UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

TRABAJO DE INTEGRACIÓN CURRICULAR

TEMA:

"PROPUESTA DE SEGURIDAD PARA UNA INFRAESTRUCTURA DE TECNOLOGÍA DE LA INFORMACIÓN (TI) EN ENTORNOS DE CLOUD COMPUTING: CASO DE ESTUDIO UNA PYME DE LA CIUDAD DE QUITO"

Trabajo de titulación previo a la obtención del título de Magíster en Computación con mención en Seguridad Informática

Línea de investigación: Desarrollo, aplicación de software y cyber security (seguridad cibernética)

AUTOR:

Ayde Marlene Rochina Rochina

DIRECTOR:

Pablo Andres Landeta Lopez

Ibarra – Ecuador 2025

DEDICATORIA

Dedico este trabajo a Dios quien ilumino mi camino y me sostuvo en cada desafío. A mis padres, pilares fundamentales de mi vida, por su apoyo constante y ejemplo de dedicación, su sacrificio y entrega han sido la base sobre la que he construido mis sueños, su confianza en mí me ha impulsado a alcanzar cualquier meta propuesta.

A mi esposo, mi compañero de vida y cómplice de cada una de mis aventuras, le dedico este logro con todo mi amor. Su paciencia, comprensión y apoyo incondicional han sido mi mayor refugio en momentos difíciles. A mis preciados y amados hijos que son mi mayor inspiración y motivación en todas mis metas propuesta, les dedico este esfuerzo con la esperanza que en el futuro les sirva como ejemplo de perseverancia y pasión.

Sin dejar de lado también le dedico este logro a toda mi familia que estuvieron presentes en esta trayectoria de mi vida.

AGRADECIMIENTOS

Deseo expresar mi sincero agradecimiento a Dios por guiarme y darme las fuerzas y fortalezas necesarias para superar cada obstáculo que se me presentó durante esta etapa. A mis padres, por su amor incondicional, su apoyo constante y por siempre haber creído en mí.

A mi esposo por estar a mi lado y apoyarme en todo lo que estaba a su alcance. A mis hijos que muchas veces me acompañaban mientras hacía mis deberes y por siempre inspirarme a ser mejor cada día.

Así mismo, agradezco profundamente a mi tutor Msc. Pablo Landeta y asesor Msc. Alexander Guevara por su orientación y apoyo a lo largo del desarrollo de mi proyecto. Sus valiosos comentarios y sugerencias impulsaron el desarrollo de este proyecto, guiándome hacia su culminación.

Por último, quiero agradecer a la Universidad Técnica del Norte y a todos sus docentes que formaron parte de este proceso de crecimiento profesional y por brindarme la oportunidad de alcanzar esta meta.

UNIVERSIDAD TÉCNICA DEL NORTE
BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	1206192294		
APELLIDOS Y NOMBRES:	Ayde Marlene Rochina Rochina		
DIRECCIÓN:	Quito		
EMAIL:	aydee_2263rr@outlook.com		
TELÉFONO FIJO:		**TELÉFONO MÓVIL:**	0991652634

DATOS DE LA OBRA	
TÍTULO:	PROPUESTA DE SEGURIDAD PARA UNA INFRAESTRUCTURA DE TECNOLOGÍA DE LA INFORMACIÓN (TI) EN ENTORNOS DE CLOUD COMPUTING: CASO DE ESTUDIO UNA PYME DE LA CIUDAD DE QUITO
AUTOR (ES):	Ayde Marlene Rochina Rochina
FECHA: DD/MM/AAAA	02/06/2025
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	☐ **PREGRADO** ■ **POSGRADO**
TITULO POR EL QUE OPTA:	**MAGÍSTER EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA**

ASESOR /	**Msc. Alexander Guevara Vega /**
DIRECTOR:	**Msc. Landeta Lopez Pablo Andres**

2. CONSTANCIAS

El autor (es) manifiesta (n) que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es (son) el (los) titular (es) de los derechos patrimoniales, por lo que asume (n) la responsabilidad sobre el contenido de la misma y saldrá (n) en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 02 días del mes de junio de 2025

EL AUTOR:

Ayde Marlene Rochina Rochina

REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

Acreditada Resolución Nro. 173-SE-33-CACES-2020

FACULTAD DE POSGRADO

Ibarra, 17 de marzo de 2025

Dra.
Lucía Yépez
DECANA FACULTAD DE POSGRADO

ASUNTO: Conformidad con el documento final

Señor(a) Decano(a):

Nos permitimos informar a usted que revisado el Trabajo final de Grado Propuesta de seguridad para una infraestructura de tecnología de la información (TI) en entornos de cloud computing: caso de estudio una PYME de la ciudad de Quito del/la maestrante Ayde Marlene Rochina Rochina, de la Maestría de Computación con Mención en Seguridad Informática, certificamos que han sido acogidas y satisfechas todas las observaciones realizadas.

Atentamente,

	Apellidos y Nombres	**Firma**
Director/a	Msc. Landeta López Pablo	PABLO ANDRES LANDETA LOPEZ
Asesor/a	Msc. Guevara Vega Alexander	VICENTE ALEXANDER GUEVARA VEGA

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURA

RESUMEN

Contexto: La adopción de cloud computing por las pequeñas y medianas empresas (PYMEs) en Quito ha crecido significativamente, impulsada por la búsqueda de eficiencia y reducción de costos. Esta transición también ha revelado importantes desafíos en seguridad de la información, generando preocupación sobre la protección de datos críticos. **Problema:** La falta de infraestructuras de seguridad adecuadas expone a las PYMEs a ciberataques y violaciones de datos, comprometiendo su continuidad operativa y reputación. Las brechas de seguridad pueden resultar en pérdidas económicas significativas y daños a la confianza del cliente. **Objetivo:** Este estudio propone el diseño de un sistema de seguridad para la infraestructura de tecnología de la información (TI) en entornos de cloud computing, garantizando la protección de datos y la integridad de los sistemas de información en una PYME de Quito. **Metodología:** Se realizó una encuesta y diagnóstico de las vulnerabilidades existentes en las infraestructuras de TI, identificando áreas de riesgo. A partir de este análisis, se propusieron mecanismos de seguridad avanzados, y se validó su efectividad para mejorar la ciberseguridad en las PYMEs. **Resultados:** El diagnóstico de las infraestructuras de TI en Pymes que operan en la nube reveló un crecimiento en la adopción de SaaS y AWS, aunque con brechas de seguridad significativas, ya que solo el 20% cuenta con una capacitación alta en ciberseguridad. Para mitigar riesgos, se propuso mecanismos como la autenticación multifactor (MFA), cifrado de datos, monitoreo de amenazas y capacitación técnica continúa al personal de TI. Los Expertos en ciberseguridad confirman que los mecanismos propuestos cumplen altos estándares de seguridad y son viables para entornos de cloud computing.

Palabras clave: Cloud computing, TI, PYMEs, SaaS, AWS.

ABSTRACT

Context: The adoption of cloud computing by small and medium-sized enterprises (SMEs) in Quito has grown significantly, driven by the search for efficiency and cost reduction. However, this transition has also revealed significant challenges in information security, raising concerns about the protection of critical data. **Problem:** The lack of adequate security infrastructures exposes SMEs to cyberattacks and data breaches, compromising their operational continuity and reputation. Security breaches can result in significant economic losses and damage to customer trust. **Objective:** This study proposes the design of a security system for information technology (IT) infrastructure in cloud computing environments, ensuring data protection and the integrity of information systems in an SME in Quito. **Methodology:** A diagnosis of the existing vulnerabilities in IT infrastructures was carried out, identifying risk areas. Based on this analysis, advanced security mechanisms were proposed, and their effectiveness in improving cybersecurity in SMEs was validated. **Results:** The diagnosis of IT infrastructures in SMEs operating in the cloud revealed a growth in the adoption of SaaS and AWS, although with significant security gaps, as only 20% have high cybersecurity training. To mitigate risks, mechanisms such as multi-factor authentication (MFA), data encryption, threat monitoring, and continuous technical training for IT staff were proposed. Cybersecurity experts confirm that the proposed mechanisms meet high security standards and are viable for cloud computing environments.

Keywords: Cloud computing, TI, PYMEs, SaaS, AWS.

CAPITULO I

EL PROBLEMA

1.1. Problema de investigación

En la actualidad, la adopción de soluciones de computación en la nube (cloud computing) se ha convertido en una necesidad para las Pequeñas y Medianas Empresas (PYMEs) debido a sus múltiples beneficios, como la reducción de costos, la flexibilidad y la escalabilidad.

La creciente adopción de tecnologías de cloud computing a nivel mundial ha transformado la manera en que las empresas operan y gestionan sus datos. Según un informe de Gartner, se espera que el mercado global de servicios en la nube crezca un 17% en 2023, alcanzando un valor de $331.2 mil millones. Este crecimiento exponencial ha sido impulsado por la necesidad de flexibilidad, escalabilidad y eficiencia en la gestión de recursos de TI.

A nivel internacional, las violaciones de seguridad y los ciberataques han aumentado en frecuencia y sofisticación. En 2021, el Informe de Investigación de Violaciones de Datos de Verizon destacó que el 43% de los ciberataques se dirigieron a pequeñas y medianas empresas. (*CardonaSergio_2022_VulnerabilidadCloudComputing*, n.d.). Las PYMEs, a menudo con recursos limitados, son particularmente vulnerables a los ciberataques debido a la falta de infraestructuras de seguridad robustas y de personal especializado en ciberseguridad.

Un ejemplo destacado de vulnerabilidades en el cloud computing es el incidente de 2019, donde Capital One sufrió una violación de datos que expuso la información personal de más de 100 millones de clientes en EE.UU. y Canadá. El ataque se debió a una configuración incorrecta de una infraestructura en la nube, subrayando la importancia de implementar medidas de seguridad adecuadas y de realizar auditorías periódicas (Jones, 2020).

Las normativas internacionales como el Reglamento General de Protección de Datos (GDPR) en Europa impone estrictas regulaciones sobre la protección de datos y la privacidad. Estas leyes obligan a las organizaciones a adoptar infraestructuras de seguridad robustas para evitar sanciones severas en caso de incumplimiento (Martínez, 2022).

En este sentido, el diseño de infraestructuras de seguridad para la tecnología de la información (TI) en entornos de cloud computing se ha convertido en una prioridad estratégica para las organizaciones de todo el mundo. Empresas de todos los tamaños deben invertir en tecnologías avanzadas, prácticas de gestión de riesgos y capacitación continua del personal para proteger sus activos digitales y garantizar la resiliencia de sus sistemas de información.

En este orden, la seguridad de TI en cloud computing es un desafío global que requiere un enfoque proactivo y multifacético. La creciente sofisticación de las amenazas cibernéticas y las estrictas normativas legales subrayan la necesidad de una infraestructura de seguridad bien diseñada y mantenida. Las PYMEs, en particular, deben prestar especial atención a estos aspectos para protegerse de los riesgos y asegurar su continuidad operativa en un entorno cada vez más digitalizado.

En un contexto nacional, en Ecuador, la adopción de tecnologías de cloud computing ha ido en aumento, especialmente entre las pequeñas y medianas empresas (PYMEs) que buscan aprovechar las ventajas de flexibilidad, escalabilidad y reducción de costos operativos que ofrece esta tecnología. Este crecimiento también ha venido acompañado de desafíos significativos en términos de seguridad de la información y protección de datos (Flores, 2023).

A nivel nacional, el entorno de ciberseguridad ha mostrado vulnerabilidades preocupantes. Un estudio de la Universidad de las Américas (UDLA) en 2020 indicó que más del 60% de las PYMEs en Ecuador no cuentan con políticas de seguridad de la información

adecuadas. Muchas de estas empresas subestiman la importancia de invertir en infraestructura de seguridad robusta, lo que las deja expuestas a ciberataques y violaciones de datos (Ordoñez, 2020).

El incidente de ciberseguridad más notable en Ecuador ocurrió en 2019, cuando una violación de datos masiva expuso información personal de más de 20 millones de personas, incluyendo a ciudadanos fallecidos. Este evento subrayó la necesidad urgente de fortalecer las medidas de seguridad de TI en el país. La falta de prácticas de seguridad adecuadas y la baja inversión en tecnologías de protección fueron identificadas como factores clave que contribuyeron a esta brecha de seguridad (Flores, 2023).

En respuesta a estos desafíos, el gobierno ecuatoriano ha implementado regulaciones y marcos legales para mejorar la seguridad de la información. La Ley de Protección de Datos Personales, promulgada en 2021, establece directrices claras sobre cómo las empresas deben manejar y proteger los datos personales de los ciudadanos. Esta ley busca alinearse con estándares internacionales como el GDPR, imponiendo sanciones significativas para las empresas que no cumplan con las normativas de seguridad y privacidad (Dirección Nacional de Registros Públicos, 2021).

La implementación de estas regulaciones enfrenta obstáculos significativos. Muchas PYMEs carecen de los recursos financieros y humanos necesarios para cumplir plenamente con estas normativas. La falta de conciencia y capacitación en ciberseguridad entre los empleados de estas empresas agrava el problema.

En resumen, Ecuador enfrenta desafíos significativos en términos de seguridad de TI, especialmente en el sector de las PYMEs. La adopción de cloud computing, aunque beneficiosa, aumenta la exposición a ciberataques y violaciones de datos. La implementación de una

infraestructura de seguridad robusta y el cumplimiento con las normativas nacionales e internacionales son esenciales para proteger los activos digitales y garantizar la continuidad del negocio en un entorno cada vez más digitalizado.

A nivel local, en la ciudad de Quito, la capital de Ecuador y el principal centro económico del país, la adopción de tecnologías de cloud computing entre las pequeñas y medianas empresas (PYMEs) ha mostrado un crecimiento notable. Las PYMEs en Quito buscan modernizar sus operaciones y mejorar su competitividad mediante la utilización de soluciones basadas en la nube (Flores, 2023).

A pesar de los beneficios claros, muchas de estas empresas no cuentan con infraestructuras de seguridad adecuadas para proteger sus datos y sistemas. Una encuesta realizada en 2022 por la Universidad San Francisco de Quito reveló que el 58% de las PYMEs locales no tiene políticas de seguridad de la información bien definidas y el 67% no ha realizado auditorías de seguridad en los últimos dos años (Álvarez, 2023).

Las PYMEs en Quito enfrentan desafíos significativos en la implementación de infraestructuras de TI seguras para sus operaciones en la nube. A menudo, estas empresas carecen de los recursos financieros y humanos necesarios para diseñar, implementar y mantener infraestructuras de seguridad robustas. Esto las hace vulnerables a amenazas cibernéticas como el robo de datos, ataques de malware, y violaciones de privacidad.

Según el estudio realizado por la Cámara de Comercio de Quito (CCQ, 2023), el 68% de las PYMEs en la ciudad han adoptado algún tipo de servicio de cloud computing. El 72% de estas empresas reportan sentirse inseguras sobre la protección de sus datos en la nube. El informe de ciberseguridad del Instituto Ecuatoriano de Seguridad Informática (IESI) de 2022 indica que el 45% de las PYMEs en Ecuador han experimentado algún tipo de incidente de seguridad en los

últimos dos años, con pérdidas financieras promedio de $15,000 por incidente (Banco Mundial, 2022).

El problema principal es la falta de una infraestructura de seguridad de TI adecuada para cloud computing en las PYMEs de Quito, lo que las hace vulnerables a múltiples amenazas cibernéticas. Si este problema no se aborda adecuadamente, las PYMEs enfrentarán serias consecuencias, de acuerdo con Flores (2023) los incidentes de seguridad pueden resultar en pérdidas económicas significativas debido al robo de datos, ataques de malware y ransomware, y otros tipos de violaciones de seguridad, las brechas de seguridad pueden dañar gravemente la reputación de una empresa, disminuyendo la confianza de los clientes y socios comerciales, la falta de cumplimiento con las regulaciones de protección de datos puede llevar a sanciones legales y multas.

En síntesis, los ataques cibernéticos pueden interrumpir las operaciones comerciales, afectando la continuidad del negocio y su capacidad de servir a los clientes. Sin una infraestructura de seguridad robusta, las PYMEs pueden ser reacias a adoptar plenamente las tecnologías en la nube, limitando su potencial de crecimiento y su competitividad en el mercado (Garzón et al., 2022).

El diseño de una infraestructura de seguridad adecuada es crucial para proteger los activos de información y garantizar la continuidad del negocio. Sin una infraestructura de seguridad bien diseñada, las PYMEs pueden sufrir pérdidas financieras, daño a su reputación, y problemas legales. La falta de seguridad puede inhibir la adopción plena de tecnologías en la nube, limitando el potencial de crecimiento y competitividad de estas empresas.

1.2. Interrogante de la investigación

- ¿Cómo se pueden diagnosticar las vulnerabilidades y brechas de seguridad en el diseño de infraestructuras de TI para cloud computing, que garantice la protección de datos y la resiliencia de los sistemas de información?
- ¿Qué mecanismos de seguridad avanzados se pueden proponer para el diseño de la infraestructura de TI en entornos de cloud computing, optimizando la gestión de accesos y fortaleciendo la defensa contra amenazas emergentes?
- ¿Cómo se puede validar la capacidad de los mecanismos de seguridad diseñados para entornos de cloud computing en la resistencia a ataques cibernéticos y en el mantenimiento de la integridad y confidencialidad de los datos?

1.3. Objetivos de la investigación

1.3.1. Objetivo general

Diseñar una propuesta de seguridad para la infraestructura de tecnología de la información (TI) en entornos de cloud computing, que garantice la protección de datos y la integridad de los sistemas de información aplicado a una PYME de la ciudad de Quito.

1.3.2 Objetivos específicos.

- Diagnosticar las vulnerabilidades y brechas de seguridad en el diseño de infraestructuras de TI para cloud computing, que garantice la protección de datos y la resiliencia de los sistemas de información.
- Proponer mecanismos de seguridad avanzados para el diseño de la infraestructura de TI en entornos de cloud computing, optimizando la gestión de accesos y fortaleciendo la defensa contra amenazas emergentes.

- Validar la capacidad de los mecanismos de seguridad diseñados para entornos de cloud computing en la resistencia a ataques cibernéticos y en el mantenimiento de la integridad y confidencialidad de los datos.

1.4. Hipótesis de Trabajo

El diseño de una infraestructura de seguridad para la tecnología de la información (TI) en entornos de cloud computing, GARANTIZARÁ la protección de datos y la integridad de los sistemas de información aplicado a una PYME de la ciudad de Quito.

1.5. Hipótesis Alternativa

El diseño de una infraestructura de seguridad para la tecnología de la información (TI) en entornos de cloud computing, NO GRANTIZARÁ la protección de datos y la integridad de los sistemas de información aplicado a una PYME de la ciudad de Quito.

1.6. Categorización de Variables

Variable Independiente: Diseñar una infraestructura de seguridad para la tecnología de la información (TI) en entornos de cloud computing.

- **Definición conceptual:** El conjunto de políticas, procesos, tecnologías y prácticas diseñadas para proteger la integridad, confidencialidad y disponibilidad de la información y los sistemas de TI en entornos de cloud computing. Esta infraestructura se enfoca en asegurar que los datos y servicios alojados en la nube estén protegidos contra amenazas internas y externas, garantizando al mismo tiempo el cumplimiento de normativas y estándares de la industria (Flores, 2023).
- **Definición operacional:** La implementación de una infraestructura de seguridad de TI en entornos de cloud computing incluye varias dimensiones clave. Primero, se desarrollan y revisan políticas y procedimientos de seguridad, los cuales

establecen directrices y reglas para proteger la información y los sistemas de TI. Estos procedimientos cubren el control de acceso, la gestión de incidentes de seguridad y el uso aceptable de recursos de TI. Luego, se implementan procesos y tecnologías para verificar la identidad de usuarios y dispositivos antes de permitirles acceso a los recursos de TI, incluyendo autenticación de dos factores (2FA), biometría, y la gestión de permisos y privilegios (Cardona, 2022).

Variable Dependiente: Protección de datos y la integridad de los sistemas de información aplicado a una PYME de la ciudad de Quito.

- **Definición** conceptual**:** El nivel de seguridad y capacidad de recuperación ante incidentes de seguridad que poseen los datos y sistemas de información de una organización en entornos de cloud computing. Esta variable evalúa cómo las medidas de seguridad implementadas protegen la información sensible de la empresa y garantizan la continuidad del negocio ante posibles amenazas (Nigro, 2022).
- **Definición operacional:** La protección de datos y la integridad de los sistemas de información se evalúa a través de varias dimensiones. La integridad de los datos se mide por el número de incidentes reportados donde los datos se han visto comprometidos, asegurando que los datos no se modifiquen de manera inapropiada. La confidencialidad de los datos se evalúa a través del número de brechas de seguridad reportadas y la cantidad de accesos no autorizados detectados, asegurando que la información sensible solo sea accesible por personal autorizado (Martínez, 2022).

Tabla 1

Operacionalización de Variables

Variable	Definición Conceptual	Definición Operacional	Dimensión	Indicador	Instrumento
Variable Independiente: Diseñar una infraestructura de seguridad para la tecnología de la información (TI) en entornos de cloud computing	El conjunto de políticas, procesos, tecnologías y prácticas diseñadas para proteger la integridad, confidencialidad y disponibilidad de la información y los sistemas de TI en entornos de cloud computing (Flores, 2023).	Implementación y revisión de políticas de seguridad, control de acceso, protección de datos, defensa contra amenazas, gestión de vulnerabilidades, monitoreo y auditoría (Bueno y Haz, 2022).	Políticas y Procedimientos de Seguridad	Número de políticas y procedimientos de seguridad implementados	Lista de verificación de políticas y procedimientos
			Control de Acceso	Sistemas de autenticación y autorización implementados	
			Protección de Datos	Implementación de cifrado y copias de seguridad	
			Defensa contra Amenazas	Presencia de firewalls y	

				sistemas IDS/IPS	
			Gestión de Vulnerabilidades	Evaluaciones de vulnerabilidad y parcheo de software	Informes de evaluaciones de vulnerabilidad y registros de actualización de software
			Monitoreo y Auditoría	Implementación de sistemas de monitoreo continuo y auditorías de seguridad	Registro de incidentes de seguridad
Variable Dependiente: Protección de datos y la integridad de los sistemas de información aplicado a una PYME de la ciudad de Quito	El nivel de seguridad y capacidad de recuperación ante incidentes de seguridad que poseen los datos y sistemas de información de una organización en entornos de cloud computing (Cardona, 2022).	Evaluación de incidentes de corrupción de datos, brechas de seguridad, accesos no autorizados, tiempo de inactividad de los sistemas, recuperación ante desastres, y capacidad de resistencia a ataques (Martínez, 2022).	Integridad de los Datos	Incidentes de corrupción de datos	

Confidencialidad de los Datos	Brechas de seguridad y accesos no autorizados	Registro de incidentes de seguridad y auditorías de acceso
Disponibilidad de los Sistemas	Tiempo de inactividad de los sistemas y recuperación ante desastres	Registros de tiempos de inactividad y planes de recuperación ante desastres
Resiliencia de los Sistemas	Capacidad de los sistemas para resistir y recuperarse de ataques	

Fuente: Elaboración propia

1.7. Justificación

La adopción de soluciones de computación en la nube se ha convertido en una estrategia vital para las Pequeñas y Medianas Empresas (PYMEs) debido a sus múltiples beneficios, como la reducción de costos, la escalabilidad y la flexibilidad operativa (Bueno y Haz, 2022). Esta transición también introduce importantes desafíos de seguridad que pueden comprometer la integridad y confidencialidad de los datos y sistemas de las empresas. De acuerdo con Flores (2023), “la falta de una infraestructura de seguridad adecuada en la nube puede llevar a consecuencias graves, tales como pérdidas financieras, daño reputacional y problemas legales” (p.13).

A nivel internacional, la adopción de cloud computing ha experimentado un crecimiento exponencial. Según Gartner (2022), se espera que el gasto global en servicios de nube pública alcance los $500 mil millones en 2023, un aumento significativo respecto a años anteriores. Este crecimiento también ha traído consigo un aumento en los incidentes de seguridad. Un estudio de McAfee (2023) reveló que el 93% de las organizaciones han experimentado algún tipo de brecha de seguridad en la nube. La falta de una infraestructura de seguridad adecuada puede resultar en consecuencias graves, como pérdidas financieras y daño reputacional.

En Ecuador, el uso de tecnologías de cloud computing también ha ido en aumento. Según el Instituto Nacional de Estadística y Censos (INEC), el 45% de las PYMEs ecuatorianas utilizan servicios de computación en la nube. Muchas de estas empresas carecen de las medidas de seguridad necesarias para proteger sus datos y sistemas. Un informe del Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) en 2023 destacó que el 60% de las PYMEs en Ecuador no cuentan con políticas de seguridad cibernética adecuadas. Esto representa un riesgo significativo para la integridad y confidencialidad de los datos empresariales.

En Quito, las PYMEs desempeñan un papel fundamental en la economía local. Según la Cámara de Comercio de Quito, más del 70% de las empresas registradas en la ciudad son PYMEs. Estas empresas están adoptando cada vez más soluciones de cloud computing para mejorar su eficiencia operativa y reducir costos. La mayoría de ellas carecen de una infraestructura de seguridad adecuada para proteger sus datos y sistemas. Un estudio de la Universidad San Francisco de Quito (USFQ) en 2023 reveló que el 65% de las PYMEs en Quito han experimentado algún tipo de incidente de seguridad relacionado con el uso de cloud computing en los últimos dos años.

La motivación para este estudio radica en la necesidad crítica de abordar estas vulnerabilidades de seguridad, especialmente en el contexto de una PYME en Quito. Las PYMEs representan una parte significativa de la economía local, y su crecimiento y sostenibilidad son cruciales para el desarrollo económico de Quito. Este estudio busca diseñar una infraestructura de seguridad específica para la computación en la nube, adaptada a las necesidades y capacidades de una PYME en Quito.

La innovación del estudio se centra en proporcionar un marco práctico y basado en la evidencia para la implementación de infraestructuras de seguridad en la nube. Este marco no solo será útil para la empresa específica, sino que también podrá ser utilizado por otras empresas y sectores, ampliando el impacto del estudio.

Los beneficiarios directos de este estudio son las PYMEs de la ciudad de Quito, mientras que los beneficiarios indirectos incluyen sus clientes. Implementar una infraestructura de seguridad robusta ayudará a proteger los datos y sistemas críticos de la empresa contra amenazas cibernéticas. Identificar y mitigar los riesgos específicos asociados con el uso de cloud computing reducirá la probabilidad de incidentes de seguridad y sus impactos negativos.

Una infraestructura de seguridad adecuada aumentará la confianza de los clientes y socios comerciales, fortaleciendo la reputación de la empresa. También ayudará a las PYMEs a cumplir con las regulaciones de protección de datos y ciberseguridad, evitando sanciones legales y multas. Facilitará la adopción plena de tecnologías en la nube, permitiendo a las PYMEs aprovechar sus beneficios para mejorar su competitividad y crecimiento en el mercado.

La justificación de este estudio radica en la necesidad crítica de abordar las vulnerabilidades de seguridad que enfrentan las PYMEs en Quito al adoptar soluciones de cloud computing. Al diseñar una infraestructura de seguridad efectiva y adaptada, el estudio no solo

protegerá a las empresas contra amenazas cibernéticas, sino que también impulsará su crecimiento y sostenibilidad, beneficiando así al desarrollo económico de la región. La implementación de medidas de seguridad adecuadas es esencial para garantizar la protección de los activos de información, la continuidad del negocio y la confianza de los clientes y socios comerciales.

CAPITULO II

MARCO REFERENCIAL

2.1.Antecedentes

Con el fin de identificar los trabajos que guardan relación con la presente investigación, se realizó una revisión preliminar de la literatura utilizando un protocolo de búsqueda estandarizado para este tipo de estudios.

