations Support System). Microsoft lidera a los proveedores de nube de hiperescala en términos de participación de mercado en el segmento de PaaS para desarrolladores de aplicaciones con su conjunto de herramientas que incluyen Azure DevOps y Github, Visual Studio Codespaces, que actualmente se encuentra en versión beta, es el primer entorno atractivo para desarrolladores de aplicaciones alojadas en la nube que une el uso de la nube pública y las herramientas de desarrollo muy populares, como Visual Studio Code.
- Las empresas convencionales a menudo tienen una alineación estratégica con Microsoft, lo que otorga a Azure importantes ventajas de ventas en este segmento del mercado.

Desventajas:

- Microsoft tiene la proporción más baja de zonas de disponibilidad a regiones de cualquier proveedor, adicional solo un conjunto limitado de servicios admite el modelo de zona de disponibilidad.

- Microsoft no proporciona ningún tipo de capacidad garantizada a los clientes; incluso los acuerdos de prepago y las instancias reservadas no son garantías de capacidad. Cuando hubo déficit de capacidad relacionados con el COVID-19 que afectaron a los clientes en varias regiones europeas durante un período de varias semanas, un pequeño número de clientes no pudo proporcionar instancias reservadas o capacidad por la que ya habían pagado.
- El soporte unificado de Microsoft puede ser muy costoso, especialmente para aquellos clientes que históricamente no han tenido servicios de soporte que cubran todo su portafolio de Microsoft. A pesar de que la competencia técnica de ventas de Microsoft ha mejorado durante los últimos años, y Microsoft está mejorando el soporte técnico de Azure, los clientes continúan reportando preocupaciones con la calidad de estas experiencias.

GOOGLE CLOUD: Es un servicio de Computación en la Nube que ofrece una arquitectura multicapa el cual proporciona seguridad en las operaciones y a los dispositivos enlazados a la infraestructura, provee comunicación por Internet cifrada, autenticación de usuarios en varios factores, cifrado de todos los datos que ingresan a la nube, y otros más. Algunas ventajas y desventajas se abordan a continuación [31]:

Ventajas:

- La infraestructura de GCP abarca una red extensa de centros de datos, lo que garantiza una alta disponibilidad y un rendimiento óptimo para aplicaciones a nivel mundial.
- GCP experimentó un aumento notable en la participación de mercado año tras año en términos de IaaS y dbPaaS, aunque más bajo, en relación con otros proveedores. Google también obtuvo ganancias significativas al cerrar una serie de brechas de capacidad críticas entre GCP y Microsoft Azure.
- la compañía está presionando hacia un nuevo territorio con Anthos, el contenedor de GCP y la capa de middleware basada en Kubernetes, que está diseñada para respaldar el desarrollo y la implementación de aplicaciones en la nube en un modelo híbrido y multi-nube.

Desventajas:

- GCP carece de capacidades de PaaS centradas en la empresa y soporte para Oracle, Google continúa luchando por tener una mentalidad empresarial en el campo.
- La estructura de precios de GCP puede ser compleja, lo que plantea desafíos para las empresas al intentar predecir y gestionar con precisión sus gastos en la nube.
- Las capacidades de red de Google han sido la causa de una serie de interrupciones de GCP durante los últimos años, generando un gran impacto en los clientes.

Dadas las características anteriores se definió AWS como nube pública para el análisis en el modelo, debido a su liderazgo en el mercado y se destaca por su gran cantidad de servicios disponibles para desplegar como IaaS, adecuados para las pymes. AWS opera en diferentes regiones del mundo, lo que garantiza una alta disponibilidad y baja latencia, esencial para un entorno hibrido, adicional cuenta con una gran comunidad de usuarios, partners y desarrolladores lo cual facilita la colaboración.

2.1.2 Clasificación de empresas

Según el Índice de Políticas para pymes en América Latina y el Caribe 2024, publicado por la OCDE en cooperación con CAF-Banco de Desarrollo de América Latina y el Caribe, y el Sistema Económico Latinoamericano y del Caribe (SELA), las empresas tipo pymes son un fundamentales en el desarrollo económico y social de América Latina y el Caribe, representando el 99,5% del total de empresas en la región y con una alta concentración en el sector de microempresas, donde nueve de cada diez negocios pertenecen a esta categoría. Además, su impacto en el empleo es significativo, ya que generan aproximadamente el 60% del empleo productivo formal, lo que resalta su papel clave en la generación de oportunidades laborales y el crecimiento económico [32].

En Colombia el Ministerio de Comercio cuenta con una reglamentación para clasificar a las pymes dependiendo de los ingresos percibidos durante un ejercicio fiscal. Para medir este criterio, se emplea la Unidad de Valor Tributario (UVT), a 2022 un UVT tiene un valor de $38.004 pesos colombianos [33]. En la tabla 1 se presentan los valores que sirven para clasificar a las micro, pequeñas y medianas empresas en el país según su sector productivo.

Tabla 1. Clasificación de las empresas pymes en Colombia.

SECTOR	MICRO	PEQUEÑA	MEDIANA
Manufacturero	Inferior o igual a 23.563 UVT	Superior a 23.563 UVT e inferior o igual a 204.995 UVT	Superior a 204.995 UVT e inferior o igual a 1'736.565 UVT
Servicios	Inferior o igual a 32.988 UVT	Superior a 32.988 UVT e inferior o igual a 131.951 UVT	Superior a 131.951 UVT e inferior o igual a 483.034 UVT
Comercio	Inferior o igual a 44.769 UVT	Superior a 44.769 e inferior o igual a 431.196 UVT	Superior a 431.196 UVT e inferior o igual a 2'160.692 UVT

Nota. Esta tabla representa el modelo para clasificar las empresas de acuerdo a el índice de UVT. Fuente: [33].

Como se puede observar en la tabla 1, las pymes son las empresas que están por debajo de 2´160.692 UVT y en Colombia representan el 91,8% del total de empresas en el país. Según datos del Registro Único Empresarial y Social (RUES), existen más de 1,8 millones de microempresas en Colombia. Además, las Pymes generan aproximadamente el 80% de los empleos formales del país [34], de allí la importancia de contar con un modelo viable y sostenible de ciberseguridad aplicado a la infraestructura como servicio IaaS usada en la nube híbrida, con base en gestión de riesgos, dado que muchas de estas carecen de recursos y experiencia para implementar una seguridad sólida, quedando expuestos ante posibles amenazas en cuanto a seguridad, adicional se ven limitados a mantener arquitecturas obsoletas que los limita para enfrentar un mercado digital cada vez más competitivo.

2.1.3 Infraestructura tecnológica para la operación de una Pyme

Todas las empresas de acuerdo a su sector y actividad económica, optan por una infraestructura de ti que se adapte a sus necesidades, por lo tanto, no se cuenta con unos componentes que rijan la construcción de sus arquitecturas, sin embargo, existen una serie de componentes que son básicos y primordiales en la infraestructura de TI de las empresas. La infraestructura de Ti es una

de las bases de cualquier empresa, y es necesario para su operación diaria contar con elementos como el correo electrónico, las impresoras, los teléfonos u otros medios de comunicación interna y externa, también se incluye el cableado, los equipos de red, como servidores, routers, que permitan el tráfico de red interno y externo (Internet), dispositivos de almacenamiento, el software necesario para administrar el negocio, adicional que estos sistemas sean lo suficientemente seguros, por lo cual necesitan unos elementos de seguridad [35].

por otro lado, Sumo Logic, manifiesta que la infraestructura de TI de una organización incluye todos los recursos de hardware, software y red necesarios para brindar servicios de TI dentro de la organización, adicional indica que una infraestructura de TI típica puede incluir algunos o todos los siguientes componentes. Hardware, que incluye centros de datos, servidores, switches, routers, computadoras; el software, que se compone del software del sistema operativo, el cual proporciona una interfaz de usuario accesible para realizar operaciones informáticas en los recursos de hardware, el otro elemento que lo compone es el o los software de negocio, como los CRM, adicional otro componente es el software para análisis y monitoreo de seguridad; por ultimo menciona las redes como componente típico, y es que mediante estas se da la conectividad interna y externa de la organización [36].

Según esta información los componentes de la infraestructura tecnológica de las pymes son los recursos que se asocian al hardware, software y servicios que permiten el funcionamiento y la gestión de los sistemas informáticos y las comunicaciones en una organización o empresa. Algunas de las marcas más comunes de hardware y software para pymes en Colombia son:

Hardware: se refiere a los dispositivos físicos que soportan la infraestructura tecnológica, como computadoras, servidores, routers, switches, teléfonos, etc. Algunas de las marcas más reconocidas de hardware son Lenovo, HP, Dell, Asus, Acer, Samsung, LG, Cisco, Huawei. Estas marcas ofrecen diferentes modelos y características de acuerdo a las necesidades y presupuestos de cada empresa [37].

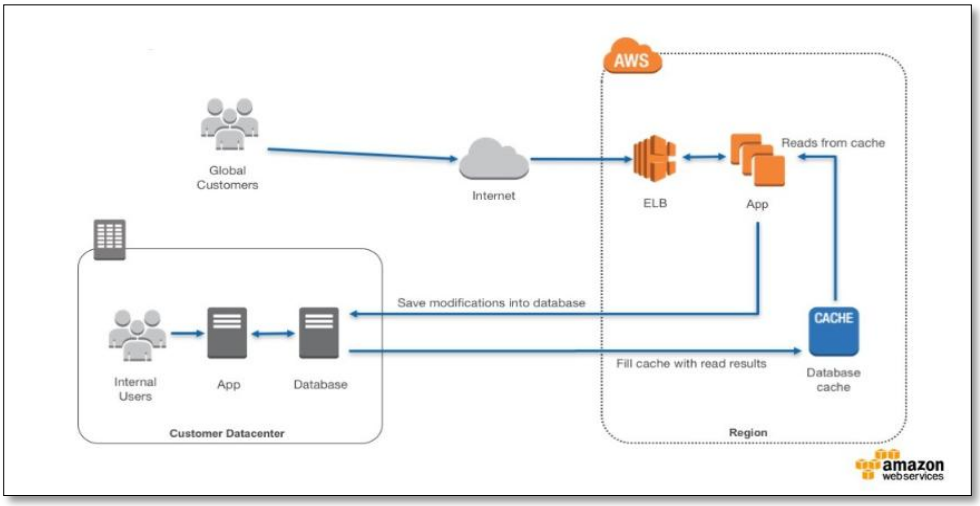
Software: se refiere a los programas y aplicaciones que se ejecutan en el hardware y que facilitan las operaciones y procesos de la empresa, como sistemas operativos, software de gestión, software

de seguridad, software de comunicación. Algunas de las marcas más populares de software son Microsoft, SAP, Oracle, Adobe, Google, IBM, Avast, Norton, Windows, Linux. Estas marcas ofrecen diferentes tipos y versiones de software para pymes en Colombia [38].

2.1.4 Caso de éxito en arquitecturas basadas en un modelo de nube hibrida

AWS da a conocer varios casos prácticos en los cuales realiza el despliegue infraestructura utilizando modelos híbridos, con la finalidad de optimizar y/o resolver problemáticas de los servicios de sus clientes, uno de los modelos más comunes para empresas pequeñas publicado por AWS, es ElastiCache para optimización de arquitecturas hibridas y bases de datos [39], en el cual se presenta una empresa con una infraestructura como se aprecia en la figura 7, allí la problemática del cliente era que los consumidores de la aplicación experimentaban tiempos de respuesta altos y se daba por que la base de datos de la aplicación estaba on-premises y por su esquema de licenciamiento no se podían migrara a la nube, por lo tanto la aplicación debía ir desde la nube hasta el datacenter on-premises para consumir dicha base de datos, generando altos tiempos de respuesta, por lo tanto se decidió hacer uso de ElastiCache, el cual es un excelente mecanismo para reducir la carga de su base de datos, y ayudar a mejorar los tiempos de respuesta puesto que, el cache se encontraría dentro de la VPC y no tendría que ir constantemente desde AWS hacía su datacenter on-premises.

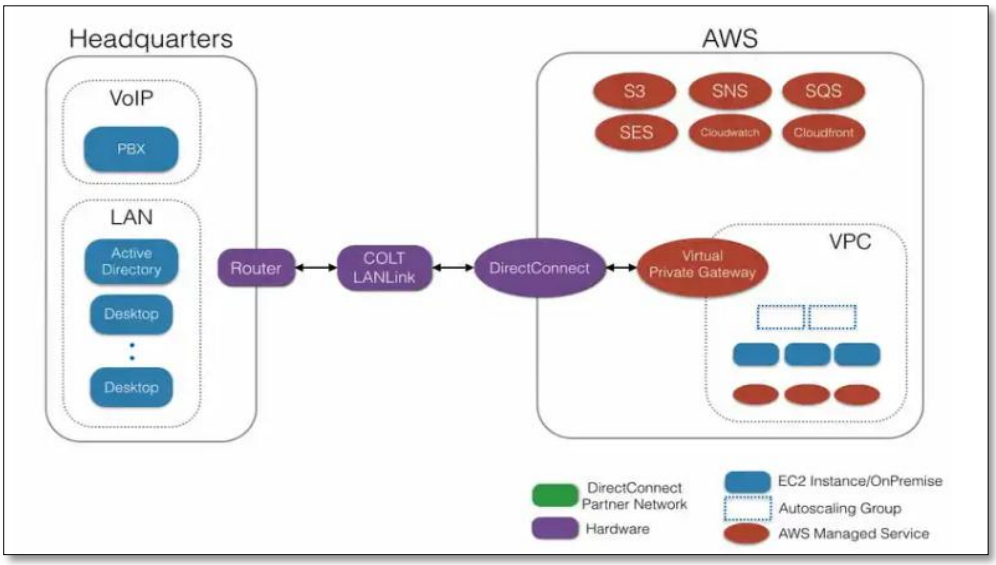
Figura 7. Arquitectura del caso de éxito de ElastiCache para optimización de arquitecturas hibridas y bases de datos.



Nota. Esta figura representa la arquitectura de un caso de éxito de un proyecto migrado a un modelo de nube hibrida. Fuente: [39]**.**

Otro caso de éxito es el que plantea Qualoom con Interflora [40], en el cual el cliente decide migrar parte de su infraestructura a nube, quedando con un modelo hibrido como se ve en la figura 8, con el cual buscaba superar los problemas de administración y disponibilidad de sus servicios.

Figura 8. Arquitectura caso de éxito Interflora.



Nota. Esta figura representa la arquitectura de un caso de éxito de un proyecto migrado a un modelo de nube hibrida. Fuente: [40].

2.1.5 Definición arquitectura de referencia

Basado en los casos de éxito presentados en el Ítem 2.1.4, se puede agrupan los requisitos de infraestructura para una pyme en cuatro áreas principales:

Computación: Las PYMES necesitan recursos de computación flexibles y escalables para ejecutar aplicaciones empresariales, sistemas de gestión (ERP, CRM) y herramientas de productividad, y para que operen de forma correcta se debe tener en cuenta los siguientes requisitos:

- Máquinas físicas y/o virtuales con configuraciones adaptables.
- Soporte para cargas de trabajo ligeras y medianas.
- Opciones de escalabilidad para picos de demanda (por ejemplo, campañas de marketing).

Almacenamiento: El almacenamiento es fundamental para gestionar grandes volúmenes de datos generados por las operaciones diarias, como documentos financieros, datos de clientes y registros de transacciones, para un funcionamiento aceptable en los recursos se debe tener en cuenta:

- Capacidad para manejar datos estructurados y no estructurados.
- Acceso rápido a datos frecuentemente utilizados.
- Opciones de respaldo y recuperación.

Redes: Las PYMES requieren conexiones seguras y confiables para integrar oficinas locales, trabajadores remotos y recursos en la nube, para esto es necesario cumplir con los siguientes requisitos:

- Redes privadas virtuales (VPN) para conectar infraestructura on-premise con la nube.
- Monitoreo y control del tráfico de red.
- Soporte para comunicación en tiempo real entre aplicaciones distribuidas.

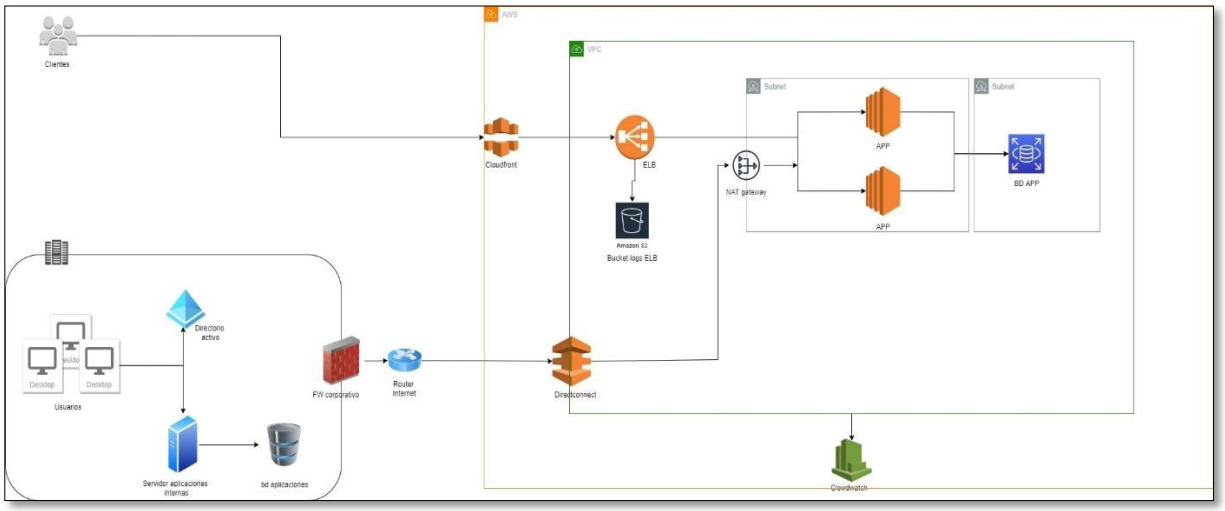
Bases de Datos: Las bases de datos son esenciales para la gestión de inventarios, datos de clientes y análisis de negocio, y estas deben cumplir con los siguientes requisitos:

- Sistemas de bases de datos relacionales (ej., MySQL, SQL Server).

- Capacidad de escalabilidad horizontal y vertical.
- Opciones de bases de datos como servicio (DBaaS) para reducir la carga administrativa.

De acuerdo a los requisitos de infraestructura tecnológica básicos y necesarios para la operación de las empresas tipo pymes, y la arquitectura planteada en las figuras 7 y 8 de casos de éxito en servicios de nube hibrida, se logra realizar la caracterización de los componentes de infraestructura de una empresa tipo pyme que pueden estar en nube, adicional desplegarlos como IaaS, lo cual se puede evidenciar en la tabla 2, también se plantea una arquitectura de referencia para estos servicios apreciada en la figura 9.

Figura 9. Arquitectura planteada.



Nota. Esta figura representa la arquitectura de referencia para empresas tipo pymes. Fuente: Elaboración propia

Tabla 2. Caracterización de servicios IaaS. Fuente propia

funcionalidad/servicio	Descripción	Nube/on-premises	Se despliega como IaaS	Proveedor/fabricante	Área perteneciente
Computador	Uso de computadores de escritorio y/o portátiles.	On-premises	No	Lenovo, HP, Asus, Dell	Computación
Correo electrónico	Uso de correo electrónico.	Nube	No	Suite de Microsoft Office 365	Computación

Internet	Uso de Internet.	On-premises	No	Claro, Movistar, Tigo, ETB	Redes
Intranet	Sitio web interno de la organización	Nube	Si	Windows server, Linux, Unix. Corre sobre instancias EC2	Computación
Red local (LAN/WLAN)	Uso de red de área local alámbrica o inalámbrica.	On-premises	No	Routers, switches (cisco, Huawei)	Redes
Software de administración	Uso de software de administración como de contabilidad, finanzas, ERP, facturación y similares.	Nube	si	SAP Business, Microsoft Dynamic 365, Corre sobre instancias EC2	Computación
Software de ventas y marketing	Uso de software de ventas, marketing y/o gestión de clientes (Ej: CRM, puntos de venta, control de cajas).	Nube	si	Windows server, Linux, Unix. Corre sobre instancias EC2	Computación
Software específico	Uso de software específico del negocio (Ejemplo de software)	Nube	si	Windows server, Linux, Unix. Corre sobre instancias EC2	Computación
Balanceador	Dispositivo encargado de balancear el tráfico de las aplicaciones	Nube	Si	AWS ALB	Redes
Sitio web	El sitio web de la organización permite conocer detalles de la empresa y de sus productos y servicios.	Nube	si	Windows server, Linux, Unix. Corre sobre instancias EC2	Computación
Base de datos	base de datos en las cual se registra y almacena la información de la aplicación	Nube/ On-premises	Mixto	Aurora, Amazon RDS, Redshift, Oracle	Bases de datos
Seguridad (firewall)	Permite/deniega el tráfico desde un origen hacia un destino	On-premises /nube	Mixto	En nube para aplicación se tiene WAF de AWS, on premise comúnmente este palo alto, Fortinet.	Redes

Seguridad (Antivirus)	Aplicativo utilizado para analizar y contener amenazas de seguridad en los dispositivos	On-premises /nube	No	Avast, Norton, Bitdefender	Computación
Directorio activo	administración de las identidades de la organización	On-premises /nube	Mixto	Windows server/ Active Directory	Computación
Conexión nube On-premises	Permite establecer conexión desde el entorno local hasta la nube de AWS	nube	No	AWS Direct connect	Redes
DNS	Gestión de nombre de dominio para la página web	Nube	No	AWS route 53	Redes
Almacenamiento de datos	Logs, backups, datos no estructurados	Nube	Si	AWS S3	Almacenamiento

Nota. Esta tabla representa la clasificación y caracterización de los componentes de una arquitectura de referencia que pueden ser desplegados como IaaS. Fuente: Elaboración propia.

De acuerdo a la tabla anterior, se determina que los componentes que califican como IaaS son, Intranet, software (administración, ventas, marketing, específico), balanceador, sitio web, almacenamiento de datos. Los componentes que no califican como IaaS son, computador, correo electrónico, internet, red local, seguridad (antivirus), conexión nube-on-premises, DNS, y los componentes mixtos, que hacen referencia si pueden tener o no como IaaS dependiendo el escenario son, base de datos, la cual si se despliega directamente en una instancia (como EC2), califica como IaaS. Si se usa como RDS, es más PaaS, o si es on-premises no aplica como IaaS, la seguridad (firewall), si se despliega el componente en nube es IaaS, si es on-premises no aplica, el directorio activo si esta on-premises no aplica como IaaS, pero si se usa el de nube si aplica.

2.2 Análisis estándares, normas y/o buenas practicas

Esta fase se basa en la revisión sistemática de la literatura, identificando y evaluado las normas y buenas prácticas que pueden ser aplicadas a la IaaS en una nube híbrida. Inicialmente, se identificaron marcos normativos reconocidos como lo son, para normas Internacionales y estándares reconocidos, se contempló ISO/IEC 27001 y NIST SP 800-53. Para regulaciones y cumplimiento legal se contempló la Ley Estatutaria 1581 de 2012 y su decreto reglamentario 1377 de 2013, y SOC 2. Para marcos de gobierno y gestión de servicios en la nube se contempló COBIT,

Cloud Controls Matrix (CCM) e ITIL. Y para las recomendaciones del aseguramiento de los servicios de nube, se contempló las recomendaciones del proveedor AWS.

Aunque estas normas o buenas prácticas en su mayoría no tienen ítems puntuales específicos sobre Infraestructura como Servicio (IaaS), abordan controles y prácticas generales de seguridad que también son aplicables a entornos de IaaS, ya que contienen controles y lineamientos que permiten asegurar aspectos fundamentales de la seguridad (confidencialidad, integridad, disponibilidad), el cumplimiento y gestión de riesgos en entornos de IaaS, adicional son ampliamente implementadas en la industria.

Posteriormente, se extrajeron únicamente los controles aplicables al contexto de las pymes en entornos IaaS de cada una de las normas y buenas prácticas identificadas. Esta selección de controles se realizó considerando criterios de aplicabilidad, madurez, viabilidad técnica y facilidad de implementación para pymes. Los controles que requerían altos niveles de automatización, inversión o madurez fueron descartados si no resultaban viables para este tipo de organizaciones.

Entendiendo madurez como el nivel de desarrollo organizacional y tecnológico que posee una pyme para implementar prácticas de seguridad, que pueden ir desde procesos informales hasta prácticas optimizadas y medibles. En este sentido, solo se priorizaron controles que no requieran de procesos sofisticados, automatización avanzada o una gestión altamente estructurada, generalmente inalcanzables para este tipo de empresas [41]. Por su parte, la viabilidad técnica se evalúa con base disponibilidad de herramientas accesibles, y la documentación existente para lograr una buena implementación del control. De este modo, se descartan controles que dependan de tecnologías emergentes o costosas, o que implicaran una alta especialización técnica, privilegiando soluciones que pudieran ser integradas con herramientas existentes en el ecosistema de las Pymes [42].

Adicional, la aplicabilidad se define como la relevancia del control para el entorno e infraestructura actual de las pymes, mientras que la facilidad de implementación mide el esfuerzo y recursos necesarios para su puesta en marcha [43].

2.2.1 ISO/IEC 27001

Estándar internacional que establece requisitos para un sistema de gestión de seguridad de la información (SGSI), los controles relevantes para servicios de IaaS en la nube Hibrida son [44]:

2.2.1.1. Controles organizacionales

- Políticas de seguridad de la información: Definir políticas específicas que incluyan directrices para gestionar servicios IaaS y conexiones híbridas.
- Roles y responsabilidades: Especificar responsabilidades de los administradores de IaaS y del entorno on-premises.
- Segregación de deberes: Asegurar que las tareas críticas, como la configuración de máquinas virtuales o redes híbridas, estén segregadas entre personal autorizado.
- Inteligencia de amenazas: Monitorear posibles amenazas relacionadas con servicios de nube e infraestructura local.
- Inventario de información y otros activos asociados: Mantener un inventario actualizado de recursos IaaS, como máquinas virtuales, bases de datos y redes.
- Control de acceso: Implementar controles estrictos de acceso lógico y físico para recursos híbridos.
- Gestión de identidades: Gestionar el ciclo de vida completo de las identidades en la nube híbrida.
- Derechos de acceso: Provisión, revisión y eliminación de permisos en IaaS y on-premise de manera regular.
- Seguridad para el uso de servicios en la nube: Establecer procesos para gestionar la seguridad en adquisición, uso y salida de servicios IaaS.
- Aprender de los incidentes de seguridad de la información: Usar incidentes pasados para mejorar la seguridad en entornos híbridos.
- Preparación de las TIC para la continuidad del negocio: Planificar y probar estrategias de continuidad para recursos IaaS y on-premises.

2.2.1.2. Controles relacionados con personas

- Conciencia, educación y formación en seguridad de la información: Capacitar al personal sobre los riesgos específicos en la gestión de entornos híbridos.

- Trabajo remoto: Proteger los accesos a recursos híbridos desde ubicaciones remotas.

2.2.1.3. Controles físicos

- Asegurar oficinas, habitaciones e instalaciones: Proteger los centros de datos on-premise y puntos de acceso físico relacionados con IaaS.
- Monitoreo de la seguridad física: Monitorear las áreas donde se encuentran los servidores o conexiones críticas para el entorno híbrido.
- Medios de almacenamiento: Gestionar adecuadamente el transporte, uso y eliminación de medios de almacenamiento físico y en la nube.
- Mantenimiento de equipos: Asegurar el mantenimiento seguro de los equipos híbridos, incluyendo servidores locales y recursos IaaS.
- Disposición o reutilización segura de los equipos: Asegurar la eliminación segura de datos en equipos físicos y virtuales.

2.2.1.4. Controles tecnológicos

- Dispositivos de punto final de usuario: Proteger los puntos de acceso que se conecten a la nube híbrida.
- Restricción de acceso a la información: Restringir el acceso a recursos IaaS según roles definidos.
- Autenticación segura: Implementar autenticación multifactorial para accesos a la nube.
- Gestión de la capacidad: Monitorear el uso de recursos IaaS para evitar sobrecargas.
- Protección contra malware: Implementar soluciones antimalware para proteger los datos en tránsito y reposo.
- Gestión de la configuración: Establecer configuraciones seguras para máquinas virtuales, redes y almacenamiento.
- Eliminación de información: Asegurar que los datos eliminados en IaaS no sean recuperables.
- Prevención de fugas de datos: Implementar medidas para prevenir fugas de información en redes híbridas.
- Copia de seguridad de la información: Realizar backups regulares de datos críticos, tanto en nube como on-premises.
- Redundancia de instalaciones de procesamiento de información: Implementar redundancia en recursos IaaS y locales para asegurar la disponibilidad.

- Actividades de seguimiento: Supervisar eventos y comportamientos anómalos en la infraestructura híbrida.
- Seguridad de redes: Proteger las redes híbridas con firewalls, VPNs y segmentación.
- Seguridad de servicios de red: Asegurar que los servicios de red en IaaS cumplan con estándares de seguridad.
- Segregación de redes: Separar redes críticas en la nube y on-premise para minimizar riesgos.
- Uso de la criptografía: Usar cifrado para proteger los datos en tránsito y en reposo en la nube híbrida.
- Ciclo de vida de desarrollo seguro: Asegurar que las aplicaciones diseñadas para IaaS sigan estándares de desarrollo seguro.
- Codificación segura: Aplicar principios de codificación segura para aplicaciones que interactúan con IaaS.
- Pruebas de seguridad en el desarrollo y aceptación: Implementar pruebas de seguridad antes de poner en producción recursos híbridos.
- Gestión del cambio: Asegurar que los cambios en configuraciones de IaaS se documenten y controlen.

2.2.2 NIST SP 800-53

Marco de control de seguridad ampliamente utilizado que proporciona controles de seguridad para sistemas de información en Estados Unidos, los controles relevantes para servicios de IaaS en la nube Hibrida son [45]:

2.2.1.2. Controles de gestión

- Plan de seguridad del sistema: Desarrollar y mantener un plan de seguridad que abarque tanto los componentes on-premises como los servicios IaaS en la nube híbrida.
- Planificación de la seguridad de la información para la computación en la nube: Establecer estrategias específicas para la integración segura de servicios en la nube, considerando la interoperabilidad y la protección de datos.
- Evaluación de riesgos: Identificar y evaluar riesgos asociados con la implementación de IaaS en una nube híbrida, incluyendo amenazas específicas de la nube y vulnerabilidades en la infraestructura local.

- Monitoreo de vulnerabilidades: Implementar procesos continuos para identificar y remediar vulnerabilidades en ambos entornos, utilizando herramientas de escaneo y análisis de seguridad.
- Líneas base de configuración: Definir y documentar configuraciones estándar para recursos IaaS y componentes on-premises, asegurando consistencia y seguridad en todo el entorno híbrido.
- Control de cambios: Establecer procedimientos para gestionar cambios en la infraestructura híbrida, incluyendo evaluaciones de impacto y aprobaciones formales.

2.2.1.3. Controles operacionales

- Gestión de cuentas de usuario: Administrar cuentas de usuario en ambos entornos, asegurando que los accesos sean apropiados y revisados periódicamente.
- Acceso remoto: Implementar medidas de seguridad para accesos remotos a recursos IaaS y on-premises, como autenticación multifactor y conexiones seguras.
- Capacitación en seguridad: Proporcionar formación específica al personal sobre riesgos y mejores prácticas en la gestión de entornos de nube híbrida.
- Respuesta a incidentes: Desarrollar procedimientos para detectar, reportar y responder a incidentes de seguridad que afecten tanto a la infraestructura local como a los servicios IaaS.
- Gestión de Incidentes en la nube: Establecer acuerdos con proveedores de IaaS para la gestión conjunta de incidentes y la comunicación efectiva durante eventos de seguridad.
- Mantenimiento controlado: Asegurar que las actividades de mantenimiento en la infraestructura híbrida se realicen de manera controlada y segura, minimizando riesgos de seguridad.
- Protección de información en tránsito: Implementar cifrado y otras medidas de protección para datos que se transfieren entre entornos on-premises y la nube.
- Control de acceso físico: Asegurar que las instalaciones físicas que alojan componentes críticos de la infraestructura híbrida estén protegidas contra accesos no autorizados.
- Plan de continuidad de operaciones: Desarrollar y probar planes que aseguren la continuidad de los servicios en caso de interrupciones, considerando la dependencia de recursos IaaS y locales.

2.2.1.4. Controles técnicos

- Protección de fronteras del sistema: Implementar firewalls y otras medidas para proteger los límites entre la infraestructura on-premises y los servicios IaaS.
- Transmisión de información de control: Protege la información de control durante la transmisión.
- Criptografía en la protección de la información: Utilizar técnicas criptográficas para proteger la confidencialidad e integridad de la información en entornos híbridos.
- Protección de la información en reposo: Asegurar que los datos almacenados en la nube y en instalaciones locales estén cifrados y protegidos contra accesos no autorizados.
- Detección de alteraciones: Implementar mecanismos para detectar cambios no autorizados en sistemas y datos en ambos entornos.
- Monitoreo del sistema: Establecer capacidades de monitoreo continuo para identificar actividades sospechosas o anómalas en la infraestructura híbrida.

2.2.1.5. Controles de privacidad

- Evaluaciones de impacto en la privacidad: Realizar evaluaciones para identificar y mitigar riesgos de privacidad asociados con el uso de servicios IaaS en la nube híbrida.

2.2.1.6. Controles de auditoría y responsabilidad

- Eventos de auditoría: Genera registros de auditoría para supervisar y revisar la actividad del sistema.
- Contenido de eventos de auditoría: Define qué información se debe incluir en los registros de auditoría.

2.2.2. Ley Estatutaria 1581 de 2012 y su decreto reglamentario 1377 de 2013

son las regulaciones específicas para la protección de datos personales y privacidad en Colombia, los controles relevantes para servicios de IaaS en la nube Hibrida son [46]:

2.2.2.1. Consentimiento y finalidad (Ley 1581 de 2012, Artículo 12):

Establece que el tratamiento de datos personales requiere el consentimiento informado del titular de los datos y debe realizarse para una finalidad específica, la cual debe ser informada al titular.

2.2.2.2. Derechos de los titulares (Ley 1581 de 2012, Capítulo III)

Reconoce los derechos de los titulares de datos personales, incluyendo el derecho a conocer, actualizar y rectificar la información, así como el derecho a suprimirla y acceder a ella.

2.2.2.3. Responsables y encargados del tratamiento (Ley 1581 de 2012, Capítulo IV)

Establece las obligaciones de los responsables y encargados del tratamiento de datos personales para asegurar la protección y seguridad de la información.

2.2.2.4. Transferencia internacional de datos (Ley 1581 de 2012, Artículo 26)

Regula la transferencia internacional de datos personales, estableciendo los requisitos para dicha transferencia y los países con niveles adecuados de protección.

2.2.2.5. Registro de bases de datos (Decreto 1377 de 2013):

Establece la obligación de inscribir las bases de datos que contengan información personal en el Registro Nacional de Bases de Datos.

2.2.3 SOC 2

Informe de control que evalúa la seguridad, disponibilidad, integridad, confidencialidad y privacidad de los sistemas de una organización, los controles relevantes para servicios de IaaS en la nube Hibrida son [47]:

2.2.3.1. Seguridad

- Control de acceso: Implementar políticas de control de acceso basadas en roles (RBAC), uso de autenticación multifactor (MFA), supervisión de accesos y generación de registros de auditoría.

- Monitoreo y detección de amenazas: Implementar herramientas como SIEM (Security Information and Event Management) para detectar actividades sospechosas, uso de firewalls y sistemas de prevención de intrusiones (IPS).
- Gestión de cambios: Todas las modificaciones al sistema sean documentadas, aprobadas y evaluadas por su impacto en la seguridad.
- Seguridad en la red: Implementar segmentación de redes y uso de VPN para conexiones seguras.
- Protección contra malware: Asegurar que los sistemas estén protegidos con soluciones antimalware y políticas de actualizaciones regulares.}

2.2.3.2. Disponibilidad

- Monitoreo del rendimiento del sistema: Supervisar métricas clave como tiempo de actividad, latencia y capacidad.
- Planificación de la capacidad: Evaluar regularmente la capacidad de los sistemas para cumplir con los requisitos actuales y futuros.
- Planes de continuidad: Implementar planes de recuperación ante desastres y continuidad del negocio, realizar pruebas regulares de recuperación.
- Gestión de incidentes: Establecer procesos claros para detectar, responder y resolver incidentes que afecten la disponibilidad.

2.2.3.3. Integridad del Procesamiento

- Validación de datos: Implementar controles para verificar que los datos ingresados sean válidos y completos.
- Gestión de cambios en los sistemas: Asegurar que las modificaciones a los sistemas sean revisadas y probadas antes de la implementación.
- Registro de actividades: Registrar todas las actividades de procesamiento, incluidas las fallas o errores.

2.2.3.4. Confidencialidad

- Cifrado: Uso de cifrado en tránsito (TLS/SSL) y en reposo para proteger datos confidenciales.
- Clasificación de la información: Definir y documentar políticas de clasificación de datos según su nivel de confidencialidad.

2.2.3.5. Privacidad

- Consentimiento del titular: Asegurar que el uso de información personal esté respaldado por el consentimiento del usuario.
- Transparencia: Proveer a los usuarios información clara sobre cómo se recopilan, usan y comparten sus datos.
- Retención y eliminación de datos: Implementar políticas de retención y eliminación seguras para la información personal.

2.2.4 COBIT (Control Objectives for Information and Related Technologies)

Es un marco de referencia desarrollado por ISACA para la gobernanza y gestión de la información y la tecnología empresarial., los puntos de referencia más relevantes para servicios de IaaS en la nube Hibrida son [48]:

2.2.4.1 Objetivos de gobierno

- Asegurar la gestión del riesgo: Identificar y evaluar riesgos relacionados con la nube híbrida, establecer políticas y procedimientos para mitigación de riesgos.
- Asegurar la gestión del desempeño: Monitorear y medir el rendimiento de los servicios IaaS.

2.2.4.2 Objetivos de gestión

- Gestión del marco de gobernanza: Establecer un marco que defina roles, responsabilidades y políticas para la gestión de servicios híbridos.
- Gestión de activos: Aborda la adquisición, mantenimiento y disposición de activos, asegurando alineación con objetivos organizacionales.

- Gestión de la configuración: Define estrategias para gestionar configuraciones y relaciones de activos.
- Gestión de riesgos: Desarrollar un programa de gestión de riesgos para abordar vulnerabilidades en la infraestructura híbrida.
- Seguridad de la información: Implementar y monitorear controles de seguridad en recursos on-premise y en la nube.

2.2.4.3. Construcción, adquisición e implementación

- BAI02: Gestión de cambios: Gestionar los cambios en recursos de nube híbrida para minimizar riesgos operativos.
- BAI06: Gestión de cambios tecnológicos: Asegurar que los nuevos servicios de nube estén alineados con las políticas organizacionales.

2.2.4.4. Entrega, servicio y soporte

- Gestión de operaciones: Monitorear y asegurar la continuidad operativa en sistemas híbridos.
- Continuidad del servicio: Aborda planes de recuperación ante desastres y continuidad del negocio.
- Gestión de problemas: Identificar y resolver incidentes en la infraestructura híbrida de manera efectiva.

2.2.4.5. Monitoreo, evaluación y valoración

- Monitoreo y evaluación del desempeño: Medir el cumplimiento de los objetivos de TI relacionados con IaaS y la nube híbrida.
- Evaluación de la conformidad: Asegurar que los servicios de nube cumplan con las normativas relevantes, como GDPR o ISO 27001.

2.2.5 Cloud Controls Matrix (CCM)

Conjunto de controles de seguridad de la información para ayudar a las organizaciones a adoptar y medir las mejores prácticas de seguridad para la nube, los controles relevantes para servicios de IaaS en la nube Hibrida son [49]:

2.2.5.1. Gestión de identidad y acceso

- Implementar controles de acceso basados en roles (RBAC) y el principio de privilegio mínimo.
- Usar autenticación multifactorial (MFA) para usuarios y administradores.
- Auditar regularmente los accesos a los sistemas híbridos.

2.2.5.2. Control de cambios y configuración

- Establecer procesos de gestión de cambios para prevenir errores en configuraciones críticas.
- Documentar y aprobar todos los cambios antes de su implementación.
- Implementar monitoreo continuo de configuraciones para detectar desviaciones.

2.2.5.3. Continuidad del negocio y resiliencia

- Diseñar planes de continuidad del negocio para servicios de IaaS.
- Implementar redundancia para datos y servicios críticos entre los entornos on-premise y nube.
- Realizar simulaciones de desastres para probar la resiliencia de los sistemas híbridos.

2.2.5.4. Seguridad y privacidad de los datos

- Cifrar datos en reposo y en tránsito, tanto en la nube como en sistemas locales.
- Implementar controles de acceso para datos sensibles.
- Desarrollar políticas de retención y eliminación de datos según las normativas aplicables.

2.2.5.5. Gestión de amenazas y vulnerabilidades

- Realizar evaluaciones periódicas de vulnerabilidades en infraestructura local y de nube.
- Implementar planes de mitigación para los riesgos identificados.
- Implementar parches de seguridad de manera proactiva para mitigar riesgos.
- Usar herramientas de análisis de amenazas para detectar actividades maliciosas.

2.2.5.6. Registro y monitoreo

- Configurar registros centralizados para eventos de seguridad en la nube y on-premise.
- Analizar logs de acceso y actividades sospechosas.
- Configurar alertas automatizadas para incidentes de alto impacto.

2.2.5.7. Criptografía y gestión de claves

- Implementar almacenamiento seguro de claves criptográficas.
- Rotar claves periódicamente según las políticas de seguridad.
- Asegurar que las claves sean gestionadas de forma segura entre entornos híbridos.

2.2.5.8. Gestión de incidentes de seguridad y forense

- Desarrollar planes de respuesta a incidentes específicos para entornos híbridos.
- Definir roles y responsabilidades claras para la gestión de incidentes.
- Usar herramientas forenses para investigar incidentes en la nube y en infraestructura local.
- Establecer procedimientos de notificación y comunicación durante incidentes.

2.2.5.9. Gobierno, riesgo y cumplimiento

- Monitorear cambios regulatorios y evaluar su impacto en el modelo híbrido.
- Realizar auditorías periódicas para asegurar el cumplimiento normativo.

2.2.5.10. Virtualización de infraestructura y seguridad

- Mantener un inventario actualizado de todos los activos en la nube.

- Implementar controles para la gestión del ciclo de vida de los activos.

2.2.6 Gestión de Servicios ITIL (Service Management Practices)

ITIL define 34 prácticas organizadas en tres categorías principales: Gestión General, Gestión de Servicios y Gestión Técnica. Las más relevantes para un modelo de nube híbrida y servicios de IaaS son [50]:

2.2.6.1. Prácticas de gestión de servicios: Estas prácticas aseguran la calidad, disponibilidad y seguridad de los servicios en la nube híbrida.

- Gestión de incidentes: Gestionar y resolver incidentes de seguridad y operativos rápidamente para minimizar el impacto en el negocio.
- Gestión de problemas: Identificar y eliminar las causas raíz de problemas recurrentes para prevenir incidentes futuros.
- Gestión de cambios: Implementar cambios de forma controlada y minimizar riesgos asociados.
- Gestión de la disponibilidad: Asegurar que los servicios híbridos estén disponibles según los acuerdos establecidos.
- Gestión de niveles de servicio: Monitorear y asegurar el cumplimiento de los SLA (Service Level Agreements) relacionados con seguridad y disponibilidad.