En primer lugar, se estableció una cadena de búsqueda que facilite responder a la siguiente pregunta de investigación: ¿Cómo diseñar una infraestructura de seguridad para la tecnología de la información (TI) en entornos de cloud computing, que garantice la protección de datos y la integridad de los sistemas de información aplicado a una PYME de la ciudad de Quito?

Para identificar los artículos que respondan a esta pregunta, se estableció la siguiente cadena de búsqueda:"Document Title": cloud computing) AND ("All Metadata": security infrastructure for information technology).

La cadena de búsqueda se implementó en la base de datos IEEE Xplore (IEEEX), lo que resultó en un total de 25 artículos publicados en revistas. Se aplicó como criterio de inclusión aquellos trabajos publicados en los últimos 5 años, como se ilustra en la imagen siguiente:

Figura 1

Base de datos IEEE Xplore

Fuente: IEEE Xplore

Con los resultados obtenidos, se revisaron todos los artículos para identificar los más relevantes para el estudio. De este análisis, se eligieron 6 artículos científicos, cuyos detalles se presentan a continuación.

Un estudio realizado por (Skafi et al., 2020), señala que la computación en la nube está ganando relevancia y su uso está aumentando rápidamente en diferentes organizaciones, incluidas las pequeñas y medianas empresas (PYME). Aún se conoce poco sobre qué factores afectan la adopción de estos servicios en PYME de países en desarrollo como Líbano.

Este estudio utiliza el marco de tecnología-organización-entorno (TOE) y la teoría contextual para investigar de manera práctica qué determina la adopción de servicios de computación en la nube en el Líbano. Se ha desarrollado un modelo y se han recopilado y analizado datos de 139 personas que trabajan en PYME en el país.

Según (Tang et al., 2022) manifiestan que la computación en la nube de borde y la segmentación de red son opciones atractivas para las aplicaciones de IoT que funcionan con 5G y más allá. Estas soluciones enfrentan retos significativos. Por un lado, la computación en la nube de borde está formada por varios dispositivos, lo que dificulta su manejo y supervisión. Por otro lado, aunque la segmentación de red permite compartir recursos, también puede ser susceptible a ataques que afectan su diseño y provocar un uso ineficiente de los mismos. Para abordar estos problemas, se sugiere un nuevo enfoque denominado "computación en la nube de borde definida por software" (SD-ECC) y un algoritmo de "orquestación segura de recursos" (SS-RO). Este algoritmo se enfoca en asignar recursos de manera más efectiva, considerando posibles amenazas, y los resultados indican que supera a otros métodos en cuanto a eficiencia y rendimiento.

Un análisis de los autores(Eljak et al., 2024), investigaron la unión entre el aprendizaje electrónico y la computación en la nube permite entender cómo se complementan y qué efectos pueden tener. Se plantean dos preguntas clave: primero, ¿de qué manera el aprendizaje electrónico impacta elementos como la arquitectura, la seguridad y el hardware? Y segundo, ¿cómo se analizan los diferentes servicios y modelos de computación en la nube, como SaaS, PaaS e IaaS? El propósito es ofrecer información sobre cómo se integra el aprendizaje electrónico en un entorno de computación en la nube, destacando sus beneficios y oportunidades.

Los hallazgos más relevantes muestran que el aprendizaje electrónico en la nube se centra en elementos como la arquitectura, el software y el rendimiento. También se observa que los entornos virtuales tienden a tener menos problemas de seguridad. En cuanto a los servicios de nube más populares, destacan SaaS, IaaS y PaaS, con muchos estudios centrados en nubes públicas. El estudio señala limitaciones en el uso de nubes híbridas y privadas, así como vacíos en las ofertas de plataformas e infraestructura para facilitar la integración del aprendizaje electrónico en la computación en la nube.

Según los autores (Al Reshan et al., 2023), la computación en la nube es el aprovisionamiento dinámico de recursos para proporcionar servicios a los usuarios finales a través de Internet. La realización de la computación en la nube requiere abordar varios desafíos, como el descubrimiento de recursos, la seguridad, la programación y el equilibrio de carga. Entre estos problemas de investigación, el equilibrio de carga es el más desafiante. Esta investigación propone un enfoque combinado de GWO-PSO que capitaliza los beneficios de la convergencia rápida y la optimización global. Los resultados de esta investigación son prometedores, ya que logran una convergencia rápida optimizada globalmente y reducen el tiempo de respuesta general en un 12% en comparación con otros algoritmos. El mejor valor óptimo obtenido a partir de la

función objetivo del algoritmo GWO-PSO propuesto mejora el PSO al 97,253% en términos de convergencia.

Un estudio realizado por los autores (Irshad et al., 2020), la computación en la nube móvil (MCC) combina la computación en la nube con la computación móvil, lo que ha transformado la forma en que se ofrecen los servicios de aplicaciones. Esto ha llevado a la necesidad de establecer acuerdos de autenticación sólidos y eficientes, especialmente con el aumento de dispositivos móviles portátiles. Aunque se han sugerido varios esquemas de autenticación multiservidor para MCC, las soluciones actuales tienen limitaciones.

Este estudio presenta un nuevo protocolo de autenticación multiservidor que no requiere emparejamiento, diseñado específicamente para el entorno MCC. Utiliza un sistema de criptografía de curva elíptica que no solo es eficiente, sino que también elimina brechas de seguridad, como se ha demostrado teóricamente mediante un modelo de seguridad formal.

El ultimo análisis fue de (Albshaier et al., 2024) que indican que la combinación de la Internet de las cosas (IoT) y la computación en la nube está surgiendo como un factor esencial en la próxima generación de Internet, con el potencial de transformar diversas aplicaciones. Esta integración no solo optimiza la funcionalidad de IoT al facilitar el acceso a recursos y datos dispersos, sino que también presenta retos de seguridad, ya que las soluciones tradicionales no siempre son efectivas en el entorno de la nube. Recientes estudios han investigado cómo la tecnología blockchain puede ayudar a mitigar estas inquietudes, mejorando la integridad, la privacidad y la seguridad de los datos en sistemas interconectados, lo que resulta fundamental para el avance de la ciberseguridad en el futuro.

Tabla 2

Lista de literatura

Artículo	Autor	Año de publicación	Tipo de organización estudiada	Factores de éxito	Dificultadas encontradas	Página web
1	Skafi et al.,	2020	cloud computing	Los resultados indican que los factores tecnológicos (es decir, complejidad y seguridad) y organizacionales (es decir, apoyo de la alta gerencia y experiencia previa en TI) están relacionados positivamente con la decisión de adoptar servicios de computación en la nube	Se sabe poco sobre los factores que probablemente estén asociados con el comportamiento de adopción de servicios de computación en la nube entre las pequeñas y medianas empresas	https://ieeexplore.ieee.org/document/9064559/citations#citations
2	Tang et al.,	2021	Segmentación de red en la computación en la nube	Los resultados experimentales demuestran que el algoritmo SS-RO propuesto supera a los esquemas de referencia en términos de la relación de tareas de ataque aceptadas, consumo de energía y rendimiento del sistema.	Los sistemas de computación en la nube de borde se componen de varias instalaciones de hardware, lo que genera dificultades en el control y la gestión del hardware	https://ieeexplore.ieee.org/document/9521992/citations?tabFilter=papers#citations
3	Eljak et al.,	2023	cloud computing	Los entornos virtuales tienen menos problemas de seguridad, mientras que el almacenamiento y el enfoque de red son más frecuentes.	La influencia del aprendizaje electrónico en factores como la arquitectura, el software, el rendimiento, la seguridad, el hardware, la red y los aspectos virtuales, y el examen de los servicios y modelos de computación en la nube como SaaS, PaaS, IaaS y SOA	https://ieeexplore.ieee.org/document/10341232
4	Al Reshan et al.,	2023	Cloud Computing	Se propone un enfoque combinado de GWO-PSO que capitaliza los	Entre estos problemas de investigación, el equilibrio	https://ieeexplore.ieee.org/docume

				beneficios de la convergencia rápida y la optimización global. Estas dos técnicas mejoran la eficiencia del sistema y la asignación de recursos, trabajando juntas para resolver el desafío del equilibrio de carga	de carga es el más desafiante	nt/10034760
5	Irshad et al.,	2020	Mobile Cloud Computing	Proponemos un nuevo protocolo de autenticación multiservidor sin emparejamiento para el entorno MCC basado en un criptosistema de curva elíptica que no solo es eficiente, sino que también está libre de lagunas de seguridad	Los esquemas de autenticación multiservidor basados en MCC son inseguras o emplean operaciones de emparejamiento bilineal demasiado costosas para su implementación	https://ieeexplore.ieee.org/document/9121321
6	Albshaier et al.,	2024	Cloud Computing	Esta investigación explora cómo la tecnología blockchain aborda eficazmente las preocupaciones de seguridad dentro de esta combinación, enfatizando su capacidad para mejorar la integridad y la privacidad de los datos y garantizar transacciones seguras	La rápida migración a la nube ha generado preocupaciones de seguridad, ya que las medidas de seguridad convencionales para computadoras no siempre se aplican de manera efectiva a los sistemas basados en la nube	https://ieeexplore.ieee.org/document/10614583

Fuente: Elaboración propia

Estos casos aportan al estudio de demostrar cómo la adopción de tecnologías en la nube puede mejorar la eficiencia y reducir los problemas asociados con la infraestructura tradicional de TI, justificando la necesidad de diseñar una infraestructura de seguridad adecuada para la TI en el contexto de Cloud Computing en una PYME.

En esta línea se analizaron reportes con modelos de nube como SaaS, PaaS, IaaS, FaaS, DaaS, STaaS, los cuales representan para la investigación una fundamentación teórica para contrate con los resultados y hallazgos obtenidos en la sección de resultados de este estudio.

El artículo de Geekflare (2025) proporciona una visión integral de los modelos más comunes, como SaaS, PaaS, IaaS, DaaS, APIaaS, XaaS y FaaS, explicando sus características y usos en el ámbito empresarial y tecnológico. Este estudio es relevante porque permite a empresas y desarrolladores seleccionar el modelo adecuado según sus necesidades operativas y estratégicas, optimizando así el uso de recursos en la nube. Además, los ejemplos prácticos incluidos en el artículo facilitan la comprensión de estos conceptos, permitiendo su aplicación en distintos sectores, desde el desarrollo de software hasta el almacenamiento de datos y la infraestructura digital.

Por otro lado, el estudio de Ortiz et al. (2024) titulado "Seguridad de la Información en la Nube: Una revisión sistemática" publicado en Revistas UNH, profundiza en los riesgos y desafíos de seguridad asociados con los entornos de nube. Aunque su enfoque principal es la ciberseguridad, su análisis sobre los modelos SaaS, PaaS e IaaS resulta esencial para comprender cómo proteger datos y servicios en estos entornos. Esta investigación ofrece estrategias y mejores prácticas para mitigar vulnerabilidades, garantizando la integridad, disponibilidad y confidencialidad de la información. Su aporte es crucial para empresas y organizaciones que buscan implementar servicios en la nube sin comprometer la seguridad de su infraestructura digital, abordando aspectos como encriptación, autenticación y gestión de accesos.

Finalmente, el artículo de Martínez et al. (2020) "Arquitectura de Servidores en la Nube IaaS" de Eumed se enfoca en la infraestructura de servidores en la nube bajo el modelo IaaS, proporcionando un análisis técnico sobre máquinas virtuales, redes e interactividad. Este estudio permite comprender cómo se configuran y gestionan los servidores en la nube, asegurando un rendimiento eficiente y seguro. Además, el artículo examina los mecanismos de control de seguridad dentro de este modelo, destacando la importancia de la segmentación de redes, la

redundancia de datos y las estrategias de recuperación ante desastres. Su contribución resulta valiosa para administradores de sistemas y arquitectos de TI, ya que proporciona conocimientos aplicables para la optimización de infraestructuras empresariales basadas en la nube.

Estos modelos también proporcionan un marco sólido para que las PYMEs evalúen su preparación tecnológica y necesidades específicas en el contexto de Cloud Computing. Facilitan una transición efectiva al identificar aspectos cruciales como la seguridad de datos, la gestión de costos y la adaptabilidad del software. Esta información es esencial para diseñar una infraestructura de seguridad adecuada para TI en PYMEs, asegurando que puedan adoptar tecnologías de la nube de manera eficiente y sostenible.

2.2.Marco Teórico:

2.2.1. Diseñar

El diseño en el contexto de la tecnología de la información (TI) implica la planificación estratégica de sistemas y estructuras para cumplir con requisitos específicos de seguridad y funcionalidad. Según Xu y Cai (2021), "el diseño de sistemas seguros requiere una integración meticulosa de componentes y políticas que respondan a las amenazas emergentes".

2.2.2. Infraestructura de seguridad TI

La infraestructura de seguridad TI es fundamental para proteger los recursos digitales de las organizaciones frente a amenazas cibernéticas. Según Tineo (2023), una infraestructura robusta debe incluir componentes como firewalls, sistemas de detección de intrusiones y soluciones de encriptación. Estos elementos trabajan en conjunto para salvaguardar la integridad, confidencialidad y disponibilidad de la información. Es esencial mantener actualizados estos sistemas para prevenir vulnerabilidades que puedan ser explotadas por atacantes.

La planificación de una infraestructura de seguridad efectiva requiere una comprensión profunda de los riesgos específicos a los que se enfrenta una organización. Angamarca y Guaraca (2021) señalan que la evaluación de riesgos debe ser un proceso continuo, adaptándose a las

nuevas amenazas que emergen constantemente. La identificación de activos críticos y la implementación de medidas de protección adecuadas son pasos clave para garantizar la resiliencia de los sistemas. Este enfoque proactivo minimiza las posibilidades de interrupciones en las operaciones debido a incidentes de seguridad.

Por otra parte, la infraestructura de seguridad TI también debe ser escalable y flexible para adaptarse a los cambios en la estructura organizativa y en el entorno tecnológico (Buenaventur y Uzoma, 2022). Las empresas deben considerar soluciones que permitan una fácil integración de nuevas tecnologías sin comprometer la seguridad. La adopción de arquitecturas modulares y el uso de servicios en la nube son estrategias que pueden facilitar esta adaptabilidad, permitiendo a las organizaciones responder de manera efectiva a las necesidades emergentes.

Finalmente, la capacitación continua del personal es un componente crucial de la infraestructura de seguridad TI. Según Gutiérrez, Almeida y Romero (2018), el factor humano sigue siendo uno de los eslabones más débiles en la cadena de seguridad. Los programas de formación deben enfocarse en sensibilizar a los empleados sobre las mejores prácticas de seguridad, como el manejo de contraseñas y la identificación de intentos de phishing. Un equipo bien entrenado es fundamental para prevenir incidentes y reducir el impacto de posibles brechas de seguridad.

2.2.3. Cloud Computing

El Cloud Computing ha transformado la forma en que las organizaciones gestionan y almacenan sus datos, ofreciendo beneficios como la escalabilidad, la flexibilidad y la reducción de costos. Según Parra et al (2023), las empresas pueden aprovechar los servicios en la nube para acceder a recursos tecnológicos avanzados sin la necesidad de realizar grandes inversiones en infraestructura. Esta tecnología permite a las organizaciones adaptarse rápidamente a las demandas cambiantes del mercado, proporcionando una ventaja competitiva significativa.

La adopción de Cloud Computing también plantea desafíos, especialmente en términos de seguridad. Bueno y Haz (2022) argumentan que las empresas deben ser conscientes de los riesgos asociados con el almacenamiento de datos sensibles en la nube, como la posibilidad de violaciones de datos y el acceso no autorizado. Es fundamental que las organizaciones implementen medidas de seguridad robustas, como el cifrado de datos y la autenticación multifactorial, para proteger la información almacenada en la nube.

La gestión adecuada de la nube requiere un enfoque estratégico que considere tanto los aspectos técnicos como los operativos. Flores (2023) señala que la integración de servicios en la nube con los sistemas existentes debe realizarse de manera cuidadosa para evitar incompatibilidades y problemas de seguridad. Las organizaciones deben establecer políticas claras de gestión de la nube, incluyendo la definición de roles y responsabilidades, para asegurar una administración eficiente y segura de los recursos en la nube.

Por último, es importante que las organizaciones realicen una evaluación continua de sus servicios en la nube para garantizar que cumplan con los estándares de seguridad y las normativas legales aplicables (Álvarez et al., 2022). Esto incluye la realización de auditorías regulares y la supervisión de las prácticas de los proveedores de servicios en la nube. Mantener un alto nivel de seguridad en la nube es crucial para proteger los activos digitales y garantizar la continuidad del negocio.

2.2.4. Seguridad informática

La seguridad informática es un aspecto crítico en la protección de los sistemas y la información de las organizaciones. Martínez (2022) subraya que la seguridad informática abarca una serie de prácticas y tecnologías diseñadas para proteger la información contra accesos no autorizados, alteraciones o destrucción. Esto incluye la implementación de políticas de

seguridad, la utilización de software de protección y la capacitación constante del personal en las mejores prácticas de seguridad.

La evolución de las amenazas cibernéticas ha obligado a las organizaciones a adoptar enfoques más sofisticados para la seguridad informática. Saltos (2020) destaca la importancia de una estrategia integral que no solo se enfoque en la tecnología, sino también en los procesos y las personas. La combinación de tecnologías avanzadas como la inteligencia artificial y el aprendizaje automático con una cultura organizacional que priorice la seguridad es fundamental para enfrentar los desafíos actuales.

Asimismo, la colaboración entre diferentes áreas de la organización es clave para garantizar una protección efectiva. Cardona (2022) sugiere que la seguridad informática debe ser vista como una responsabilidad compartida, donde todos los departamentos contribuyan a la protección de los activos digitales. Esto implica la implementación de controles de seguridad en todos los niveles de la organización, desde el acceso físico hasta la protección de las redes y los datos.

La seguridad informática no es un objetivo estático, sino un proceso continuo de mejora. Buenaventura y Uzoma (2022) enfatizan la necesidad de revisiones regulares de las políticas de seguridad y la actualización constante de las tecnologías de protección para mantenerse al día con las nuevas amenazas. Un enfoque proactivo en la seguridad informática permite a las organizaciones no solo proteger sus sistemas, sino también construir confianza con sus clientes y socios.

2.2.5. Protección de datos

La protección de datos es fundamental para garantizar la privacidad y seguridad de la información en un entorno digital. Según Lee y Kim (2021), "las organizaciones deben

implementar políticas de protección de datos robustas para cumplir con normativas como el GDPR y evitar sanciones".

2.2.6. Integridad

La integridad se refiere a la precisión y consistencia de los datos y sistemas durante todo su ciclo de vida. Zhang y Wang (2020) explican que "la integridad es crítica para garantizar que los datos no sean alterados de manera no autorizada, lo que podría comprometer la confiabilidad del sistema".

2.2.7. Gestión de riesgos

La gestión de riesgos es un proceso clave para detectar, analizar y reducir los riesgos que podrían impactar a una organización. Flores (2023) describe la gestión de riesgos como una disciplina que permite a las organizaciones anticiparse a posibles amenazas y tomar medidas preventivas para minimizarlas. Esto incluye la identificación de riesgos potenciales, la evaluación de su impacto y la implementación de estrategias para gestionarlos de manera efectiva.

Un elemento clave en la gestión de riesgos es la clasificación de los riesgos según su probabilidad e impacto. Gutiérrez, Almeida y Romero (2018) señalan que no todos los riesgos tienen el mismo nivel de importancia, por lo que es crucial que las organizaciones se enfoquen en aquellos que representan las mayores amenazas para sus operaciones. La asignación de recursos adecuados para mitigar estos riesgos es una parte integral de este proceso.

La comunicación es otro componente clave en la gestión de riesgos. Martínez (2022) destaca la importancia de mantener informados a todos los niveles de la organización sobre los riesgos identificados y las medidas adoptadas para mitigarlos. Esto no solo ayuda a crear

conciencia sobre la importancia de la gestión de riesgos, sino que también asegura que todos los empleados estén alineados con las políticas y procedimientos establecidos.

Por último, la gestión de riesgos debe ser un proceso dinámico que se adapte a las cambiantes condiciones del entorno (Tineo, 2023). Las organizaciones deben revisar y actualizar regularmente sus planes de gestión de riesgos para asegurarse de que siguen siendo efectivos frente a nuevas amenazas y oportunidades. Esta capacidad de adaptación es crucial para la resiliencia a largo plazo de la organización (CCQ, 2023).

2.2.8. PYMEs

Las pequeñas y medianas empresas (PYMEs) se destacan por tener una estructura organizativa reducida, tanto en términos de empleados como de ingresos, lo que las diferencias de las grandes corporaciones. Estas empresas son esenciales para el funcionamiento de la economía, ya que constituyen una parte importante del tejido empresarial y son responsables de una gran proporción del empleo. Según López y García (2021), las PYMEs, aunque operan con recursos limitados, tienen la capacidad de adaptarse rápidamente a los cambios del mercado, lo que les permite competir eficazmente. En muchos contextos, se clasifican en microempresas, pequeñas y medianas empresas, utilizando criterios como el número de empleados y el volumen de ingresos, tal como señalan Martínez y Fernández (2022).

Aunque las PYMEs suelen enfrentar desafíos significativos, como la adopción de nuevas tecnologías y el acceso a financiamiento, su capacidad para adaptarse rápidamente a las necesidades del mercado y su proximidad a los clientes les otorgan ventajas competitivas considerables (Rodríguez & Torres, 2020). En un entorno cada vez más digitalizado, las PYMEs están cada vez más obligadas a adoptar soluciones tecnológicas que optimicen su eficiencia

operativa y amplíen su presencia en el mercado, lo que es fundamental para su crecimiento y sostenibilidad a largo plazo (Hernández & Pérez, 2021).

2.3.Marco Legal

Las normativas ecuatorianas establecen un marco legal sólido para la protección de datos personales y la regulación de servicios en el entorno digital, asegurando derechos fundamentales y responsabilidades para todos los actores involucrados. Estas leyes reflejan la importancia creciente de la seguridad en el manejo de la información y la prestación de servicios electrónicos en un mundo cada vez más interconectado. A continuación, se analizarán algunas de las principales leyes en Ecuador que regulan estos aspectos, abordando la protección de datos personales, la propiedad intelectual, el comercio electrónico, y las telecomunicaciones.

La Constitución de la República del Ecuador consagra en su artículo 66, numeral 19, el derecho a la protección de datos personales. Este derecho garantiza a los ciudadanos la capacidad de controlar su información personal, incluyendo la autorización necesaria para su recolección, archivo, procesamiento y difusión. Este principio constitucional se convierte en un pilar fundamental para la protección de la privacidad en la era digital (Constitución de la República del Ecuador, 2008, art. 66, num. 19).

Por otro lado, la Ley de Propiedad Intelectual se enfoca en proteger la información no divulgada, especialmente en contextos donde dicha información no es de conocimiento general ni accesible a personas fuera de los círculos que manejan este tipo de datos. El artículo 183 de esta ley resalta la importancia de proteger configuraciones y composiciones específicas que no sean fácilmente accesibles, garantizando así la seguridad y exclusividad de la información sensible (Ley de Propiedad Intelectual, 1998, art. 183).

En el ámbito del comercio electrónico, la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos establece principios esenciales como la confidencialidad y la reserva de los mensajes de datos. La ley exige el consentimiento expreso del titular de los datos para su uso y transferencia, garantizando que estos procesos se realicen bajo estrictas normas de privacidad. Los proveedores de servicios electrónicos deben utilizar sistemas seguros y transparentes, informando a los usuarios sobre los riesgos potenciales asociados a la falta de seguridades adecuadas (Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, 2002, arts. 5, 9, 21).

La Ley para la Transformación Económica del Ecuador y la Ley Orgánica de Telecomunicaciones introducen regulaciones específicas en el sector de las telecomunicaciones. Estas leyes promueven la competencia libre y justa, garantizando la seguridad nacional y la calidad en la prestación de servicios. Se enfatiza el derecho de los usuarios a recibir servicios en condiciones justas y acordadas, y la responsabilidad de los operadores de redes para cumplir con los estándares de calidad establecidos por las autoridades regulatorias (Ley para la Transformación Económica del Ecuador, 2000, arts. 38, 39; Ley Orgánica de Telecomunicaciones, 2015, art. 21).

Por último, la Ley Orgánica de Protección de Datos Personales del Ecuador, promulgada en el año 2021, establece el marco normativo para garantizar el derecho a la protección de los datos personales. Esta ley es especialmente relevante en el contexto de la computación en la nube, ya que regula el tratamiento, almacenamiento, transferencia y seguridad de la información personal, incluyendo aquellas actividades realizadas por proveedores de servicios en la nube

CAPITULO III

MARCO METODOLÓGICO

3.1. Descripción del área de estudio / Descripción del grupo de estudio

Descripción del área de estudio:

El área de estudio se centró en la ciudad de Quito, Ecuador, que es una ciudad con un sector empresarial vibrante, donde las Pequeñas y Medianas Empresas (Pymes) juegan un papel clave en el crecimiento económico. Según la Cámara de Comercio de Quito (CCQ, 2023), en la ciudad operan alrededor de 8,500 Pymes en diversos sectores, como tecnología, comercio, manufactura y servicios. La adopción de tecnologías avanzadas, particularmente el cloud computing, ha experimentado un crecimiento considerable en los últimos años, con muchas empresas impulsadas por la necesidad de optimizar procesos, reducir costos y mejorar la seguridad de su infraestructura tecnológica.

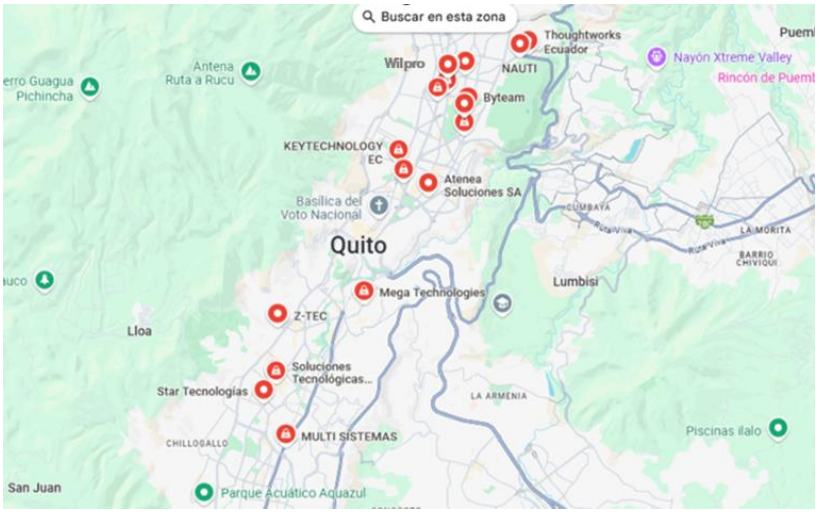
La infraestructura tecnológica en Quito ha mejorado notablemente, con un incremento en la conectividad y acceso a servicios en la nube, lo que ha permitido a las Pymes implementar soluciones tecnológicas más robustas para gestionar sus operaciones y proteger sus datos. Este estudio se enfoca en comprender cómo las Pymes locales han adoptado estas tecnologías y cómo enfrentan los desafíos de seguridad asociados.

Descripción del grupo de estudio:

El grupo de estudio estuvo compuesto por una muestra representativa de 10 Pymes ubicadas en la ciudad de Quito (ver figura 2) que han adoptado o están en proceso de adoptar soluciones de cloud computing.