2.2.6.2. Prácticas de gestión general: Apoyan la planificación, implementación y monitoreo de la seguridad en la nube híbrida.

- Gestión de riesgos: Identificar, evaluar y mitigar riesgos asociados con servicios de IaaS en una nube híbrida.
- Gestión de la seguridad de la información: Proteger la confidencialidad, integridad y disponibilidad de los datos en todo el entorno híbrido.
- Gestión de proveedores: Asegurar que los proveedores de servicios de nube cumplan con los estándares y requisitos de seguridad.

2.2.6.3. Prácticas de gestión técnica: Aseguran la operatividad y seguridad de la infraestructura híbrida.

- Gestión de implementaciones: Controlar la implementación de servicios, software y hardware en entornos híbridos.
- Gestión de Infraestructura y plataforma: Supervisar y mantener los recursos físicos y virtuales.
- Gestión de monitoreo y eventos: Recopilar y analizar datos para identificar posibles fallos o amenazas.

2.2.7 Amazon Web Services (AWS):

AWS establece el Well-Architected Framework, que se estructura en seis pilares fundamentales, los cuales proporcionan principios y prácticas esenciales que pueden ser adaptados para implementar un modelo de ciberseguridad en IaaS para una nube híbrida. Algunas de las practicas más relevantes para servicios de IaaS en la nube Hibrida son [51]:

2.2.7.1. Excelencia operativa: Busca asegurar que las operaciones relacionadas con la seguridad sean confiables, monitoreadas y mejoradas continuamente mediante:

- Automatización de operaciones: Usar herramientas como AWS Systems Manager para automatizar tareas de administración y monitoreo en recursos locales y de nube.
- Monitoreo continuo: Configurar sistemas de monitoreo unificados como CloudWatch y AWS Config para rastrear eventos y configuraciones en ambos entornos.
- Pruebas frecuentes: Probar simulaciones de fallos o violaciones de seguridad para verificar la preparación de ambos entornos.

2.2.7.2. Seguridad: Busca proteger datos, sistemas y activos mediante medidas de protección como control de acceso, monitoreo y cifrado mediante:

- Gestión de identidades y accesos: Usar AWS IAM para definir políticas de acceso detalladas y habilitar AWS Single Sign-On (SSO) para gestionar accesos híbridos, implementar autenticación multifactorial (MFA) en ambos entornos.

- Protección de datos: Cifrar datos en tránsito utilizando TLS y datos en reposo con AWS Key Management Service (KMS), establecer políticas de clasificación de datos para definir niveles de protección en recursos híbridos.
- Registro y auditoría: Usar AWS CloudTrail para registrar todas las acciones realizadas en el entorno de AWS, Implementar un SIEM para centralizar registros de ambos entornos.
- Evaluación continua de vulnerabilidades: Usar AWS Inspector para evaluar configuraciones de seguridad en máquinas virtuales y contenedores en AWS.
- Seguridad de Red: Usar Amazon Virtual Private Cloud (VPC) para crear redes aisladas y seguras en la nube, con control sobre subredes, grupos de seguridad y listas de control de acceso, configurar el AWS WAF, el cual es un firewall de aplicaciones web que permite crear reglas de seguridad personalizables para proteger cargas de trabajo y aplicaciones que se ejecutan en AWS.

2.2.7.3. Fiabilidad: Busca asegurar la recuperación de sistemas ante fallos y su capacidad para cumplir con los requisitos operativos, mediante:

- Resiliencia de la infraestructura: Configurar instancias en múltiples zonas de disponibilidad (AZ) en AWS y replicar servicios críticos en la nube y on-premise.
- Planificación de recuperación: Implementar estrategias de recuperación ante desastres (DR) utilizando servicios como AWS Backup y replicación entre regiones.
- Gestión de fallos: Configurar servicios como Elastic Load Balancing (ELB) para manejar automáticamente interrupciones en sistemas híbridos.

2.2.7.4. Eficiencia del rendimiento: Busca asegurar que los sistemas sean eficientes y escalables para cumplir con las demandas, mediante:

- Monitoreo de recursos híbridos: Usar AWS CloudWatch Metrics para identificar cuellos de botella de rendimiento en la nube y sistemas locales.
- Monitoreo centralizado: Usar Amazon GuardDuty para la detección de amenazas en AWS y combinarlo con soluciones SIEM para visibilidad híbrida.
- Optimización de redes: Configurar AWS Direct Connect para reducir la latencia entre sistemas locales y la nube.

- Escalado automático: Implementar AWS Auto Scaling para ajustarse dinámicamente a las necesidades del negocio.

2.2.7.5. Optimización de costos: Busca minimizar los costos operativos mientras se garantizan niveles adecuados de seguridad y rendimiento.

- Monitoreo de costos: Usar AWS Cost Explorer para rastrear el uso de recursos y ajustar configuraciones según las necesidades.
- Uso eficiente de recursos: Aprovechar instancias reservadas para servicios críticos en AWS y balancear cargas entre entornos híbridos.

2.2.7.6. Sostenibilidad: Busca minimizar el impacto ambiental y optimizar el uso de recursos tecnológicos.

- Consolidación de recursos: Usar tecnologías de contenedores (ECS o EKS) para reducir el consumo energético en sistemas híbridos.
- Reducción de desperdicios: Monitorear recursos ociosos en AWS y on-premise para liberar recursos innecesarios.

2.2.8 Dominios de acuerdo a la clasificación de los controles de las normas y/o estándares

Analizando los controles de cada norma, se identificaron múltiples similitudes entre ellos. Por esta razón, se procedió a unificar los controles similares y agruparlos en grupos temáticos definidos como dominios del modelo, los cuales se organizaron con base en su propósito común, determinado a partir de su similitud funcional y de las referencias cruzadas entre las normas y buenas prácticas revisadas, estos dominios son los siguientes:

Gestión de accesos: Verificar la identidad de los usuarios y permitir o denegar el acceso a los recursos con base en políticas de seguridad, roles y privilegios asignados. Implementar controles como autenticación multifactorial (MFA), gestión de identidades (IAM) y auditoría de accesos.

Gestión de riesgos: Identificar, analizar y mitigar los riesgos de seguridad en la infraestructura IaaS. Involucra la evaluación de amenazas, la implementación de controles, la gestión de

vulnerabilidades y la planificación de estrategias para reducir el impacto de incidentes de seguridad.

Protección de datos: Asegurar la confidencialidad, integridad y disponibilidad de la información almacenada, procesada o transmitida en la nube híbrida. Incluye la implementación de cifrado, prevención de fugas de datos (DLP), control de accesos y políticas de retención y eliminación segura de datos.

Gestión de incidentes: Detectar, responder y recuperar la infraestructura ante incidentes de seguridad en la nube híbrida. Implica la definición de procedimientos de respuesta, el uso de herramientas de monitoreo, la gestión forense y la comunicación efectiva con las partes interesadas.

Monitoreo de actividades: Supervisar en tiempo real las actividades en la infraestructura IaaS para detectar amenazas, anomalías o comportamientos sospechosos. Incluye la recopilación y análisis de logs, la implementación de SIEMs y la correlación de eventos de seguridad para una detección proactiva.

Gestión de configuraciones: Definir, aplicar y mantener configuraciones seguras en la infraestructura IaaS y entornos híbridos. Incluye la gestión de cambios, la automatización de configuraciones seguras, la auditoría de configuraciones y la estandarización de entornos para reducir riesgos.

Continuidad y recuperación ante desastres: Asegurar la disponibilidad y recuperación de la información ante fallos, incidentes o ataques en la nube híbrida. Incluye la implementación de backups automatizados, estrategias de recuperación ante desastres (DRP) y pruebas periódicas de restauración de datos.

Nota: Para tener más claridad sobre los controles que se identificaron en cada norma y buena práctica de acuerdo a los dominios, se puede revisar el anexo B.

En la tabla 3 se tienen los estándares, normas y buenas prácticas analizados, los dominios definidos y se representa con una “x” cual de esos estándares, normas o buenas prácticas contiene definiciones de controles referentes a cada dominio.

Tabla 3. Cobertura de dominios de seguridad en normas y marcos de referencia.

Dominio	ISO/IEC 27001	NIST SP 800-53	Ley estatutaria 1581 y decreto 1377	SOC 2	COBIT	CSA CCM	ITIL	Recomendaciones AWS
Gestión de accesos	x	x	x	x	x	x		x
Gestión de riesgos	x	x	x	x	x	x	x	x
Protección de datos	x	x	x	x	x	x	x	x
Gestión de incidentes	x	x		x	x	x	x	x
Monitoreo de actividades	x	x		x	x	x	x	x
Gestión de configuraciones	x	x		x	x	x	x	x
Continuidad y recuperación ante desastres	x	x		x	x	x		x

Nota. Esta tabla representa el cumplimiento de las normas, estándares y buenas prácticas de acuerdo a los dominios definidos. Fuente: Elaboración propia.

2.3 Riesgos en infraestructuras híbridas para servicios IaaS

La adopción de una infraestructura de nube híbrida combina entornos de nube pública y privada, lo que conlleva de forma implícita una serie de riesgos relacionados con la seguridad, la privacidad y la gestión de datos, que es necesario contemplarlos, para eso se requiere una correcta identificación y valoración de estos riesgos, permitiendo así una mejor gestión y mitigación dentro de los servicios IaaS.

2.3.1 Identificación de riesgos

En concordancia con la norma ISO/IEC 27005:2022, la identificación de riesgos de este estudio se realiza mediante el enfoque basado en activos. Este enfoque consiste en identificar los activos de información que forman parte de la arquitectura de nube híbrida de referencia para pymes, la cual se plantea en el ítem 2.1.5, y a continuación son analizadas los escenarios de amenaza que pueden afectarlos, qué vulnerabilidades presentan, y cómo estas combinaciones podrían generar un riesgo.

- **Configuraciones incorrectas**

Los errores en la configuración de servicios en la nube pueden exponer datos sensibles y sistemas críticos a accesos no autorizados.

Amenaza: Exposición de recursos críticos debido a errores en la configuración de servicios en la nube.

Vulnerabilidades asociadas: Permisos excesivos, políticas mal definidas, uso de configuraciones por defecto, ausencia de validación de cambios.

Activos afectados: Políticas de seguridad, sistemas de almacenamiento, bases de datos, recursos de cómputo y redes [52].

- **Acceso no autorizado**

Componentes como APIs inseguras y malas prácticas de autenticación pueden permitir que atacantes accedan a recursos críticos sin permiso.

Amenaza: Acceso indebido a recursos sin autorización.

Vulnerabilidades asociadas: APIs inseguras, malas prácticas de autenticación, configuración débil de roles IAM.

Activos afectados: Interfaces y puntos de acceso, sistemas de gestión de identidades y accesos (IAM) [53].

- **Gestión deficiente de identidades (IAM)**

La falta de controles y buenas prácticas en la configuración de IAM puede facilitar el secuestro de cuentas y accesos indebidos a los recursos.

Amenaza: Suplantación o secuestro de cuentas por mala gestión de credenciales y privilegios.

Vulnerabilidades asociadas: Configuraciones incorrectas en IAM, privilegios excesivos, falta de autenticación multifactor.

Activos afectados: Sistemas IAM, paneles de administración de servicios cloud [54].

- **Amenazas internas**

Los empleados o colaboradores con intenciones maliciosas pueden hacer uso de sus privilegios para comprometer la seguridad de la información bien sea desde con el alcance que tienen o aprovechando brechas para obtener privilegios más elevados.

Amenaza: Acciones maliciosas o negligentes por parte de empleados con privilegios.

Vulnerabilidades asociadas: Ausencia de monitoreo de privilegios, falta de segregación de funciones, permisos excesivos.

Activos afectados: Bases de datos, sistemas de almacenamiento, IAM [53].

- **Vulnerabilidades en aplicaciones web**

Las aplicaciones desplegadas en la nube pueden contener malas configuraciones, las cuales, si son explotadas, pueden comprometen la integridad y disponibilidad de los sistemas.

Amenaza: Explotación de errores de seguridad en aplicaciones desplegadas en la nube.

Vulnerabilidades asociadas: Inyecciones, configuración insegura, exposición de APIs.

Activos afectados: Aplicaciones, interfaces web, recursos de cómputo [55].

- **Interceptación de datos**

Dado el flujo de datos entre componentes on-premises y nube se puede presentar una intercepción maliciosa de en tránsito.

Amenaza: Captura maliciosa de información en tránsito.

Vulnerabilidades asociadas: Falta de cifrado, uso de protocolos inseguros, redes mal segmentadas.

Activos afectados: Canales de comunicación entre nube y on-premises [56].

- **Fugas de datos y exfiltración de información**

Los datos pueden ser extraídos o filtrados debido a configuraciones inadecuadas, accesos indebidos o malware.

Amenaza: Robo o pérdida de información confidencial.

Vulnerabilidades asociadas: Permisos abiertos, buckets de almacenamiento mal configurados, malware.

Activos afectados: Sistemas de almacenamiento, bases de datos, políticas de seguridad [57].

- **Ataques a la red y DDoS**

Los servicios en la nube pueden ser víctimas de ataques de denegación de servicio, sobrecarga de tráfico o intentos de intrusión, todo esto de acuerdo a el modelo de exposición de datos en cloud computing.

Amenaza: Interrupción de servicios por sobrecarga o saturación de red.

Vulnerabilidades asociadas: Falta de protección perimetral, nula mitigación DDoS.

Activos afectados: Interfaces públicas, recursos de red, balanceadores de carga [58].

Nota: para más detalle de los riesgos identificados, su agente generador y la causa raíz se puede apreciar el Anexo D.

2.3.2 Valoración de riesgos según ISO 27005

En el modelo propuesto, se evalúa el "impacto tiempo" el cual hace referencia a la duración o prolongación del daño que un evento puede generar, mientras que "impacto alcance" describe la extensión del efecto sobre procesos o activos. Estos elementos se utilizan como referencia visual para sugerir controles orientados a reducir la probabilidad (mediante detección o prevención) o el impacto (mediante contención o recuperación), tal como lo plantea la ISO/IEC 27005 en sus fases de tratamiento del riesgo [11], en la tabla 4, se definen los riesgos de acuerdo a las amenazas identificadas en el ítem 2.3.1.

Tabla 4. Formato para la valoración de riesgos según ISO 27005.

RIESGOS DEL PROYECTO	PROBABILIDAD		IMPACTO TIEMPO		Riesgo P*Impacto	IMPACTO ALCANCE		Riesgo P*Impacto
	Severidad	Valor	Severidad	Valor	Probabilidad/Tiempo	Severidad	Valor	Probabilidad/Alcance
Acceso indebido a sistemas críticos mediante credenciales débiles o robadas.								
Explotación de fallas en interfaces o APIs para comprometer sistemas o extraer datos.								
Compromiso de cuentas de usuario por intentos automatizados de fuerza bruta.								

Interrupción de servicios por sobrecarga maliciosa de tráfico (DDoS).								
Exposición de recursos sensibles por configuraciones erróneas o permisos inadecuados.								
Acceso no autorizado por uso de contraseñas débiles, compartidas o mal gestionadas.								
Elevación ilegítima de privilegios por fallos en el control de accesos.								
Acceso no autorizado debido a errores en los mecanismos de autenticación.								
Exposición de información en tránsito por interceptación en canales no cifrados.								
Alteración maliciosa de comunicaciones entre componentes o sistemas conectados.								

Pérdida o filtración de datos sensibles durante la transferencia entre nubes.								
Pérdida de información por fallos en la replicación o sincronización entre entornos.								
Compromiso del sistema mediante la inyección de código malicioso en aplicaciones.								
Exposición pública de datos críticos por errores de configuración o falta de control.								
Incidentes de seguridad causados por políticas débiles o mal implementada								

Nota. Esta tabla representa el formato para valoración de riesgos adaptado de la ISO27005. Fuente: Adaptado de la norma IS027005 [11].

Para realizar la calificación de los riesgos es necesario basarse en los aspectos definidos en la tabla 5 y 6.

Tabla 5. valores para calificar el impacto (tiempo y alcance).

TABLAS DE IMPACTOS NEGATIVOS				TABLAS DE IMPACTOS POSITIVOS
Nivel	**Rangos**	**Alcance**	**Cronograma/ Tiempo**	**Cronograma/ Tiempo**
1	Muy bajo	Disminución del alcance apenas perceptible	Aumento del tiempo insignificante	Entrega del proyecto con una disminución del tiempo poco perceptible
2	Bajo	Áreas secundarias del alcance afectadas	Aumento del tiempo <5%	Entrega del proyecto en 95% del tiempo estimado
3	Medio	Áreas principales del alcance afectadas	aumento del tiempo del 5 % - 10%	Entrega del proyecto en 95% del tiempo estimado
4	Alto	Reducción del alcance inaceptable para el patrocinador	aumento del tiempo del 10% - 20 %	Entrega del proyecto en 95% del tiempo estimado
5	Muy Alto	El elemento final del proyecto es efectivamente inservible	aumento del tiempo > 20%	Entrega del proyecto en 95% del tiempo estimado

Nota. Esta tabla representa los valores posibles para calificar el impacto (alcance y tiempo) de los riesgos.
Fuente: [11]

Tabla 6. valores para calificar la probabilidad.

TABLAS DE PROBABILIDAD		
Nivel	**Rangos**	**Ejemplo detallado de la descripción**
5	Muy Alta	La expectativa de ocurrencia se da en la mayoría de circunstancias
4	Alta	Probabilidad de ocurrencia en la mayoría de las circunstancias
3	Media	Puede ocurrir en algún momento
2	Baja	Podría ocurrir algunas veces
1	Muy Baja	Puede ocurrir en circunstancias excepcionales

Nota. Esta tabla representa los valores posibles para calificar la probabilidad de ocurrencia de los riesgos. Fuente: [11].

2.4 Modelo

A continuación, se describe el modelo de ciberseguridad aplicable a la infraestructura como servicio IaaS usada en la nube híbrida para pymes, basado en la gestión de riesgos, fundamentado en el análisis de ISO/IEC 27001, NIST SP 800-53, Ley Estatutaria 1581 y Decreto 1377, SOC 2, COBIT, CSA CCM, ITIL y recomendaciones de AWS. El objetivo es proporcionar un conjunto de controles y estrategias para mitigar amenazas y asegurar la protección de los activos en entornos de nube hibrida.

2.4.1 Dominios del modelo

A continuación, se describen los dominios que estructuran el modelo de ciberseguridad propuesto. Cada dominio agrupa un conjunto de controles enfocados en un área específica de protección dentro del entorno IaaS en una nube híbrida.

2.4.1.1 Gestión de accesos

- Roles y responsabilidades

  Especificar responsabilidades claras para los administradores de IaaS y el entorno on-premise, garantizando una asignación adecuada de permisos y acceso.

- Segregación de deberes

  Descripción: Asegurar que las tareas críticas, como la configuración de máquinas virtuales o redes híbridas, estén segregadas entre personal autorizado para evitar conflictos de interés o accesos no autorizados.

- Control de acceso

  Implementar controles estrictos, tanto lógicos como físicos, basados en roles (RBAC) y el principio de mínimo privilegio. Incluir supervisión de accesos, generación de registros de auditoría y autenticación multifactorial (MFA).

- Gestión de identidades

  Gestionar el ciclo de vida completo de las identidades, desde la creación hasta la eliminación, utilizando herramientas como AWS IAM y Single Sign-On (SSO) para asegurar políticas de acceso detalladas en la nube híbrida.

- Ciclo de vida permisos de acceso

  Proveer, revisar y eliminar permisos de acceso regularmente para usuarios en entornos IaaS y on-premise, asegurando que los accesos sean apropiados y actualizados.

- Seguridad de acceso remoto

  Proteger los accesos a recursos híbridos desde ubicaciones remotas mediante autenticación segura (MFA), conexiones cifradas y monitoreo.

- Gestión de usuarios privilegiados

  Controlar y monitorear las acciones realizadas por usuarios con altos privilegios en ambos entornos (IaaS y on-premise).

- Gestión de derechos de los titulares

  Asegurar que los titulares de datos personales puedan conocer, actualizar, rectificar, suprimir y acceder a su información de forma segura y controlada.

- Segregación de redes y ambientes

  Separar redes y ambientes en la nube y on-premise para minimizar riesgos y controlar accesos no autorizados.

2.4.1.2 Gestión de riesgos

- Inventario de información y activos

  Mantener un inventario actualizado de recursos IaaS, como máquinas virtuales, bases de datos y redes, para asegurar su gestión y seguridad adecuadas.

- Capacitación en seguridad

  Proporcionar formación específica al personal sobre riesgos y mejores prácticas en la gestión de entornos híbridos, fomentando la conciencia y educación en seguridad de la información.

- Pruebas de seguridad en ambientes de desarrollo

  Implementar pruebas de seguridad antes de poner en producción recursos híbridos para asegurar que las configuraciones y aplicaciones sean seguras.

- Plan de seguridad del sistema

  Desarrollar y mantener un plan de seguridad que abarque tanto los componentes on-premise como los servicios IaaS en la nube híbrida.

- Planificación de la seguridad de la información

  Establecer estrategias específicas para la integración segura de servicios en la nube, considerando interoperabilidad, protección de datos y resiliencia del sistema.

- Evaluación de riesgos

  Identificar y evaluar riesgos asociados con la implementación de IaaS en una nube híbrida, considerando amenazas específicas de la nube (usando herramientas especializadas como AWS Inspector) y vulnerabilidades en la infraestructura local.

- Evaluaciones de impacto en la privacidad

  Realizar evaluaciones periódicas para identificar y mitigar riesgos de privacidad asociados con el uso de servicios IaaS, asegurando el cumplimiento normativo.

- Consentimiento del titular

  Asegurar que el tratamiento de datos personales esté respaldado por el consentimiento informado del usuario y cumplir con la finalidad específica definida.