Figura 2

Mapa de las ubicaciones de las empresas caso de estudio

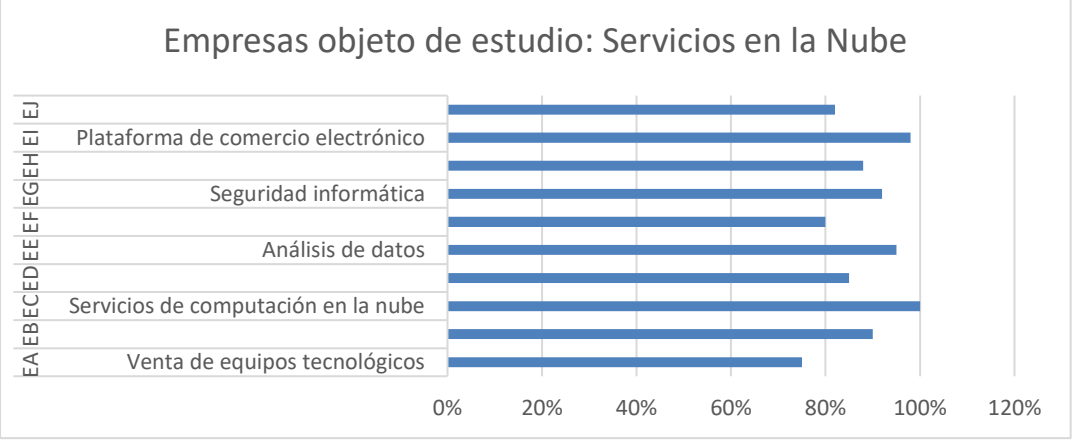


Fuente: Google Maps

Las empresas se seleccionaron de sectores como tecnología, comercio, manufactura y servicios, asegurando diversidad en tamaño empresarial, capacidad tecnológica y nivel de adopción de soluciones en la nube.

Figura 3

Datos de las PYMEs objeto de estudio



Fuente: Elaboración propia a partir de los datos obtenidos de las empresas objeto de estudio. (2025)

Dentro de las actividades de las pymes objeto de investigación, se tienen; aquellas que se dedican a la venta de equipos tecnológicos, marketing y desarrollo de software ERP/CRM, quienes ofrecen facturación electrónica y servicios de computación en la nube, publicidad digital y análisis de datos, diseño y desarrollo web, desarrollo de aplicaciones móviles, plataforma de comercio electrónico, entre otras.

Aquellas con porcentajes más altos, como los servicios de computación en la nube y las plataformas de comercio electrónico, indican una implementación robusta y probablemente extendida de servicios en la nube, ya que son los servicios que oferta y que ya han implementado para sí mismas. En otro grupo hay organizaciones que están incursionando en el cloud computing desde hace 6 meses a un año.

En contraste, empresas como las de venta de equipos tecnológicos o consultoría de TI, marketing, publicidad y diseño de web, con porcentajes más bajos, se encuentran dentro de la adopción más reciente, específicamente en etapas iniciales de exploración o implementación piloto.

Las encuestas se dirigieron a las áreas de Tecnología de la Información (TI), específicamente a responsables de la infraestructura tecnológica y la seguridad informática. Esto incluye a jefes de TI, administradores de sistemas y personal encargado de la gestión de riesgos tecnológicos y ciberseguridad. En empresas más pequeñas, donde las funciones tecnológicas podían estar concentradas en una sola persona, se encuestó a los gerentes generales o a los responsables directos de la implementación de tecnología.

Se consideraron tanto empresas que ya han experimentado incidentes de seguridad relacionados con la nube como las que no han reportado tales eventos. Esto permitió obtener una

visión completa sobre la preparación y respuesta ante incidentes de seguridad en la nube, así como sobre las prácticas actuales de ciberseguridad en las Pymes de Quito.

3.2. Enfoque y tipo de investigación

Para garantizar la validez y confiabilidad de los resultados, se empleó un enfoque metodológico mixto que permitió la triangulación de datos.

Según Hernández et al. (2014), el enfoque cualitativo se caracteriza por la exploración en profundidad de fenómenos complejos a través de la recolección y el análisis de datos no numéricos, como entrevistas, observaciones y documentos. Este enfoque busca comprender las experiencias, percepciones y significados que las personas atribuyen a sus contextos y acciones. A diferencia del enfoque cuantitativo, que se centra en medir y analizar datos estadísticos, el enfoque cualitativo se enfoca en la riqueza de la información y la interpretación subjetiva para desarrollar teorías y conceptos a partir de la experiencia directa y la interacción con los participantes.

Según Hernández et al. (2014), el enfoque cuantitativo se caracteriza por la recolección y análisis de datos numéricos para establecer patrones, probar teorías y generalizar resultados. Este enfoque busca medir variables objetivas y estadísticamente significativamente, utilizando encuestas, experimentos y análisis estadísticos para obtener resultados que puedan replicarse y validarse en contextos similares.

La investigación se centró en diagnosticar las vulnerabilidades y brechas de seguridad, para alcanzar este objetivo, se adoptó un enfoque mixto, combinando métodos cualitativos y cuantitativos. En el ámbito cualitativo, se revisó documentales exhaustivos, analizando normativas, estándares de seguridad, informes técnicos y estudios previos relacionados con la protección de infraestructuras de TI en entornos de computación en la nube. Para ello se empleó

una gestión de búsqueda en el buscador IEEE Xplore accediendo mediante https://ieeexplore.ieee.org/Xplorehelp/searching-ieee-xplore/search-results-page .

Este análisis permitió identificar factores internos, como las políticas de seguridad y la gestión de accesos, así como factores externos, incluyendo amenazas emergentes y regulaciones aplicables. A través de esta revisión, se obtuvo una visión holística de las principales brechas de seguridad, facilitando la formulación de estrategias adaptadas a la realidad de la PYME en estudio. Por otro lado, el componente cuantitativo implicó la recopilación y análisis de datos a través de encuestas enfocadas en las vulnerabilidades y métricas que midieron el alcance y la frecuencia de las amenazas en los sistemas de cloud computing.

La investigación se clasificó como exploratoria y descriptiva; fue exploratoria porque se propuso descubrir y comprender vulnerabilidades y brechas de seguridad aún no completamente identificadas en entornos específicos de cloud computing, y descriptiva porque tuvo como objetivo detallar las características de las vulnerabilidades encontradas y su impacto en la infraestructura. En la fase de diagnóstico, se analizaron los sistemas de TI para identificar debilidades en su diseño, combinando los métodos cualitativos con los cuantitativos obtenidos de pruebas técnicas.

Para la propuesta de mecanismo de seguridad en entornos de Cloud Computing se utilizó un enfoque mixto, puesto que, en el ámbito cualitativo, se realizó un análisis profundo de las mejores prácticas de seguridad mediante consultas a expertos, con el objetivo de diseñar mecanismos de seguridad avanzados adaptados a los riesgos específicos de cloud computing. La investigación se clasificó como propositiva y aplicada; fue propositiva porque se diseñó una propuesta de nuevos mecanismos de seguridad, tales como sistemas de autenticación avanzados y políticas de cifrado, que se ajustaron a los riesgos identificados en la fase anterior, y fue

aplicada porque las soluciones se enfocaron en problemas reales relacionados con la protección de datos y la optimización de accesos en infraestructuras cloud. En la fase de diseño, se desarrollaron las propuestas de mecanismos de seguridad, integrando el análisis cualitativo con la evaluación cuantitativa de su rendimiento, y se probaron en un entorno simulado para garantizar su viabilidad.

Para esta última fase validó los mecanismos de seguridad diseñados, se empleó un enfoque cuantitativo, se realizó un análisis retrospectivo de los incidentes de seguridad simulados realizados por las empresas, lo que permitió entender cómo reaccionaban ante escenarios de ataque. También se validó la propuesta para determinar si se adaptaba a las necesidades identificadas en la fase de diagnóstico. La investigación se clasificó como descriptiva, ya que se valoró si la propuesta se ajustaba a las condiciones controladas para evaluar la efectividad de los mecanismos de seguridad diseñados, y se describieron las conclusiones alcanzadas a partir del análisis retrospectivo.

Es decir, para este trabajo de investigación se utilizó un enfoque mixto, que garantizó una comprensión completa y profunda de los problemas de seguridad en las infraestructuras de cloud computing. El método cualitativo permitió obtener insights detallados y contextuales sobre las vulnerabilidades y brechas de seguridad desde la perspectiva de expertos y usuarios, facilitando así el diseño de mecanismos de seguridad adaptados a las necesidades específicas. Por su parte, el método cuantitativo resultó esencial para medir el impacto de las vulnerabilidades identificadas y validar la efectividad de los mecanismos propuestos, utilizando datos medibles y replicables que respaldaron las conclusiones alcanzadas.

Población y muestra

Población

La población de este estudio estuvo compuesta por todas las Pequeñas y Medianas Empresas (PYMEs) que operaban en la ciudad de Quito, Ecuador, y que habían adoptado o estaban en proceso de adoptar soluciones de cloud computing. Esta población incluyó 10 empresas de diversos sectores, como tecnología, comercio, manufactura, y servicios, abarcando diferentes niveles de capacidad tecnológica y tamaño organizacional.

Muestra

La muestra seleccionada para este estudio fue representativa de la población mencionada y se compuso de un conjunto de 10 PYMEs ubicadas en Quito que utilizan servicios de cloud computing. Se consideraron criterios de inclusión y exclusión claramente definidos, seleccionando aquellas empresas que presentaban una infraestructura de TI relevante para el diagnóstico de vulnerabilidades y brechas de seguridad en el uso de cloud computing.

Instrumento y técnicas

El instrumento empleado respondió a un cuestionario estructurado. Según Hernández et al. (2014), un cuestionario es un instrumento de recolección de datos que se compone de un conjunto de preguntas previamente diseñadas, las cuales se aplican de manera uniforme a todos los participantes de un estudio. Su principal propósito es obtener información específica y comparable sobre diversas variables, permitiendo a los investigadores cuantificar aspectos como opiniones, comportamientos, actitudes o características demográficas de una población. La estructura y formulación de las preguntas son fundamentales para asegurar la validez y confiabilidad de los datos recolectados.

En el contexto de esta investigación, se diseñó un cuestionario estructurado compuesto por 24 preguntas, cuidadosamente formuladas para abordar el objetivo de diagnosticar las vulnerabilidades y brechas de seguridad en el diseño de infraestructuras de TI para cloud

computing en las PYMEs de Quito. Estas preguntas se enfocaron en diferentes aspectos clave, como las prácticas actuales de seguridad, el nivel de adopción de medidas de protección, la frecuencia de incidentes de seguridad y la percepción de los riesgos asociados. El cuestionario fue diseñado para ser claro y directo, asegurando que los participantes pudieran responder con precisión y sin ambigüedades, lo que permitió obtener datos relevantes y útiles para el diagnóstico planteado.

Según Hernández et al. (2014), la encuesta es ampliamente utilizada en investigaciones sociales y de mercado, debido a su capacidad para obtener información directa de los individuos sobre temas específicos. Las encuestas pueden ser administradas de diversas maneras, como en persona, por teléfono, en línea o por correo, y su éxito depende de la claridad de las preguntas, la representatividad de la muestra y la precisión en la interpretación de los resultados.

En esta investigación, la técnica utilizada fue la encuesta, empleando un cuestionario basado en preguntas abiertas y cerradas. Esta técnica permitió medir actitudes, percepciones y opiniones de manera cualitativa, facilitando la obtención de datos estandarizados y comparables.

La escala Likert es un tipo de escala de respuesta que se utiliza comúnmente en cuestionarios para evaluar el grado de acuerdo o desacuerdo de los encuestados con una serie de afirmaciones o ítems. Según Hernández et al. (2014), la escala Likert se caracteriza por ofrecer opciones de respuesta que suelen variar en un rango de cinco a siete puntos, desde "totalmente en desacuerdo" hasta "totalmente de acuerdo." Este enfoque permite a los investigadores captar la intensidad de las opiniones de los participantes, proporcionando datos más matizados y facilitando el análisis estadístico de las actitudes y percepciones estudiadas.

3.3. Procedimiento de investigación

Fase 1: Diagnostico de vulnerabilidades y brechas de seguridad: En esta fase, se realizaron encuestas y un análisis exhaustivo de los sistemas de TI en una PYME para identificar

las vulnerabilidades en el diseño de la infraestructura de cloud computing. En el ámbito cualitativo, se llevó a cabo una revisión documental de normativas internacionales, estándares de seguridad informática (como ISO 27001 y NIST), informes técnicos, estudios académicos e informes de incidentes en infraestructuras de TI en entornos de computación en la nube. Esta revisión permitió identificar factores internos, como la gestión de accesos y la aplicación de políticas de seguridad, así como factores externos, incluyendo amenazas cibernéticas emergentes y regulaciones vigentes. A partir del análisis de estos documentos, se obtuvo una profunda comprensión de las brechas de seguridad existentes, lo que facilitó la formulación de estrategias adaptadas a la realidad de la PYME en estudio. Además, los datos obtenidos de pruebas técnicas, como escaneos de vulnerabilidades y auditorías, fueron cruciales para medir el alcance y la frecuencia de las amenazas. La combinación de los enfoques cualitativos y cuantitativos permitió obtener una visión integral de las brechas de seguridad en el sistema, brindando así una base sólida para diseñar una propuesta de seguridad efectiva para la infraestructura de TI en entornos de cloud computing.

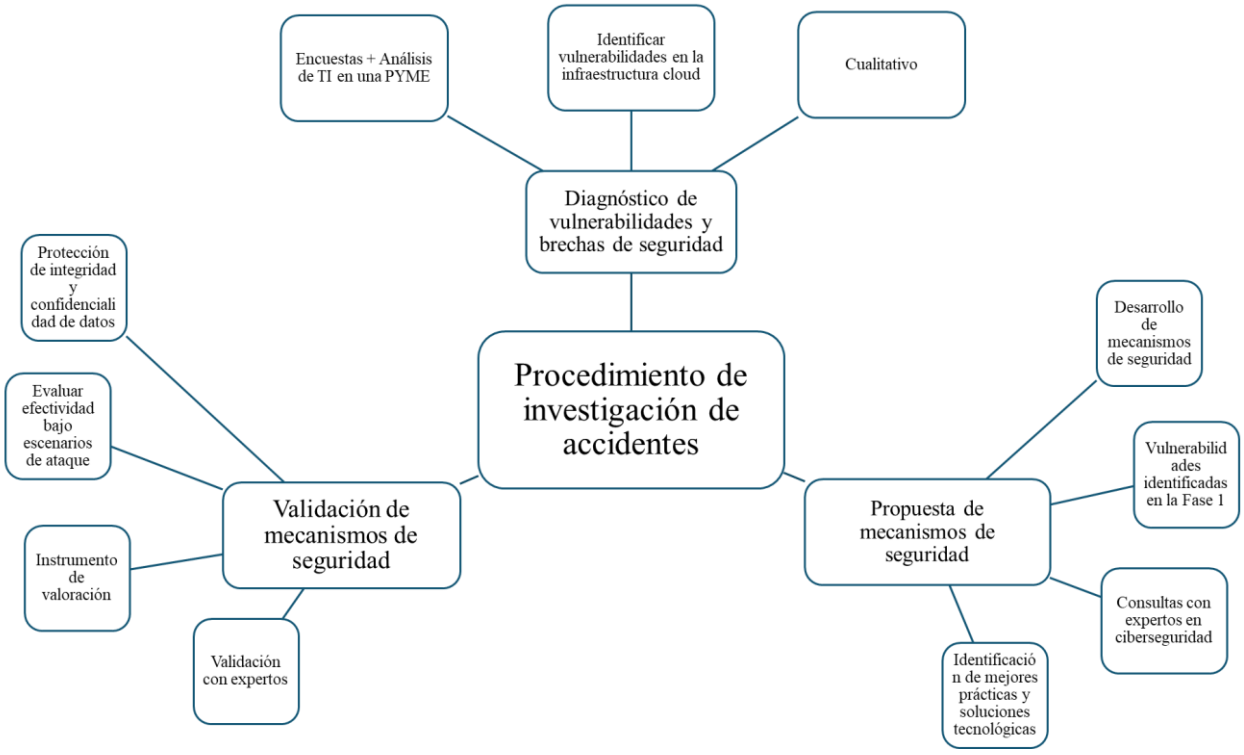
Fase 2: Propuesta de mecanismo de seguridad en entornos de Cloud Computing: Durante esta fase, se desarrollaron propuestas de mecanismos de seguridad avanzados, adaptados a las vulnerabilidades identificadas en la fase de diagnóstico. Para garantizar su efectividad, se realizaron consultas con expertos en ciberseguridad, quienes evaluaron y validaron los mecanismos propuestos. A través de este proceso, se identificaron las mejores prácticas y soluciones tecnológicas, asegurando que estuvieran alineadas con las necesidades específicas de la infraestructura de cloud computing de la PYME. Además, los expertos proporcionaron recomendaciones clave para mejorar la seguridad y optimizar la implementación de las medidas,

lo que permitió realizar ajustes en las estrategias y garantizar una protección adecuada de los sistemas de información.

Fase 3: Validación de los mecanismos de seguridad diseñados: En esta etapa, se llevó a cabo una validación de los mecanismos de seguridad diseñados, en colaboración con expertos en ciberseguridad, utilizando un instrumento de valoración (ver anexo 2). Los validadores analizaron la efectividad de los mecanismos bajo diferentes escenarios de ataque, evaluando su capacidad para mantener la integridad y confidencialidad de los datos. A través de un enfoque cuantitativo, se midió la respuesta de los sistemas ante diversos riesgos, mientras que se evaluó la resistencia de los mecanismos y su capacidad para mitigar amenazas. Paralelamente, el análisis cualitativo, basado en la retroalimentación de los expertos, permitió identificar vulnerabilidades, proponer ajustes y optimizar los mecanismos de seguridad. Este proceso de validación garantizó que las soluciones propuestas fueran técnicamente viables y adecuadas para proteger los sistemas de información en entornos de cloud computing.

Figura 4

Procedimiento de investigación



Fuente: Elaboración propia

3.4. Consideraciones bioéticas

Consentimiento Informado

Se garantizó que todos los participantes en la investigación otorgaran su consentimiento informado de manera consciente y voluntaria. Para ello, se les proporcionó una explicación detallada sobre el propósito del estudio, los procedimientos involucrados, los posibles riesgos y beneficios, así como su derecho a retirarse en cualquier momento sin enfrentar ninguna consecuencia negativa. Para asegurar la comprensión de todos los aspectos del estudio, se utilizaron formularios de consentimiento claros y redactados en un lenguaje accesible, ajustados al nivel de comprensión de los participantes. Se ofreció asistencia personalizada para responder a

cualquier pregunta o duda que los participantes pudieran tener, garantizando así que todos comprendieran plenamente los términos y condiciones antes de dar su consentimiento.

Confidencialidad

La confidencialidad de la información proporcionada por los participantes fue estrictamente mantenida a lo largo de todo el estudio. Los datos recopilados fueron anonimizados desde el principio, asignando códigos únicos a cada participante para proteger su identidad y la de sus respectivas empresas. Estos datos se almacenaron en sistemas altamente seguros, tanto físicos como digitales, para prevenir cualquier acceso no autorizado. Se implementaron medidas de seguridad robustas, como el cifrado de archivos y el acceso restringido, para asegurar la protección total de la información sensible. Solo el equipo de investigación tuvo acceso a la información identificable, y se establecieron protocolos rigurosos para garantizar que la privacidad de los participantes fuera resguardada en todo momento.

Transparencia y Honestidad

Durante todas las etapas de la investigación, se mantuvo un compromiso firme con la transparencia y la honestidad. Los resultados obtenidos fueron presentados de manera precisa, objetiva y sin sesgos, asegurando que reflejaran fielmente los datos recopilados. Cualquier conflicto de interés que surgiera fue declarado de manera explícita para mantener la integridad del estudio. Se garantizó a los participantes el acceso a los resultados del estudio, ofreciéndoles la oportunidad de conocer cómo se utilizaron los datos que proporcionaron y los hallazgos que surgieron de la investigación. Esta transparencia no solo fortaleció la confianza entre los participantes y el equipo de investigación, sino que también contribuyó a la credibilidad y utilidad de los resultados.

Evaluación de Riesgos y Beneficios

Se realizó una evaluación exhaustiva de los riesgos y beneficios asociados con la investigación, asegurando que estos fueran claramente identificados y abordados. Se tomaron todas las medidas necesarias para minimizar cualquier posible riesgo para los participantes, como la implementación de protocolos de seguridad adicionales y la supervisión constante del bienestar de los involucrados. Al mismo tiempo, se trabajó para maximizar los beneficios del estudio, tanto para las PYMEs participantes como para la comunidad empresarial en general. Esta evaluación también incluyó una revisión ética independiente del estudio, la cual se llevó a cabo para asegurar que todos los procedimientos y prácticas fueran apropiados, respetuosos y alineados con los más altos estándares éticos. Esta evaluación ética fue fundamental para garantizar que la investigación no solo cumpliera con las normativas vigentes, sino que también respetara los derechos y el bienestar de todos los participantes.

CAPITULO IV

RESULTADOS Y DISCUSIÓN

4.1. Análisis de Resultados

A continuación, se presentan los resultados tabulados y graficados del estudio, que han sido elaborados para proporcionar una visión clara y concisa de los hallazgos obtenidos. Estos resultados son el producto de un análisis exhaustivo de los datos recopilados, y están diseñados para facilitar la comprensión de las tendencias, patrones y relaciones identificadas a lo largo de la investigación.

Las tablas y gráficos ilustran de manera visual las estadísticas clave, permitiendo una interpretación más rápida y efectiva de la información. Este enfoque gráfico no solo realza la claridad de los datos, sino que también subraya la relevancia de estos en el contexto del estudio. A medida que se exploren los resultados, se destacarán las implicaciones y significados detrás de las cifras, ofreciendo un fundamento sólido para las conclusiones y recomendaciones que se derivan de este trabajo.

Sección 1: Información General

Tabla 3

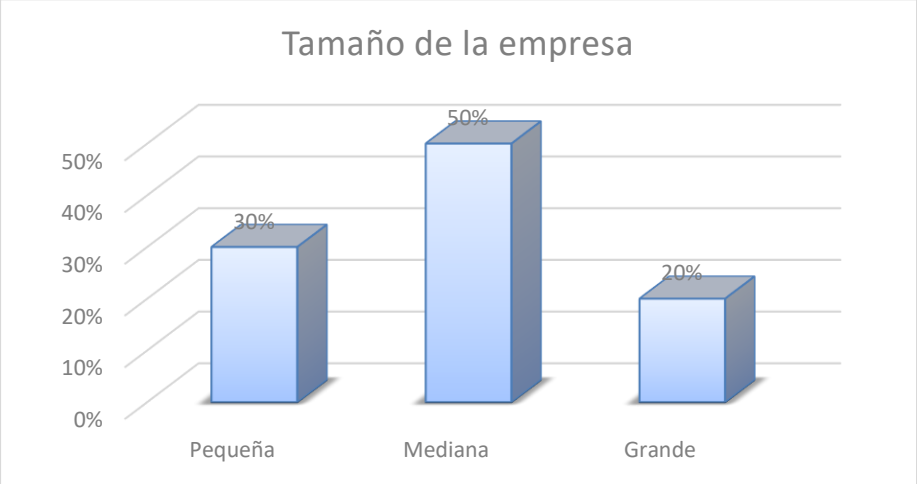
Pregunta 1. ¿Cuál es el tamaño de su empresa?

Opciones	Frecuencia	Porcentaje
Pequeña	3	30%
Mediana	5	50%
Grande	2	20%
Total	**10**	**100%**

Nota: Datos obtenidos a partir de la aplicación de la encuesta a Pymes en la ciudad de Quito (2025)

Figura 5

Tamaño de la empresa



Nota: Datos obtenidos a partir de la aplicación de la encuesta a Pymes en la ciudad de Quito (2025)

La mayoría de las empresas encuestadas son medianas (50%), seguidas de pequeñas (30%) y grandes (20%). Esto sugiere que las soluciones de computación en la nube están siendo adoptadas en mayor medida por empresas de tamaño medio, lo que puede indicar una mayor flexibilidad presupuestaria y operativa en comparación con las pequeñas y grandes empresas.

Tabla 4

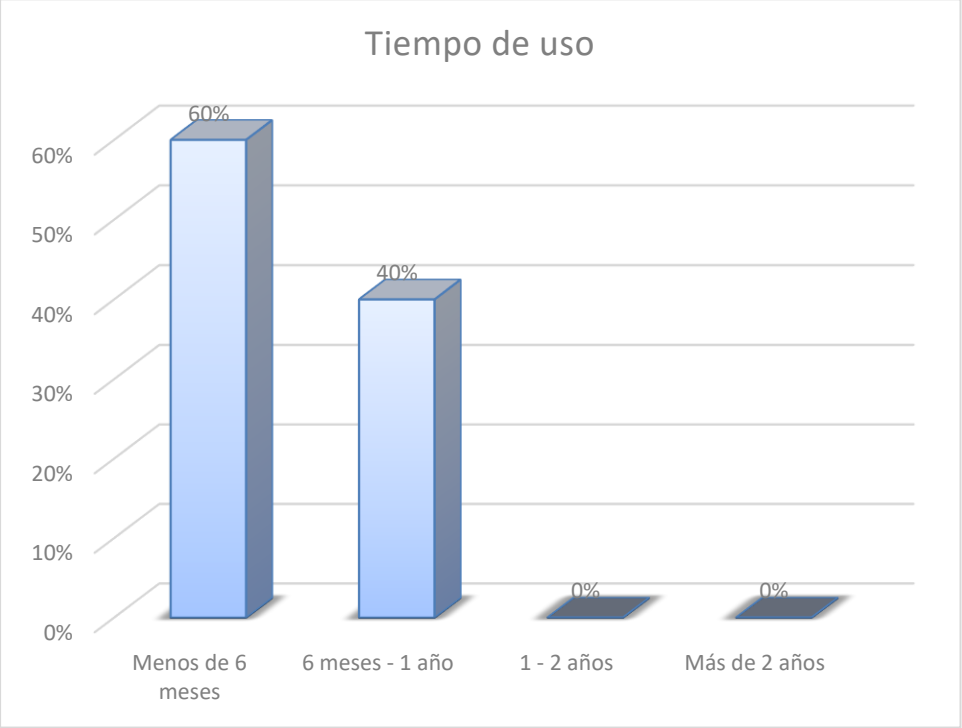
Pregunta 2. ¿Cuánto tiempo lleva su empresa utilizando soluciones de cloud computing?

Opciones	Frecuencia	Porcentaje
Menos de 6 meses	6	60%
6 meses - 1 año	4	40%
1 - 2 años	0	0%
Más de 2 años	0	0%
Total	**10**	**100%**

Nota: Datos obtenidos a partir de la aplicación de la encuesta a Pymes en la ciudad de Quito (2025)

Figura 6

Tiempo de uso de soluciones cloud computing



Nota: Datos obtenidos a partir de la aplicación de la encuesta a Pymes en la ciudad de Quito (2025)

El 60% de las empresas ha adoptado soluciones de computación en la nube en los últimos seis meses, mientras que el 40% lleva entre seis meses y un año. Ninguna empresa ha usado la nube por más de un año, lo que evidencia que su implementación es reciente y aún en proceso de consolidación.

Tabla 5

Pregunta 3. ¿Qué tipo de servicios de cloud computing utiliza su empresa?

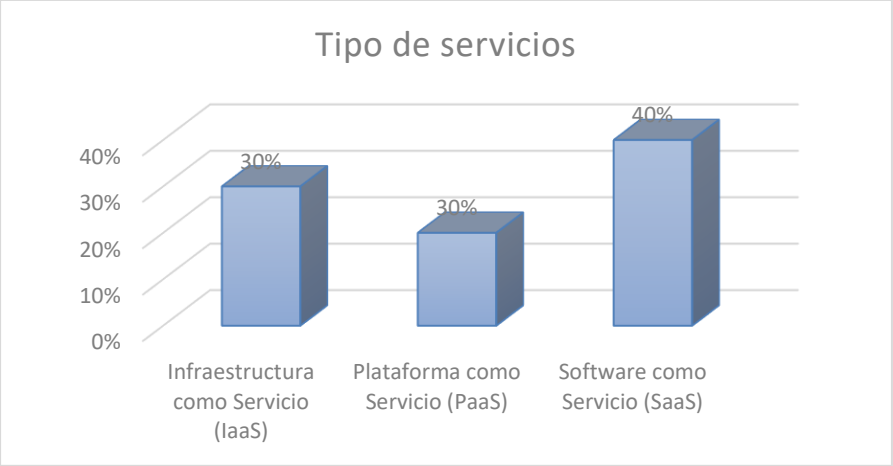
Opciones	Frecuencia	Porcentaje
Infraestructura como Servicio (IaaS)	3	30%
Plataforma como Servicio (PaaS)	2	20%
Software como Servicio (SaaS)	4	40%

Total	**10**	**100%**

Nota: Datos obtenidos a partir de la aplicación de la encuesta a Pymes en la ciudad de Quito (2025)

Figura 7

Tipo de servicios de cloud computing



Nota: Datos obtenidos a partir de la aplicación de la encuesta a Pymes en la ciudad de Quito (2025)

El Software como Servicio (SaaS) es el servicio más utilizado (40%), seguido de Infraestructura como Servicio (30%) y Plataforma como Servicio (30%). Esto sugiere que las empresas buscan soluciones listas para usar en lugar de gestionar infraestructura o plataformas complejas.

Tabla 6

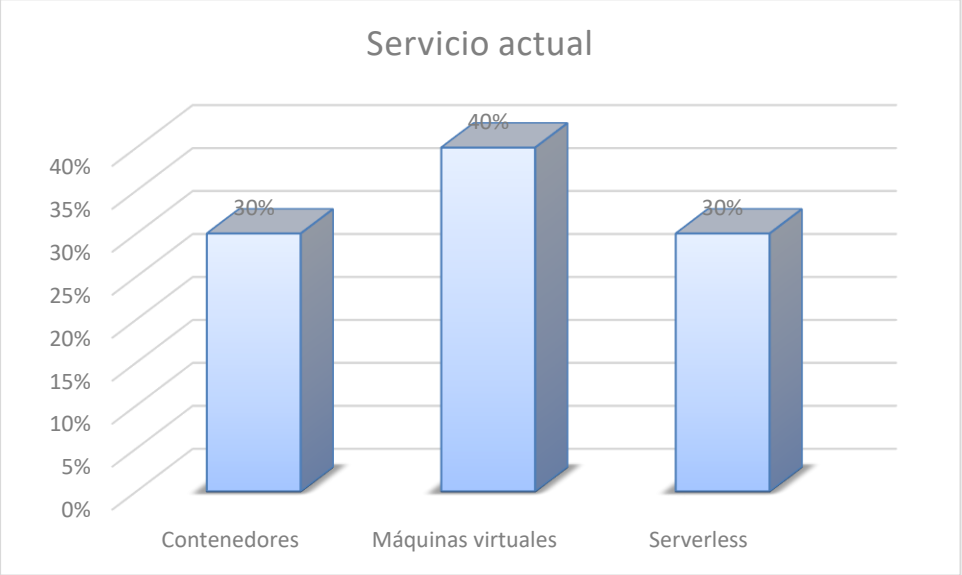
Pregunta 4. ¿Qué tipo de infraestructura en la nube está utilizando actualmente su empresa?

Opciones	Frecuencia	Porcentaje
Contenedores	3	30%
Máquinas virtuales	4	40%
Serverless	3	30%
Total	**10**	**100%**

Nota: Datos obtenidos a partir de la aplicación de la encuesta a Pymes en la ciudad de Quito (2025)

Figura 8

Servicio utilizado actualmente



Nota: Datos obtenidos a partir de la aplicación de la encuesta a Pymes en la ciudad de Quito (2025)

La mayoría de las empresas usa máquinas virtuales (40%), seguidas de contenedores (30%) y soluciones serverless (30%). Esto indica que la virtualización sigue siendo una opción popular por su compatibilidad y facilidad de gestión.

Tabla 7

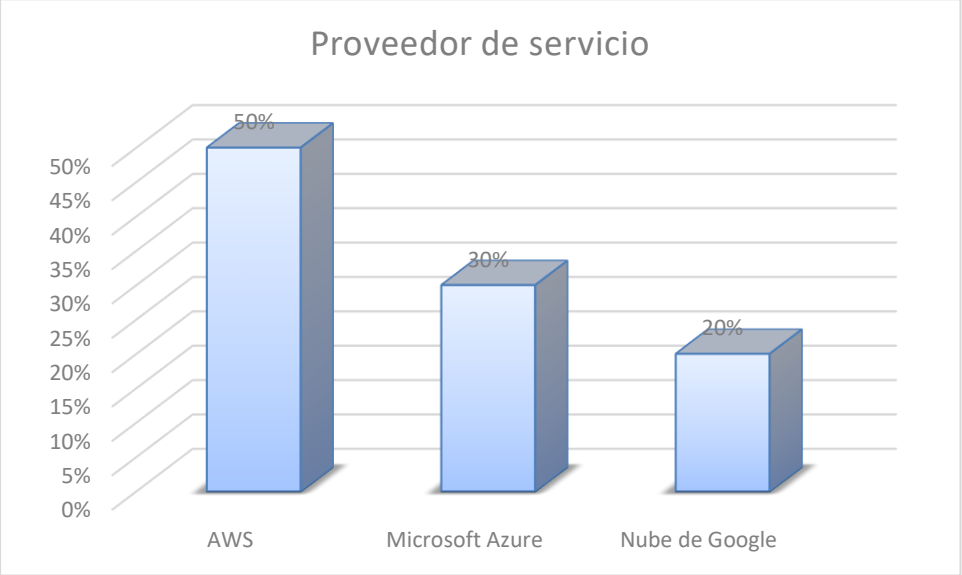
Pregunta 5. ¿Con qué proveedor tiene contratado el servicio de cloud computing?

Opciones	Frecuencia	Porcentaje
AWS	5	50%
Microsoft Azure	3	30%
Nube de Google	2	20%
Total	**10**	**100%**

Nota: Datos obtenidos a partir de la aplicación de la encuesta a Pymes en la ciudad de Quito (2025)

Figura 9

Proveedor del servicio cloud computing



Nota: Datos obtenidos a partir de la aplicación de la encuesta a Pymes en la ciudad de Quito (2025)

AWS es el proveedor más utilizado (50%), seguido por Microsoft Azure (30%) y Google Cloud (20%). Esto refleja la dominancia de AWS en el mercado de computación en la nube y la preferencia de las empresas por sus servicios y soporte.

Tabla 8

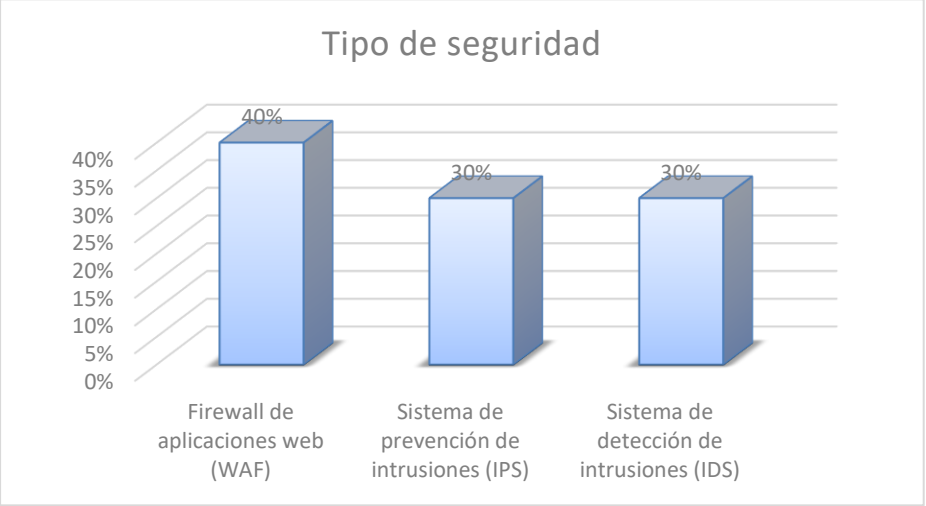
Pregunta 6. ¿Qué tipo de seguridad utiliza en su infraestructura de cloud computing?

Opciones	Frecuencia	Porcentaje
Firewall de aplicaciones web (WAF)	4	40%
Sistema de prevención de intrusiones (IPS)	3	30%
Sistema de detección de intrusiones (IDS)	3	30%
Total	**10**	**100%**

Nota: Datos obtenidos a partir de la aplicación de la encuesta a Pymes en la ciudad de Quito (2025)

Figura 10

Tipo de seguridad



Nota: Datos obtenidos a partir de la aplicación de la encuesta a Pymes en la ciudad de Quito (2025)

El Firewall de Aplicaciones Web (WAF) es la medida de seguridad más implementada (40%), mientras que el Sistema de Prevención de Intrusiones (IPS) y el de Detección de Intrusiones (IDS) se utilizan en menor medida (30% cada uno). Esto sugiere que las empresas priorizan la protección de aplicaciones web, pero aún hay margen para mejorar la seguridad en otros niveles.

Tabla 9

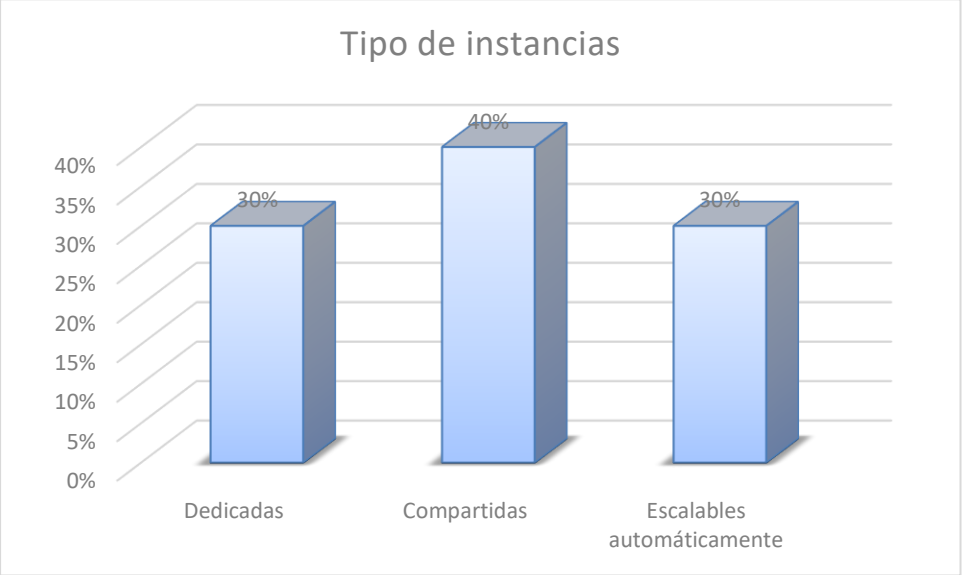
Pregunta 7. ¿Qué tipo de instancias utiliza su empresa en la nube?

Opciones	Frecuencia	Porcentaje
Dedicadas	3	30%
Compartidas	4	40%
Escalables automáticamente	3	30%
Total	**10**	**100%**

Nota: Datos obtenidos a partir de la aplicación de la encuesta a Pymes en la ciudad de Quito (2025)

Figura 11

Tipo de instancias



Nota: Datos obtenidos a partir de la aplicación de la encuesta a Pymes en la ciudad de Quito (2025)

La mayoría de las empresas usa instancias compartidas (40%), mientras que las dedicadas y escalables representan automáticamente el 30% cada una. Esto indica que las empresas buscan eficiencia en costos sin perder flexibilidad en el uso de recursos.

Tabla 10

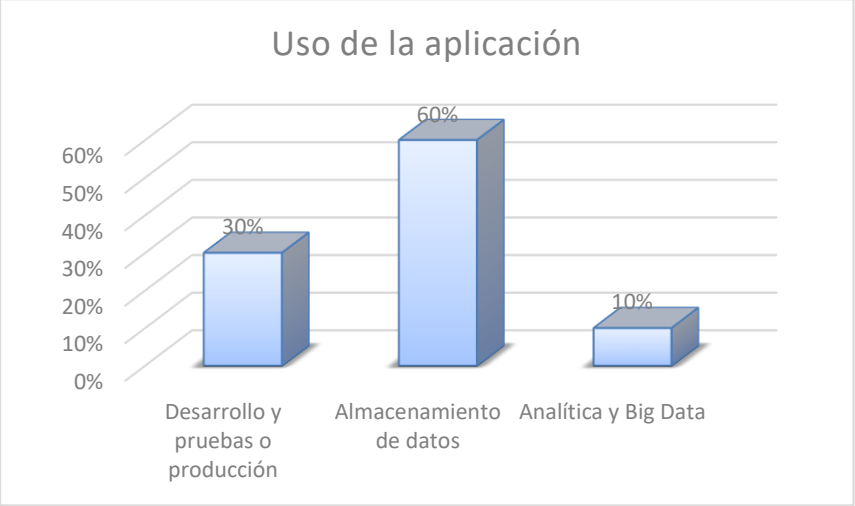
Pregunta 8. ¿Cómo utiliza su empresa las aplicaciones en la nube?

Opciones	Frecuencia	Porcentaje
Desarrollo y pruebas o producción	3	30%
Almacenamiento de datos	6	60%
Analítica y Big Data	1	10%
Total	**10**	**100%**

Nota: Datos obtenidos a partir de la aplicación de la encuesta a Pymes en la ciudad de Quito (2025)

Figura 12

Uso de aplicaciones en la nube



Nota: Datos obtenidos a partir de la aplicación de la encuesta a Pymes en la ciudad de Quito (2025)

La nube se usa principalmente para almacenamiento de datos (60%), seguido de desarrollo y pruebas o producción (30%). Esto refuerza la idea de que las empresas ven la nube como una solución confiable para la gestión de información, pero aún en exploración para otros usos estratégicos.

Sección 2: Diagnóstico de vulnerabilidades y brechas de seguridad

Tabla 11

Pregunta 9. ¿Cómo calificaría el nivel de seguridad general de su infraestructura de cloud computing?

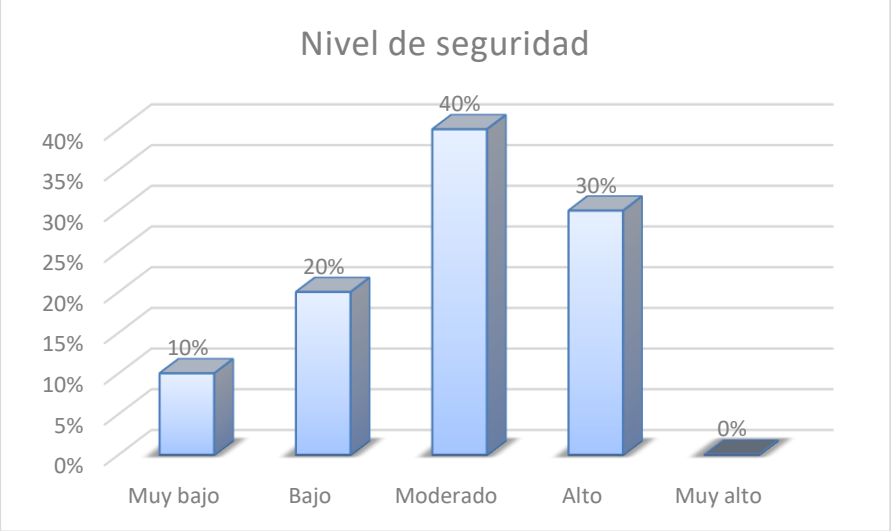
Opciones	Frecuencia	Porcentaje
Muy bajo	1	10%
Bajo	2	20%
Moderado	4	40%
Alto	3	30%

Muy alto	0	0%
Total	**10**	**100%**

Nota: Datos obtenidos a partir de la aplicación de la encuesta a Pymes en la ciudad de Quito (2025)

Figura 13

Nivel de seguridad de la infraestructura



Nota: Datos obtenidos a partir de la aplicación de la encuesta a Pymes en la ciudad de Quito (2025)

La mayoría de las empresas consideran que su seguridad en la nube es moderada (40%), seguida de alta (30%), baja (20%) y muy baja (10%). Esto indica que, aunque existen medidas de seguridad, aún hay oportunidades de mejora para alcanzar niveles óptimos de protección.

Tabla 12

Pregunta 10. ¿Qué tipo de incidentes de seguridad ha experimentado su empresa?

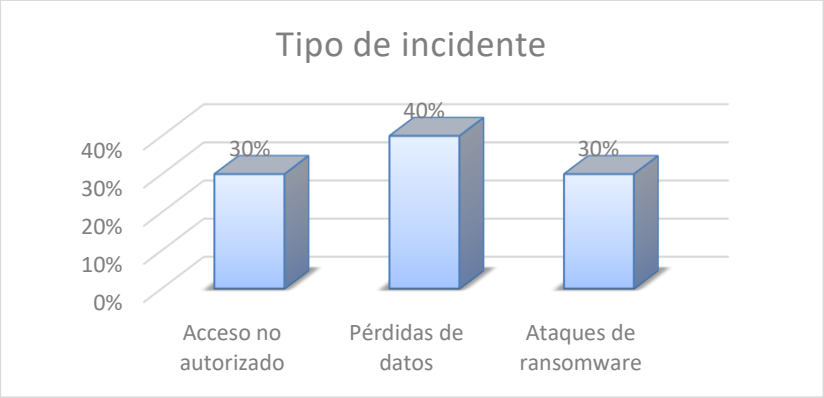
Opciones	Frecuencia	Porcentaje
Acceso no autorizado	3	30%
Pérdidas de datos	4	40%
Ataques de ransomware	3	30%

Total	**10**	**100%**

Nota: Datos obtenidos a partir de la aplicación de la encuesta a Pymes en la ciudad de Quito (2025)

Figura 14

Tipo de incidente



Nota: Datos obtenidos a partir de la aplicación de la encuesta a Pymes en la ciudad de Quito (2025)

Los incidentes más reportados fueron pérdidas de datos (40%), seguidos por accesos no autorizados y ataques de ransomware (ambos con 30%). Esto indica que la seguridad en la empresa enfrenta riesgos tanto internos como externos, con una vulnerabilidad significativa en la protección y recuperación de datos. La prevalencia del ransomware también sugiere la necesidad de reforzar las estrategias de prevención y respuesta ante ciberataques.

Tabla 13

Pregunta 11. ¿Qué medidas de seguridad a implementado o intentado implementar para proteger los datos en la nube?

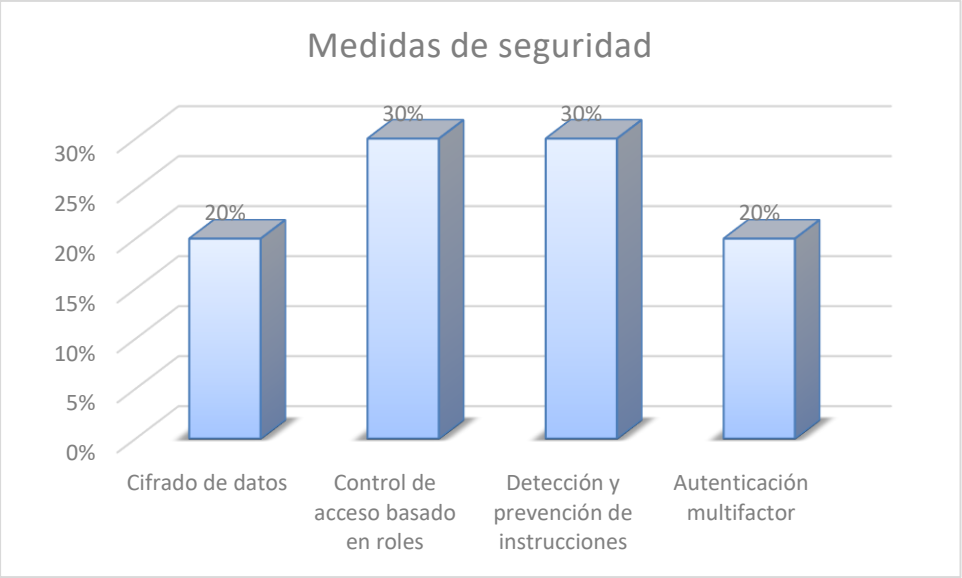
Opciones	**Frecuencia**	**Porcentaje**
Cifrado de datos	2	20%
Control de acceso basado en roles	3	30%
Detección y prevención de instrucciones	3	30%

Autenticación multifactor	2	20%
Total	**10**	**100%**

Nota: Datos obtenidos a partir de la aplicación de la encuesta a Pymes en la ciudad de Quito (2025)

Figura 15

Medidas de seguridad



Nota: Datos obtenidos a partir de la aplicación de la encuesta a Pymes en la ciudad de Quito (2025)

El control de acceso basado en roles y la detección de intrusiones fueron las medidas más adoptadas (30% cada una), mientras que la autenticación multifactor y el cifrado de datos fueron menos utilizados (20% cada una). Esto sugiere que, aunque existen esfuerzos por mejorar la seguridad, aún hay oportunidades para fortalecer la protección de los datos mediante tecnologías avanzadas.

Tabla 14

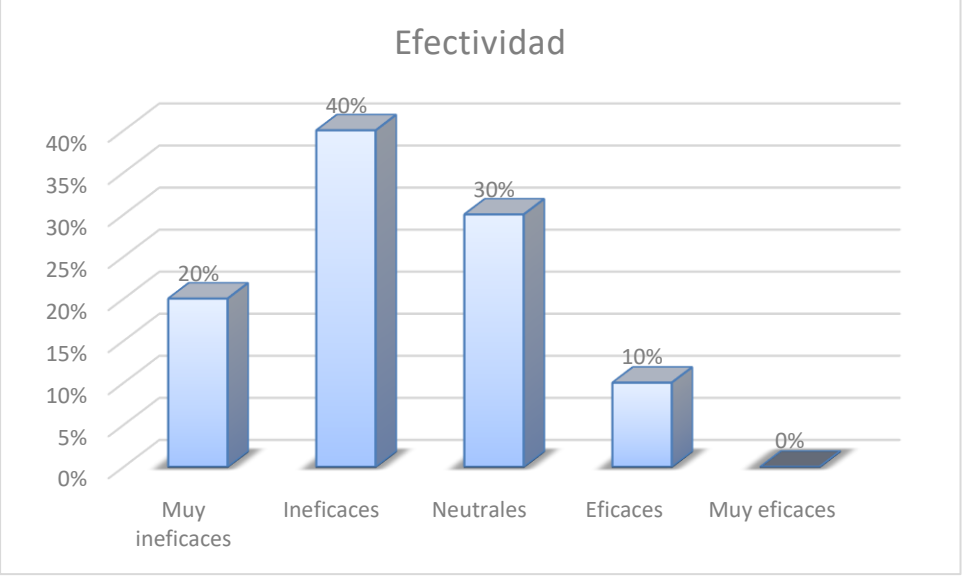
Pregunta 12. ¿Qué tan efectivas considera que son las medidas de seguridad que ha implementado?

Opciones	Frecuencia	Porcentaje
Muy ineficaces	2	20%
Ineficaces	4	40%
Neutrales	3	30%
Eficaces	1	10%
Muy eficaces	0	0%
Total	**10**	**100%**

Nota: Datos obtenidos a partir de la aplicación de la encuesta a Pymes en la ciudad de Quito (2025)

Figura 16

Efectividad de las medidas de seguridad



Nota: Datos obtenidos a partir de la aplicación de la encuesta a Pymes en la ciudad de Quito (2025)

El 60% de los encuestados considera que las medidas implementadas son ineficaces o muy ineficaces, mientras que solo el 10% las percibe como eficaces y ninguna las califica como muy eficaz. Y el 30% menciona que es neutral. Esto refleja una percepción generalizada de insuficiencia en las estrategias de seguridad actuales y la necesidad de mejoras sustanciales.

Tabla 15

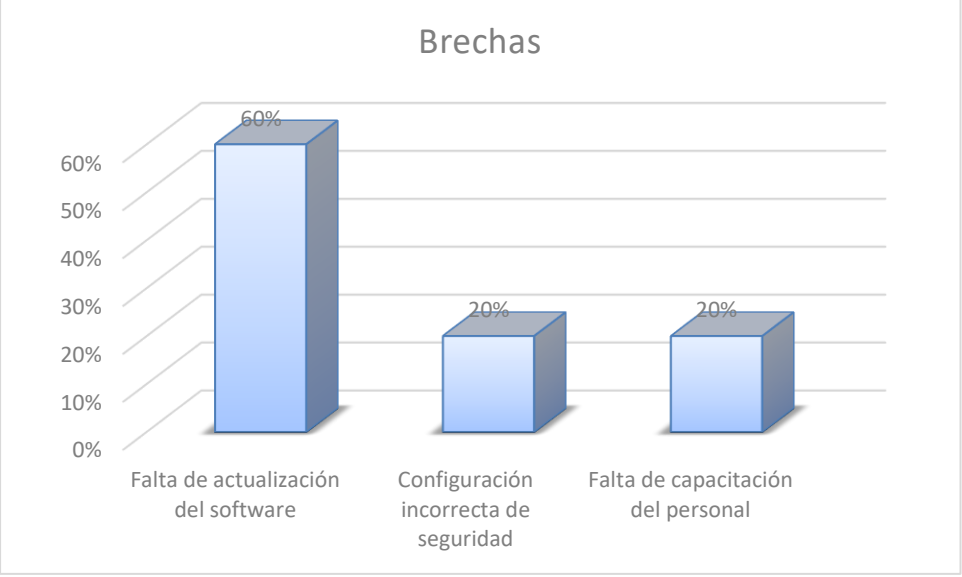
Pregunta 13. ¿Qué brechas de seguridad a identificado en su infraestructura de cloud computing?

Opciones	Frecuencia	Porcentaje
Falta de actualización del software	6	60%
Configuración incorrecta de seguridad	2	20%
Falta de capacitación del personal	2	20%
Total	**10**	**100%**

Nota: Datos obtenidos a partir de la aplicación de la encuesta a Pymes en la ciudad de Quito (2025)

Figura 17

Brechas de seguridad



Nota: Datos obtenidos a partir de la aplicación de la encuesta a Pymes en la ciudad de Quito (2025)

La falta de actualización del software es la principal brecha de seguridad (60%), seguida de configuraciones incorrectas y falta de capacitación del personal (20% cada una). Esto evidencia que las vulnerabilidades pueden mitigarse con mejores prácticas en mantenimiento técnico y una mayor formación del equipo.

Sección 3 Propuesta de mecanismos de seguridad avanzados

Tabla 16

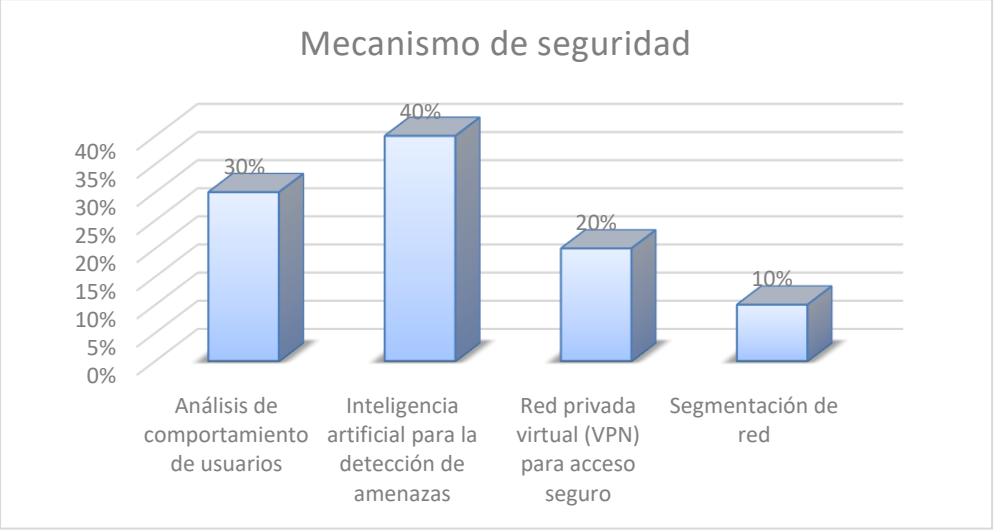
Pregunta 14. ¿Qué mecanismos de seguridad avanzados considera necesario para su infraestructura de TI en la nube?