- Planificación de la capacidad

  Evaluar regularmente la capacidad de los sistemas para cumplir con los requisitos actuales y futuros, asegurando su disponibilidad y escalabilidad.

- Gestión del riesgo

  Desarrollar programas para identificar, evaluar y mitigar riesgos en la infraestructura híbrida, implementando políticas y procedimientos efectivos.

- Marco de gobierno

  Establecer un marco que defina roles, responsabilidades y políticas para la gestión y supervisión de servicios híbridos.

- Gestión de activos

  Abordar la adquisición, mantenimiento y disposición de activos, asegurando que estén alineados con los objetivos organizacionales y de seguridad.

- Evaluación de la conformidad

  Asegurar que los servicios en la nube híbrida cumplan con normativas relevantes como ISO 27001, mediante auditorías y evaluaciones periódicas.

- Simulaciones de desastres

  Realizar simulaciones regulares de fallos o desastres para probar la resiliencia de los sistemas híbridos y verificar la efectividad de los planes de recuperación.

- Mitigación de riesgos

  Implementar planes de mitigación para riesgos identificados en la infraestructura híbrida, reduciendo la probabilidad e impacto de incidentes.

- Gestión de proveedores

  Asegurar que los proveedores de servicios de nube cumplan con los estándares y requisitos de seguridad establecidos, mediante evaluaciones y acuerdos formales.

- Gestión de parches

  Implementar parches de seguridad de manera proactiva en la infraestructura híbrida para mitigar riesgos asociados con vulnerabilidades conocidas.

2.4.1.3 Protección de datos

- Gestión de medios de almacenamiento

  Administrar adecuadamente el transporte, uso y eliminación de medios de almacenamiento físico y en la nube para asegurar la seguridad de los datos.

- Disposición segura de equipos

  Asegurar la eliminación segura de datos en equipos físicos y virtuales antes de su disposición o reutilización, siguiendo normativas y buenas prácticas, evitando que los datos sean recuperables.

- Protección contra malware

  Implementar soluciones antimalware actualizadas para proteger datos en tránsito y en reposo, junto con políticas de actualización regular.

- Prevención de fugas de datos

  Establecer medidas de seguridad para prevenir fugas de información en redes híbridas con herramienta como DLP, adicional incluir monitoreo continuo y controles de acceso.

- Seguridad de redes

  Proteger redes híbridas mediante firewalls, VPNs, segmentación de redes, usar tecnologías como Amazon VPC y AWS WAF para crear redes aisladas y seguras en la nube, logrando minimizar riesgos.

- Seguridad de servicios de red

  Asegurar que los servicios de red en IaaS cumplan con estándares de seguridad para proteger datos y sistemas conectados.

- Uso de la criptografía

  Implementar técnicas criptográficas para proteger datos en tránsito y en reposo, utilizando estándares como TLS/SSL y cifrado en reposo (KMS).

- Clasificación de la información

  Definir y documentar políticas para clasificar los datos según su nivel de confidencialidad y aplicar los controles de seguridad adecuados.

- Retención y eliminación de datos

  Implementar políticas seguras de retención y eliminación de datos personales, cumpliendo con normativas aplicables.

- Validación de datos

  Implementar controles para verificar que los datos ingresados sean válidos, completos y cumplan con los estándares establecidos.

- Criptografía en la gestión de claves

  Asegurar el almacenamiento seguro de claves criptográficas, implementando rotación periódica y gestión segura en entornos híbridos.

- Gestión de la seguridad de la información

  Proteger la confidencialidad, integridad y disponibilidad de los datos en todo el entorno híbrido mediante la implementación y monitoreo de controles de seguridad.

- Políticas de privacidad y transferencias de datos con terceros

  Establecer políticas para la transferencia de datos con terceros, buscando que se cumplan los requisitos normativos y que se protejan los datos personales.

2.4.1.4 Gestión de incidentes

- Aprendizaje de incidentes pasados

  Analizar incidentes de seguridad previos para identificar lecciones aprendidas y mejorar las medidas de prevención y respuesta en entornos híbridos.

- Respuesta a incidentes

  Desarrollar procedimientos para la detección, reporte y respuesta rápida a incidentes de seguridad que afecten tanto la infraestructura local como los servicios IaaS.

- Gestión de incidentes en la nube

  Establecer acuerdos con proveedores de IaaS para la gestión conjunta de incidentes y asegurar una comunicación efectiva durante eventos de seguridad.

- Procesos para la gestión de incidentes

  Desarrollar planes específicos para detectar, responder y resolver incidentes, asegurando la continuidad operativa y la disponibilidad de los sistemas.

- Alertas automatizadas

  Configurar alertas automatizadas para incidentes de alto impacto, facilitando respuestas rápidas y oportunas.

- Roles y responsabilidades bien definidos

  Definir claramente los roles, responsabilidades y protocolos de actuación de los equipos involucrados en la gestión de incidentes para asegurar una respuesta eficiente.

- Herramientas forenses

  Usar herramientas forenses para investigar incidentes de seguridad en la nube y en infraestructura local, asegurando una comprensión completa de los eventos.

- Procedimientos de notificación y comunicación

  Establecer procedimientos formales para la notificación interna y externa durante incidentes, incluyendo comunicación con proveedores y stakeholders.

- Gestión de fallos

  Configurar servicios que permitan balancear la carga a componentes activos, así como Elastic Load Balancing (ELB), buscando manejar automáticamente interrupciones y minimizar el impacto de fallos en sistemas híbridos.

2.4.1.5 Monitoreo de actividades

- Monitoreo y detección de amenazas

  Implementar herramientas como SIEM (Security Information and Event Management), firewalls y sistemas de prevención de intrusiones (IPS) para detectar actividades sospechosas o anómalas en la infraestructura híbrida. Supervisar amenazas en servicios de nube e infraestructura local, incluyendo análisis de amenazas y detección de actividades maliciosas.

- Monitoreo de seguridad física

  Supervisar áreas donde se encuentran servidores y conexiones críticas dentro del entorno híbrido para prevenir accesos no autorizados y mitigar riesgos físicos.

- Gestión de la capacidad y rendimiento

  Monitorear el uso de recursos IaaS para evitar sobrecargas. Supervisar métricas clave como tiempo de actividad, latencia y capacidad de sistemas en la nube híbrida. Identificar cuellos de botella de rendimiento en la nube y sistemas locales mediante herramientas como AWS CloudWatch Metrics.

- Registro y auditoría de eventos

  Generar registros de auditoría y definir qué información debe incluirse para supervisar y revisar la actividad del sistema. Usar soluciones como AWS CloudTrail para registrar acciones en la nube y un SIEM para centralizar registros. Realizar auditorías periódicas para asegurar cumplimiento normativo.

- Monitoreo de operaciones y continuidad

  Supervisar y asegurar la continuidad operativa en entornos híbridos, asegurando el cumplimiento de los SLA (Service Level Agreements) relacionados con seguridad y disponibilidad. Medir el cumplimiento de los objetivos de TI en IaaS y nube híbrida.

- Monitoreo regulatorio y cumplimiento

  Supervisar cambios en normativas y evaluar su impacto en el modelo híbrido. Asegurar la inscripción de bases de datos personales en registros nacionales y cumplir con requisitos regulatorios mediante auditorías y monitoreo continuo.

- Monitoreo financiero y optimización de recursos

  Supervisar costos y uso de recursos en AWS y entornos on-premises con herramientas como AWS Cost Explorer. Identificar recursos ociosos y ajustar configuraciones para optimizar costos y reducir desperdicios.

- Monitoreo centralizado y correlación de eventos

  Usar herramientas como Amazon GuardDuty y AWS Config para centralizar la detección de amenazas en la nube y combinarlo con soluciones SIEM para visibilidad híbrida. Implementar registros centralizados y correlación de eventos en sistemas on-premises y en la nube.

- Inteligencia de amenazas

  Establecer mecanismos para recopilar, analizar y utilizar información sobre amenazas cibernéticas que permita anticiparse a posibles ataques y reforzar sus capacidades de defensa y respuesta.

2.4.1.6 Gestión de configuraciones

- Definición de políticas y directrices para la gestión de configuraciones

  Establecer políticas de seguridad específicas para la gestión de servicios IaaS y conexiones híbridas, asegurando que incluyan directrices para adquisición, uso y salida de servicios en la nube. Definir estrategias para gestionar configuraciones y relaciones de activos.

- Gestión de configuraciones seguras en la infraestructura híbrida

  Definir y documentar configuraciones estándar para máquinas virtuales, redes y almacenamiento en entornos híbridos, garantizando consistencia y seguridad. Implementar herramientas de automatización para mejorar la eficiencia en la administración y monitoreo de configuraciones.

- Gestión y control de cambios en la infraestructura híbrida

  Establecer procedimientos para gestionar cambios en la infraestructura IaaS y on-premise, incluyendo documentación, evaluación de impacto, revisiones, pruebas y aprobaciones formales antes de la implementación.

- Mantenimiento seguro de la infraestructura híbrida

  Asegurar que el mantenimiento de equipos físicos y recursos IaaS se realice de manera segura, controlada y periódica, minimizando riesgos operativos y de seguridad.

- Gestión del ciclo de vida de los activos y aplicaciones en la nube

  Mantener un inventario actualizado de activos en la nube y establecer controles para su gestión en todo su ciclo de vida. Asegurar que las aplicaciones diseñadas para IaaS sigan estándares de desarrollo seguro y políticas organizacionales.

- Optimización y automatización de recursos en la nube híbrida

  Implementar soluciones como AWS Systems Manager, Auto Scaling y Direct Connect para mejorar la disponibilidad, reducir latencia y optimizar el uso de recursos. Aprovechar instancias reservadas y tecnologías de contenedores para eficiencia energética y balance de cargas en entornos híbridos.

2.4.1.7 Continuidad y recuperación ante desastres

- Realización de backups periódicos

  Implementar estrategias de respaldo automáticas y programadas para todos los recursos críticos (bases de datos, configuraciones, archivos y máquinas virtuales), tanto en la nube como en entornos físicos. Establecer políticas claras sobre la frecuencia, el tipo (completo, incremental, diferencial) y el cifrado de los respaldos. Utilizando servicios como Amazon S3 Glacier, AWS Backup.

- Pruebas de recuperación documentadas

  Diseñar y ejecutar pruebas periódicas de restauración de servicios y recuperación de datos, documentando los resultados, tiempos de respuesta y lecciones aprendidas. Estas pruebas

deben incluir simulaciones realistas de escenarios como pérdida total del sitio físico, corrupción de datos o indisponibilidad de servicios en la infraestructura.

- Replicación entre nubes y on-premise

  Establecer mecanismos de replicación de datos y servicios entre la infraestructura on-premise y la nube pública (y viceversa), garantizando sincronización continua o casi en tiempo real. Usar soluciones como AWS CloudEndure o replicación de bases de datos multi-región. Este control fortalece la tolerancia a fallos y la disponibilidad incluso en escenarios de desastre físico o ciberataques.

- Existencia de un DRP

  Desarrollar y mantener actualizado un plan de recuperación ante desastres (DRP), alineados con los riesgos identificados y el apetito de riesgo de la organización. Deben estar formalmente aprobado, difundido entre los equipos clave y probado regularmente mediante ejercicios simulados.

La selección de los controles incluidos en cada dominio del modelo se encuentra detallada en el Anexo C. Esta selección se realizó tomando como base los riesgos identificados en la sección 2.3.1, con el objetivo de asegurar una cobertura coherente y directa frente a los escenarios de amenaza específicos para entornos IaaS en nube híbrida para pymes. Se priorizaron controles que ofrecieran una mitigación efectiva frente a los riesgos de mayor probabilidad e impacto, considerando la aplicabilidad técnica y la viabilidad operativa en empresas de este segmento.

2.4.2 Formulario de evaluación del cumplimiento para el modelo de ciberseguridad

Para evaluar el cumplimiento del modelo de ciberseguridad se diseña el siguiente formulario, el cual permite medir de manera estructurada la implementación de los controles en diferentes categorías mediante una escala de cumplimiento definida de acuerdo a, cumple completamente (CC), cumple parcialmente (CP), no cumple (NC), no aplica (NA), y adicional se puede agregar observaciones o evidencia, si se requiere.

2.4.2.1. Gestión de accesos

Verificar la identidad de los usuarios y permitir o denegar el acceso a los recursos con base en políticas de seguridad, roles y privilegios asignados. Implementar controles como autenticación multifactorial (MFA), gestión de identidades (IAM) y auditoría de accesos.

Tabla 7. Formulario para la calificación de los controles definidos para la gestión de accesos.

Control	CC	CP	NC	NA	Observaciones / Evidencia
Definición de roles y responsabilidades					
Segregación de deberes					
Implementación de control de acceso					
Gestión de identidades					
Ciclo de vida permisos de acceso					
Seguridad de accesos remotos					
Gestión de usuarios privilegiados					
Gestión de derechos de los titulares					
Segregación de redes y ambientes					

Nota. Esta tabla representa el formulario para la calificación del nivel de cumplimiento de los controles para gestión de accesos definidos en el modelo. Fuente: Elaboración propia.

2.4.2.2. Gestión de riesgos

Identificar, analizar y mitigar los riesgos de seguridad en la infraestructura IaaS. Involucra la evaluación de amenazas, la implementación de controles, la gestión de vulnerabilidades y la planificación de estrategias para reducir el impacto de incidentes de seguridad.

Tabla 8. Formulario para calificación de los controles definidos para la gestión de riesgos.

Control	CC	CP	NC	NA	Observaciones / Evidencia
Inventario de información y activos					
Capacitación en seguridad					
Pruebas de seguridad en ambientes de desarrollo					
Plan de seguridad del sistema					
Planificación de la seguridad de la información					
Evaluación de riesgos					
Evaluaciones de impacto en la privacidad					
Consentimiento del titular					
Planificación de la capacidad					
Gestión del riesgo					
Marco de gobierno					
Gestión de activos					
Evaluación de la conformidad					
Simulaciones de desastres					
Mitigación de riesgos					
Gestión de proveedores					
Gestión de parches					

Nota. Esta tabla representa el formulario para la calificación del nivel de cumplimiento de los controles para la gestión de riesgos definidos en el modelo. Fuente: Elaboración propia.

2.4.2.3. Protección de datos

Asegurar la confidencialidad, integridad y disponibilidad de la información almacenada, procesada o transmitida en la nube híbrida. Incluye la implementación de cifrado, prevención de fugas de datos (DLP), control de accesos y políticas de retención y eliminación segura de datos.

Tabla 9. Formulario para calificación de controles asociados a la protección de datos.

Control	CC	CP	NC	NA	Observaciones / Evidencia
Gestión de medios de almacenamiento					
Disposición segura de equipos					
Protección contra malware					
Prevención de fugas de datos					
Seguridad de redes					
Seguridad de servicios de red					
Uso de la criptografía					
Clasificación de la información					
Retención y eliminación de datos					
Validación de datos					
Criptografía en la gestión de claves					
Transmisión de información de control					
Gestión de la seguridad de la información					
Políticas de privacidad y transferencias de datos con terceros					

Nota. Esta tabla representa el formulario para la calificación del nivel de cumplimiento para los controles de protección de datos. Fuente: Elaboración propia.

2.4.2.4. Gestión de incidentes

Detectar, responder y recuperar la infraestructura ante incidentes de seguridad en la nube híbrida. Implica la definición de procedimientos de respuesta, el uso de herramientas de monitoreo, la gestión forense y la comunicación efectiva con las partes interesadas.

Tabla 10. Formulario para calificación de los controles definidos para la gestión de incidentes.

Control	CC	CP	NC	NA	Observaciones / Evidencia
Aprendizaje de incidentes pasados					
Respuesta a incidentes					
Gestión de incidentes en la nube					
Procesos claros de gestión de incidentes					

Alertas automatizadas					
Roles y responsabilidades claras					
Herramientas forenses					
Procedimientos de notificación y comunicación					
Gestión de fallos					

Nota. Esta tabla representa el formulario para la calificación del nivel de cumplimiento para los controles en cuanto a gestión de incidentes. Fuente: Elaboración propia.

2.4.2.5 Monitoreo de actividades

Supervisar en tiempo real las actividades en la infraestructura IaaS para detectar amenazas, anomalías o comportamientos sospechosos. Incluye la recopilación y análisis de logs, la implementación de SIEMs y la correlación de eventos de seguridad para una detección proactiva.

Tabla 11. Formulario para calificación de los controles definidos para el monitoreo de actividades.

Control	CC	CP	NC	NA	Observaciones / Evidencia
Monitoreo y detección de amenazas					
Monitoreo de seguridad física					
Gestión de la capacidad y rendimiento					
Registro y auditoría de eventos					
Monitoreo de operaciones y continuidad					
Monitoreo regulatorio y cumplimiento					
Monitoreo financiero y optimización de recursos					
Monitoreo centralizado y correlación de eventos					
Inteligencia de amenazas					

Nota. Esta tabla representa el formulario para la calificación del nivel de cumplimiento para los controles en cuanto a el monitoreo de actividades. Fuente: Elaboración propia.

2.4.2.6. Gestión de configuraciones

Definir, aplicar y mantener configuraciones seguras en la infraestructura IaaS y entornos híbridos. Incluye la gestión de cambios, la automatización de configuraciones seguras, la auditoría de configuraciones y la estandarización de entornos para reducir riesgos.

Tabla 12. Formulario para calificación de los controles definidos para la gestión de configuraciones.

Control	CC	CP	NC	NA	Observaciones / Evidencia
Definición de políticas y directrices para la gestión de configuraciones					
Gestión de configuraciones seguras en la infraestructura híbrida					
Gestión y control de cambios en la infraestructura híbrida					
Mantenimiento seguro de la infraestructura híbrida					
Gestión del ciclo de vida de los activos y aplicaciones en la nube					
Optimización y automatización de recursos en la nube híbrida					

Nota. Esta tabla representa el formulario para la calificación del nivel de cumplimiento para los controles en cuanto a la gestión de configuraciones. Fuente: Elaboración propia.

2.4.2.7. Continuidad y recuperación ante desastres

Establecer, probar y mantener mecanismos de continuidad operativa y recuperación ante desastres en entornos IaaS y nubes híbridas. Incluye la realización de respaldos periódicos, la replicación de datos entre nubes y sistemas on-premise, la ejecución de pruebas de recuperación documentadas y la implementación de un plan DRP, garantizando la disponibilidad de los servicios críticos ante incidentes o interrupciones mayores.

Tabla 13. Formulario para calificación de los controles definidos para la 2.4.2.7. Continuidad y recuperación ante desastres

Control	CC	CP	NC	NA	Observaciones / Evidencia
Realización de backups periódicos					
Pruebas de recuperación documentadas					

Replicación entre nubes y on-premise					
Existencia de un DRP					

Nota. Esta tabla representa el formulario para la calificación del nivel de cumplimiento para los controles en cuanto a la continuidad y recuperación ante desastres. Fuente: Elaboración propia.

3. Resultados

Para la evaluación del modelo ciberseguridad se realizó la validación en una empresa, la cual presta servicios a terceros, y en algunos casos proporciona soluciones cloud para facilitar la transformación de las empresas que solicitan sus servicios, por razones de confidencialidad, los datos específicos de dicha empresa y las empresas a las cuales presta sus servicios han sido reservados. No obstante, como evidencia de la veracidad de la evaluación, se incluye en el Anexo 2 el intercambio de correos que respalda el estudio realizado.

3.1 Caso de estudio para la evaluación del modelo

Como paso inicial para la evaluación de acuerdo al caso de estudio se solicitó la identificación de proyectos en los cuales la infraestructura de estos terceros se asemejaba a la infraestructura de referencia planteada en el ítem 2.1.5, y adicional se solicita una breve descripción y se caracterización las arquitecturas.

- **Proyecto 1 - Plataforma de ventas online**

Descripción: Proyecto dedicado a la venta de productos de tecnología mediante una plataforma e-commerce. Utiliza infraestructura en la nube para administrar su sistema de ventas, inventario y marketing.

Tabla 14. caracterización de la arquitectura.

Funcionalidad/Servicio	La arquitectura incluye el servicio (SI/NO)	Donde se despliega Nube/ On-premises	Proveedor/Fabricante
Computador	No		
Correo electrónico	SI	Nube	Microsoft 365
Internet	SI	On-premises	Tigo
Intranet	No		
Red local (LAN/WLAN)	SI	On-premises	Cisco

Software de administración	SI	Nube	Microsoft Dynamics 365 (EC2)
Software de ventas y marketing	SI	Nube	Linux (EC2)
Software específico	SI	Nube	Windows Server (EC2)
Balanceador	SI	Nube	AWS ALB
Sitio web	SI	Nube	Linux (EC2)
Base de datos	SI	Mixto	Amazon RDS/Oracle
Seguridad (firewall)	SI	Mixto	AWS WAF/Fortinet
Seguridad (Antivirus)	SI	Nube	Bitdefender
Directorio activo	SI	Mixto	Windows AD
Conexión nube- On-premises	SI	Nube	AWS Direct Connect
DNS	SI	Nube	AWS Route 53
Almacenamiento de datos	SI	Nube	AWS S3

Nota. Esta tabla representa la clasificación de la arquitectura para el primer proyecto evaluado en el caso de estudio. Fuente: Elaboración propia.

- **Proyecto 2 - Plataforma de servicios financieros**

Descripción: Proyecto que proporciona soluciones financieras a pymes, para facturación electrónica. Utiliza infraestructura híbrida con almacenamiento de datos en la nube y procesamiento local.

Tabla 15. Caracterización de la arquitectura.

Funcionalidad/Servicio	La arquitectura incluye el servicio (SI/NO)	Donde se despliega Nube/ On-premises	Proveedor/Fabricante
Computador	No		
Correo electrónico	SI	Nube	Microsoft 365
Internet	SI	On-premises	Tigo
Intranet	No		
Red local (LAN/WLAN)	SI	On-premises	Cisco
Software de administración	SI	Nube	SAP Business (EC2)
Software de ventas y marketing	SI	Nube	Windows Server (EC2)
Software específico	SI	Nube	Linux (EC2)
Balanceador	SI	Nube	AWS ALB
Sitio web	SI	Nube	Windows Server (EC2)
Base de datos	SI	Nube	Amazon RDS
Seguridad (firewall)	SI	Mixto	AWS WAF/Fortinet
Seguridad (Antivirus)	SI	Nube	Bitdefender
Directorio activo	SI	Mixto	Windows AD
Conexión nube- On-premises	SI	Nube	AWS Direct Connect

DNS	SI	Nube	AWS Route 53
Almacenamiento de datos	SI	Nube	AWS S3

Nota. Esta tabla representa la clasificación de la arquitectura para el segundo proyecto evaluado en el caso de estudio. Fuente: Elaboración propia.

- **Proyecto 3 - Aplicación de gestión empresarial**

Descripción: aplicación que permite a las empresas administrar sus procesos comerciales, incluyendo ventas, inventarios y contabilidad. Utiliza infraestructura en la nube con integraciones a sistemas on-premises.

Tabla 16. Caracterización de la arquitectura.

Funcionalidad/Servicio	La arquitectura incluye el servicio (SI/NO)	Donde se despliega Nube/ On-premises	Proveedor/Fabricante
Computador	No		
Correo electrónico	SI	Nube	Microsoft 365
Internet	SI	On-premises	Tigo
Intranet	SI	Nube	Linux (EC2)
Red local (LAN/WLAN)	SI	On-premises	Cisco
Software de administración	SI	Nube	SAP Business (EC2)
Software de ventas y marketing	SI	Nube	Windows Server (EC2)
Software específico	SI	Nube	Linux (EC2)
Balanceador	SI	Nube	AWS ALB
Sitio web	SI	Nube	Linux (EC2)
Base de datos	SI	Nube	Amazon RDS/Redshift

Seguridad (firewall)	SI	Mixto	AWS WAF/Palo Alto
Seguridad (Antivirus)	SI	Nube	Avast
Directorio activo	SI	Mixto	Windows AD
Conexión nube- On-premises	SI	Nube	AWS Direct Connect
DNS	SI	Nube	AWS Route 53
Almacenamiento de datos	SI	Nube	AWS S3

Nota. Esta tabla representa la clasificación de la arquitectura para el tercer proyecto evaluado en el caso de estudio. Fuente: Elaboración propia.

De acuerdo a la validación realizada por la empresa se identificaron múltiples proyectos cuyas arquitecturas presentaban similitudes con la infraestructura de referencia proporcionada, proyectos de los cuales solo se tomaron 3 para realizar el análisis de sus componentes a más detalle, este análisis permitió dar a conocer la importancia del modelo de ciberseguridad de acuerdo a los modelos y componentes de despliegue que se están siendo utilizado por las pequeñas y medianas empresas.

3.1.1 Evaluación del modelo de acuerdo al caso de estudio

La evaluación del cumplimiento del modelo propuesto se realizó con base en las políticas, normas y buenas prácticas de seguridad que estaban vigentes en la empresa en evaluación. Este proceso permitió verificar el grado de alineación del modelo con los requerimientos organizacionales y regulatorios que se tienen en la empresa, permitiendo identificar si las medidas de seguridad implementadas son efectivas para mitigar los riesgos identificados en la infraestructura como servicio (IaaS) dentro del entorno de nube híbrida.

Nota: La información para la evaluación del modelo se puede apreciar en el Anexo E.

Tabla 17. Cumplimiento para la gestión de accesos.

Control	CC	CP	NC	NA	Observaciones / Evidencia
Definición de roles y responsabilidades		X			Existen roles definidos, pero algunas áreas requieren mayor granularidad.
Segregación de deberes		X			En algunos entornos heredados no hay una adecuada segregación de funciones
Implementación de control de acceso		X			Se han implementado controles, pero aún hay sistemas con autenticación básica en proceso de mejora.
Gestión de identidades	X				Uso centralizado de IAM
Ciclo de vida permisos de acceso		X			Existen procesos definidos, pero en ocasiones los accesos no son revocados oportunamente.
Seguridad de accesos remotos		X			Se usa VPN con autenticación fuerte, pero se requiere monitoreo más efectivo.
Gestión de usuarios privilegiados	X				Se han implementado controles para cuentas privilegiadas con monitoreo de accesos.
Gestión de derechos de los titulares		X			Se gestionan los datos, pero no en un proceso autogestionado
Segregación de redes y ambientes	X				Se cuenta con la segregación

Nota. Esta tabla representa la calificación del nivel de cumplimiento de los controles para gestión de accesos definidos en el modelo. Fuente: Elaboración propia.

Tabla 18. Cumplimiento para la gestión de riesgos.

Control	CC	CP	NC	NA	Observaciones / Evidencia
Inventario de información y activos		X			Se mantiene un inventario de activos, pero no siempre actualizado.
Capacitación en seguridad	X				Existen capacitaciones periódicas obligatorias para todos los empleados.
Pruebas de seguridad en ambientes de desarrollo		X			Se cuenta con la definición de realizar pruebas de seguridad a todos los sistemas

Plan de seguridad del sistema	X				Existe un plan documentado, con revisiones periódicas.
Planificación de la seguridad de la información	X				Estamos basados en estándares internacionales
Evaluación de riesgos	X				Se evalúan y priorizan los riesgos
Evaluaciones de impacto en la privacidad	X				La información se clasifica y así mismo se evalúa
Consentimiento del titular	X				Se solicita
Planificación de la capacidad	X				Se monitorea y ajusta la capacidad según la demanda.
Gestión del riesgo	X				Controles establecidos con planes de mitigación definidos
Marco de gobierno	X				Marco basado en estándares de la industria.
Gestión de activos	X				Activos identificados y clasificados
Evaluación de la conformidad	X				Auditorías periódicas.
Simulaciones de desastres		X			Se realizan pruebas, pero no para todos activos
Mitigación de riesgos	X				Proceso documentado
Gestión de proveedores		X			En proceso de evaluación de todos los proveedores
Gestión de parches	X				Se realizan parchados de forma periódica

Nota. Esta tabla representa la calificación del nivel de cumplimiento de los controles para gestión de riesgos definidos en el modelo. Fuente: Elaboración propia.

Tabla 19. Cumplimiento para la protección de datos.

Control	CC	CP	NC	NA	Observaciones / Evidencia
Gestión de medios de almacenamiento	X				Proceso definido
Disposición segura de equipos	X				Proceso definido
Protección contra malware	X				Antivirus y EDR activos en todos los endpoints.
Prevención de fugas de datos		X			Implementado en entornos críticos, falta extenderlo a toda la organización.

Seguridad de redes	X				Firewalls y segmentación implementada.
Seguridad de servicios de red	X				Controles definidos
Uso de la criptografía		X			No se cumple para todo
Clasificación de la información		X			Se tiene el proceso, pero falta validación en cumplimiento
Retención y eliminación de datos		X			proceso definido
Validación de datos		X			proceso definido
Criptografía en la gestión de claves		X			proceso definido
Transmisión de información		X			proceso definido
Gestión de la seguridad de la información		X			proceso definido
Políticas de privacidad y transferencias de datos con terceros		X			proceso definido

Nota. Esta tabla representa la calificación del nivel de cumplimiento de los controles para la protección de datos definidos en el modelo. Fuente: Elaboración propia.

Tabla 20. Cumplimiento para la gestión de incidentes.

Control	CC	CP	NC	NA	Observaciones / Evidencia
Aprendizaje de incidentes pasados		X			Falta documentar algunos procesos
Respuesta a incidentes	X				proceso definido Y evaluado
Gestión de incidentes en la nube	X				Soporte de proveedor y equipos internos
Procesos claros de gestión de incidentes	X				proceso definido
Alertas automatizadas		X			Solo algunas
Roles y responsabilidades claras	X				
Herramientas forenses	X				
Procedimientos de notificación y comunicación	X				Definido
Gestión de fallos	X				

Nota. Esta tabla representa la calificación del nivel de cumplimiento de los controles para gestión de incidentes en el modelo. Fuente: Elaboración propia.

Tabla 21. Cumplimiento para el monitoreo de actividades.

Control	CC	CP	NC	NA	Observaciones / Evidencia
Monitoreo y detección de amenazas	X				SIEM

Monitoreo de seguridad física		X			responsabilidad compartida con terceros
Gestión de la capacidad y rendimiento		X			no está en todo
Registro y auditoría de eventos		X			Faltan casos de uso
Monitoreo de operaciones y continuidad		X			Proceso definido
Monitoreo regulatorio y cumplimiento		X			Proceso definido
Monitoreo financiero y optimización de recursos			X		se deben optimizar costos
Monitoreo centralizado y correlación de eventos		X			falta correlacionar más eventos
Inteligencia de amenazas		X			se tienen notificaciones automáticas del proveedor de servicios de nube y del antivirus corporativo, pendiente por formalizar un proceso sistemático de recolección, análisis y aplicación de inteligencia de amenazas que permita anticipar ataques o ajustar proactivamente las medidas de defensa.

Nota. Esta tabla representa la calificación del nivel de cumplimiento de los controles para el monitoreo de actividades definidos en el modelo. Fuente: Elaboración propia.

Tabla 22. Cumplimiento para la gestión de configuraciones.

Control	CC	CP	NC	NA	Observaciones / Evidencia
Definición de políticas y directrices para la gestión de configuraciones	X				Definidas y aplicadas.
Gestión de configuraciones seguras en la infraestructura híbrida		X			En proceso de automatizar
Gestión y control de cambios en la infraestructura híbrida	X				se tiene el seguimiento
Mantenimiento seguro de la infraestructura híbrida	X				
Gestión del ciclo de vida de los activos y aplicaciones en la nube		X			pendiente proceso en algunos recursos
Optimización y automatización de recursos en la nube híbrida			x		en proceso de automatización

Nota. Esta tabla representa la calificación del nivel de cumplimiento de los controles para gestión de configuraciones definidos en el modelo. Fuente: Elaboración propia.

Tabla 23. Cumplimiento para la continuidad y recuperación ante desastres.

Control	CC	CP	NC	NA	Observaciones / Evidencia
Realización de backups periódicos		x			Algunos componentes no tienen el Backup
Pruebas de recuperación documentadas		x			
Replicación entre nubes y on-premise	x				
Existencia de un DRP		x			Falta integrar planes de algunos componentes

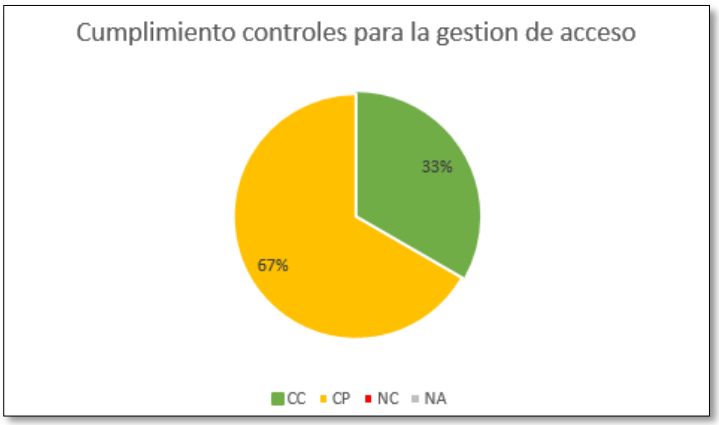
Nota. Esta tabla representa la calificación del nivel de cumplimiento de los controles para la continuidad y recuperación ante desastres definidos en el modelo. Fuente: Elaboración propia.

3.1.2 Porcentaje de cumplimiento del modelo

El porcentaje de cumplimiento del modelo refleja el grado en que los controles de seguridad definidos han sido implementados y se cumplen en la empresa. Esta métrica permite evaluar la efectividad del modelo de ciberseguridad propuesto y detectar áreas de mejora en la gestión de riesgos, accesos, incidentes y protección de datos dentro del entorno de nube híbrida.

En las Figuras 10 a la 16, se presenta la distribución del cumplimiento de los controles, clasificándolos en "CC", "CP", "NC" y "NA". Lo cual proporcionó una visión clara sobre los controles que requieren ajustes o refuerzos para garantizar un nivel de seguridad óptimo en la infraestructura evaluada.

Figura 10. Porcentaje de cumplimiento para controles de gestión de acceso.

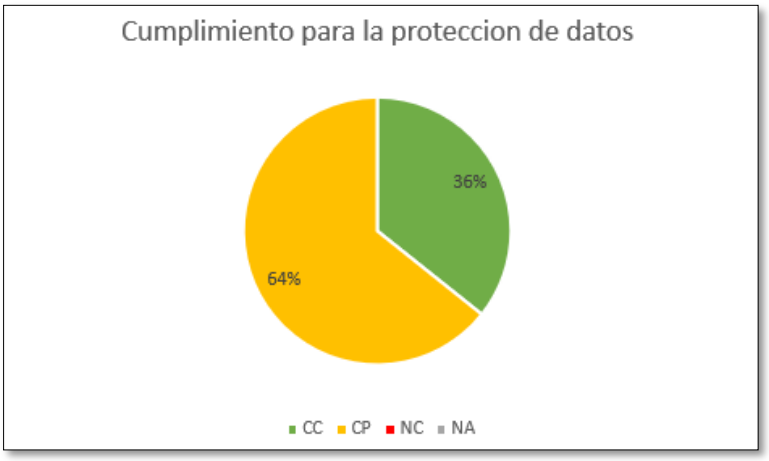


Nota. Esta figura representa el porcentaje de cumplimiento de controles para la gestión de accesos definido en el modelo. Fuente: elaboración propia.

Figura 11. Porcentaje de cumplimiento para controles de la gestión de riesgos.

Nota. Esta figura representa el porcentaje de cumplimiento de controles para la gestión de riesgos definido en el modelo. Fuente: elaboración propia.

Figura 12. Porcentaje de cumplimiento para controles de la protección de datos.

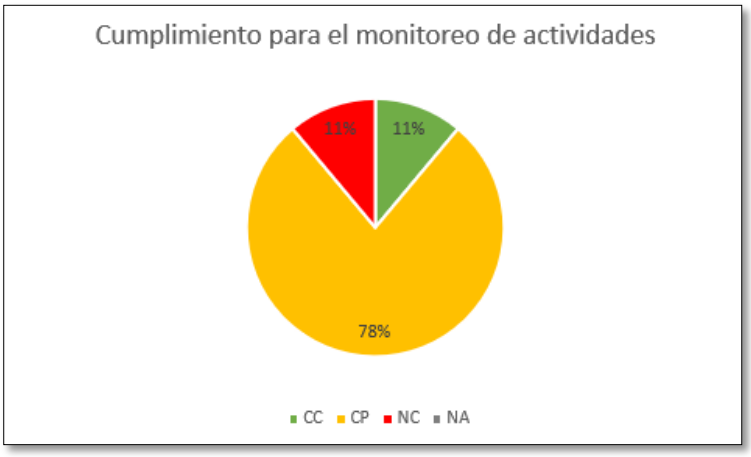


Nota. Esta figura representa el porcentaje de cumplimiento de controles para la protección de datos definido en el modelo. Fuente: elaboración propia.

Figura 13. Porcentaje de cumplimiento para controles de la gestión de incidentes.

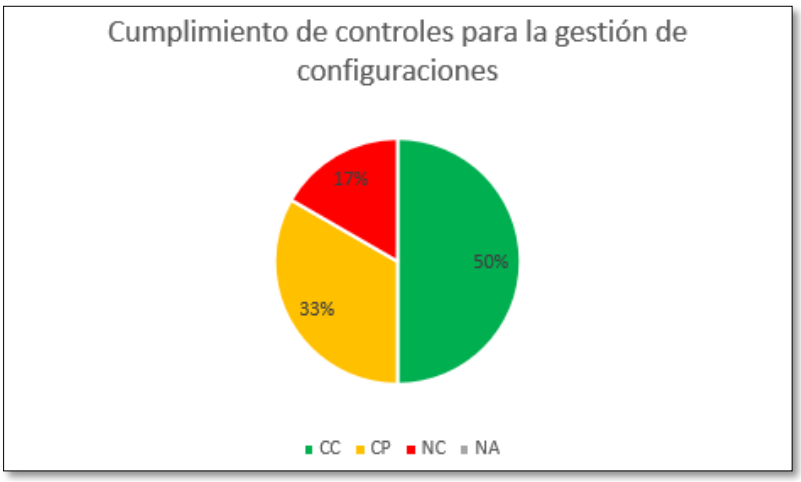
Nota. Esta figura representa el porcentaje de cumplimiento de controles para la gestión de incidentes definido en el modelo. Fuente: elaboración propia.

Figura 14. Cumplimiento de controles para el monitoreo de actividades.



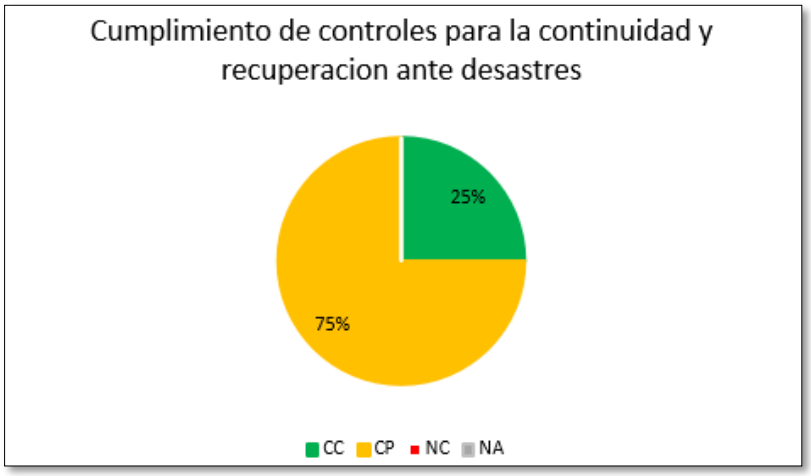
Nota. Esta figura representa el porcentaje de cumplimiento de controles para el monitoreo de actividades definido en el modelo. Fuente: elaboración propia.

Figura 15. Cumplimiento de controles para la gestión de configuraciones.



Nota. Esta figura representa el porcentaje de cumplimiento de controles para la gestión de configuraciones definido en el modelo. Fuente: elaboración propia.

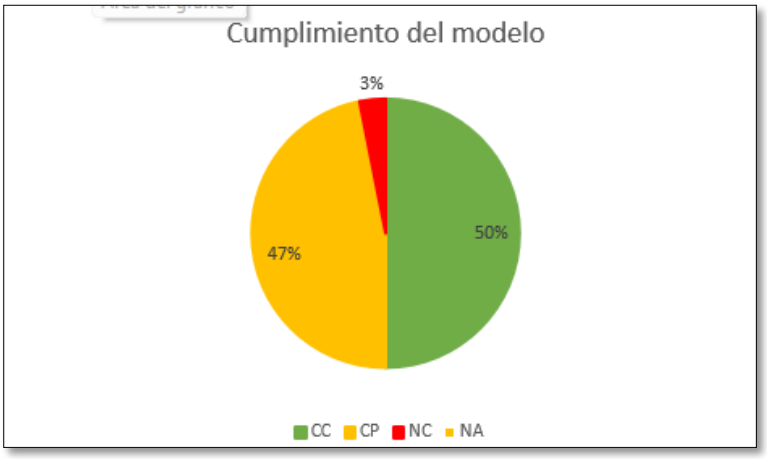
Figura 16. Cumplimiento de controles para la continuidad y recuperación ante desastres.



Nota. Esta figura representa el porcentaje de cumplimiento de controles para la continuidad y recuperación ante desastres definido en el modelo. Fuente: elaboración propia.

Adicional a la evaluación de cumplimento de controles de acuerdo los componentes del modelo, se realizó una evaluación a nivel general del cumplimiento del modelo según los datos entregados, y se puede apreciar en la figura 17.

Figura 17. Porcentaje general de cumplimiento del modelo.



Nota. Esta figura representa el porcentaje de cumplimiento de controles a nivel general definidos en todos los dominios del modelo. Fuente: elaboración propia.

Con este porcentaje se logró identificar que el 50% de los controles del modelo están siendo cumplidos por la empresa en el proyecto evaluado, el 47% están en cumple parcialmente y solo el 3% de los controles no cumplen.

3.1.2 Evaluación de riesgos de acuerdo a la ISO 27005

Para continuar con el estudio se entregaron los principales riesgos, a los cuales se pueden encuentran expuestos este tipo de infraestructuras, estos riesgos se definen en el Ítem 2.3, y se solicitó realizar la calificación del impacto tiempo, alcance y la probabilidad de ocurrencia de acuerdo a el contexto y conocimiento de la empresa, estos datos al ser 3 proyectos en los cuales se basan en las mismas políticas de seguridad, solo se realizó un análisis.

Según los datos entregados, se realizó la evaluación del riesgo de acuerdo a la probabilidad vs el impacto en el alcance la cual se puede apreciar en la tabla 24, y la probabilidad vs el impacto en tiempo que se puede apreciar en la tabla 25.

Tabla 24. Calificación de riesgos de acuerdo a el impacto en el alcance.