Opciones	Frecuencia	Porcentaje
Análisis de comportamiento de usuarios	3	30%
Inteligencia artificial para la detección de amenazas	4	40%
Red privada virtual (VPN) para acceso seguro	2	20%
Segmentación de red	1	10%
Total	**10**	**100%**

Nota: Datos obtenidos a partir de la aplicación de la encuesta a Pymes en la ciudad de Quito (2025)

Figura 18

Mecanismos de seguridad



Nota: Datos obtenidos a partir de la aplicación de la encuesta a Pymes en la ciudad de Quito (2025)

La inteligencia artificial para la detección de amenazas es la opción más valorada (40%), seguida del análisis de comportamiento de usuarios (30%). Esto indica un interés por soluciones avanzadas que permitan una detección más proactiva de amenazas y un enfoque más automatizado en la gestión de riesgos.

Tabla 17

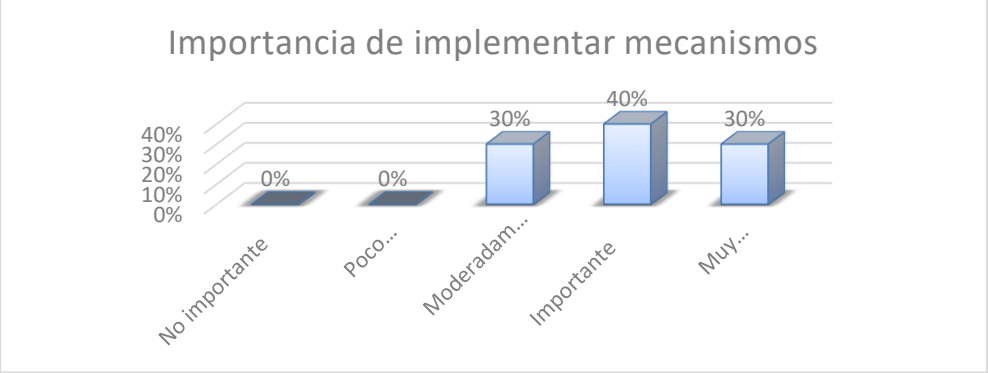
Pregunta 15. ¿Cómo calificaría la importancia de implementar mecanismos de seguridad avanzados en su infraestructura de cloud computing?

Opciones	Frecuencia	Porcentaje
No importante	0	0%
Poco importante	0	0%
Moderadamente importante	3	30%
Importante	4	40%
Muy importante	3	30%
Total	**10**	**100%**

Nota: Datos obtenidos a partir de la aplicación de la encuesta a Pymes en la ciudad de Quito (2025)

Figura 19

Importancia de implementar mecanismos de seguridad



Nota: Datos obtenidos a partir de la aplicación de la encuesta a Pymes en la ciudad de Quito (2025)

El 70% de los encuestados considera que implementar mecanismos avanzados de seguridad es importante o muy importante, mientras que el 30% lo califica como moderadamente importante. Esto refuerza la necesidad de adoptar estrategias más sofisticadas para mejorar la seguridad en la nube.

Tabla 18

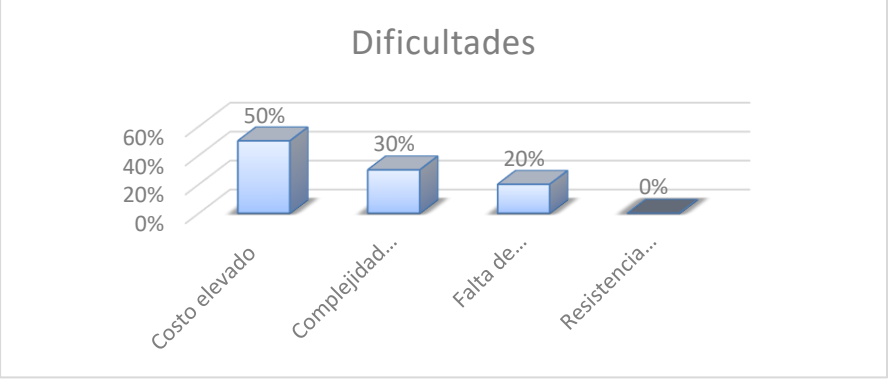
Pregunta 16. ¿Qué dificultades ha encontrado al implementar mecanismos de seguridad avanzados?

Opciones	Frecuencia	Porcentaje
Costo elevado	5	50%
Complejidad técnica	3	30%
Falta de conocimientos especializados	2	20%
Resistencia del personal	0	0%
Total	**10**	**100%**

Nota: Datos obtenidos a partir de la aplicación de la encuesta a Pymes en la ciudad de Quito (2025)

Figura 20

Dificultades en la implementación de mecanismos de seguridad



Nota: Datos obtenidos a partir de la aplicación de la encuesta a Pymes en la ciudad de Quito (2025)

El costo elevado (50%) y la complejidad técnica (30%) son las principales barreras para la implementación de mecanismos avanzados. La falta de conocimientos especializados (20%) también representa un desafío, lo que resalta la necesidad de inversión en capacitación y recursos adecuados.

Tabla 19

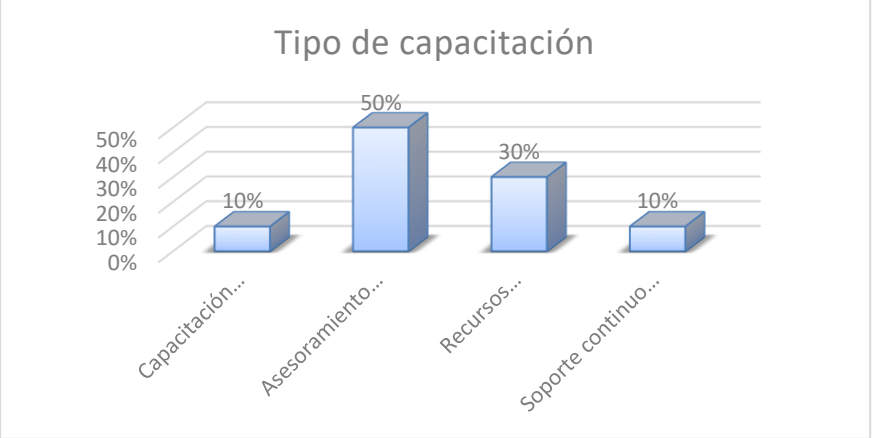
Pregunta 17. ¿Qué tipo de capacitación o soporte adicional considera necesario para mejorar la seguridad en la nube?

Opciones	Frecuencia	Porcentaje
Capacitación técnica	1	10%
Asesoramiento en mejores prácticas	5	50%
Recursos financieros	3	30%
Soporte continuo de proveedores	1	10%
Total	**10**	**100%**

Nota: Datos obtenidos a partir de la aplicación de la encuesta a Pymes en la ciudad de Quito (2025)

Figura 21

Tipo de capacitación



Nota: Datos obtenidos a partir de la aplicación de la encuesta a Pymes en la ciudad de Quito (2025)

El asesoramiento en mejores prácticas es la principal necesidad identificada (50%), seguida por recursos financieros (30%). Esto sugiere que la formación y el acceso a financiamiento son claves para mejorar la seguridad en la nube y optimizar la implementación de nuevas estrategias.

Sección 4 Validación de mecanismos de seguridad

Tabla 20

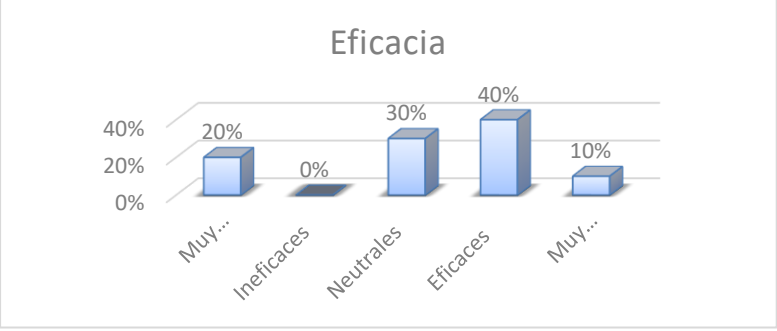
Pregunta 18. ¿Qué tan eficaz considera que serían los mecanismos de seguridad avanzados propuestos para resistir ataques cibernéticos?

Opciones	Frecuencia	Porcentaje
Muy ineficaces	2	20%
Ineficaces	0	0%
Neutrales	3	30%
Eficaces	4	40%
Muy eficaces	1	10%
Total	**10**	**100%**

Nota: Datos obtenidos a partir de la aplicación de la encuesta a Pymes en la ciudad de Quito (2025)

Figura 22

Eficacia de los mecanismos de seguridad



Nota: Datos obtenidos a partir de la aplicación de la encuesta a Pymes en la ciudad de Quito (2025)

El 50% de los encuestados considera que los mecanismos propuestos serán eficaces o muy eficaces, mientras que el 30% se mantiene neutral. Un 20% los califica como muy ineficaces, lo que indica la necesidad de pruebas y ajustes para asegurar su efectividad en el contexto específico de la empresa.

Tabla 21

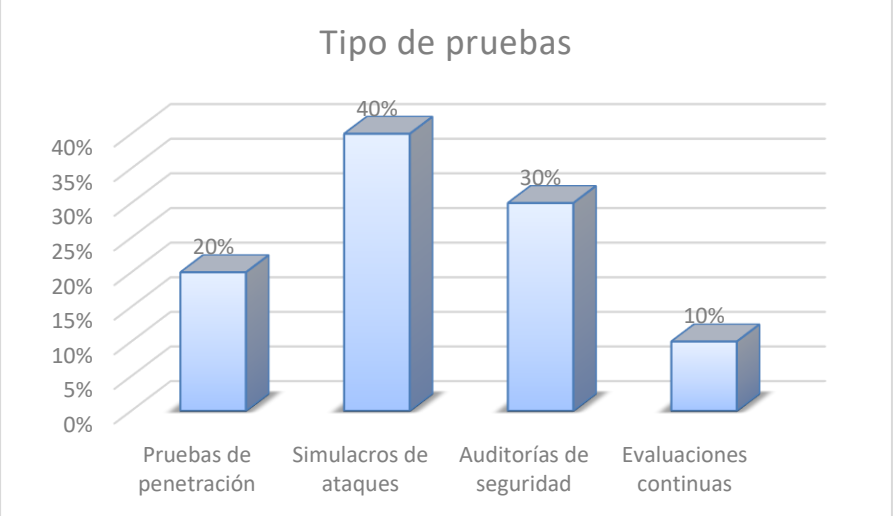
Pregunta 19. ¿Qué tipo de pruebas realiza su empresa para validar la eficacia de los mecanismos de seguridad en la nube?

Opciones	Frecuencia	Porcentaje
Pruebas de penetración	2	20%
Simulacros de ataques	4	40%
Auditorías de seguridad	3	30%
Evaluaciones continuas	1	10%
Total	**10**	**100%**

Nota: Datos obtenidos a partir de la aplicación de la encuesta a Pymes en la ciudad de Quito (2025)

Figura 23

Tipos de prueba para validar la eficacia de los mecanismos de seguridad



Nota: Datos obtenidos a partir de la aplicación de la encuesta a Pymes en la ciudad de Quito (2025)

Los simulacros de ataques (40%) y las auditorías de seguridad (30%) son las pruebas más comunes, pruebas de penetración con un (20%), mientras que las evaluaciones continuas son poco utilizadas (10%). Esto sugiere que, si hay buenos esfuerzos por evaluar la seguridad, se requiere un enfoque más sistemático y recurrente.

Tabla 22

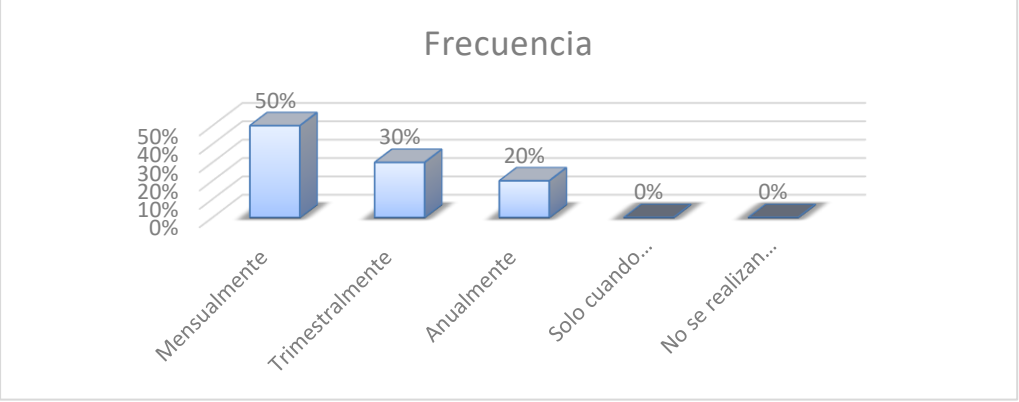
Pregunta 20. ¿Con que frecuencia realiza su empresa evaluaciones de seguridad en su infraestructura de cloud computing?

Opciones	Frecuencia	Porcentaje
Mensualmente	5	50%
Trimestralmente	3	30%
Anualmente	2	20%
Solo cuando ocurre u incidente	0	0%
No se realizan evaluaciones	0	0%
Total	**10**	**100%**

Nota: Datos obtenidos a partir de la aplicación de la encuesta a Pymes en la ciudad de Quito (2025)

Figura 24

Frecuencias de las evaluaciones de seguridad



Nota: Datos obtenidos a partir de la aplicación de la encuesta a Pymes en la ciudad de Quito (2025)

El 50% de las empresas realiza evaluaciones mensuales, mientras que el 30% las hace trimestralmente y el 20% anual. La ausencia de respuestas en las opciones "solo cuando ocurre un incidente" o "no se realizan evaluaciones" indica un compromiso con la seguridad, aunque con variaciones en la periodicidad.

Tabla 23

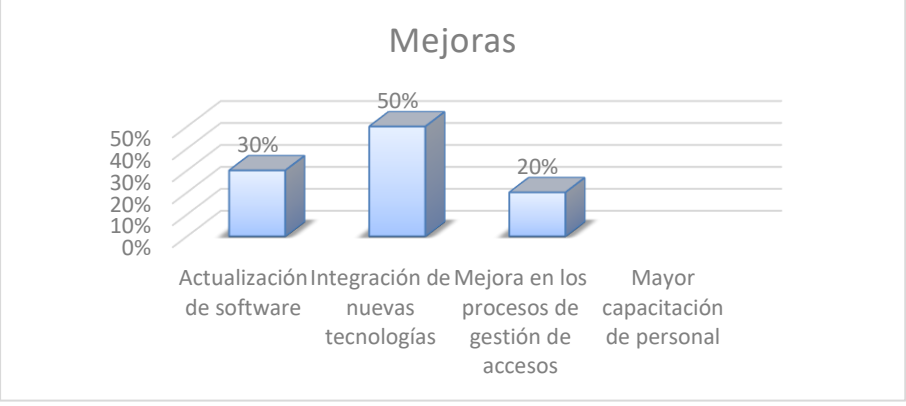
Pregunta 21. ¿Qué mejoras considera necesarias en los mecanismos de seguridad actuales para fortalecer la defensa contra amenazas emergentes?

Opciones	Frecuencia	Porcentaje
Actualización de software	3	30%
Integración de nuevas tecnologías	5	50%
Mejora en los procesos de gestión de accesos	2	20%
Mayor capacitación de personal	0%	0%
Total	**10**	**100%**

Nota: Datos obtenidos a partir de la aplicación de la encuesta a Pymes en la ciudad de Quito (2025)

Figura 25

Mejoras necesarias en los mecanismos



Nota: Datos obtenidos a partir de la aplicación de la encuesta a Pymes en la ciudad de Quito (2025)

La integración de nuevas tecnologías (50%) es la principal mejora requerida, seguida de la actualización de software (30%). Esto sugiere que la modernización de la infraestructura y la implementación de soluciones innovadoras son esenciales para reforzar la ciberseguridad.

Tabla 24

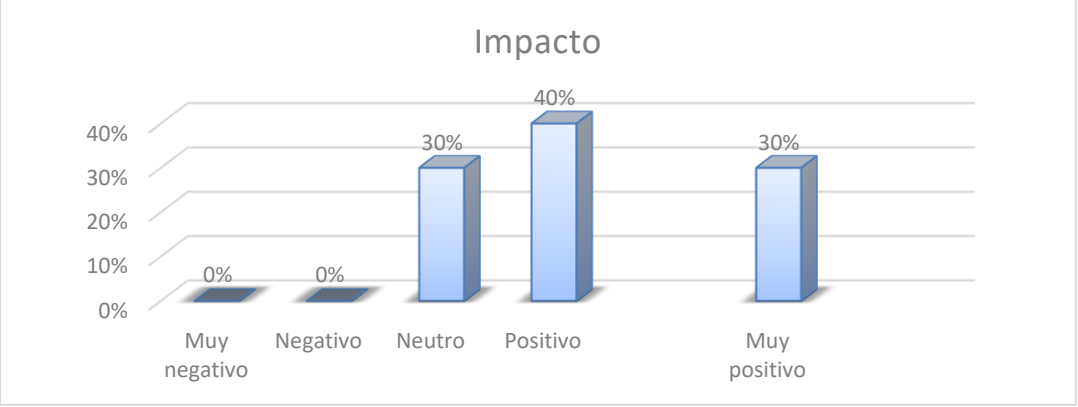
Pregunta 22. ¿Qué impacto ha tenido la implementación de mecanismos de seguridad avanzados en la integridad y confidencialidad de los datos en su empresa?

Opciones	Frecuencia	Porcentaje
Muy negativo	0	0%
Negativo	0	0%
Neutro	3	30%
Positivo	4	40%
Muy positivo	3	30%
Total	**10**	**100%**

Nota: Datos obtenidos a partir de la aplicación de la encuesta a Pymes en la ciudad de Quito (2025)

Figura 26

Impacto de la implementación de mecanismos



Nota: Datos obtenidos a partir de la aplicación de la encuesta a Pymes en la ciudad de Quito (2025)

El 70% de los encuestados considera que la implementación de estos mecanismos ha tenido un impacto positivo o muy positivo, mientras que el 30% se mantiene neutral. Esto indica que las mejoras en seguridad han sido beneficiosas, pero aún hay espacio para optimizar su efectividad.

Tabla 25

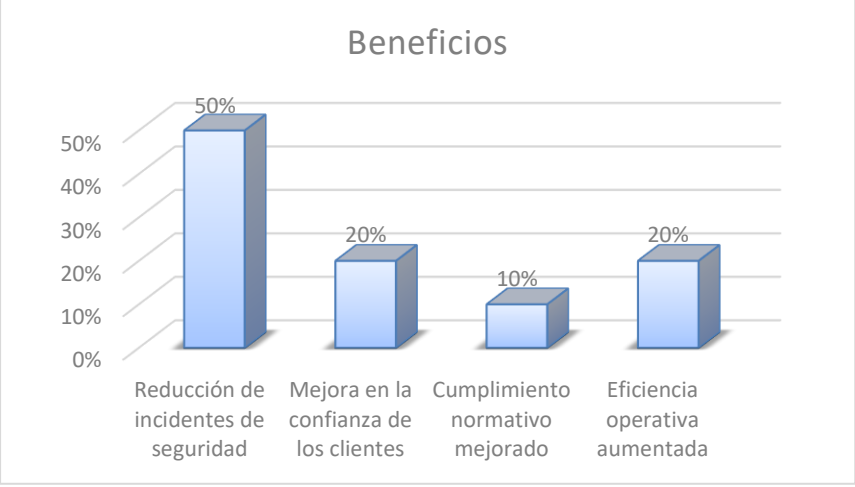
Pregunta 23: ¿Qué beneficios adicionales ha observado su empresa al fortalecer la infraestructura de seguridad en cloud computing?

Opciones	Frecuencia	Porcentaje
Reducción de incidentes de seguridad	5	50%
Mejora en la confianza de los clientes	2	20%
Cumplimiento normativo mejorado	1	10%
Eficiencia operativa aumentada	2	20%
Total	**10**	**100%**

Nota: Datos obtenidos a partir de la aplicación de la encuesta a Pymes en la ciudad de Quito (2025)

Figura 27

Beneficios adicionales al fortalecer la infraestructura de seguridad



Nota: Datos obtenidos a partir de la aplicación de la encuesta a Pymes en la ciudad de Quito (2025)

La reducción de incidentes de seguridad (50%) es el beneficio más destacado, seguido de la mejora en la confianza de los clientes y la eficiencia operativa (20% cada uno). Esto demuestra que una infraestructura de seguridad robusta no solo protege los datos, sino que también aporta valor a la empresa en términos de reputación y desempeño.

Tabla 26

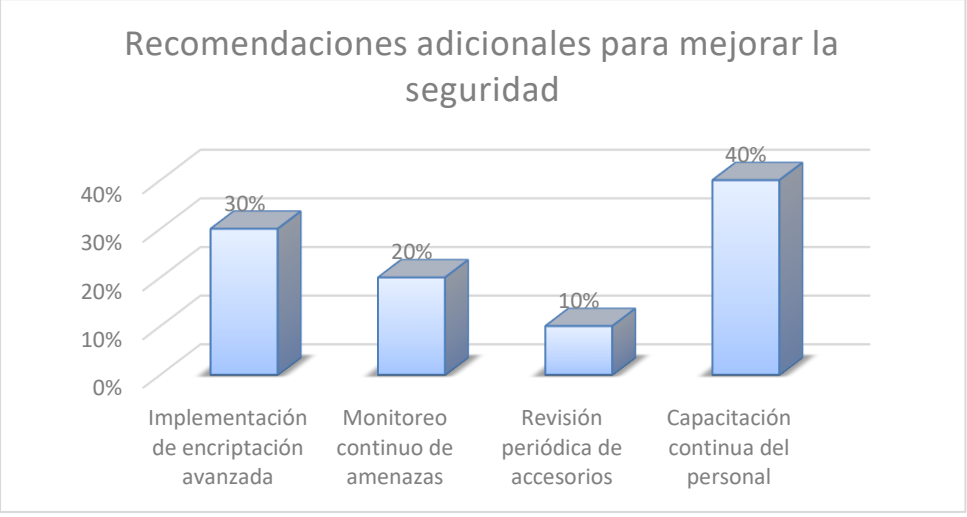
Pregunta 24: ¿Qué recomendaciones adicionales tiene para mejorar la seguridad en entornos de cloud computing en su empresa?

Opciones	Frecuencia	Porcentaje
Implementación de encriptación avanzada	3	30%
Monitoreo continuo de amenazas	2	20%
Revisión periódica de accesorios	1	10%
Capacitación continua del personal	4	40%
Total	**10**	**100%**

Nota: Datos obtenidos a partir de la aplicación de la encuesta a Pymes en la ciudad de Quito (2025)

Figura 28

Recomendaciones adicionales tiene para mejorar la seguridad



Nota: Datos obtenidos a partir de la aplicación de la encuesta a Pymes en la ciudad de Quito (2025)

La capacitación continua del personal es la recomendación más mencionada (40%), seguida de la implementación de encriptación avanzada (30%) y el monitoreo continuo de amenazas (20%). Esto refuerza la idea de que la seguridad en la nube depende no solo de la tecnología, sino también del conocimiento y preparación del equipo.

4.2. Resultados Cualitativos

A través del análisis documental de estándares, informes y estudios previos, se identificaron prácticas esenciales en la protección de datos y gestión de amenazas, destacando la importancia de mecanismos como la autenticación multifactor, el cifrado de datos y el monitoreo de amenazas. Se evidencia que las empresas utilizan herramientas avanzadas como Splunk, ELK Stack y Wireshark para la evaluación de riesgos, lo que permite una respuesta eficiente ante incidentes de seguridad. Sin embargo, se observa una brecha en la implementación de estrategias de seguridad integrales, lo que sugiere la necesidad de fortalecer políticas internas y procesos de auditoría. En esta línea a continuación se presenta en la siguiente matriz de descripción de análisis cualitativo:

Tabla 27

Matriz de descripción de análisis cualitativo

Categoría	Fuente	Resultados	Recomendaciones
Documentos Analizados	Normativas ISO 27001, NIST 800-53, GDPR	Se identificó la necesidad de aplicar controles más rigurosos en la gestión de accesos y cifrado de datos.	Implementar autenticación multifactor y cifrado robusto.
	Políticas de seguridad interna de empresas estudiadas	Variaciones en la aplicación de medidas de seguridad, dependiendo del tamaño y recursos de la empresa.	Estandarizar políticas de seguridad para todas las Pymes.
Análisis de Estándares	ISO 27001, NIST 800-53, CIS Controls	Se detectó un bajo nivel de cumplimiento en Pymes, especialmente en la gestión de incidentes.	Aplicar protocolos de respuesta ante incidentes de seguridad.

Informes y Estudios	Reportes de ciberseguridad de AWS y Google	Falta de actualización en herramientas de monitoreo y respuesta ante ataques.	Automatizar procesos de seguridad y capacitar al personal.
	Estudios sobre brechas en seguridad en Cloud Computing	Se evidencia desconocimiento sobre herramientas avanzadas de protección en la nube.	Realizar programas de formación en seguridad informática.
Descripción Comparativa	Comparación de herramientas de seguridad en Pymes	Las empresas con estrategias definidas utilizan herramientas como AWS CloudTrail y Google SCC, mientras que otras carecen de monitoreo activo.	Fomentar la adopción de plataformas de seguridad escalables.
	Evaluación del nivel de madurez en ciberseguridad	Empresas con auditorías regulares y capacitación presentan menor índice de incidentes de seguridad.	Incentivar auditorías continuas y simulaciones de ataques.

Nota: Datos obtenidos a partir de la revisión de la literatura (2025)

4.3. Discusión de Resultados

La adopción de soluciones de computación en la nube por parte de empresas medianas (50%) sugiere una correlación entre el tamaño organizacional y la flexibilidad operativa. Según Parra et al. (2023) las empresas medianas tienen mayor capacidad para adaptarse a nuevas tecnologías en comparación con las pequeñas, que pueden enfrentar limitaciones presupuestarias, y las grandes, que pueden tener infraestructuras más rígidas. La reciente incorporación de la nube, con un 60% de empresas adoptándola en los últimos seis meses, coincide con lo señalado por Bueno y Haz (2022), quienes destacan que la computación en la nube está en constante crecimiento debido a su escalabilidad y reducción de costos. Sin embargo, la falta de empresas con más de un año de uso refleja un proceso de adopción aún en fase temprana y la necesidad de evaluar su impacto a largo plazo.

El predominio de Software como Servicio (SaaS) (40%) sobre Infraestructura como Servicio (IaaS) (30%) y Plataforma como Servicio (PaaS) (30%) confirma la tendencia observada por Cardona (2022), quien sostiene que las empresas prefieren soluciones listas para

usar que minimicen la gestión de infraestructura. Además, el uso mayoritario de máquinas virtuales (40%) en comparación con contenedores (30%) y soluciones serverless (30%) respalda lo argumentado por Eljak et al. (2024), quienes afirman que la virtualización sigue siendo la opción dominante por su compatibilidad con sistemas heredados y su facilidad de administración. Estos hallazgos evidencian que, aunque hay un interés creciente en arquitecturas modernas, las empresas aún dependen de enfoques tradicionales.