RIESGOS DEL PROYECTO	PROBABILIDAD		IMPACTO ALCANCE		Riesgo P*Impacto Probabilidad/Alcance
Acceso indebido a sistemas críticos mediante credenciales débiles o robadas.	Baja	2	Medio (0,20)	3	6
Explotación de fallas en interfaces o APIs para comprometer sistemas o extraer datos.	Baja	2	Medio (0,20)	3	6
Compromiso de cuentas de usuario por intentos automatizados de fuerza bruta.	Media	3	Medio (0,20)	3	9
Interrupción de servicios por sobrecarga maliciosa de tráfico (DDoS).	Baja	2	Medio (0,20)	3	6
Exposición de recursos sensibles por configuraciones erróneas o permisos inadecuados.	Baja	2	Medio (0,20)	3	6
Acceso no autorizado por uso de contraseñas débiles, compartidas o mal gestionadas.	Baja	2	Alto (0,40)	4	8
Elevación ilegítima de privilegios por fallos en el control de accesos.	Media	3	Alto (0,40)	4	12
Acceso no autorizado debido a errores en los mecanismos de autenticación.	Muy Baja	1	Bajo (0,10)	2	2
Exposición de información en tránsito por interceptación en canales no cifrados.	Baja	2	Medio (0,20)	3	6
Alteración maliciosa de comunicaciones entre componentes o sistemas conectados.	Baja	2	Medio (0,20)	3	6
Pérdida o filtración de datos sensibles durante la transferencia entre nubes.	Media	3	Alto (0,40)	4	12
Pérdida de información por fallos en la replicación o sincronización entre entornos.	Baja	2	Bajo (0,10)	2	4
Compromiso del sistema mediante la inyección de código malicioso en aplicaciones.	Muy Baja	1	Bajo (0,10)	2	2
Exposición pública de datos críticos por errores de configuración o falta de control.	Muy Baja	1	Alto (0,40)	4	4
Incidentes de seguridad causados por políticas débiles o mal implementadas.	Baja	2	Medio (0,20)	3	6

Nota. Esta tabla representa la calificación de los riesgos de acuerdo a la probabilidad y el impacto en el alcance. Fuente: Elaboración propia.

De acuerdo a los datos entregados en la tabla 24, se obtuvo el siguiente análisis para cada riesgo:

- **Acceso indebido a sistemas críticos mediante credenciales débiles o robadas:** Tiene una probabilidad baja (2), debido a la implementación de controles de acceso y gestión de identidades en la empresa. Sin embargo, sigue existiendo la posibilidad de que credenciales sean comprometidas. El impacto en el alcance es medio (3), ya que, aunque puede permitir accesos no autorizados, las capas adicionales de seguridad mitigan el riesgo de afectar sistemas críticos. Su riesgo total es 6, por lo que se considera una amenaza moderada

- **Explotación de fallas en interfaces o APIs para comprometer sistemas o extraer datos:** Tiene una probabilidad baja (2), ya que la empresa ha reforzado las pruebas de seguridad en desarrollo y aceptación. Aun así, persisten riesgos en configuraciones inadecuadas o software desactualizado. El impacto en el alcance es medio (3), pues una vulnerabilidad explotada puede comprometer los servicios que interactúan mediante las interfaces expuestas. Su riesgo total es 6, lo que indica un riesgo bajo a moderado.

- **Compromiso de cuentas de usuario por intentos automatizados de fuerza bruta:** Tiene una probabilidad media (3), ya que estos ataques siguen siendo recurrentes en sistemas accesibles por la red, aunque la empresa ha implementado controles para mitigarlos. El impacto en el alcance es medio (3), ya que generalmente afectan cuentas individuales o servicios específicos, sin comprometer toda la infraestructura. Su riesgo total es 9, lo que lo ubica en un nivel de riesgo moderado.

- **Interrupción de servicios por sobrecarga maliciosa de tráfico (DDoS):** Tiene una probabilidad baja (2), ya que la empresa ha implementado estrategias de mitigación y monitoreo para detectar y responder a estos ataques. El impacto en el alcance es medio (3), dado que un ataque DDoS podría afectar la disponibilidad de algunos servicios, aunque las medidas de respuesta ayudan a minimizar el tiempo de afectación. Su riesgo total es 6, considerándose una amenaza controlable.

- **Exposición de recursos sensibles por configuraciones erróneas o permisos inadecuados:** Tiene una probabilidad baja (2), ya que los controles de configuración segura y revisión de roles han reducido el riesgo de parametrizaciones incorrectas. El impacto en el alcance es

medio (3), pues un acceso indebido a ciertos recursos puede exponer información o generar cambios en configuraciones críticas. Su riesgo total es 6, lo que indica un nivel de riesgo bajo.

- **Acceso no autorizado por uso de contraseñas débiles, compartidas o mal gestionadas:** Tiene una probabilidad baja (2), debido a la implementación de políticas de contraseñas y autenticación multifactor en la organización. El impacto en el alcance es alto (4), ya que, si ocurre, puede facilitar el acceso no autorizado y comprometer cuentas críticas. Su riesgo total es 8, ubicándose en un nivel de riesgo moderado.

- **Elevación ilegítima de privilegios por fallos en el control de accesos:** Tiene una probabilidad media (3), ya que, aunque la gestión de accesos restringidos está en funcionamiento, pueden existir configuraciones erróneas que permitan elevar privilegios. El impacto en el alcance es alto (4), pues este tipo de ataque puede comprometer sistemas enteros y permitir movimientos laterales dentro de la red. Su riesgo total es 12, lo que lo hace un riesgo significativo que requiere monitoreo continuo.

- **Acceso no autorizado debido a errores en los mecanismos de autenticación:** Tiene una probabilidad muy baja (1), ya que la autenticación fuerte y los controles de acceso minimizan este tipo de fallos. El impacto en el alcance es bajo (2), pues, aunque podría permitir accesos indebidos, los mecanismos de detección y respuesta ayudan a mitigarlo. Su riesgo total es 2, considerándose un riesgo mínimo.

- **Exposición de información en tránsito por interceptación en canales no cifrados:** Tiene una probabilidad baja (2), debido al uso de cifrado en tránsito y redes seguras dentro de la organización. El impacto en el alcance es medio (3), ya que, si ocurre, puede comprometer la confidencialidad de la información sensible. Su riesgo total es 6, por lo que se mantiene en un nivel bajo de amenaza.

- **Alteración maliciosa de comunicaciones entre componentes o sistemas conectados:** Tiene una probabilidad baja (2), debido a la protección de los canales de comunicación y la

implementación de controles criptográficos. El impacto en el alcance es medio (3), ya que podría afectar la integridad de los mensajes y las interacciones entre sistemas. Su riesgo total es 6, ubicándose en un nivel bajo.

- **Pérdida o filtración de datos sensibles durante la transferencia entre nubes:** Tiene una probabilidad media (3), ya que aún existen riesgos asociados a configuraciones inadecuadas y la exposición de datos en tránsito. El impacto en el alcance es alto (4), pues la fuga de información podría comprometer datos sensibles y generar repercusiones legales y operativas. Su riesgo total es 12, lo que indica un nivel significativo de riesgo.

- **Pérdida de información por fallos en la replicación o sincronización entre entornos:** Tiene una probabilidad baja (2), ya que los sistemas cuentan con mecanismos de respaldo y redundancia para evitar pérdidas de información. El impacto en el alcance es bajo (2), pues la afectación generalmente es limitada a copias de datos específicas. Su riesgo total es 4, considerándose un riesgo bajo.

- **Compromiso del sistema mediante la inyección de código malicioso en aplicaciones:** Tiene una probabilidad muy baja (1), debido a las pruebas de seguridad en desarrollo y protección contra malware implementadas en la empresa. El impacto en el alcance es bajo (2), ya que los sistemas cuentan con mecanismos de detección y respuesta ante código malicioso. Su riesgo total es 2, siendo una amenaza controlada.

- **Exposición pública de datos críticos por errores de configuración o falta de control:** Tiene una probabilidad muy baja (1), ya que la clasificación y protección de información sensible está bien definida dentro de la organización. El impacto en el alcance es alto (4), pues si ocurre, puede generar consecuencias graves en términos de confidencialidad y cumplimiento normativo. Su riesgo total es 4, manteniéndose en un nivel bajo.

- **Incidentes de seguridad causados por políticas débiles o mal implementadas:** Tiene una probabilidad baja (2), debido a la existencia de políticas documentadas y auditorías regulares. El impacto en el alcance es medio (3), ya que una política deficiente podría

exponer múltiples activos al riesgo. Su riesgo total es 6, ubicándose en un nivel bajo a moderado.

Tabla 25. Calificación de riesgos de acuerdo a el impacto en el tiempo.

RIESGOS DEL PROYECTO	PROBABILIDAD		IMPACTO TIEMPO		Riesgo P*Impacto Probabilidad/Tiempo
Acceso indebido a sistemas críticos mediante credenciales débiles o robadas.	Baja	2	Medio (0,20)	3	6
Explotación de fallas en interfaces o APIs para comprometer sistemas o extraer datos.	Baja	2	Bajo (0,10)	2	4
Compromiso de cuentas de usuario por intentos automatizados de fuerza bruta.	Media	3	Bajo (0,10)	2	6
Interrupción de servicios por sobrecarga maliciosa de tráfico (DDoS).	Baja	2	Medio (0,20)	3	6
Exposición de recursos sensibles por configuraciones erróneas o permisos inadecuados.	Baja	2	Medio (0,20)	3	6
Acceso no autorizado por uso de contraseñas débiles, compartidas o mal gestionadas.	Baja	2	Alto (0,40)	4	8
Elevación ilegítima de privilegios por fallos en el control de accesos.	Media	3	Alto (0,40)	4	12
Acceso no autorizado debido a errores en los mecanismos de autenticación.	Muy Baja	1	Bajo (0,10)	2	2
Exposición de información en tránsito por interceptación en canales no cifrados.	Baja	2	Alto (0,40)	4	8
Alteración maliciosa de comunicaciones entre componentes o sistemas conectados.	Baja	2	Medio (0,20)	3	6
Pérdida o filtración de datos sensibles durante la transferencia entre nubes.	Media	3	Alto (0,40)	4	12
Pérdida de información por fallos en la replicación o sincronización entre entornos.	Baja	2	Bajo (0,10)	2	4
Compromiso del sistema mediante la inyección de código malicioso en aplicaciones.	Muy Baja	1	Bajo (0,10)	2	2
Exposición pública de datos críticos por errores de configuración o falta de control.	Muy Baja	1	Alto (0,40)	4	4
Incidentes de seguridad causados por políticas débiles o mal implementadas.	Baja	2	Medio (0,20)	3	6

Nota. Esta tabla representa la calificación de los riesgos de acuerdo a la probabilidad y el impacto en el tiempo. Fuente: Elaboración propia.

De acuerdo a los datos entregados en la tabla 25, se obtuvo el siguiente análisis para cada riesgo:

- **Acceso indebido a sistemas críticos mediante credenciales débiles o robadas:** Tiene una probabilidad baja (2), lo cual puede darse debido a la implementación de controles de acceso y gestión de identidades en la empresa. Sin embargo, sigue existiendo la posibilidad de que las credenciales sean comprometidas. El impacto en el alcance es medio (3), ya que, aunque puede permitir accesos no autorizados, las capas adicionales de seguridad mitigan el riesgo de afectar sistemas críticos. Su riesgo total es 6, por lo que se considera una amenaza moderada, pero manejable.

- **Explotación de fallas en interfaces o APIs para comprometer sistemas o extraer datos:** Tiene una probabilidad baja (2), ya que las pruebas de seguridad en desarrollo han reducido significativamente este riesgo. El impacto en el tiempo es bajo (2), pues una vulnerabilidad detectada y explotada puede ser mitigada rápidamente con parches y actualizaciones. Su riesgo total es 4, lo que indica un nivel de riesgo bajo.

- **Compromiso de cuentas de usuario por intentos automatizados de fuerza bruta:** Tiene una probabilidad media (3), ya que estos ataques siguen siendo comunes en sistemas expuestos a internet. El impacto en el tiempo es bajo (2), ya que la detección y bloqueo automático mediante herramientas de seguridad disminuye su efecto. Su riesgo total es 6, clasificándose como moderado.

- **Interrupción de servicios por sobrecarga maliciosa de tráfico (DDoS):** Tiene una probabilidad baja (2), gracias a la implementación de soluciones de mitigación de tráfico malicioso. El impacto en el tiempo es medio (3), pues una interrupción en el servicio podría afectar la disponibilidad por un periodo significativo. Su riesgo total es 6, ubicándose en un nivel bajo a moderado.

- **Exposición de recursos sensibles por configuraciones erróneas o permisos inadecuados:** Tiene una probabilidad baja (2), debido a la mejora en la configuración de seguridad y revisiones periódicas. El impacto en el tiempo es medio (3), ya que una mala configuración puede requerir tiempo para su corrección sin afectar de inmediato la operación. Su riesgo total es 6, siendo un riesgo bajo a moderado.

- **Acceso no autorizado por uso de contraseñas débiles, compartidas o mal gestionadas:** Tiene una probabilidad baja (2), ya que la empresa ha implementado políticas de seguridad en la gestión de contraseñas. El impacto en el tiempo es alto (4), pues un incidente de contraseñas comprometidas podría tardar en resolverse, afectando múltiples cuentas y sistemas. Su riesgo total es 8, considerándose moderado.

- **Elevación ilegítima de privilegios por fallos en el control de accesos:** Tiene una probabilidad media (3), ya que, aunque existen controles, aún hay riesgos en entornos mal configurados. El impacto en el tiempo es alto (4), debido a que una escalación de privilegios exitosa puede permitir un acceso extendido sin detección inmediata. Su riesgo total es 12, siendo un riesgo significativo que requiere monitoreo.
- **Acceso no autorizado debido a errores en los mecanismos de autenticación:** Tiene una probabilidad muy baja (1), ya que los mecanismos de autenticación están bien implementados y monitoreados. El impacto en el tiempo es bajo (2), dado que un fallo en autenticación suele detectarse y corregirse rápidamente. Su riesgo total es 2, considerándose un riesgo mínimo.

- **Exposición de información en tránsito por interceptación en canales no cifrados:** Tiene una probabilidad baja (2), ya que los protocolos de cifrado en la organización protegen la información en tránsito. El impacto en el tiempo es alto (4), porque una brecha de datos podría tardar en detectarse y mitigar su impacto. Su riesgo total es 8, clasificándose como moderado.

- **Alteración maliciosa de comunicaciones entre componentes o sistemas conectados:** Tiene una probabilidad baja (2), ya que el uso de protocolos seguros minimiza el riesgo de ataques "man-in-the-middle". El impacto en el tiempo es medio (3), ya que, si ocurre, puede afectar la

comunicación interna de la organización y requerir una investigación. Su riesgo total es 6, manteniéndose en un nivel bajo a moderado.

- **Pérdida o filtración de datos sensibles durante la transferencia entre nubes:** Tiene una probabilidad media (3), ya que sigue existiendo un riesgo en la transferencia de datos entre entornos. El impacto en el tiempo es alto (4), pues una fuga de información podría generar problemas de cumplimiento normativo y sanciones. Su riesgo total es 12, lo que lo clasifica como un riesgo significativo.

- **Pérdida de información por fallos en la replicación o sincronización entre entornos:** Tiene una probabilidad baja (2), ya que se han implementado respaldos y redundancias. El impacto en el tiempo es bajo (2), ya que las copias de seguridad pueden restaurar los datos sin afectar demasiado la operación. Su riesgo total es 4, ubicándose en un nivel bajo.

- **Compromiso del sistema mediante la inyección de código malicioso en aplicaciones:** Tiene una probabilidad muy baja (1), debido a las prácticas de desarrollo seguro y pruebas de seguridad implementadas. El impacto en el tiempo es bajo (2), ya que los sistemas tienen detección y respuesta ante este tipo de ataques. Su riesgo total es 2, considerándose una amenaza menor.

- **Exposición pública de datos críticos por errores de configuración o falta de control:** Tiene una probabilidad muy baja (1), ya que existen políticas de clasificación y protección de datos sensibles. El impacto en el tiempo es alto (4), pues si ocurre, puede traer consecuencias regulatorias y de reputación para la organización. Su riesgo total es 4, manteniéndose en un nivel bajo.

- **Incidentes de seguridad causados por políticas débiles o mal implementadas:** Tiene una probabilidad baja (2), ya que las auditorías periódicas ayudan a mantener las políticas actualizadas. El impacto en el tiempo es medio (3), pues una política deficiente podría generar

retrasos en la implementación de medidas de seguridad efectivas. Su riesgo total es 6, clasificándose como un riesgo bajo a moderado.

3.1.3 Identificación de controles para mitigar los riesgos

Después de identificar los riegos, se definieron los posibles controles para mitigar el impacto en alcance y tiempo, de acuerdo a los controles identificados en el modelo planteados en el ítem 2.4.1, y se plasman en la tabla 26.

Tabla 26. Identificación de controles para mitigar los riesgos.

RIESGOS	Controles IMPACTO ALCANCE	Controles IMPACTO TIEMPO
Acceso indebido a sistemas críticos mediante credenciales débiles o robadas.	• Implementación de control de acceso • Gestión de identidades • Seguridad de accesos remotos • Gestión de usuarios privilegiados	• Autenticación multifactor (MFA) Registro y auditoría de eventos • Monitoreo y detección de amenazas
Explotación de fallas en interfaces o APIs para comprometer sistemas o extraer datos.	• Pruebas de seguridad en desarrollo y aceptación • Gestión del riesgo Evaluación de conformidad	• Gestión de parches • Protección contra malware • Mitigación de riesgos
Compromiso de cuentas de usuario por intentos automatizados de fuerza bruta.	• Implementación de control de acceso • Seguridad de accesos remotos	• Alertas automatizadas • Registro y auditoría de eventos • Herramientas forenses

	Gestión de usuarios privilegiados	
Interrupción de servicios por sobrecarga maliciosa de tráfico (DDoS).	• Seguridad de redes • Seguridad de servicios de red • Uso de la criptografía	• Monitoreo y detección de amenazas • Gestión de la capacidad y rendimiento • Planificación de la capacidad
Exposición de recursos sensibles por configuraciones erróneas o permisos inadecuados.	• Gestión de configuraciones seguras en la infraestructura híbrida • Definición de roles y responsabilidades • Evaluación de riesgos	• Monitoreo centralizado y correlación de eventos • Gestión y control de cambios en la infraestructura híbrida
Acceso no autorizado por uso de contraseñas débiles, compartidas o mal gestionadas.	• Gestión de identidades • Ciclo de vida de permisos de acceso • Seguridad de accesos remotos	• Capacitación en seguridad • Políticas de privacidad y transferencias de datos con terceros
Elevación ilegítima de privilegios por fallos en el control de accesos.	• Gestión de usuarios privilegiados • Implementación de control de acceso • Gestión de la seguridad de la información	• Registro y auditoría de eventos • Alertas automatizadas
Acceso no autorizado debido a errores en los mecanismos de autenticación.	• Definición de roles y responsabilidades • Gestión de identidades	• Respuesta a incidentes • Procedimientos de notificación y comunicación

	• Gestión de usuarios privilegiados	
Exposición de información en tránsito por interceptación en canales no cifrados.	• Uso de la criptografía • Transmisión de información de control • Seguridad de redes	• Monitoreo de seguridad física • Mitigación de riesgos
Alteración maliciosa de comunicaciones entre componentes o sistemas conectados.	• Seguridad de servicios de red • Uso de la criptografía • Implementación de control de acceso	• Monitoreo regulatorio y cumplimiento • Gestión de incidentes en la nube
Pérdida o filtración de datos sensibles durante la transferencia entre nubes.	• Políticas de privacidad y transferencias de datos con terceros • Clasificación de la información • Uso de la criptografía	• Registro y auditoría de eventos • Validación de datos
Pérdida de información por fallos en la replicación o sincronización entre entornos.	• Gestión del ciclo de vida de los activos y aplicaciones en la nube • Planificación de la capacidad • Gestión del riesgo	• Simulaciones de desastres • Mitigación de riesgos
Compromiso del sistema mediante la inyección de código malicioso en aplicaciones.	• Pruebas de seguridad en ambientes de desarrollo • Protección contra malware • Evaluación de riesgos	• Respuesta a incidentes • Gestión de parches
Exposición pública de datos críticos por errores de configuración o falta de control.	• Políticas de privacidad y transferencias de datos con terceros	• Evaluaciones de impacto en la privacidad

	Clasificación de la información Retención y eliminación de datos	• Monitoreo de operaciones y continuidad
Incidentes de seguridad causados por políticas débiles o mal implementadas.	• Definición de políticas y directrices para la gestión de configuraciones • Evaluación de conformidad • Gestión del riesgo	• Monitoreo regulatorio y cumplimiento • Definición de políticas y directrices para la gestión de configuraciones

Nota. Esta tabla representa los controles definidos en el modelo que ayudan a mitigar los riesgos identificados. Fuente: Elaboración propia.

3.1.4 Cumplimiento de controles del modelo definidos para mitigar los riesgos de seguridad identificados

A partir de la evaluación del cumplimiento del modelo, se determinó el nivel de adopción de la empresa de acuerdo a los controles definidos en el modelo para mitigar los riesgos de seguridad identificados, tanto en el impacto alcance como en el impacto tiempo, todo el detalle del proceso de calificación del cumplimiento se puede apreciar en el anexo C, y en la tabla 27 se consolidan los porcentajes.

Tabla 27. Cumplimiento de controles de acuerdo al modelo para mitigar riesgos identificados.

Riesgos	Controles para mitigar los riesgos en el impacto alcance de acuerdo al modelo	Porcentaje de cumplimiento de acuerdo al modelo	Controles para mitigar los riesgos en el impacto Tiempo de acuerdo al modelo	Porcentaje de cumplimiento de acuerdo al modelo
Acceso indebido a sistemas críticos mediante credenciales débiles o robadas.	Implementación de control de acceso	66,6%	Registro y auditoría de eventos	75%
	Ciclo de vida permisos de acceso		Monitoreo y detección de amenazas	
	Segregación de redes y ambientes			

Explotación de fallas en interfaces o APIs para comprometer sistemas o extraer datos.	Seguridad de redes	66,6%	Monitoreo y detección de amenazas	75,0%
	Validación de datos		Alertas automatizadas	
	Gestión de configuraciones seguras en la infraestructura híbrida			
Compromiso de cuentas de usuario por intentos automatizados de fuerza bruta.	Implementación de control de acceso	66,6%	Alertas automatizadas	66,6%
	Seguridad de accesos remotos		Registro y auditoría de eventos	
	Gestión de usuarios privilegiados		Herramientas forenses	
Interrupción de servicios por sobrecarga maliciosa de tráfico (DDoS).	Seguridad de redes	83,3%	Monitoreo y detección de amenazas	83,3%
	Seguridad de servicios de red		Gestión de la capacidad y rendimiento	
	Uso de la criptografía		Planificación de la capacidad	
Exposición de recursos sensibles por configuraciones erróneas o permisos inadecuados.	Gestión de configuraciones seguras en la infraestructura híbrida	66,6%	Monitoreo centralizado y correlación de eventos	75%
	Definición de roles y responsabilidades		Gestión y control de cambios en la infraestructura híbrida	
	Evaluación de riesgos			
Acceso no autorizado por uso de contraseñas débiles, compartidas o mal gestionadas.	Gestión de identidades	66,6%	Capacitación en seguridad	75,0%
	Ciclo de vida de permisos de acceso		Políticas de privacidad y transferencias de datos con terceros	
	Seguridad de accesos remotos			

Elevación ilegítima de privilegios por fallos en el control de accesos.	Gestión de usuarios privilegiados	66,6%	Registro y auditoría de eventos	50,0%
	Implementación de control de acceso		Alertas automatizadas	
	Gestión de la seguridad de la información			
Acceso no autorizado debido a errores en los mecanismos de autenticación.	Definición de roles y responsabilidades	83,3%	Respuesta a incidentes	100,0%
	Gestión de identidades		Procedimientos de notificación y comunicación	
	Gestión de usuarios privilegiados			
Exposición de información en tránsito por interceptación en canales no cifrados.	Uso de la criptografía	66,6%	Monitoreo de seguridad física	75,0%
	Transmisión de información		Mitigación de riesgos	
	Seguridad de redes			
Alteración maliciosa de comunicaciones entre componentes o sistemas conectados.	Seguridad de servicios de red	66,6%	Monitoreo regulatorio y cumplimiento	75,0%
	Uso de la criptografía		Gestión de incidentes en la nube	
	Implementación de control de acceso			
Pérdida o filtración de datos sensibles durante la transferencia entre nubes.	Políticas de privacidad y transferencias de datos con terceros	50,0%	Registro y auditoría de eventos	50,0%
	Clasificación de la información		Validación de datos	
	Uso de la criptografía			
Pérdida de información por fallos en la replicación o sincronización entre entornos.	Gestión del ciclo de vida de los activos y aplicaciones en la nube	83,3%	Simulaciones de desastres	75%
	Planificación de la capacidad		Mitigación de riesgos	
	Gestión del riesgo			

Compromiso del sistema mediante la inyección de código malicioso en aplicaciones.	Pruebas de seguridad en desarrollo y aceptación	83,3%	Respuesta a incidentes	100,0%
	Protección contra malware		Gestión de parches	
	Evaluación de riesgos			
Exposición pública de datos críticos por errores de configuración o falta de control.	Políticas de privacidad y transferencias de datos con terceros	100%	Evaluaciones de impacto en la privacidad	75%
	Clasificación de la información		Monitoreo de operaciones y continuidad	
	Retención y eliminación de datos			
Incidentes de seguridad causados por políticas débiles o mal implementadas.	Definición de políticas y directrices para la gestión de configuraciones	100,0%	Monitoreo regulatorio y cumplimiento	75,0%
	Evaluación de conformidad		Definición de políticas y directrices para la gestión de configuraciones	
	Gestión del riesgo			

Nota. Esta tabla representa el porcentaje de cumplimiento de los controles identificados para mitigar los riesgos de acuerdo a el caso de estudio. Fuente: Elaboración propia.

Nota: Para ver todo el detalle del cumplimiento de controles y la identificación del porcentaje de cumplimiento ver el Anexo C.

3.1.5 Matriz de riesgos de acuerdo a la ISO 27005

Para realizar el análisis de los riesgos, se realizó la calificación de los riesgos de acuerdo a su probabilidad de ocurrencia vs el impacto en el alcance y en el tiempo, adicional los riesgos fueron categorizados en diferentes niveles de impacto (de muy bajo a muy alto) y probabilidad (de muy baja a muy alta), según el proceso definido en la norma ISO27005

3.1.3.1. Matriz de riesgos de probabilidad vs el impacto en el alcance

De acuerdo a la matriz generada mediante la ISO27005, la cual se puede apreciar en la tabla 28, muestra una matriz de aceptabilidad que clasifica los riesgos de acuerdo a su impacto negativo frente al alcance y su probabilidad.

Tabla 28. Matriz de aceptabilidad Impacto alcance vs probabilidad, evaluado mediante ISO27005.

Probabilidad		**IMPACTO NEGATIVO ALCANCE**				
	valor	Muy bajo (0,05)	Bajo (0,10)	Medio (0,20)	Alto (0,4)	Muy Alto (0,80)
		1	**2**	**3**	**4**	**5**
Muy Alta	**5**					
Alta	**4**					
Media	**3**			**Compromiso de cuentas de usuario por intentos automatizados de fuerza bruta. ||**	**Elevación ilegítima de privilegios por fallos en el control de accesos. || Pérdida o filtración de datos sensibles durante la transferencia entre nubes. ||**	

Baja	**2**		**Pérdida de información por fallos en la replicación o sincronización entre entornos. ||**	**Acceso indebido a sistemas críticos mediante credenciales débiles o robadas. || Explotación de fallas en interfaces o APIs para comprometer sistemas o extraer datos. || Interrupción de servicios por sobrecarga maliciosa de tráfico (DDoS). || Exposición de recursos sensibles por configuraciones erróneas o permisos inadecuados. || Exposición de información en tránsito por interceptación en canales no cifrados. || Alteración maliciosa de comunicaciones entre componentes o sistemas conectados. || Incidentes de seguridad causados por políticas débiles o mal implementadas. ||**	**Acceso no autorizado por uso de contraseñas débiles, compartidas o mal gestionadas. ||**	
Muy Baja	**1**		**Acceso no autorizado debido a errores en los mecanismos de autenticación. || Compromiso del sistema mediante la inyección de código malicioso en aplicaciones. ||**		**Exposición pública de datos críticos por errores de configuración o falta de control. ||**	

Nota. Esta tabla representa la matriz de aceptabilidad en cuanto a el impacto sobre el alcance vs la probabilidad. Fuente: Elaboración propia.

De acuerdo a la matriz se identifican los siguientes aspectos:

- **En probabilidad media (3),** se identifican los siguientes riesgos y sus impactos:
  - Impacto en alcance medio (3): Compromiso de cuentas de usuario por intentos automatizados de fuerza bruta, elevación ilegítima de privilegios por fallos en el control de accesos, pérdida o filtración de datos sensibles durante la transferencia entre nubes.

- Posible impacto: Los ataques de fuerza bruta pueden vulnerar credenciales débiles o mal gestionadas, lo que permitiría accesos no autorizados a sistemas críticos. El escalamiento de privilegios podría otorgar acceso extendido a atacantes si logran explotar errores en la configuración de permisos. La fuga de información en la nube híbrida puede comprometer datos confidenciales si no se implementan controles adecuados de cifrado y segmentación de tráfico, estos riesgos presentan una probabilidad moderada de ocurrencia y pueden comprometer la seguridad de la organización en diferentes niveles, no obstante, requieren monitoreo constante, endurecimiento de credenciales y refuerzo en la seguridad de las transferencias de datos en entornos híbridos.

- **En probabilidad baja (2),** se identifican los siguientes riesgos y sus impactos:
  - Impacto en alcance bajo (2): Pérdida de información por fallos en la replicación o sincronización entre entornos.

    Posible impacto: Si se materializa este tipo de riesgos, puede afectar la disponibilidad de la información, causando interrupciones operativas, este riesgo tiene una baja probabilidad de ocurrencia debido a la existencia de copias de seguridad y redundancia en los sistemas.

  - Impacto en alcance medio (3): Acceso indebido a sistemas críticos mediante credenciales débiles o robadas, explotación de fallas en interfaces o APIs para comprometer sistemas o extraer datos, interrupción de servicios por sobrecarga maliciosa de tráfico (DDoS), exposición de recursos sensibles por configuraciones erróneas o permisos inadecuados, exposición de información en tránsito por interceptación en canales no cifrados, Alteración maliciosa de comunicaciones entre componentes o sistemas conectados, incidentes de seguridad causados por políticas débiles o mal implementadas, acceso no autorizado por uso de contraseñas débiles, compartidas o mal gestionadas.

    Posible impacto: El acceso no autorizado y la explotación de vulnerabilidades en interfaces pueden exponer información crítica si existen fallos en la autenticación o configuración de accesos. Los ataques DDoS pueden afectar la disponibilidad de los sistemas, aunque existen mecanismos de mitigación en la infraestructura de red. La mala gestión de contraseñas y

accesos indebidos puede facilitar ataques de ingeniería social o el acceso no autorizado a sistemas internos, estos riesgos presentan una baja probabilidad de ocurrencia gracias a la existencia de controles de seguridad, pero aún pueden comprometer la organización si se materializa, por lo tanto requieren auditorías periódicas en configuraciones de seguridad, que permitan el fortalecimiento de la autenticación y la segmentación de redes para minimizar sus impactos.

- **En probabilidad muy baja (1),** se identifican los siguientes riesgos y sus impactos:
  - Impacto en alcance bajo (2): Acceso no autorizado debido a errores en los mecanismos de autenticación, compromiso del sistema mediante la inyección de código malicioso en aplicaciones.

    Posible impacto: Si se materializan fallos en la autenticación, se puede llegar a permitir accesos no autorizados a sistemas críticos, comprometiendo la confidencialidad y la integridad de la información, por otro laso si logran aprovecharse de la inyección de código malicioso, se puede presentar una ejecución de código no autorizado en aplicaciones vulnerables, lo que podría derivar en la manipulación de datos, robo de información o toma de control del sistema, y aunque la probabilidad de ocurrencia y el alcance es bajo debido a los controles implementados, se debe hacer un seguimiento constante del cumplimiento.

  - Impacto en alcance muy alto (5): Exposición pública de datos críticos por errores de configuración o falta de control.

    Posible impacto: La exposición de datos críticos puede generar consecuencias legales, regulatorias y de reputación, por lo que se deben reforzar las medidas de protección de datos sensibles mediante cifrado avanzado y segmentación de acceso.

3.1.3.2. Matriz de riesgos de probabilidad vs el impacto en el tiempo

En la tabla 29 se puede apreciar matriz generada mediante la ISO27005 para la clasifica los riesgos de acuerdo a su impacto en el tiempo y su probabilidad

Tabla 29. Matriz de aceptabilidad Impacto tiempo vs probabilidad, evaluado mediante ISO27005.

Probabilidad		**IMPACTO NEGATIVO TIEMPO**				
	valor	Muy bajo (0,05)	Bajo (,10)	Medio (0,20)	Alto (0,4)	Muy Alto (0,80)
		1	**2**	**3**	**4**	**5**
Muy Alta	**5**					
Alta	**4**					
Media	**3**		**Compromiso de cuentas de usuario por intentos automatizados de fuerza bruta. ||**		**Elevación ilegítima de privilegios por fallos en el control de accesos. || Pérdida o filtración de datos sensibles durante la transferencia entre nubes. ||**	
Baja	**2**		**Explotación de fallas en interfaces o APIs para comprometer sistemas o extraer datos. || Pérdida de información por fallos en la replicación o sincronización entre entornos. ||**	**Acceso indebido a sistemas críticos mediante credenciales débiles o robadas. || Interrupción de servicios por sobrecarga maliciosa de tráfico (DDoS). || Exposición de recursos sensibles por configuraciones erróneas o permisos inadecuados. || Alteración maliciosa de comunicaciones entre componentes o sistemas conectados. || Incidentes de seguridad causados por políticas débiles o mal implementadas. ||**	**Acceso no autorizado por uso de contraseñas débiles, compartidas o mal gestionadas. || Exposición de información en tránsito por interceptación en canales no cifrados. ||**	

Muy Baja	**1**		**Acceso no autorizado debido a errores en los mecanismos de autenticación. || Compromiso del sistema mediante la inyección de código malicioso en aplicaciones. ||**		**Exposición pública de datos críticos por errores de configuración o falta de control. ||**	

Nota. Esta tabla representa la matriz de aceptabilidad en cuanto a el impacto en el tiempo vs la probabilidad. Fuente: Elaboración propia.

De acuerdo a la matriz se identifican los siguientes aspectos:

- **En probabilidad media (3),** se identifican los siguientes riesgos y sus impactos:

- Impacto en tiempo medio (3): Compromiso de cuentas de usuario por intentos automatizados de fuerza bruta, elevación ilegítima de privilegios por fallos en el control de accesos, pérdida o filtración de datos sensibles durante la transferencia entre nubes.

  Posible impacto: Los ataques de fuerza bruta pueden provocar bloqueos de cuentas y afectar el acceso legítimo a sistemas, generando tiempos de inactividad para usuarios y equipos de soporte, el escalamiento de privilegios puede retrasar la identificación y contención del incidente, afectando la continuidad del negocio, y la fuga de información en la nube híbrida puede generar tiempos de respuesta prolongados debido a investigaciones y medidas correctivas que deben implementarse, estos riesgos presentan una probabilidad moderada de ocurrencia y pueden generar retrasos en la operatividad y disponibilidad de los sistemas afectados, por tal razón requieren monitoreo activo, detección temprana y planes de respuesta bien definidos para minimizar su impacto en el tiempo.

- **En probabilidad baja (2),** se identifican los siguientes riesgos y sus impactos:

- Impacto en tiempo bajo (2): Explotación de fallas en interfaces o APIs para comprometer sistemas o extraer datos, pérdida de información por fallos en la replicación o sincronización entre entornos.

Posible impacto: Las vulnerabilidades en las interfaces pueden requerir tiempo adicional para parcheo y pruebas, afectando el ciclo de despliegue de aplicaciones, la pérdida de datos por fallos en la replicación o sincronización puede generar periodos de inactividad hasta que se logre restaurar la información afectada, estos riesgos según el análisis presentan una baja probabilidad de ocurrencia, pero su impacto en el tiempo puede generar retrasos en la recuperación del servicio o en la operación normal.

- Impacto en tiempo medio (3): Acceso indebido a sistemas críticos mediante credenciales débiles o robadas, interrupción de servicios por sobrecarga maliciosa de tráfico (DDoS), exposición de recursos sensibles por configuraciones erróneas o permisos inadecuados, alteración maliciosa de comunicaciones entre componentes o sistemas conectados, incidentes de seguridad causados por políticas débiles o mal implementadas, acceso no autorizado por uso de contraseñas débiles, compartidas o mal gestionadas, exposición de información en tránsito por interceptación en canales no cifrados.

  Posible impacto: Los accesos no autorizados y la mala gestión de contraseñas pueden requerir procesos extensivos de auditoría y corrección de credenciales comprometidas, los ataques DDoS pueden afectar temporalmente la disponibilidad de sistemas críticos, requiriendo medidas de mitigación en la infraestructura de red, las configuraciones incorrectas y la manipulación de comunicaciones pueden causar interrupciones en la comunicación entre sistemas, afectando la continuidad operativa, estos riesgos, aunque tienen una baja probabilidad de ocurrencia, pueden generar retrasos significativos en la operación y restauración de los servicios si llegan a materializarse, por eso requieren planes de contingencia bien estructurados, pruebas periódicas de resiliencia y estrategias de respuesta ágil para minimizar el impacto en el tiempo.

- **En probabilidad muy baja (1),** se identifican los siguientes riesgos y sus impactos:

- Impacto en tiempo bajo (2): Acceso no autorizado debido a errores en los mecanismos de autenticación, compromiso del sistema mediante la inyección de código malicioso en aplicaciones.

  Posible impacto: Los fallos en autenticación pueden retrasar accesos legítimos y requerir reconfiguración de credenciales, la inyección de código malicioso puede afectar aplicaciones y requerir medidas de remediación en el código fuente, estos riesgos según el análisis han sido mitigados significativamente con controles compensativos, lo que reduce su probabilidad de ocurrencia, pero si llegan a presentarse, pueden requerir tiempos adicionales para su detección y mitigación.

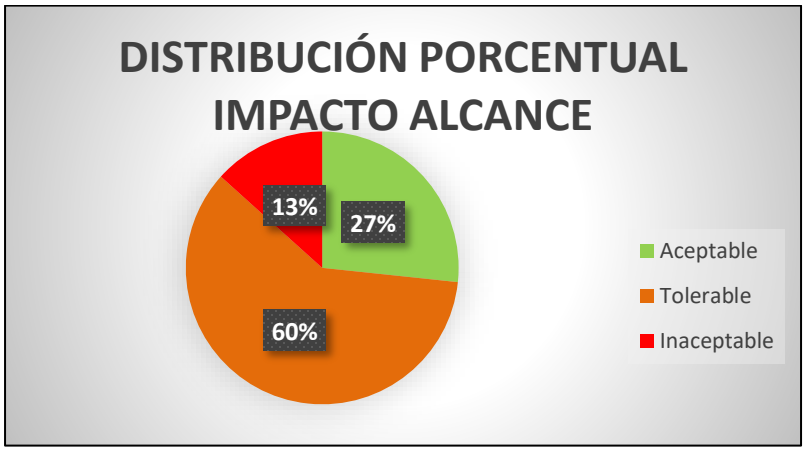
- Impacto en tiempo muy alto (5): Exposición pública de datos críticos por errores de configuración o falta de control.

  Posible impacto: La exposición de datos críticos puede generar procesos legales, revisiones regulatorias y esfuerzos significativos de recuperación de confianza y cumplimiento normativo, lo que puede prolongar su impacto en el tiempo y aunque la probabilidad de este riesgo es muy baja, su impacto en el tiempo es muy alto, debido al tiempo necesario para contener y mitigar una fuga de información sensible.

3.1.3.3. Distribución porcentual para la clasificación de riesgos de acuerdo a los impactos en tiempo y alcance

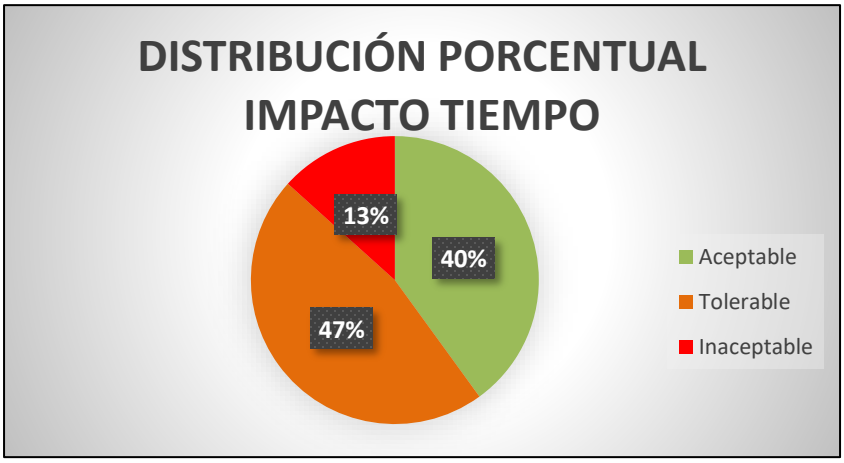
El análisis de la clasificación de los riesgos permitió determinar el nivel de criticidad de los riesgos de acuerdo a si eran, aceptables, tolerables o inaceptables, el detalle en cuanto a la clasificación de acuerdo al alcance se puede apreciar en la figura 18, y en cuanto a el impacto en el tiempo se puede apreciar en la figura 19.

Figura 18. Distribución porcentual impacto alcance.



Nota. Esta figura representa la distribución porcentual de la calificación de los riesgos (aceptable, tolerable, inaceptable) de acuerdo a el impacto en el alcance. Fuente: Elaboración propia.

Figura 19. Distribución porcentual impacto alcance.



Nota. Esta figura representa la distribución porcentual de la calificación de los riesgos (aceptable, tolerable, inaceptable) de acuerdo a el impacto en el tiempo. Fuente: Elaboración propia.

En el análisis para estos porcentajes se da a continuación:

- **Riesgos inaceptables (Rojo):** El análisis indico un 13% de riesgos inaceptables tanto para el impacto en tiempo como en alcance, estos riesgos se concentran en los niveles de impacto Muy Alto y Alto con probabilidades altas y medias, estos riesgos requieren atención inmediata y medidas de mitigación urgentes.

- **Riesgos tolerables (Naranja):** Los riesgos tolerables en el impacto alcance está en un 60%, mientras que en el impacto tiempo están en un 47%, estos riesgos se encuentran principalmente en niveles de impacto Medio con probabilidades medias y altas, aunque no son tan críticos como los inaceptables, aún requieren monitoreo y controles adecuados.
- **Riesgos aceptables (Verde):** Los riesgos aceptables se encuentran en un 27% para el impacto en alcance y para el impacto en tiempo se encuentran en un 40%, estos riesgos tienen un impacto bajo, una probabilidad de ocurrencia reducida y no representan una amenaza significativa para la organización por lo tanto pueden ser gestionados con medidas de control estándar sin necesidad de acciones inmediatas.

3.1.6 Análisis del caso de estudio

Con esta evaluación se lograron identificaron controles que pueden ser implementados para evitar brechas de seguridad y así tener oportunidades de mejora que contribuyan a fortalecer la postura de ciberseguridad de la empresa.

De acuerdo al caso de estudio evaluado se cómo recomendación para la empresa, de acuerdo a la matriz de riesgo realizada, se evidencia que muchos de los impactos tanto en el alcance como en el tiempo, se pueden llegar a reducir aún más, si es aplicado el Modelo de ciberseguridad aplicado a la infraestructura como servicio IaaS usada en la nube híbrida para pymes, con base en gestión de riesgos, teniendo como principio mitigar los riesgos identificados que afectan mayormente este tipo de infraestructuras, y adicional que presentan una impacto con clasificación inaceptable tanto el impacto de alcance como en tiempo, como lo se puede apreciar en las tabla 30 y 31.