En cuanto a los proveedores de cloud computing, AWS lidera el mercado con un 50%, seguido por Microsoft Azure (30%) y Google Cloud (20%), lo cual coincide con las estadísticas presentadas por Flores (2023), quien establece que AWS es el proveedor con mayor participación global. Este dominio puede explicarse por la amplitud de servicios que ofrece y su infraestructura consolidada (Rountree & Castrillo, 2013). Sin embargo, la diversificación de proveedores sugiere que las empresas están evaluando distintas opciones en función de costos, compatibilidad y soporte técnico.

En términos de seguridad, el Firewall de Aplicaciones Web (WAF) es la medida más implementada (40%), mientras que la detección y prevención de intrusiones (30% cada una) son menos utilizadas. De acuerdo con Garzón et al. (2022), la preferencia por WAF refleja la prioridad de las empresas en la protección contra ataques basados en web, aunque la baja adopción de otras medidas indica vulnerabilidades en otros niveles. Esto se corrobora con los incidentes reportados, donde la pérdida de datos (40%) y los accesos no autorizados (30%) son las amenazas más comunes, alineándose con lo identificado por Gutiérrez (2018), que resalta la importancia del cifrado de datos y la autenticación multifactorial para mitigar estos riesgos.

El 60% de las empresas considera que sus medidas de seguridad actuales son ineficaces o muy ineficaces, lo que demuestra una percepción de insuficiencia en las estrategias de

protección. Según Irshad et al. (2021) muchas organizaciones implementan medidas de seguridad sin una evaluación integral de riesgos, lo que reduce su efectividad. La falta de actualización del software, identificada como la principal brecha de seguridad (60%), coincide con lo expuesto por Jones (2020) que destaca la necesidad de mantener parches y configuraciones adecuadas para reducir vulnerabilidades.

La inteligencia artificial para la detección de amenazas es el mecanismo de seguridad avanzado más demandado (40%), lo que respalda lo señalado por Martínez (2022), quienes destacan que el análisis predictivo y el machine learning pueden mejorar la identificación y respuesta ante ciberataques. No obstante, el costo elevado (50%) y la complejidad técnica (30%) son las principales barreras para su implementación, lo que coincide con los desafíos descritos por Sun et al. (2019), quienes enfatizan que la inversión en capacitación es clave para superar estas limitaciones.

Finalmente, la integración de nuevas tecnologías es vista como la principal mejora en seguridad (50%), lo que concuerda con la necesidad de modernizar la infraestructura para hacer frente a amenazas emergentes (Nigro, 2022). Además, la capacitación continua del personal (40%) se destaca como una estrategia fundamental, lo que refuerza la importancia de la formación en ciberseguridad señalada por Orozco y Pozo (2023). En conjunto, estos hallazgos indican que, aunque las empresas han avanzado en la adopción del cloud computing, aún existen desafíos en seguridad que requieren soluciones integrales y estrategias a largo plazo.

A partir del análisis de estos datos, se puede indicar que la adopción del cloud computing ha revolucionado la forma en que las organizaciones gestionan y almacenan sus datos, proporcionando flexibilidad, escalabilidad y reducción de costos. Este modelo también plantea desafíos significativos en términos de seguridad, haciendo que el diagnóstico de vulnerabilidades

y la implementación de mecanismos de seguridad avanzados sean esenciales para garantizar la integridad de los datos y la resiliencia de los sistemas de información.

Una de las principales vulnerabilidades en las infraestructuras de TI para cloud computing es la incorrecta configuración de los servicios. Investigaciones como las de Angamarca y Guaraca (2021), estiman que hasta el 80% de las brechas de seguridad en la nube son atribuibles a configuraciones erróneas (Angamarca y Guaraca, 2021). Esto puede incluir la exposición de datos sensibles debido a permisos de acceso mal gestionados o a la falta de medidas de cifrado adecuadas. La complejidad de los entornos en la nube, donde se integran múltiples servicios y herramientas, puede llevar a errores que comprometan la seguridad.

La falta de actualización de software es un factor crítico que aumenta la vulnerabilidad. Las organizaciones que no mantienen sus sistemas actualizados pueden ser blanco fácil para los atacantes, quienes se aprovechan de vulnerabilidades conocidas en versiones anteriores de software (Bueno y Haz, 2022). Esto resalta la importancia de establecer procesos de actualización regulares y la monitorización continua de las amenazas emergentes.

La visibilidad y el control sobre quién accede a los datos es otro aspecto clave. Muchas organizaciones subestiman la importancia de implementar un monitoreo eficaz de acceso y actividades. Según Garzón et al. (2022), la falta de visibilidad en la nube puede resultar en incidentes de seguridad significativos, ya que las empresas no pueden detectar accesos no autorizados o actividades inusuales a tiempo. Esto se ve agravado por la dependencia de los proveedores de servicios en la nube, lo que puede generar una falsa sensación de seguridad.

Por último, la amenaza de ataques internos ya sea por descuido o malicia, presenta un riesgo considerable. Las organizaciones deben considerar que sus propios empleados, con acceso legítimo a los sistemas, pueden inadvertida o intencionadamente comprometer la seguridad

(Martínez, 2022). La falta de capacitación adecuada y conciencia sobre la seguridad cibernética dentro de la organización contribuye a esta vulnerabilidad.

El diagnóstico de vulnerabilidades y la adopción de mecanismos de seguridad avanzados son cruciales para garantizar la protección de los datos y la resiliencia de las infraestructuras de TI en entornos de cloud computing. Las organizaciones que implementen estos mecanismos no solo reducirán el riesgo de incidentes de seguridad, sino que también fortalecerán su confianza en la gestión de datos, lo que es esencial en un mundo cada vez más digital y conectado. La combinación de tecnología, procesos y capacitación del personal es la clave para construir una infraestructura de seguridad robusta y efectiva.

En esta línea, los hallazgos de esta investigación subrayan que, a pesar de la creciente adopción de soluciones de cloud computing, las PYMEs todavía enfrentan desafíos significativos en términos de seguridad y capacitación. Aunque la mayoría de las empresas han comenzado a implementar medidas de seguridad básicas, la percepción de seguridad moderada y la incidencia de eventos de seguridad resaltan la necesidad de mejoras. Para facilitar una adopción más robusta de estas tecnologías, es esencial que las PYMEs inviertan en capacitación, en la implementación de mecanismos de seguridad avanzados y en auditorías regulares. Esto no solo mejorará la confianza en las soluciones en la nube, sino que también fortalecerá la resiliencia organizativa frente a las amenazas cibernéticas emergentes, alineándose con las recomendaciones y tendencias observadas en la literatura consultada.

Para reducir las vulnerabilidades en entornos digitales, es crucial adoptar un enfoque integral de seguridad que combine controles de acceso estrictos, cifrado avanzado y monitoreo inteligente de amenazas. La autenticación multifactor (MFA) se ha consolidado como una de las estrategias más efectivas para prevenir accesos no autorizados, al exigir múltiples capas de

verificación, como credenciales y códigos de un solo uso enviados a dispositivos de confianza (Jones, 2020). Este enfoque es especialmente relevante en entornos de trabajo remoto, donde la dispersión geográfica de los usuarios amplifica los riesgos de seguridad.

El Control de Acceso Basado en Roles (RBAC) es otra medida clave para minimizar la exposición de datos sensibles. Al restringir los permisos según las funciones específicas de cada empleado, se reduce significativamente la superficie de ataque y se evita el acceso innecesario a información crítica (Orozco y Pozo, 2023). No obstante, para que este modelo sea efectivo, las políticas de acceso deben someterse a revisiones constantes y adaptarse a los cambios organizacionales.

El cifrado de datos, tanto en tránsito como en reposo, debe ser un estándar inquebrantable dentro de cualquier estrategia de ciberseguridad. La adopción de protocolos robustos garantiza que, incluso en caso de una filtración, la información permanezca inaccesible sin las claves adecuadas (Flores, 2023). Complementariamente, la integración de soluciones de inteligencia artificial permite detectar anomalías en el tráfico de red y anticipar amenazas con una precisión superior a los métodos tradicionales (Tang et al., 2022).

Para evaluar y fortalecer continuamente la postura de seguridad, es esencial la ejecución periódica de auditorías y simulaciones de ataques. Estas pruebas no solo exponen posibles debilidades, sino que también brindan información valiosa para refinar estrategias y optimizar los mecanismos de defensa (Skafi et al., 2020). Sin embargo, la tecnología por sí sola no basta: la capacitación continua del personal es un pilar fundamental en la protección contra ciberataques. Un 40% de las empresas encuestadas reconoce que el fortalecimiento de la formación técnica ha sido clave para mejorar la seguridad en la nube (Albshaier et al., 2024). Fomentar una cultura

organizacional centrada en la seguridad es, en última instancia, el mejor escudo contra amenazas digitales emergentes.

El análisis de los hallazgos cualitativos permitió identificar brechas críticas en la seguridad de la infraestructura de TI en entornos de cloud computing para Pymes en Quito. La revisión de documentos normativos como ISO 27001, NIST 800-53 y GDPR resalta la necesidad de implementar controles más estrictos en la gestión de accesos y cifrado de datos, lo que confirma que muchas empresas aún no cumplen con estándares internacionales. La evaluación de políticas internas demuestra que la aplicación de medidas de seguridad varía significativamente entre empresas, dependiendo de sus recursos y nivel de madurez en ciberseguridad. Este aspecto es clave para el estudio, ya que subraya la importancia de estandarizar prácticas de seguridad para reducir vulnerabilidades.

El análisis de estándares refuerza la evidencia de que las Pymes presentan deficiencias en la gestión de incidentes y respuesta ante amenazas. A pesar de la existencia de frameworks bien estructurados, las empresas aún carecen de protocolos eficientes para abordar riesgos emergentes. Los informes de ciberseguridad de AWS y Google revelan que muchas Pymes no actualizan sus herramientas de monitoreo ni implementan soluciones avanzadas de protección. Esta información es fundamental para el estudio, pues señala la necesidad de promover una mayor adopción de tecnologías de seguridad en la nube, tales como AWS CloudTrail y Google Security Command Center, para mejorar la capacidad de respuesta ante ataques.

Esta matriz de descripción de análisis cualitativo admitió una visión comparativa del estado de ciberseguridad en las Pymes, destacando que aquellas con auditorías regulares y capacitación presentan menor incidencia de problemas de seguridad. Esto confirma que la formación del personal y la realización de simulaciones de ataques son estrategias efectivas para

fortalecer la seguridad informática. La información recopilada contribuye significativamente al estudio, ya que proporciona evidencia empírica sobre las deficiencias actuales y permite formular recomendaciones concretas para mejorar la seguridad en infraestructuras de TI en la nube, garantizando así un entorno más seguro y resiliente para las Pymes en Quito.

La evaluación documental permitió comparar el uso de herramientas como AWS CloudTrail y Google Security Command Center, destacando sus capacidades para la detección y gestión de amenazas. Se identificó que muchas Pymes carecen de una estrategia estructurada para la actualización y mantenimiento de estas plataformas, lo que puede aumentar su vulnerabilidad ante ataques cibernéticos. En este contexto, se recomienda la adopción de protocolos de respuesta rápida y simulaciones de ataques periódicas para evaluar la efectividad de sus sistemas de defensa y garantizar el cumplimiento normativo.

Se constató que las organizaciones con mayor madurez en ciberseguridad aplican auditorías constantes y capacitación especializada para su personal, mientras que las empresas con menores recursos presentan deficiencias en la gestión de incidentes y en la protección de datos sensibles. La documentación analizada sugiere que la implementación de planes de formación, junto con la automatización de procesos de seguridad, contribuiría a mitigar riesgos y fortalecer la resiliencia de las Pymes frente a amenazas digitales emergentes.

Tabla 28

Matriz de hallazgos

Categoría	**Hallazgo**	**Implicaciones**	**Relación con las Interrogantes**
Análisis Cualitativo	El 80% de los encuestados en las PYMES identificaron la falta de capacitación como	La falta de preparación en ciberseguridad pone en riesgo la infraestructura de TI, aumentando la	La capacitación es fundamental para mejorar la seguridad en la nube y responder a las

	un desafío clave en la implementación de medidas de seguridad en la nube.	probabilidad de incidentes de seguridad y filtraciones de datos.	vulnerabilidades de las PYMES, lo cual está directamente relacionado con las interrogantes sobre cómo optimizar la seguridad.
Adopción de Cloud Computing	El 50% de las empresas medianas adoptan soluciones de cloud computing, sugiriendo correlación con el tamaño organizacional.	Las empresas medianas tienen mayor flexibilidad para adaptarse a la nube en comparación con las pequeñas y grandes. Las pequeñas enfrentan limitaciones presupuestarias.	La adopción de la nube varía según el tamaño de la empresa, lo cual ayuda a responder cómo el tamaño organizacional influye en las decisiones de migración y seguridad.
Adopción reciente de Cloud Computing	El 60% de las empresas adoptaron la nube en los últimos seis meses, reflejando una adopción temprana.	La nube sigue en una fase temprana de adopción, lo que significa que las empresas aún no están evaluando completamente su impacto a largo plazo.	Este hallazgo responde a la interrogante sobre el nivel de madurez de la adopción de la nube en las empresas y cómo eso afecta su infraestructura de seguridad.
Preferencia por SaaS	El 40% de las empresas prefieren SaaS sobre IaaS (30%) y PaaS (30%).	Las empresas prefieren soluciones listas para usar que requieren menos gestión de infraestructura. Esto facilita la adopción rápida de la nube.	Relacionado con la interrogante de qué tipo de servicios en la nube están siendo más adoptados, lo que afecta directamente las decisiones de seguridad que toman las empresas.
Uso de máquinas virtuales	El 40% de las empresas usan máquinas virtuales, mientras que el 30% utiliza contenedores y	La virtualización sigue siendo la opción predominante debido a su compatibilidad con sistemas heredados	Responde a la interrogante sobre las arquitecturas de nube más comunes y cómo se manejan las medidas de seguridad para cada

	soluciones serverless.	y facilidad de administración.	tipo de infraestructura.
Proveedor de Cloud Computing	AWS lidera el mercado con el 50% de las empresas, seguido por Microsoft Azure (30%) y Google Cloud (20%).	AWS tiene una infraestructura más consolidada y una mayor amplitud de servicios, lo que lo convierte en el proveedor preferido.	Este hallazgo está relacionado con la interrogante sobre los proveedores de nube más utilizados y cómo sus ofertas afectan las medidas de seguridad implementadas.
Medidas de Seguridad en la Nube	El Firewall de Aplicaciones Web (WAF) es la medida más implementada (40%), seguido por detección y prevención de intrusiones (30%).	Las empresas se centran en proteger aplicaciones web, pero otras medidas de seguridad como la prevención de intrusiones no están tan adoptadas, lo que puede generar vulnerabilidades.	Responde a las interrogantes sobre qué medidas de seguridad están siendo implementadas en la nube y si son suficientes para mitigar riesgos en la infraestructura.
Percepción de la seguridad	El 60% de las empresas considera que sus medidas de seguridad son ineficaces o muy ineficaces.	Hay una percepción de insuficiencia en las estrategias de protección actuales, lo que sugiere que las medidas de seguridad no están bien evaluadas ni implementadas.	Relacionado con la percepción de las empresas sobre la efectividad de sus medidas de seguridad, lo que contribuye a la evaluación de las vulnerabilidades y riesgos de la infraestructura.
Brechas de Seguridad	La falta de actualización de software es la principal brecha de seguridad (60%).	La no actualización de software deja a las empresas vulnerables a ataques, ya que los atacantes aprovechan vulnerabilidades conocidas.	Relacionado con las interrogantes sobre las principales brechas de seguridad en las PYMES y cómo afectan la protección de los datos y sistemas.
Demanda de IA para la detección de amenazas	El 40% de las empresas demandan inteligencia artificial para la	La IA y el machine learning son vistos como soluciones para mejorar la identificación y	Responde a la interrogante sobre qué tecnologías emergentes están siendo demandadas

	detección de amenazas.	respuesta ante ciberataques, aunque el costo y la complejidad son barreras.	para mejorar la seguridad en la nube, y cómo podrían impactar las estrategias de seguridad.
Barreras para la Implementación de IA	El 50% de las empresas citan el alto costo y el 30% la complejidad técnica como barreras para la implementación de IA.	A pesar del interés por la IA, las barreras económicas y técnicas retrasan su adopción generalizada, lo que limita su impacto en la mejora de la seguridad.	Relacionado con las barreras que enfrentan las empresas para implementar tecnologías avanzadas de seguridad, como la IA, lo que es esencial para fortalecer sus defensas.
Integración de nuevas tecnologías	El 50% de las empresas considera que la integración de nuevas tecnologías es la principal mejora en seguridad.	La modernización de la infraestructura tecnológica es vista como clave para enfrentar amenazas emergentes y mejorar la seguridad a largo plazo.	Responde a la interrogante sobre cómo la adopción de nuevas tecnologías puede mejorar la seguridad, y cómo puede impactar la protección de los sistemas en la nube.
Capacitación continua	El 40% de las empresas destacan la capacitación continua del personal como una estrategia de mejora.	La capacitación continua del personal es fundamental para prevenir incidentes de seguridad y fortalecer la resiliencia frente a amenazas cibernéticas.	Relacionado con la interrogante sobre el papel de la capacitación en la mejora de la seguridad y cómo influye en la preparación de los empleados frente a ciberamenazas.
Diagnóstico de vulnerabilidades	Se identifican brechas críticas como la incorrecta configuración de los servicios, la falta de actualización de	Estas vulnerabilidades pueden generar accesos no autorizados o filtraciones de datos sensibles, lo	Relacionado con la interrogante sobre cuáles son las principales vulnerabilidades en la infraestructura de TI de las

	software y la visibilidad limitada.	que compromete la seguridad.	PYMES y cómo afectan la protección de sus datos.
Adopción de controles avanzados	Se recomienda la adopción de controles de acceso estrictos, cifrado avanzado, y monitoreo inteligente de amenazas.	La implementación de estos controles es clave para reducir riesgos y fortalecer la postura de seguridad, especialmente frente a accesos no autorizados.	Relacionado con la interrogante sobre cómo las empresas pueden mejorar su seguridad mediante el uso de controles avanzados para proteger sus sistemas en la nube.

CAPITULO V

PROPUESTA

Título: Propuesta de seguridad para infraestructura de TI en entornos de Cloud Computing

5.1. Descripción de la propuesta

La propuesta consiste en el diseño e implementación de un conjunto de mecanismos avanzados de seguridad para la infraestructura de TI en entornos de computación en la nube, aplicables a las Pymes de Quito. El objetivo principal es garantizar la protección de datos y la integridad de los sistemas de información en un contexto donde las amenazas cibernéticas son cada vez más sofisticadas. Estos mecanismos estarán diseñados para optimizar la gestión de accesorios, fortalecer la defensa contra ataques emergentes y garantizar la continuidad operativa de las empresas.

Esta iniciativa surge para dotar a las Pymes de herramientas efectivas que les permitan aprovechar el potencial de la computación en la nube sin comprometer la seguridad de sus operaciones. Abarca desde la implementación de protocolos de autenticación multifactor, cifrado de datos en reposo y en tránsito, hasta la adopción de sistemas de monitoreo de amenazas en tiempo real, con un enfoque en soluciones escalables y de bajo costo.

La propuesta también incluye la validación de la efectividad de los mecanismos diseñados mediante pruebas controladas, como simulaciones de ataques cibernéticos y análisis de su impacto en la confidencialidad e integridad de los datos. Esto garantiza que las soluciones sean prácticas y robustas, permitiendo a las Pymes fortalecer su infraestructura tecnológica de manera sostenible y confiable.

En definitiva, esta propuesta no solo busca fortalecer la seguridad informática, sino también fomentar la competitividad de las Pymes en un entorno digital cada vez más exigente. Al proteger sus activos digitales, estas empresas podrán enfocarse en sus objetivos comerciales, contribuyendo al desarrollo económico y tecnológico de la región.

5.2. Objetivos de la propuesta

5.2.1. Objetivo general

Diseñar mecanismos avanzados de seguridad para la infraestructura de TI en entornos de computación en la nube, con el propósito de garantizar la protección de datos, la integridad de los sistemas de información y la continuidad operativa de las Pymes en Quito.

5.2.2. Objetivos específicos

- Proponer mecanismos de seguridad avanzada, como cifrado, autenticación multifactor y monitoreo continuo, adaptados a las necesidades y recursos de las Pymes.
- Diseñar un programa de capacitación dirigida al personal de las Pymes, enfocada en la correcta gestión de los mecanismos de seguridad y en la adopción de prácticas seguras para la protección de datos en entornos de computación en la nube.
- Evaluar la factibilidad de los mecanismos diseñados para mitigar las vulnerabilidades y brechas de seguridad en el diseño de infraestructuras de TI para cloud computing, mediante la validación de propuestas con base en el criterio de expertos en Ciberseguridad.

5.3. Justificación

La seguridad de la información es un desafío crítico para las Pymes, especialmente en entornos de computación en la nube, donde los datos están expuestos a múltiples amenazas cibernéticas. Esta propuesta es relevante porque permite a las empresas adoptar tecnologías

avanzadas con confianza, minimizando riesgos de pérdida de datos, brechas de seguridad y afectaciones operativas.

En el contexto de Quito, donde las Pymes son una parte esencial del tejido económico, contar con una infraestructura de TI segura y eficiente resulta imprescindible para su competitividad. Este proyecto impactará directamente en la sostenibilidad y resiliencia de estas empresas frente a un panorama digital en constante evolución, esto abarca:

- Reducción del riesgo de ciberataques y violaciones de datos.
- Mejora en la gestión de accesos y control de información sensible.
- Incremento de la confianza de clientes y socios comerciales en los procesos tecnológicos.

Los beneficiarios principales de esta propuesta son las Pymes de Quito que integran la computación en la nube como parte de su infraestructura tecnológica, ya que podrán optimizar la seguridad de sus operaciones. Asimismo, los empleados encargados de gestionar los sistemas de TI en estas empresas se beneficiarán al disponer de herramientas más seguras, eficientes y fáciles de manejar. Finalmente, los clientes y socios comerciales también resultarán favorecidos, ya que la implementación de estos mecanismos garantizará la protección de sus datos, reforzando la confianza en los servicios ofrecidos por las Pymes.

5.4. Estructura de la propuesta

5.4.1. Diagnóstico inicial

El diagnóstico inicial realizado a las Pymes siguió metodologías estructuradas que abarcaron tres áreas principales: identificación de activos críticos, evaluación de vulnerabilidades y análisis de incidentes previos. Este proceso permitió comprender el estado actual de la seguridad de TI en la empresa y sentar las bases para diseñar mecanismos de protección avanzados.

- **Identificación de Activos Críticos de TI**

Se llevó a cabo un levantamiento exhaustivo de los activos tecnológicos y de información utilizados por la Pyme, priorizando aquellos que resultan esenciales para sus operaciones. El inventario incluido:

- Base de datos: Contiene información confidencial de clientes, transacciones financieras y datos internos del negocio.
- Aplicaciones empresariales: Herramientas como un sistema ERP (Enterprise Resource Planning) basado en la nube, usado para la gestión de inventarios y facturación.
- Accesos remotos: Utilizados por el equipo de trabajo para conectarse a la infraestructura desde ubicaciones externas, especialmente para tareas administrativas y de soporte técnico.
- Infraestructura de red: Incluye servidores virtuales proporcionados por un proveedor de nube pública, almacenamiento en la nube y puntos de conexión remota.

Resultado: Se identificaron 15 activos críticos:

- Servidores en la nube
- Bases de datos empresariales
- Aplicaciones de gestión empresarial (ERP, CRM)
- Plataformas de comunicación y colaboración
- Sistemas de autenticación y control de accesos
- Infraestructura de red en la nube
- Repositorios de código fuente y sistemas de desarrollo
- Sistemas de copias de seguridad y recuperación ante desastres
- Plataformas de monitoreo y análisis de seguridad

- Servicios de almacenamiento de archivos
- Aplicaciones de productividad empresarial
- Sistemas de análisis de datos e inteligencia de negocios
- Interfaces de programación de aplicaciones (APIs)
- Máquinas virtuales y contenedores en la nube
- Plataformas de e-commerce o servicios digitales, de los cuales el 80% dependían exclusivamente de servicios en la nube, evidenciando la necesidad de robustecer los controles de seguridad para minimizar riesgos.
- **Evaluación de vulnerabilidades existentes**

Con el apoyo de herramientas de análisis como AWS Security Hub, se evaluaron las vulnerabilidades en los activos identificados.

Este proceso incluyó:

- Revisión de configuraciones de seguridad en la nube: Se detectó que los permisos de acceso a ciertas aplicaciones empresariales eran excesivos, permitiendo a usuarios no autorizados acceder a datos sensibles.
- Auditorías de cifrado**:** Se encontró que las bases de datos almacenadas en la nube no estaban cifradas en reposo, lo que incrementa el riesgo de robo de información en caso de acceso no autorizado.
- Accesos remotos: El 70% de las contraseñas utilizadas por los empleados no cumplían con los estándares de complejidad recomendados, y no se había implementado la autenticación multifactor.

- Monitoreo de tráfico de red: Los registros mostraron intentos de acceso fallidos desde direcciones IP no autorizadas en múltiples ocasiones, sin que se activen alertas automáticas.

Resultado: Se identificaron 12 vulnerabilidades críticas:

- Falta de cifrado en bases de datos en reposo.
- Configuraciones incorrectas de permisos que permitieron acceso no autorizado a datos sensibles.
- Contraseñas débiles utilizados por el 70% de los empleados
- Ausencia de autenticación multifactor.
- Intentos de acceso fallidos desde direcciones IP no autorizados sin alertas automáticas.
- Uso de protocolos inseguros en conexiones remotas.
- Falta de segmentación de red para limitar movimientos laterales de atacantes.
- Escasez de auditorías de seguridad periódicas.
- Deficiencias en la gestión de identidades y accesos.
- Exposición de servicios críticos sin protección adecuada.
- Ausencia de detección y respuesta automatizada ante amenazas.
- Políticas de seguridad desactualizadas que no cumplían con los estándares recomendados.
- **Análisis de Incidentes Anteriores**

  El análisis histórico reveló varios incidentes relevantes:

- Intentos de acceso no autorizado: En los últimos seis meses, se registraron más de 50 intentos de acceso fallidos desde ubicaciones no reconocidas.
- Phishing exitoso: Un empleado cayó en un ataque de phishing, comprometiendo las credenciales que fueron utilizadas para acceder a datos sensibles.

- Fallas en la continuidad operativa**:** Un ataque de ransomware interrumpió las operaciones durante dos días, generando pérdidas económicas y afectando la confianza de los clientes.

Resultado: Los incidentes tuvieron un impacto significativo en la reputación y las operaciones de la empresa, evidenciando una necesidad urgente de implementar controles preventivos y reactivos.

- **Resultados del diagnóstico**

  La siguiente tabla resume los hallazgos más críticos durante el diagnóstico:

Tabla 29

Matriz de diagnostico

Crítico activo	**Vulnerabilidad detectada**	**Impacto potencial**
Base de datos	Falta de cifrado en reposo	Robo de información confidencial
Aplicaciones empresariales	Permisos de acceso excesivos	Exposición de datos sensibles
Accesos remotos	Contraseñas débiles	Acceso no autorizado
Infraestructura de red	Falta de monitoreo en tiempo real	Retraso en la detección de amenazas

Fuente: Elaboración propia

La aplicación del diagnóstico permitió a la Pyme:

- Comprender la criticidad de sus activos tecnológicos y priorizar su protección.
- Identificar brechas significativas en su infraestructura de TI que podrían ser explotadas por atacantes.
- Reconocer la importancia de establecer controles proactivos, como el cifrado, autenticación multifactor y monitoreo continuo, para mitigar riesgos futuros.

5.4.2. Diseño de mecanismos de seguridad avanzados

5.4.2.1. Autenticación Multifactor (MFA)

La Autenticación Multifactor (MFA) es un sistema de seguridad que agrega capas adicionales de protección a la hora de acceder a un sistema o servicio. En lugar de depender únicamente de una contraseña, que puede ser fácilmente activada, MFA requiere que los usuarios proporcionen múltiples formas de verificación antes de permitir el acceso.

La MFA se basa generalmente en tres factores de autenticación:

- Algo que el usuario sabe: Una contraseña o PIN.
- Algo que el usuario tiene: Un dispositivo físico (por ejemplo, un teléfono móvil o una tarjeta de seguridad) que genera un código temporal o una aplicación de autenticación como Google Authenticator o Microsoft Authenticator.
- Algo que el usuario es: Un factor biométrico, como huellas dactilares, reconocimiento facial o escaneo de retina**.**

El proceso comienza cuando el usuario ingresa su nombre de usuario y contraseña. Luego, el sistema solicita el segundo factor, que puede ser un código enviado a un teléfono móvil o un dispositivo de autenticación, o incluso la verificación de una característica biométrica. En algunos casos, se pueden utilizar tres factores, pero dos suelen ser los más comunes y suficientes para mantener una alta seguridad.

Los beneficios de la Autenticación Multifactor (MFA) incluyen una mejora significativa en la protección contra accesos no autorizados, ya que, al requerir más de un método de verificación, la MFA reduce el riesgo de accesos ilegítimos incluso si la contraseña de un usuario se ve comprometida. Así mismo disminuye la efectividad de los ataques de phishing, pues los atacantes que intentan obtener acceso con credenciales robadas no pueden acceder fácilmente sin

tener el segundo factor de autenticación. Por último, la MFA ofrece un mayor control y seguimiento, ya que las soluciones de MFA pueden incluir registros de acceso que permiten realizar auditorías más precisas y detectar intentos de acceso no autorizados.

La MFA contribuye a un entorno de TI más seguro al garantizar que solo los usuarios legítimos puedan acceder a datos sensibles y sistemas críticos. Este mecanismo es especialmente útil en entornos de computación en la nube, donde los accesos remotos son frecuentes. La implementación de MFA mejora la seguridad general, reduciendo las posibilidades de que los atacantes obtengan acceso a cuentas sensibles y, por lo tanto, protege la infraestructura tecnológica, los datos de clientes y la propiedad intelectual de las Pymes.

5.4.2.2. Cifrado de datos en reposo y en tránsito

El cifrado de datos es un procedimiento en el que la información se convierte en un formato incomprensible sin la clave correcta para descifrarla. El cifrado puede aplicarse tanto a los datos almacenados como a los que están siendo transmitidos entre sistemas, redes o dispositivos.

- Cifrado de Datos en Reposo: Protege los datos que se almacenan en servidores, bases de datos, dispositivos de almacenamiento o en la nube. Los datos están cifrados cuando no están en uso y, por lo tanto, permanecen protegidos incluso si un atacante logra acceder a los dispositivos de almacenamiento. Por ejemplo, si un atacante obtiene acceso a una base de datos sin cifrar, podría leer toda la información almacenada (incluidos datos sensibles). Con el cifrado de datos en reposo, cualquier intento de acceso no autorizado resultará en datos ilegibles, a menos que se posea la clave de descifrado correcta.
- Cifrado de Datos en Tránsito: Protege los datos cuando se transfieren entre sistemas o a través de redes, como cuando un usuario accede a la nube, realiza pagos en línea o

envía correos electrónicos. El cifrado de datos en tránsito asegura que, aunque los datos puedan ser interceptados por un tercero durante la transferencia, no podrán ser leídos ni manipulados. Los protocolos de cifrado utilizados para esto son SSL/TLS, que cifran los canales de comunicación entre el servidor y el cliente, asegurando que la conexión sea segura**.**

Los beneficios del cifrado de datos son fundamentales para garantizar la seguridad de la información. Primero, proporciona protección de datos sensibles, asegurando que los datos no puedan ser leídos o modificados por terceros no autorizados, incluso si logran acceder a los sistemas o redes. El cifrado facilita el cumplimiento con las regulaciones de seguridad, ya que muchas normativas de protección de datos, como el GDPR o HIPAA, exigen que los datos personales y sensibles estén cifrados tanto en reposo como en tránsito para garantizar su protección. Finalmente, el cifrado contribuye a garantizar tanto la confidencialidad como la integridad de los datos, ya que no solo protege la confidencialidad, sino que también asegura que la información no haya sido alterada durante la transferencia, preservando así su integridad.

El cifrado permite que las Pymes en entornos de computación en la nube mantengan sus datos seguros, tanto cuando están almacenados como cuando están siendo transferidos. Con esta medida, las organizaciones pueden cumplir con las normativas legales de protección de datos y garantizar que la información confidencial de sus clientes y empleados esté siempre protegida, minimizando el riesgo de filtraciones de datos o ataques de man-in-the-middle. También contribuye a fortalecer la confianza de los clientes en la empresa, ya que saber que sus datos están protegidos aumenta la percepción de seguridad**.**

En este caso, AWS y Google Cloud proporcionan cifrado avanzado para proteger los datos en tránsito y en reposo. AWS utiliza AWS Key Management Service (KMS) para la

gestión de claves, permitiendo cifrar almacenamiento en Amazon S3, EBS y RDS con algoritmos como AES-256. Además, AWS implementa cifrado en tránsito mediante TLS 1.2 y 1.3, junto con opciones de seguridad para redes privadas como VPN y AWS Direct Connect Encryption. Google Cloud, por su parte, cifra automáticamente los datos en reposo con AES-256 y permite a los clientes gestionar claves con Customer-Managed Encryption Keys (CMEK) o proporcionar sus propias claves mediante Customer-Supplied Encryption Keys (CSEK). Para la seguridad en tránsito, emplea TLS/SSL y herramientas como Cloud VPN e Interconnect Encryption.

Ambas plataformas cumplen con estándares de seguridad internacionales como FIPS 140-2, SOC 2, ISO 27001 y HIPAA, garantizando una protección sólida para la información almacenada y transmitida. AWS ofrece múltiples capas de cifrado en almacenamiento y bases de datos, integradas con sus servicios de seguridad, mientras que Google Cloud destaca por su cifrado automático y opciones avanzadas de administración de claves. Estas medidas aseguran que los datos sean inaccesibles sin autorización, reduciendo los riesgos de exposición y cumplimiento normativo. En entornos empresariales, la combinación de estas tecnologías permite mejorar la privacidad, la integridad y la seguridad de la infraestructura en la nube**.**

5.4.2.3. Monitoreo y respuesta a incidentes

El monitoreo y la respuesta a incidentes son actividades cruciales para detectar, analizar y responder rápidamente a amenazas y ataques en el entorno de la nube. Estas herramientas permiten observar el comportamiento de los sistemas, detectar patrones anómalos y actuar en tiempo real cuando se identifica un incidente de seguridad.

- Monitoreo: Se refiere a la recopilación y análisis en tiempo real de datos de acceso, actividades de usuario, tráfico de red, logs del sistema y cualquier otro indicador que pueda revelar comportamientos anómalos o intentos de acceso no autorizado. Las

herramientas de monitoreo generalmente utilizan técnicas de análisis de comportamiento e inteligencia artificial para detectar patrones que podrían indicar un ataque.

- Respuesta a Incidentes: Una vez que se ha detectado una anomalía o posible incidente, el sistema debe ser capaz de alertar a los administradores de seguridad para que tomen las medidas apropiadas, como aislar el sistema afectado, bloquear accesos no autorizados o ejecutar scripts de contención. Este proceso incluye protocolos automatizados y manuales para contener la amenaza y minimizar su impacto, permitiendo una rápida recuperación de la normalidad.

Los beneficios del monitoreo y respuesta a incidentes son cruciales para la seguridad en entornos de computación en la nube. En primer lugar, permite la detección temprana de amenazas, ya que el monitoreo constante facilita la identificación rápida de incidentes, como intentos de intrusión o ataques de denegación de servicio (DDoS), lo que permite tomar medidas preventivas antes de que el daño se propague. Las respuestas a los incidentes son rápidas y efectivas gracias a la integración de protocolos de respuesta automatizada y manual, lo que permite reducir el tiempo de inactividad y minimizar los daños causados por los incidentes de seguridad. Finalmente, el monitoreo mejora el control y la trazabilidad, ya que genera registros detallados que facilitan el rastreo de actividades sospechosas y las investigaciones posteriores, asegurando que todas las acciones de respuesta se gestionen de manera adecuada y se mantengan un histórico.

El monitoreo y respuesta a incidentes permite que las Pymes detecten y actúen rápidamente frente a amenazas en tiempo real, reduciendo el riesgo de pérdida de datos y la interrupción de servicios. Este mecanismo contribuye a una mayor resiliencia frente a incidentes

de seguridad, garantizando la continuidad operativa en entornos digitales y protegiendo la infraestructura TI de ataques maliciosos. Al contar con un sistema de respuesta eficaz, las empresas pueden minimizar los impactos de un incidente y restaurar rápidamente su normalidad.

La implementación de estos mecanismos avanzados de seguridad, como la Autenticación Multifactor (MFA), el Cifrado de Datos y el Monitoreo y Respuesta a Incidentes, proporciona una defensa integral para las infraestructuras de TI en entornos de computación en la nube. Estos mecanismos son esenciales para proteger la información confidencial y garantizar la continuidad operativa, permitiendo que las PYMEs puedan operar de manera segura y eficiente en el entorno digital. Así también, ayudan a cumplir con las normativas de seguridad y mejoran la confianza de los clientes y socios comerciales.

Tabla 30

Matriz Mecanismos propuestos

Mecanismo	Descripción	Monitoreo	Indicadores de Monitoreo	Métodos de evaluación	Herramientas de evaluación	Herramientas AWS	Herramientas Google
Autenticación Multifactor (MFA)	Mecanismo de autenticación que requiere más de un factor de verificación para permitir el acceso, como contraseñas, dispositivos móviles, biometría, etc.	Monitoreo de intentos de autenticación fallidos, actividad de inicio de sesión, patrones de acceso inusuales.	- Número de intentos fallidos de autenticación. - Frecuencia de acceso desde dispositivos no habituales. - Registros de actividad inusual (p. ej., horas fuera de lo común).	- Análisis de registros de autenticación. - Revisión de políticas de acceso y autenticación. - Evaluación de pruebas de penetración para identificar debilidades.	Splunk, ELK Stack, Kali Linux.	AWS IAM, AWS CloudTrail.	Google Identity-Aware Proxy (IAP), Google Cloud Audit Logs.
Cifrado de datos	Técnica para convertir los datos en un	Monitoreo de procesos de cifrado, accesos a	- Número de accesos no autorizados a datos	- Revisión de políticas de cifrado. - Auditorías	OpenSSL, Wireshark, Varonis.	AWS Key Management Service (KMS),	Google Cloud Key Management, Google Cloud

	formato ilegible para garantizar que solo los usuarios autorizados puedan acceder a ellos. Aplicable tanto en reposo como en tránsito.	datos sensibles y uso de claves de cifrado.	cifrados. - Frecuencia de utilización de claves de cifrado. - Tiempos de acceso a datos cifrados.	de cumplimiento con normativas como GDPR. - Pruebas de integridad y validación de procesos de cifrado.		AWS CloudHSM.	Security Command Center.
Monitoreo de Amenazas	Sistema de monitoreo en tiempo real que detecta y responde a incidentes de seguridad, como intrusiones, ataques de DDoS y otras amenazas emergentes.	Monitoreo de eventos de seguridad en tiempo real, detección de anomalías, análisis de patrones de tráfico de red.	- Número de incidentes detectados en tiempo real. - Tiempo de respuesta a incidentes. - Frecuencia de alertas de posibles amenazas.	- Evaluación de protocolos de respuesta ante incidentes. - Simulación de ataques para medir tiempos de respuesta.	SIEM (Splunk, ELK Stack), Snort, Metasploit.	AWS GuardDuty, AWS Security Hub.	Google Chronicle Security Operations, Google Security Command Center.

Fuente: Elaboración propia

5.4.2.4. Capacitación del Personal de TI en las Pymes

La capacitación del personal de Tecnologías de la Información (TI) es un paso esencial en la implementación de un plan de seguridad eficaz, ya que este personal es el encargado de gestionar, monitorear y mantener los mecanismos de seguridad de la empresa. Un equipo de TI bien capacitado puede identificar, prevenir y mitigar ataques cibernéticos antes de que causen daños significativos. La capacitación debe ir más allá de los aspectos técnicos, a incluir también la conciencia de seguridad en la empresa y cómo los usuarios finales pueden prevenir incidentes.

- **Objetivos de la Capacitación**
    - Desarrollar competencias técnicas: El personal de TI debe recibir formación especializada en herramientas y plataformas de seguridad cibernética, como firewalls, sistemas de detección de intrusos (IDS), software de protección contra malware, cifrado de datos y protección contra ataques de denegación de servicio. (DoS).
    - Concientización sobre amenazas emergentes: Capacitar al personal sobre las últimas amenazas y técnicas utilizadas por los cibercriminales, tales como phishing, ransomware, ataques DDoS y fraudes en línea.
    - Mejorar la respuesta ante incidentes: El personal debe estar preparado para responder rápidamente a un incidente de seguridad, con planes establecidos de respuesta ante incidentes (IRP). Esto incluye procedimientos para la contención, erradicación y recuperación ante incidentes cibernéticos.
- **Estrategias para la Capacitación**
    - Entrenamiento práctico: A través de simulaciones y ejercicios prácticos, los equipos de TI pueden enfrentarse a situaciones de ciberataques reales para poner en práctica sus habilidades de resolución de problemas y respuesta ante emergencias. Por ejemplo, la creación de entornos de laboratorio que simulan ataques de ransomware o intrusiones en la red.
    - Capacitación continua: Dado que las amenazas cibernéticas evolucionan rápidamente, es fundamental que la capacitación sea un proceso continuo. Esto incluye la actualización periódica sobre nuevas amenazas, tecnologías y mejores prácticas de seguridad.

- Evaluación periódica de conocimientos: Mediante pruebas o exámenes, se puede evaluar el nivel de comprensión y la capacidad del personal para aplicar lo aprendido en escenarios reales.

- **Beneficios de la Capacitación**
  - Mejora de la respuesta ante ciberamenazas ¿: Un personal capacitado está mejor preparado para reconocer las amenazas de manera temprana y tomar medidas preventivas.
  - Reducción del error humano: Muchos incidentes de seguridad ocurren debido a fallos humanos, como la apertura de correos electrónicos de phishing o la configuración incorrecta de sistemas. La capacitación ayuda a minimizar estos riesgos.
  - Cumplimiento de normativas de seguridad: Muchas normativas de seguridad exigen que las empresas capaciten a su personal en la protección de datos personales y en la prevención de incidentes de seguridad.

Tabla 31

Programa de capacitación enfocado en la seguridad para una infraestructura de TI en entornos de Cloud Computing.

Módulo	Tema	Objetivo	Duración	Público Objetivo	Metodología	Recursos
Módulo 1	Introducción a la Seguridad en Cloud Computing	Comprender los conceptos básicos de seguridad en la nube y los riesgos asociados.	2 horas	Personal de TI y administrativos	Exposición teórica y discusión	Presentación, material digital
Módulo 2	Gestión de Accesos y Autenticación	Implementar controles de acceso robustos y autenticación multifactor para proteger los	3 horas	Personal de TI y usuarios con acceso a sistemas sensibles	Taller práctico y simulaciones	Software de autenticación, manuales de configuración

		sistemas.				
Módulo 3	Protección de Datos y Políticas de Backup	Establecer estrategias de respaldo y recuperación para evitar pérdidas de información.	2 horas	Administradores de bases de datos y gerencia	Ejercicio práctico de recuperación de datos	Software de backup, casos de estudio
Módulo 4	Identificación y Prevención de Ciberataques	Capacitar sobre amenazas comunes (phishing, ransomware) y cómo mitigarlas.	3 horas	Todo el personal	Simulación de ataques y análisis de casos reales	Plataforma de ciberseguridad, videos ilustrativos
Módulo 5	Configuración Segura de Infraestructura en la Nube	Aplicar buenas prácticas en la configuración segura de servidores y redes en la nube.	4 horas	Equipo de TI y administradores de sistemas	Laboratorio práctico en entorno de prueba	Acceso a entornos virtuales de prueba
Módulo 6	Cumplimiento Normativo y Políticas de Seguridad	Garantizar que la empresa cumpla con normativas locales e internacionales en seguridad de TI.	2 horas	Gerencia y personal de TI	Análisis de normativas y desarrollo de políticas internas	Normativas ISO 27001, GDPR, Ley Orgánica de Protección de Datos
Módulo 7	Monitoreo y Respuesta a Incidentes	Implementar estrategias de detección y respuesta ante incidentes de seguridad en la nube.	3 horas	Equipo de TI y personal clave	Simulación de respuesta ante incidentes	Herramientas SIEM, manual de respuesta a incidentes
Módulo 8	Cultura de Seguridad y Concienciación	Fomentar hábitos seguros en el uso de sistemas y datos en la nube.	2 horas	Todo el personal	Dinámicas interactivas y estudio de casos	Infografías, vídeos, evaluación de conocimientos

Fuente: Elaboración propia

5.4.3. Validación de la propuesta

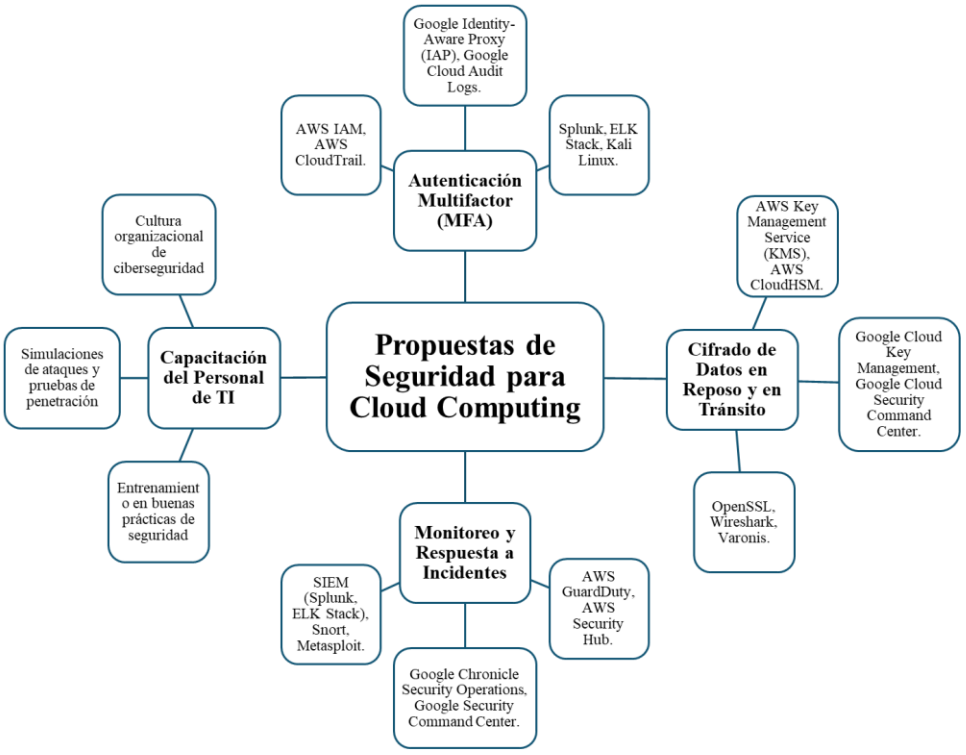
La seguridad en el uso de servicios en la nube es un reto continuo para las PYMEs, debido a la constante aparición de nuevas amenazas en el ámbito digital y la necesidad de salvaguardar la confidencialidad, integridad, disponibilidad de la información, y resiliencia de los sistemas de información. El presente proyecto de investigación de tesis de maestría propone

soluciones de seguridad para reforzar la infraestructura tecnológica en la nube, con el fin de reducir brechas, vulnerabilidades y evitar problemas de seguridad.

Para asegurar que estas soluciones sean viables y efectivas, un grupo de expertos en seguridad informática ha realizado un proceso de evaluación. Este análisis permite comprobar los efectos generados por las propuestas de mecanismos de seguridad en situaciones reales, su conformidad con las mejores prácticas de seguridad y su capacidad para enfrentar de manera efectiva los riesgos relacionados con el uso de la nube, con la finalidad de validar las propuestas que abordan la problemática presentada.

Figura 29

Propuestas de Seguridad para Cloud Computing



Fuente: Elaboración propia

La validación de los mecanismos de seguridad se llevó a cabo a través de un enfoque estructurado compuesto por cuatro fases principales:

5.4.3.1. Conformación del grupo de evaluadores

Se convocó a un grupo de expertos en ciberseguridad con experiencia en infraestructuras de TI en la nube y gestión de riesgos. Los evaluadores fueron seleccionados con base en su trayectoria profesional y conocimientos en normativas de seguridad, estándares, herramientas de monitoreo y mitigación de amenazas. Los expertos participaron en sesiones de análisis en las que se les presentaron los mecanismos propuestos en seguridad, para su evaluación.

5.4.3.2. Definición de la matriz de evaluación

Para evaluar las propuestas de manera objetiva, se diseñó una matriz de evaluación basada en una escala del 1 al 5, donde cada nivel representa el grado de implementación o efectividad del mecanismo evaluado:

1. No satisfactorio: Representa una propuesta deficiente o inexistente.
2. Bajo: Indica que la propuesta es parcial o limitada en su alcance.
3. Medio: Denota que la propuesta es adecuada, pero con espacio para mejoras.
4. Alto: Refleja que la propuesta posee un buen nivel de cumplimiento y aplicabilidad.
5. Excelente: Representa una propuesta ejemplar, con un diseño completo y alineado a las mejores prácticas.

Se estableció que:

- Las propuestas con una puntuación de 4 o 5 se consideran factibles y recomendadas para su implementación.
- Aquellas con 3 puntos requieren mejoras antes de su adopción.
- Las que obtienen una calificación de 1 o 2 se clasifican como no factibles.

5.4.3.3. Evaluación individual de cada mecanismo

Cada experto analizó las propuestas de seguridad y aplicó la matriz de evaluación de manera independiente. Para ello, se consideraron aspectos clave como:

- **Eficacia:** Grado en el que el mecanismo mitiga las vulnerabilidades detectadas.
- **Viabilidad:** Facilidad de implementación en el contexto específico de una PYME.
- **Compatibilidad:** Adaptabilidad con herramientas y tecnologías existentes en el entorno cloud.
- **Impacto en la seguridad:** Nivel de protección que proporciona contra amenazas actuales.

Una vez completada la evaluación individual, los resultados fueron consolidados en la matriz de evaluación general.

5.4.3.4. Análisis y validación conjunta

Tras la evaluación individual, los expertos realizaron una sesión de discusión grupal, en la que se analizaron las puntuaciones asignadas y se discutieron las observaciones sobre cada mecanismo.

Esta fase permitió:

- Identificar coincidencias y discrepancias en la evaluación.
- Refinar los criterios de calificación según la aplicabilidad de las propuestas.
- Emitir una validación final basada en consenso.

5.4.3.5. Resultados de la Validación

La siguiente tabla muestra los resultados finales de la evaluación de los mecanismos de seguridad:

Tabla 32

Resultados de la evaluación de los mecanismos

Propuestas de Mecanismos	1 (No satisfactorio)	2 (Bajo)	3 (Medio)	4 (Alto)	5 (Excelente)	Puntaje asignado
Autenticación Multifactor (MFA)					X	5
Cifrado de Datos					X	5
Monitoreo de Amenazas					X	5
Plan de Capacitación				X		4

Elaboración propia

5.4.3.6. Observaciones Generales

5.4.3.6.1. *Mecanismos con Puntaje 5 (Factibles y Recomendados)*

- **Autenticación Multifactor (MFA):** Considerado un estándar esencial para la seguridad en la nube, su implementación garantiza una mayor protección frente a accesos no autorizados.
- **Cifrado de Datos:** Evaluado como una medida fundamental para la protección de la información en tránsito y en reposo, alineándose con normativas como GDPR.
- **Monitoreo de Amenazas:** Se destacó su capacidad de detección en tiempo real, lo que permite una respuesta inmediata ante incidentes de seguridad.

Estos mecanismos cumplen con las mejores prácticas de seguridad y se recomienda su adopción sin modificaciones significativas.

5.4.3.6.2. Mecanismo con Puntaje 4 (Factible con Mejoras)

Plan de Capacitación: Si bien la propuesta es sólida y adecuada, los expertos sugieren:

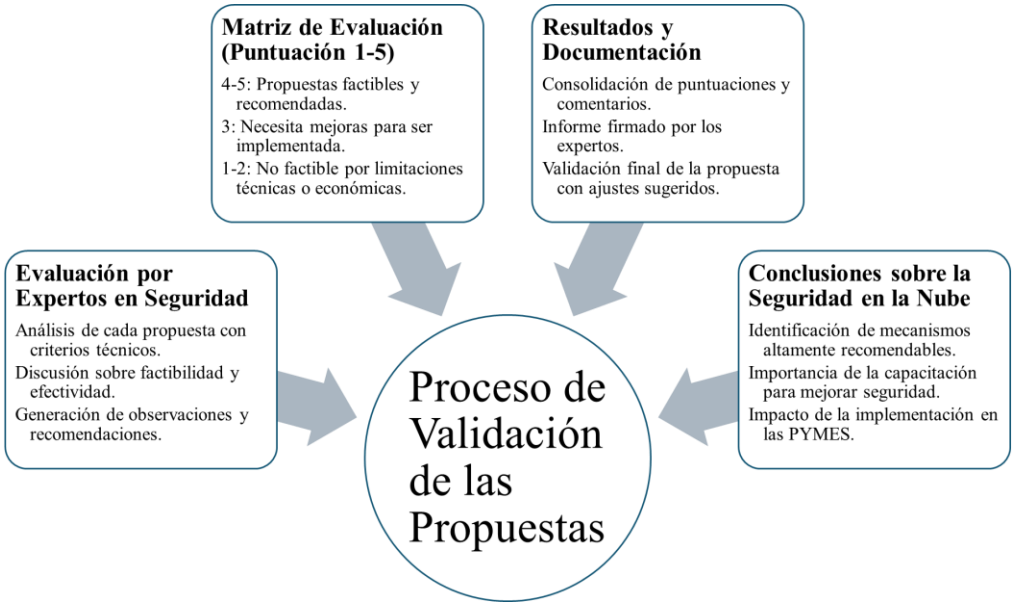
- Incluir simulaciones más realistas para preparar mejor a los empleados ante incidentes de seguridad.
- Actualizar periódicamente los módulos para abordar nuevas amenazas.
- Ampliar la cobertura del programa de formación a todos los niveles de la organización.

5.5. Validación de las propuestas

A partir del análisis realizado por los expertos en Ciberseguridad y los resultados obtenidos, las propuestas reciben la validación de los mecanismos de seguridad avanzados presentados en este trabajo de investigación. Con el objetivo de respaldar las soluciones planteadas para la problemática identificada, se certifica la viabilidad de estas propuestas.