Tabla 30. Recomendaciones sobre controles para mitigar los riesgos inaceptables evidenciados en impacto alcance.

Riesgos Inaceptables en impacto Alcance	Controles de acuerdo al modelo	Estado de cumplimiento en la empresa	Acción recomendada
Elevación ilegítima de privilegios por	Gestión de usuarios privilegiados	CC	Monitorear que se siga cumpliendo

fallos en el control de accesos.	Implementación de control de acceso	CP	Evaluar para llevar lo a CC
	Gestión de la seguridad de la información	CP	Evaluar para llevar lo a CC
Pérdida o filtración de datos sensibles durante la transferencia entre nubes.	Políticas de privacidad y transferencias de datos con terceros	CP	Evaluar para llevar lo a CC
	Clasificación de la información	CP	Evaluar para llevar lo a CC
	Uso de la criptografía	CP	Evaluar para llevar lo a CC

Nota. Esta tabla representa las recomendaciones para la empresa del caso de estudio en cuanto a los riesgos inaceptables de cara a el impacto en el alcance. Fuente: Elaboración propia.

Tabla 31. Recomendaciones sobre controles para mitigar los riesgos inaceptables evidenciados en impacto tiempo. Fuente propia

Riesgos Inaceptables en impacto tiempo	**Controles de acuerdo al modelo**	**Estado de cumplimiento en la empresa**	**Acción recomendada**
Elevación ilegítima de privilegios por fallos en el control de accesos.	Registro y auditoría de eventos	CP	Evaluar para llevar lo a CC
	Alertas automatizadas	CP	Evaluar para llevar lo a CC
Pérdida o filtración de datos sensibles durante la transferencia entre nubes.	Registro y auditoría de eventos	CP	Evaluar para llevar lo a CC
	Validación de datos	CP	Evaluar para llevar lo a CC

Nota. Esta tabla representa las recomendaciones para la empresa del caso de estudio en cuanto a los riesgos inaceptables de cara a el impacto en el tiempo. Fuente: Elaboración propia.

Adicional se podría realizar el mismo ejercicio con los riesgos que presenta una clasificación tolerable, identificando los controles que no están en estado CP y/o NA de acuerdo a los controles para los riesgos identificados y priorizarlos para llevarlos a un estado de CC.

4. Conclusiones y recomendaciones

4.1 Conclusiones

La caracterización de los servicios Infraestructura como Servicio (IaaS) en el contexto de una nube híbrida para empresas pymes permitió identificar los componentes tecnológicos más comunes en este tipo de entornos y establecer una arquitectura de referencia sobre la cual se desarrolló el modelo de ciberseguridad. Esta caracterización fue clave para orientar la aplicación contextual de controles de seguridad alineados con las necesidades operativas de las pymes.

El análisis de los estándares, normas y buenas prácticas de seguridad aplicables a los servicios en la nube híbrida permitió establecer una base para el diseño de un modelo de ciberseguridad integral en entornos pymes. Con este estudio se logró evidenciar que la seguridad en la nube híbrida requiere un enfoque estructurado, basado en marcos normativos que permitan garantizar la confidencialidad, integridad y disponibilidad de los activos físicos y digitales, mediante los estándares analizados, tales como ISO/IEC 27001, NIST SP 800-53 y el marco de seguridad de la Cloud Security Alliance (CSA), ofrecieron directrices fundamentales para la gestión de riesgos, el control de accesos, la protección de datos y la respuesta a incidentes en infraestructuras híbridas. Así mismo, las buenas prácticas promovidas por el proveedor de servicios en la nube seleccionado, fueron claves para identificar mecanismos específicos de protección en entornos híbridos.

La clasificación de los principales riesgos en la nube híbrida permitió estructurar un enfoque sistemático para la gestión de riesgos en entornos pymes, asegurando la identificación, evaluación y priorización de amenazas que pueden comprometer la seguridad de la infraestructura. El análisis realizado ha evidenciado que los riesgos en la nube híbrida pueden clasificarse en categorías clave, tales como riesgos de accesos no autorizados, fallos en la autenticación, vulnerabilidades en la infraestructura, fuga de datos, ataques de denegación de servicio (DDoS), errores de configuración y dependencia de terceros (proveedores de nube). Estos riesgos varían en impacto y probabilidad según la arquitectura utilizada y el nivel de madurez en ciberseguridad de cada organización.

Se realizó la evaluación del modelo de ciberseguridad en un caso de estudio, aplicado en un escenario real, el cual permitió validar su efectividad en la protección de infraestructuras IaaS en

una nube híbrida, identificando fortalezas, áreas de mejora y el nivel de cumplimiento de los controles de seguridad propuestos, a partir de este análisis se evidenció que el modelo cumple en gran medida con los estándares y buenas prácticas establecidas, dado que el escenario en el cual fue evaluado ya contaba con lineamientos y políticas de seguridad, sin embargo con la evaluación de cumplimiento del modelo presentados en el ítem 3.1.6 se evidenciaron oportunidades de mejora para la empresa, debido a que algunos controles aún se encuentran con un cumplimiento parcial incluso algunos no tienen un cumplimiento, lo cual permitió entregar una serie de controles adicionales que pueden proteger aún más la infraestructura evaluada.

De acuerdo a el análisis realizado se determina que el modelo es viable y adaptable para las empresas tipo pymes, debido a que el caso de estudio es con una empresa bien constituida y que vela por el cumplimiento de la seguridad, sin embargo, el modelo aporto para que se tengan en cuenta aspectos a mejorar. Por lo tanto, en una empresa que tenga menos recursos tanto económicos como a nivel de documentación optima, el modelo entregado le permitirá hacer un análisis y definir los controles que debe tener en cuenta para asegurar su infraestructura.

4.2 Recomendaciones

De acuerdo a los resultados obtenidos en esta investigación y la evaluación del modelo de ciberseguridad para IaaS en una nube híbrida en pymes, se proponen las siguientes recomendaciones a futuro para mejorar la seguridad y optimizar la implementación del modelo:

Se recomienda la integración del modelo con herramientas de gestión automatizada que permita la configuración e implementación de los controles planteados en el modelo de forma automática, con el fin de reducir errores manuales y mejorar la eficiencia operativa, mediante el uso de tecnologías como Infrastructure as Code (IaC), escaneo continuo de vulnerabilidades y monitoreo automatizado que permitan una mayor resiliencia frente a amenazas emergentes.

Se recomienda que las empresas que adopten el modelo de ciberseguridad propuesto establezcan formalmente su apetito de riesgo, entendiendo este como el nivel de riesgo que están dispuestas a aceptar en función de sus objetivos estratégicos, capacidad operativa y recursos disponibles. Esta

definición permitirá priorizar acciones de tratamiento y tomar decisiones informadas sobre los controles a implementar. Como trabajo futuro, se propone incorporar una fase metodológica específica dentro del modelo que permita alinear la gestión de riesgos con el apetito de riesgo definido, especialmente enfocado en el contexto operativo y económico de las pymes.

En evaluaciones futuras del modelo se recomienda realizar auditorías de seguridad periódicas para evaluar la efectividad del modelo propuesto, identificar nuevas brechas y actualizar controles en función de las tendencias emergentes en ciberseguridad. Además, se recomienda la implementación de pruebas de penetración y simulaciones de ataques para validar la resiliencia del modelo en entornos reales.

Dado que la infraestructura en la nube híbrida está en constante evolución, se recomienda verificar regularmente las variables y parámetros definidos en el modelo, considerando los diferentes cambios que se presentan a nivel de riesgos y en los servicios cloud. Esto permitirá optimizar los controles de seguridad y mantener el modelo alineado con nuevas normativas, estándares de la industria y amenazas emergentes.

A. Anexo A: Evaluación marco de referencia.

B. Anexo B: Relación estándares.

C. Anexo C: cumplimiento controles vs riesgos.

D. Anexo D: Evaluación ISO27005.

E. Anexo E: Soporte evaluación caso de uso

Bibliografía

[1] Acens, «Los ataques a redes en la nube crecieron un 48% en 2022». Accedido: 19 de enero de 2025. [En línea]. Disponible en: https://blog.acens.com/informes/los-ataques-a-redes-en-la-nube-crecieron-un-48-en-2022/

[2] DatacenterDynamics, «Los gastos globales de los usuarios finales en nube pública alcanzarán los 723.000 millones de dólares en 2025». Accedido: 5 de enero de 2025. [En línea]. Disponible en: https://www.datacenterdynamics.com/es/noticias/los-gastos-globales-de-los-usuarios-finales-en-nube-publica-alcanzaran-los-723000-millones-de-dolares-en-2025/

[3] Mordor Intelligence, «Mercado de nube híbrida - Participación, tamaño, crecimiento y análisis de tendencias». Accedido: 5 de enero de 2025. [En línea]. Disponible en: https://www.mordorintelligence.com/es/industry-reports/hybrid-cloud-market

[4] J. García, «Denodo Global Cloud Survey 2020», Denodo. [En línea]. Disponible en: https://www.denodo.com/en/document/whitepaper/denodo-global-cloud-survey-2020

[5] Fortinet, «Latinoamérica y Caribe sufrieron 200.000 millones de intentos de ciberataques en 2023». Accedido: 5 de agosto de 2024. [En línea]. Disponible en: https://www.segurilatam.com/ciberilatam/ciberseguridad-ciberilatam/latinoamerica-y-caribe-sufrieron-200-000-millones-de-intentos-ciberataques-en-2023_20240415.html

[6] CyberWar Mag, «Seguridad en la nube: desafíos y soluciones en América Latina». Accedido: 5 de agosto de 2024. [En línea]. Disponible en: https://cyberwarmag.com/seguridad-en-la-nube-desafios-y-soluciones-en-america-latina/

[7] A. R. Almanza J., «XXI Encuesta Nacional de Seguridad Informática. Resiliencia un aspecto clave en la ciberseguridad», *Revista SISTEMAS*, n.º 159, pp. 20-64, jul. 2021, doi: 10.29236/sistemas.n159a4.

[8] MINTIC, «Modelo de seguridad y privacidad de la información», *Vive digital Colombia*, vol. 3.0.2, jul. 2016.

[9] R. Ross, M. Winstead, y M. McEvilley, «Engineering trustworthy secure systems», nov. 2022. doi: 10.6028/NIST.SP.800-160v1r1.

[10] J. Durán, «Ciberseguridad, seguridad informática y seguridad de la información: diferencias clave», *Seginfo – Exponenciales S.A.S. (Grupo NEX)*, may 2025, Accedido: 23 de julio de 2025. [En línea]. Disponible en: https://seginfo.co/blog/ciberseguridad-seguridad-informatica-y-seguridad-de-la-informacion-diferencias-clave-2/

[11] ISO/IEC, *ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks*, 4.ª ed. Geneva, Switzerland, 2022.

[12] ISO/IEC, *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*, 4.ª ed. https://www.iso.org/standard/80585.html, 2022.

[13] T. Laguna, «Modelo de establecimiento del apetito de riesgo para una organización del sector manufactura de alimentos y bebidas», Universidad Externado de Colombia, Bogotá, 2021. Accedido: 10 de junio de 2025. [En línea]. Disponible en: https://doi.org/10.57998/bdigital.handle.001.4804

[14] P. Mell y T. Grance, «The NIST Definition of Cloud Computing», abr. 2012. Accedido: 5 de marzo de 2025. [En línea]. Disponible en: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[15] L. Bravo, «Implementación de la arquitectura de cloud computing OpenStack para la gestión de recursos informáticos en una universidad», Universidad Tecnológica del Perú, Perú, 2022. Accedido: 5 de marzo de 2025. [En línea]. Disponible en: https://repositorio.utp.edu.pe/bitstream/handle/20.500.12867/6911/L.Bravo_Trabajo_de_Investigacion_Maestria_2022.pdf

[16] P. F. Muñoz-Calderón y M. G. Zhindón-Mora, «Computación en la nube: la infraestructura como servicio frente al modelo On-Premise», *Dominio de las Ciencias*, vol. 6, n.º 4, pp. 1535-1549, 2020.

[17] L. Bravo, «IMPLEMENTACIÓN DE LA ARQUITECTURA DE CLOUD COMPUTING OPENSTACK PARA EL DESPLIEGUE Y DISPONIBILIDAD DE APLICACIONES EN LA EMPRESA DICONST», Universidad tecnológica del Perú, Perú, 2022. Accedido: 5 de marzo de 2025. [En línea]. Disponible en: https://repositorio.utp.edu.pe/bitstream/handle/20.500.12867/6911/L.Bravo_Trabajo_de_Investigacion_Maestria_2022.pdf

[18] E. X. Safla Aranha, «Propuesta de un sistema de gestión de seguridad de la información (SGSI) aplicado a la organización ABC», Universidad de las Américas, Quito, 2021.

[19] L. Gonzales, «Aspectos de seguridad informática en la utilización de cloud computing», 2016, *Cúcuta*. [En línea]. Disponible en: https://repository.unad.edu.co/handle/10596/6173

[20] L. E. Arcila Bonfante, «Recomendaciones de seguridad para los servicios de computación en la nube, a partir de los estándares y modelos de seguridad de la información», 2019. [En línea]. Disponible en: https://repository.ucatolica.edu.co/handle/10983/23388

[21] J. Quispe y D. Pedemonte, «Modelo de evaluación de riesgos de seguridad de la información basado en la ISO/IEC 27005 para analizar la viabilidad de adoptar un servicio en la nube»,

Universidad Peruana de Ciencias Aplicadas (UPC), Lima, 2019. [En línea]. Disponible en: http://hdl.handle.net/10757/625879

[22] J. Castañeda y G. Villegas, «Recomendaciones y Estrategias para la Protección de Datos en la Nube», 2020, *Tecnológico de Antioquia, Institución Universitaria*. [En línea]. Disponible en: https://dspace.tdea.edu.co/handle/tdea/1393

[23] A. Torres, «Análisis de los componentes de seguridad informática en las implementaciones de cloud computing en pequeñas y medias empresas en Colombia», 2020, *Bogotá*. [En línea]. Disponible en: https://repository.unad.edu.co/handle/10596/33263

[24] Y. Z. Giraldo Montes, «Construcción de un modelo de ciberseguridad para empresas de servicios informáticos que fortalezca un adecuado manejo de incidentes de seguridad», Instituto Tecnológico Metropolitano, Medellín, 2020.

[25] M. Reece *et al.*, «Systemic Risk and Vulnerability Analysis of Multi-cloud Environments», jun. 2023.

[26] IBM, «Ventajas y desventajas de la nube híbrida». Accedido: 7 de septiembre de 2024. [En línea]. Disponible en: https://www.ibm.com/es-es/think/insights/hybrid-cloud-advantages-disadvantages

[27] A. Vahdat y B. Calder, «Google is a Leader in Gartner Magic Quadrant for Strategic Cloud Platform Services», Google Cloud Blog. Accedido: 1 de junio de 2025. [En línea]. Disponible en: https://cloud.google.com/blog/products/infrastructure-modernization/google-is-a-leader-in-gartner-magic-quadrant-for-strategic-cloud-platform-services

[28] Amazon Web Services, «¿Qué es la computación en la nube?» Accedido: 12 de enero de 2025. [En línea]. Disponible en: https://aws.amazon.com/es/what-is-cloud-computing/

[29] Amazon Web Services, «Descripción general de Amazon Web Services». Accedido: 12 de octubre de 2024. [En línea]. Disponible en: https://docs.aws.amazon.com/es_es/whitepapers/latest/aws-overview/aws-overview.pdf

[30] Microsoft Azure, «Ventaja híbrida de Azure». Accedido: 12 de septiembre de 2024. [En línea]. Disponible en: https://azure.microsoft.com/es-mx/pricing/hybrid-benefit/#overview

[31] Hystax, «Google Cloud Platform: Strengths and Weaknesses». Accedido: 12 de julio de 2024. [En línea]. Disponible en: https://hystax.com/es/google-cloud-platform-strengths-and-weaknesses/

[32] OCDE, *Índice de Políticas para PyMEs: América Latina y el Caribe 2024*. OECD, 2024. doi: 10.1787/807e9eaf-es.

[33] Ministerio de comercio industria y turismo., *Decreto número 957 de 05 junio de 2019*. Colombia, 2019. Accedido: 11 de agosto de 2023. [En línea]. Disponible en: https://www.mipymes.gov.co/temas-de-interes/definicion-tamano-empresarial-micro-pequena-median

[34] La Nota Económica, «En Colombia el 91,8% de las empresas son PyMEs». Accedido: 9 de diciembre de 2024. [En línea]. Disponible en: https://lanotaeconomica.com.co/movidas-empresarial/en-colombia-el-918-de-las-empresas-son-pymes/

[35] Wikiaccounting, «What Does Company Infrastructure Mean? What Does It Include?» Accedido: 12 de marzo de 2023. [En línea]. Disponible en: https://www.wikiaccounting.com/company-infrastructure/

[36] Sumo Logic, «IT Infrastructure - definition & overview». Accedido: 12 de julio de 2024. [En línea]. Disponible en: https://www.sumologic.com/glossary/it-infrastructure/

[37] A. Alonso, «Todo lo que una PyME desea en materia de hardware y software». Accedido: 12 de marzo de 2025. [En línea]. Disponible en: https://www.itsitio.com/dispositivos/todo-lo-que-una-pyme-desea-en-materia-de-hardware-y-software/

[38] Guía TIC, «Software para Pymes en Colombia».

[39] A. Leon, «Amazon ElastiCache para optimización de arquitecturas hibridas y bases de datos», 2016. Accedido: 12 de marzo de 2025. [En línea]. Disponible en: https://aws.amazon.com/es/blogs/aws-spanish/amazon-elasticache-para-optimizacion-de-arquitecturas-hibridas-y-bases-de-datos/

[40] Qualoom Expertise Technology, «Caso de éxito: Interflora». Accedido: 12 de marzo de 2025. [En línea]. Disponible en: https://www.qualoom.es/casos-de-exito/caso-de-exito-interflora/

[41] J. M. González Varona, «Retos para la Transformación Digital de las PYMES: Competencia Organizacional para la Transformación Digital», Universidad de Valladolid, 2021. doi: 10.35376/10324/47767.

[42] S. Flórez, «Modelo de viabilidad técnica para la implementación de cloud-computing como estrategia de optimización de pequeñas y medianas empresas», Universidad de Córdoba, 2022.

[43] K. Martinez, «Propuesta de Mejora de los Aplicativos Existentes para la Evaluación de los Riesgos Empresariales.», Universidad Santo Tomas, Bogotá, 2023.

[44] Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC), *NTC-ISO/IEC 27001:2022 - Seguridad de la Información, Ciberseguridad y Protección de la Privacidad. Sistemas de Gestión de Seguridad de la Información. Requisitos*. Colombia, 2022.

[45] National Institute of Standards and Technology (NIST), «Security and Privacy Controls for Information Systems and Organizations, NIST Special Publication 800-53, Revision 5», Gaithersburg, MD, sep. 2020. doi: 10.6028/NIST.SP.800-53r5.

[46] Congreso de la República de Colombia, *Ley 1581 de 2012*. Bogotá, Colombia, 2012.

[47] American Institute of Certified Public Accountants (AICPA), «SOC 2®—Report on Controls at a Service Organization Relevant to Security», 2023. Accedido: 7 de marzo de 2024. [En línea]. Disponible en: https://www.aicpa.org

[48] ISACA, «COBIT 2019 Framework: Introduction and Methodology», ISACA, Schaumburg, IL, USA, 2012.

[49] Cloud Security Alliance, *The CSA Cloud Controls Matrix (CCM)*. 2024. Accedido: 11 de agosto de 2024. [En línea]. Disponible en: https://cloudsecurityalliance.org/research/cloud-controls-matrix

[50] Axelos, *ITIL foundation: ITIL 4 edition*. London, UK, 2019.

[51] Amazon Web Services, «AWS Well-Architected Framework», 2023. Accedido: 11 de junio de 2024. [En línea]. Disponible en: https://docs.aws.amazon.com/wellarchitected/latest/framework/

[52] Check Point Software Technologies Ltd., «Top 7 Cloud Vulnerabilities In 2024». Accedido: 12 de marzo de 2025. [En línea]. Disponible en: https://www.checkpoint.com/es/cyber-hub/cloud-security/what-is-cloud-security/top-7-cloud-vulnerabilities-in-2024/

[53] Check Point Software Technologies Ltd., «Los 15 problemas, amenazas y preocupaciones principales de la seguridad en la nube». Accedido: 12 de marzo de 2025. [En línea]. Disponible en: https://www.checkpoint.com/es/cyber-hub/cloud-security/what-is-cloud-security/top-cloud-security-issues-threats-and-concerns/

[54] IT Analytics, «10 principales riesgos de seguridad en la nube». Accedido: 12 de marzo de 2025. [En línea]. Disponible en: https://www.itanalytics.com.mx/2023/02/16/10-principales-riesgos-de-seguridad-en-la-nube

[55] Open Web Application Security Project (OWASP), «OWASP Top 10 – 2024: The Ten Most Critical Web Application Security Risks». Accedido: 12 de marzo de 2025. [En línea]. Disponible en: https://owasp.org/www-project-top-ten/

[56] Evaluando Software, «Amenazas y riesgos de la nube». Accedido: 12 de marzo de 2025. [En línea]. Disponible en: https://www.evaluandosoftware.com/ciberseguridad/amenazas-riesgos-la-nube/

[57] IBM, «¿Qué es la exfiltración de datos?» Accedido: 12 de marzo de 2025. [En línea]. Disponible en: https://www.ibm.com/es-es/topics/data-exfiltration

[58] TBSEK, «Estrategias para el manejo de riesgos de seguridad en la nube híbrida». Accedido: 12 de marzo de 2025. [En línea]. Disponible en: https://tbsek.mx/blog/2024/06-junio/223.nubehibrida.html