Figura 30

Proceso de Validación de las Propuestas



Fuente: Elaboración propia

CONCLUSIONES

El presente estudio se enmarcó en el diseño de propuestas de seguridad para la infraestructura de tecnología de la información (TI) en entornos de cloud computing, que garantice la protección de datos y la integridad de los sistemas de información en PYMEs de la ciudad de Quito. Concluyendo lo siguiente:

1. En cuanto al diagnóstico de las vulnerabilidades en las infraestructuras de TI de las PYMEs que operan en entornos de computación en la nube, se evidencia que la adopción infraestructura en línea es creciente, especialmente en PYMEs, con una preferencia por SaaS y AWS como proveedor líder. Así mismo, persisten desafíos en seguridad, ya que un 30% ha experimentado brechas y solo el 20% califica su capacitación en seguridad como alta. Se concluye que, si bien los servicios en la nube ofrecen beneficios significativos en eficiencia y eficacia, su uso en entornos reales requiere de mejoras en los mecanismos de Autenticación, Cifrado de datos, monitoreo de amenazas y Capacitación a usuarios, personal TI, gestores y administradores, de información sensible para las PYMEs.
2. La evaluación realizada por expertos en ciberseguridad ha demostrado que los mecanismos propuestos cumplen con los más altos estándares de seguridad y son viables para su implementación en entornos de cloud computing. Los mecanismos de Autenticación Multifactor (MFA), Cifrado de Datos y Monitoreo de Amenazas, obtuvieron una calificación superior a la media, lo que confirma su efectividad en la protección de datos y en la mitigación de amenazas cibernéticas. Estos resultados reflejan la madurez y solidez de las soluciones planteadas,

permitiendo a las PYMEs fortalecer su infraestructura de TI con estrategias de seguridad avanzadas.

3. La capacitación en seguridad de la información es un elemento fundamental para la protección de la infraestructura de TI en entornos de cloud computing. Su impacto en la seguridad organizacional está directamente relacionado con la actualización continua de sus contenidos y la capacidad de adaptación a nuevas amenazas cibernéticas. La capacitación efectiva permite que los usuarios comprendan los riesgos asociados al uso de la tecnología y adopten buenas prácticas de seguridad, reduciendo así la posibilidad de errores humanos que puedan comprometer la integridad de los sistemas de información. En este sentido, se confirma que la formación constante del personal es un pilar clave para garantizar la correcta implementación y aprovechamiento de los mecanismos de seguridad establecidos.
4. Los resultados del estudio realizado y el proceso de validación de los métodos de seguridad propuestos demuestran que crear una buena infraestructura de seguridad para la tecnología de la información en entornos de computación en la nube es fundamental para proteger los datos y mantener la integridad de los sistemas de información en PYMEs en la ciudad de Quito. Esto muestra que una infraestructura de seguridad bien diseñada, que se ajuste a las necesidades de la organización, no solo es posible, sino que es esencial para asegurar la continuidad y resiliencia de la empresa ante los desafíos de la ciberseguridad.

RECOMENDACIONES

Para las PYMEs en la ciudad de Quito el utilizar mecanismos de cifrado de datos tanto en reposo como en tránsito, fortalecerá la seguridad en los canales de comunicación y de esta manera las bases de datos se encontrarán protegidas ante cualquier intento de acceso no autorizado. Se debe adoptar la autenticación multifactor (MFA) en todos los sistemas críticos, y revisar las políticas de gestión de identidades y accesos (IAM) para asegurar que se sigan los principios de privilegios mínimos y se limite el acceso solo a usuarios autorizados.

Realizar una evaluación continua de la infraestructura para garantizar que los mecanismos de seguridad estén implementados correctamente y que se mantengan actualizados frente a nuevas amenazas. Para tal efecto, el invertir en tecnologías de monitoreo avanzado y detección de intrusiones (IDS/IPS), es crucial para identificar y responder rápidamente a amenazas emergentes, y así reforzar la capacidad de resiliencia de las PYMEs ante ataques cibernéticos.

Fortalecer las soluciones de mitigación de ataques cibernéticos, como la integración de servicios de mitigación de accesos a la información no consentido en cloud computing.

Es esencial realizar capacitaciones periódicas, al personal en la identificación y gestión de ataques de phishing y ransomware para reducir la vulnerabilidad humana ante estos riesgos. La capacitación debe incluir también la actualización en técnicas de seguridad y procedimientos de respuesta ante incidentes.

REFERENCIAS

Al Reshan, M. S., Syed, D., Islam, N., Shaikh, A., Hamdi, M., Elmagzoub, M. A., Muhammad, G., & Hussain Talpur, K. (2023). A Fast Converging and Globally Optimized Approach for Load Balancing in Cloud Computing. *IEEE Access*, *11*. https://doi.org/10.1109/ACCESS.2023.3241279

Albshaier, L., Budokhi, A., & Aljughaiman, A. (2024). A Review of Security Issues When Integrating IoT with Cloud Computing and Blockchain. *IEEE Access*. https://doi.org/10.1109/ACCESS.2024.3435845

CardonaSergio_2022_VulnerabilidadCloudComputing. (n.d.).

Eljak, H., Ibrahim, A. O., Saeed, F., Hashem, I. A. T., Abdelmaboud, A., Syed, H. J., Abulfaraj, A. W., Ismail, M. A. Bin, & Elsafi, A. (2024). E-Learning-Based Cloud Computing Environment: A Systematic Review, Challenges, and Opportunities. *IEEE Access*, *12*. https://doi.org/10.1109/ACCESS.2023.3339250

Irshad, A., Chaudhry, S. A., Alomari, O. A., Yahya, K., & Kumar, N. (2020). A Novel Pairing-Free Lightweight Authentication Protocol for Mobile Cloud Computing Framework. *IEEE Systems Journal*, *15*(3). https://doi.org/10.1109/jsyst.2020.2998721

Skafi, M., Yunis, M. M., & Zekri, A. (2020). Factors influencing SMEs' adoption of cloud computing services in Lebanon: An empirical analysis using TOE and contextual theory. *IEEE Access*, *8*. https://doi.org/10.1109/ACCESS.2020.2987331

Tang, J., Nie, J., Xiong, Z., Zhao, J., Zhang, Y., & Niyato, D. (2022). Slicing-Based Reliable Resource Orchestration for Secure Software-Defined Edge-Cloud Computing Systems. *IEEE Internet of Things Journal*, *9*(4). https://doi.org/10.1109/JIOT.2021.3107490

62.-Alvaro-Martinez-1442-1447. (n.d.).

A RESEARCH ON CLOUD COMPUTING. (n.d.). Retrieved March 20, 2025, from https://www.researchgate.net/publication/366320853_A_RESEARCH_ON_CLOUD_COMPUTING

ANÁLISIS DE LA IMPLEMENTACIÓN TECNOLÓGICA BASADA EN LA. (n.d.).

ARQUITECTURA DE SERVIDORES EN LA NUBE IAAS. - TECTZAPIC. Revista Académico-Científica. (n.d.). Retrieved March 20, 2025, from https://www.eumed.net/es/revistas/tectzapic/vol-7-no-1-mayo-2021/servidores-nube

De Titulación Previo, T., Obtención, A. La, De, D. T., Ramiro, O., & Sislema, G. (n.d.). ESCUELA POLITÉCNICA NACIONAL FACULTAD DE INGENIERÍA DE SISTEMAS PROPUESTA DE OUTSORCING DE SERVICIOS DE TI PARA CASAS DE VALORES DEL DISTRITO METROPOLITANO DE QUITO (CASO PRÁCTICO: PLUSVALORES).

DIAGNÓSTICO-DE-LAS-CAPACIDADES-DE-CIBERSEGURIDAD-Ecuador-Diciembre-2022_compressed. (n.d.).

DONADO SÁNCHEZ, A. M., MARTIN MOSQUERA, M., & PÉREZ HUÉRFANO, K. A. (2022). MEJORA EN PROCESOS DE PRODUCCIÓN Y LOGÍSTICA PARA AUMENTAR LA EFICIENCIA EN EL SISTEMA ECONÓMICO DE PEQUEÑAS EMPRESAS MANUFACTURERAS EN COLOMBIA. Revista Ingeniería, Matemáticas y Ciencias de La Información, 9(18), 141–148. https://doi.org/10.21017/rimci.2022.v9.n18.a116

Explicación de los modelos de servicios en la nube - SaaS, PaaS, DaaS, IaaS y más. (n.d.). Retrieved March 20, 2025, from https://geekflare.com/es/cloud-service-models/

Geovanny, I. W., Moreno, F., Francisco, I., & Troya, C. (n.d.). Septiembre 2023 Guayaquil-Ecuador.

Ley de Protección de Datos Personales - Dirección Nacional de Registros Públicos. (n.d.). Retrieved March 20, 2025, from https://www.registrospublicos.gob.ec/programas-servicios/servicios/proyecto-de-ley-de-proteccion-de-datos/

Parra-González, E. F., Jaramillo-Avila, U., Salazar-Linares, P., & Lara-Álvarez, C. A. (n.d.). Tendencias y Desafíos de la Computación de Alto Rendimiento en la Nube. https://doi.org/10.17013/risti.49.131-146

Santa Elena Facultad Sistemas Y Telecomunicaciones Título Del Trabajo De Titulación, D. DE, Santa Elena, D., Echeverría Emily Jazmín Modalidad Titulación, P. DE, Elena, S., & Año, E. (n.d.). UNIVERSIDAD ESTATAL PENÍNSULA AUTOR.

Security Guidance For Critical Areas of Focus in Cloud Computing v5. (2024). https://cloudsecurityalliance.org

Una guía completa de Cloud Security en 2025. (n.d.). Retrieved March 20, 2025, from https://kinsta.com/es/blog/seguridad-nube/

UPSE-MTI-2022-0006. (n.d.).

Vista de Diseño de un modelo de migración a cloud computing para entidades públicas de salud. (n.d.). Retrieved March 20, 2025, from https://revistas.unisimon.edu.co/index.php/innovacioning/article/view/2772/3339

Vista de Seguridad de la Información en la Nube: Una revisión sistemática. (n.d.). Retrieved March 20, 2025, from https://revistas.unh.edu.pe/index.php/ricci/article/view/383/957

ANEXOS

Anexo 1. Formato de encuesta

UNIVERSIDAD TÉCNICA DEL NORTE
Resolución No. 001-073 CEAACES-2013-13
INSTITUTO DE POSGRADO

CUESTIONARIO PARA EL PERSONAL ENCARGADO DE TICS. EN PYMEs

Lineamientos Generales: El presente instrumento forma parte de la tesis de maestría titulada: "**Propuesta de seguridad para una infraestructura de tecnología de la información (TI) en entornos de cloud computing: caso de estudio una PYMEs de la ciudad de Quito"**, el mismo que busca evaluar el nivel de conocimiento y percepción que tienen los responsables de TICS en PYMEs de la ciudad de Quito sobre las vulnerabilidades y brechas de seguridad más comunes en entornos cloud computing, asi como evaluar la efectividad de las medidas de seguridad implementadas actualmente.

La información que proporcione en la encuesta, será manejada con total criterio de responsabilidad y confiabilidad.

Estimado validador a continuación se presenta el sistema de objetivos de la investigación con la finalidad de proporcionar información para la evaluación de la pertinencia y coherencia del presente instrumento.

Objetivo General

- Diseñar una propuesta de seguridad para la infraestructura de tecnología de la información (TI) en entornos de cloud computing, que garantice la protección de datos y la integridad de los sistemas de información aplicado a una PYME de la ciudad de Quito.

Objetivos Específicos

- Diagnosticar las vulnerabilidades y brechas de seguridad en el diseño de infraestructuras de TI para cloud computing, que garantice la protección de datos y la resiliencia de los sistemas de información.
- Proponer mecanismos de seguridad avanzados para el diseño de la infraestructura de TI en entornos de cloud computing, optimizando la gestión de accesos y fortaleciendo la defensa contra amenazas emergentes.
- Validar la capacidad de los mecanismos de seguridad diseñados para entornos de cloud computing en la resistencia a ataques cibernéticos y en el mantenimiento de la integridad y confidencialidad de los datos.

UNIVERSIDAD TÉCNICA DEL NORTE

Resolución No. 001-073 CEAACES-2013-13

INSTITUTO DE POSGRADO

CUESTIONARIO PARA EL PERSONAL ENCARGADO DE TICS. EN PYMEs

Esta encuesta forma parte de un proyecto de investigación de tesis, que tiene como objetivo identificar las principales vulnerabilidades y brechas de seguridad, proponer mecanismos de seguridad y validar la capacidad de defensa en entornos de cloud computing, los resultados que se obtenga serán utilizados de forma estricta y confidencial por el investigador a fin de plantear una propuesta de formación.

Sección 1: Información general

1. ¿Cuál es el tamaño de su empresa?
   - Pequeña
   - Mediana
   - Grande
2. ¿Cuánto tiempo lleva su empresa utilizando soluciones de cloud computing?
   - Menos de 6 meses
   - 6 meses - 1 año
   - 1 - 2 años
   - Más de 2 años
3. ¿Qué tipo de servicios de cloud computing utiliza su empresa? (Puede seleccionar más de uno)
   - Infraestructura como Servicio (IaaS)
   - Plataforma como Servicio (PaaS)
   - Software como Servicio (SaaS)
4. ¿Qué tipo de infraestructura en la nube utiliza principalmente su empresa?
   - Contenedores
   - Máquinas virtuales
   - Serverless
   - Otros (especifique): _____

5. ¿Con qué proveedor tiene contratado el servicio de cloud computing? (Puede seleccionar más de uno)

   - AWS
   - Microsoft Azure
   - Google Cloud Platform
   - Otros (especifique): _____

6. ¿Qué tipo de seguridad utiliza en su infraestructura de cloud computing? (Puede seleccionar más de uno)

   - Firewall de aplicaciones web (WAF)
   - Sistema de prevención de intrusiones (IPS)
   - Sistema de detección de intrusiones (IDS)
   - Otros (especifique): _____

7. ¿Qué tipo de instancias utiliza su empresa en la nube?

   - Dedicadas
   - Compartidas
   - Escalables automáticamente
   - Otros (especifique): _____

8. ¿Cómo utiliza su empresa las aplicaciones en la nube? (Puede seleccionar más de uno)

   - Desarrollo y pruebas o Producción
   - Almacenamiento de datos
   - Analítica y Big Data
   - Otros (especifique): _____

Sección 2: Diagnóstico de vulnerabilidades y brechas de seguridad

9. ¿Cómo calificaría el nivel de seguridad general de su infraestructura de cloud computing?

   - Muy bajo

- Bajo
- Moderado
- Alto
- Muy alto

10. ¿Qué tipo de incidentes de seguridad ha experimentado su empresa? (Puede seleccionar más de uno)

    - Acceso no autorizado
    - Pérdida de datos
    - Ataques de ransomware
    - Otros (especifique): _____

11. ¿Qué medidas de seguridad ha implementado o intentado implementar para proteger los datos en la nube? (Puede seleccionar más de uno)

    - Cifrado de datos
    - Control de acceso basado en roles
    - Detección y prevención de intrusiones
    - Autenticación multifactor
    - Otros (especifique): _____

12. ¿Qué tan efectivas considera que son las medidas de seguridad que ha implementado?

    - Muy ineficaces
    - Ineficaces
    - Neutrales
    - Eficaces
    - Muy eficaces

13. ¿Qué brechas de seguridad ha identificado en su infraestructura de cloud computing? (Puede seleccionar más de uno)

    - Falta de actualización de software
    - Configuración incorrecta de seguridad
    - Falta de capacitación del personal

- Otros (especifique): _____

Sección 3: Propuesta de mecanismos de seguridad avanzados

14. ¿Qué mecanismos de seguridad avanzados considera necesarios para su infraestructura de TI en la nube? (Puede seleccionar más de uno)
    - Análisis de comportamiento de usuarios
    - Inteligencia artificial para detección de amenazas
    - Red privada virtual (VPN) para acceso seguro
    - Segmentación de red
    - Otros (especifique): _____
15. ¿Cómo calificaría la importancia de implementar mecanismos de seguridad avanzados en su infraestructura de cloud computing?
    - No importante
    - Poco importante
    - Moderadamente importante
    - Importante
    - Muy importante
16. ¿Qué dificultades ha encontrado al implementar mecanismos de seguridad avanzados? (Puede seleccionar más de uno)
    - Costo elevado
    - Complejidad técnica
    - Falta de conocimientos especializados
    - Resistencia del personal
    - Otros (especifique): _____
17. ¿Qué tipo de capacitación o soporte adicional considera necesario para mejorar la seguridad en la nube?
    - Capacitación técnica
    - Asesoramiento en mejores prácticas
    - Recursos financieros

- Soporte continuo de proveedores
- Otros (especifique): _____

Sección 4: Validación de Mecanismos de Seguridad

18. ¿Qué tan eficaz considera que serían los mecanismos de seguridad avanzados propuestos para resistir ataques cibernéticos?

    - Muy ineficaces
    - Ineficaces
    - Neutrales
    - Eficaces
    - Muy eficaces

19. ¿Qué tipo de pruebas realiza su empresa para validar la eficacia de los mecanismos de seguridad en la nube? (Puede seleccionar más de uno)

    - Pruebas de penetración
    - Simulacros de ataques
    - Auditorías de seguridad
    - Evaluaciones continuas
    - Otros (especifique): _____

20. ¿Con qué frecuencia realiza su empresa evaluaciones de seguridad en su infraestructura de cloud computing?

    - Mensualmente
    - Trimestralmente
    - Anualmente
    - Solo cuando ocurre un incidente
    - No se realizan evaluaciones

21. ¿Qué mejoras considera necesarias en los mecanismos de seguridad actuales para fortalecer la defensa contra amenazas emergentes?

    - Actualización de software
    - Integración de nuevas tecnologías

- Mejora en los procesos de gestión de accesos
- Mayor capacitación del personal
- Otros (especifique): _____

22. ¿Qué impacto ha tenido la implementación de mecanismos de seguridad avanzados en la integridad y confidencialidad de los datos en su empresa?

- Muy negativo
- Negativo
- Neutro
- Positivo
- Muy positivo

23. ¿Qué beneficios adicionales ha observado su empresa al fortalecer la infraestructura de seguridad en cloud computing? (Puede seleccionar más de uno)

- Reducción de incidentes de seguridad
- Mejora en la confianza de clientes
- Cumplimiento normativo mejorado
- Eficiencia operativa aumentada
- Otros (especifique): _____

24. ¿Qué recomendaciones adicionales tiene para mejorar la seguridad en entornos de cloud computing en su empresa?

- _____
- _____
- _____

GRACIAS POR SU COLABORACIÓN

UNIVERSIDAD TÉCNICA DEL NORTE

Resolución No. 001-073 CEAACES-2013-13

INSTITUTO DE POSGRADO

INSTRUMENTO DE VALIDACIÓN

Instrucciones: En el siguiente formato, indique según la escala excelente (E), bueno (B) o mejorable (M) en cada ítem, de acuerdo con los criterios de validación (coherencia, pertinencia, redacción), si es necesario agregue las observaciones que considere. Al final se deja un espacio para agregar observaciones generales.

Ítem Nro.	Validación			Observación
	Coherencia	Pertinencia	Redacción	
1	E	E	E	
2	E	E	E	
3	E	E	E	
4	E	E	E	
5	E	E	E	
6	E	E	E	
7	E	E	E	
8	E	E	E	
9	E	E	E	
10	E	E	E	
11	E	E	E	
12	E	E	E	
13	E	E	E	
14	E	E	E	
15	E	E	E	
16	E	E	E	
17	E	E	E	
18	E	E	E	
19	E	E	E	
20	E	E	E	
21	E	E	E	
22	E	E	E	
23	E	E	E	
24	E	E	E	

Observaciones generales

Se observa coherencia y pertinencia en las preguntas elaboradas en el presente instrumento.

UNIVERSIDAD TÉCNICA DEL NORTE

Resolución No. 001-073 CEAACES-2013-13

INSTITUTO DE POSGRADO

Datos del Validador

Mgs. Cristhian Gabriel Morales Hidalgo

CRISTHIAN GABRIEL MORALES HIDALGO

Firma

Magíster en Seguridad Informática

Anexo 2 Validación de las propuestas por expertos

UNIVERSIDAD TÉCNICA DEL NORTE

Resolución No. 001-073 CEAACES-2013-13

INSTITUTO DE POSGRADO

PROPUESTA DE SEGURIDAD PARA INFRAESTRUCTURA DE TI EN ENTORNOS DE CLOUD COMPUTING

Lineamientos Generales: El presente instrumento forma parte de la tesis de maestría titulada: "**Propuesta de seguridad para una infraestructura de tecnología de la información (TI) en entornos de cloud computing: caso de estudio una PYMEs de la ciudad de Quito"**, el mismo que busca validar la capacidad de los mecanismos de seguridad diseñados para entornos de cloud computing en la resistencia a ataques cibernéticos y en el mantenimiento de la integridad de los sistemas de información y confidencialidad de los datos.

La propuesta consiste en el diseño de un de un conjunto de mecanismos avanzados de seguridad para la infraestructura de TI en entornos de computación en la nube, aplicables a las Pymes de Quito. Para tal efecto el propósito del objetivo principal de la investigación es "**Diseñar una propuesta de seguridad para la infraestructura de tecnología de la información (TI) en entornos de cloud computing, que garantice la protección de datos y la integridad de los sistemas de información aplicado a una PYME de la ciudad de Quito**". Este enfoque busca garantizar la protección de datos y la integridad de los sistemas de información en un contexto donde las amenazas cibernéticas son cada vez más sofisticadas. Estos mecanismos estarán diseñados para optimizar la gestión de accesorios, fortalecer la defensa contra ataques emergentes y garantizar la continuidad operativa de las empresas.

Esta iniciativa surge para dotar a las Pymes de herramientas efectivas que les permitan aprovechar el potencial de la computación en la nube sin comprometer la seguridad de sus operaciones. Abarca desde la implementación de protocolos de autenticación multifactor, cifrado de datos en reposo y en tránsito, adopción de sistemas de monitoreo de amenazas en tiempo real, con un enfoque en soluciones escalables y de bajo costo y plan de capacitación.

Objetivo General

- Diseñar mecanismos avanzados de seguridad para la infraestructura de TI en entornos de computación en la nube, con el propósito de garantizar la protección de datos, la integridad de los sistemas de información y la continuidad operativa de las Pymes en Quito.

Objetivos Específicos

- Proponer mecanismos de seguridad avanzada, como cifrado, autenticación multifactor y monitoreo continuo, adaptados a las necesidades y recursos de las Pymes.
- Diseñar un programa de capacitación dirigida al personal de las Pymes, enfocada en la correcta gestión de los mecanismos de seguridad y en la adopción de prácticas

seguras para la protección de datos en entornos de computación en la nube.

- Evaluar la factibilidad de los mecanismos diseñados para mitigar las vulnerabilidades y brechas de seguridad en el diseño de infraestructuras de TI para cloud computing, mediante la validación de propuestas con base en el criterio de expertos en Ciberseguridad.

MECANISMOS DE SEGURIDAD PROPUESTOS PARA INFRAESTRUCTURA DE TI EN ENTORNOS DE CLOUD COMPUTING

Mecanismo	Descripción	Monitoreo	Indicadores de Monitoreo	Métodos de evaluación	Herramientas de evaluación	Herramientas AWS	Herramientas Google
Autenticación Multifactor (MFA)	Mecanismo de autenticación que requiere más de un factor de verificación para permitir el acceso, como contraseñas, dispositivos móviles, biometría, etc.	Monitoreo de intentos de autenticación fallidos, actividad de inicio de sesión, patrones de acceso inusuales.	- Número de intentos fallidos de autenticación. - Frecuencia de acceso desde dispositivos no habituales. - Registros de actividad inusual (p. ej., horas fuera de lo común).	- Análisis de registros de autenticación. - Revisión de políticas de acceso y autenticación. - Evaluación de pruebas de penetración para identificar debilidades.	Splunk, ELK Stack, Kali Linux.	AWS IAM, AWS CloudTrail.	Google Identity-Aware Proxy (IAP), Google Cloud Audit Logs.
Cifrado de datos	Técnica para convertir los datos en un formato ilegible para garantizar que solo los usuarios autorizados puedan acceder a ellos. Aplicable tanto en reposo como en tránsito.	Monitoreo de procesos de cifrado, accesos a datos sensibles y uso de claves de cifrado.	- Número de accesos no autorizados a datos cifrados. - Frecuencia de utilización de claves de cifrado. - Tiempos de acceso a datos cifrados.	- Revisión de políticas de cifrado. - Auditorías de cumplimiento con normativas como GDPR. - Pruebas de integridad y validación de procesos de cifrado.	OpenSSL, Wireshark, Varonis.	AWS Key Management Service (KMS), AWS CloudHSM.	Google Cloud Key Management, Google Cloud Security Command Center.
Monitoreo de Amenazas	Sistema de monitoreo en tiempo real que detecta y responde a incidentes de seguridad, como intrusiones, ataques de DDoS y otras amenazas emergentes.	Monitoreo de eventos de seguridad en tiempo real, detección de anomalías, análisis de patrones de tráfico de red.	- Número de incidentes detectados en tiempo real. - Tiempo de respuesta a incidentes. - Frecuencia de alertas de posibles amenazas.	- Evaluación de protocolos de respuesta ante incidentes. - Simulación de ataques para medir tiempos de respuesta.	SIEM (Splunk, ELK Stack), Snort, Metasploit.	AWS GuardDuty, AWS Security Hub.	Google Chronicle Security Operations, Google Security Command Center.

UNIVERSIDAD TÉCNICA DEL NORTE

Resolución No. 001-073 CEAACES-2013-13

INSTITUTO DE POSGRADO

Programa de capacitación enfocado en la seguridad para una infraestructura de TI en entornos de Cloud Computing.

Módulo	Tema	Objetivo	Duración	Público Objetivo	Metodología	Recursos
Módulo 1	Introducción a la Seguridad en Cloud Computing	Comprender los conceptos básicos de seguridad en la nube y los riesgos asociados.	2 horas	Personal de TI y administrativos	Exposición teórica y discusión	Presentación, material digital
Módulo 2	Gestión de Accesos y Autenticación	Implementar controles de acceso robustos y autenticación multifactor para proteger los sistemas.	3 horas	Personal de TI y usuarios con acceso a sistemas sensibles	Taller práctico y simulaciones	Software de autenticación, manuales de configuración
Módulo 3	Protección de Datos y Políticas de Backup	Establecer estrategias de respaldo y recuperación para evitar pérdidas de información.	2 horas	Administradores de bases de datos y gerencia	Ejercicio práctico de recuperación de datos	Software de backup, casos de estudio
Módulo 4	Identificación y Prevención de Ciberataques	Capacitar sobre amenazas comunes (phishing, ransomware) y cómo mitigarlas.	3 horas	Todo el personal	Simulación de ataques y análisis de casos reales	Plataforma de ciberseguridad, videos ilustrativos
Módulo 5	Configuración Segura de Infraestructura en la Nube	Aplicar buenas prácticas en la configuración segura de servidores y redes en la nube.	4 horas	Equipo de TI y administradores de sistemas	Laboratorio práctico en entorno de prueba	Acceso a entornos virtuales de prueba
Módulo 6	Cumplimiento Normativo y Políticas de Seguridad	Garantizar que la empresa cumpla con normativas locales e internacionales en seguridad de TI.	2 horas	Gerencia y personal de TI	Análisis de normativas y desarrollo de políticas internas	Normativas ISO 27001, GDPR, Ley Orgánica de Protección de Datos
Módulo 7	Monitoreo y Respuesta a Incidentes	Implementar estrategias de detección y respuesta ante incidentes de seguridad en la nube.	3 horas	Equipo de TI y personal clave	Simulación de respuesta ante incidentes	Herramientas SIEM, manual de respuesta a incidentes
Módulo 8	Cultura de Seguridad y Concienciación	Fomentar hábitos seguros en el uso de sistemas y datos en la nube.	2 horas	Todo el personal	Dinámicas interactivas y estudio de casos	Infografías, videos, evaluación de conocimientos

UNIVERSIDAD TÉCNICA DEL NORTE

Resolución No. 001-073 CEAACES-2013-13

INSTITUTO DE POSGRADO

FORMULARIO DE CALIFICACION DE PROPUESTA

Instrucciones: En el siguiente formato, utilice la escala de evaluación del 1 al 5 proporcionado. Cada número (1, 2, 3, 4, 5) tiene un significado específico que refleja el nivel de implementación o desempeño de cada Ítems, de acuerdo con el siguiente detalle:

- **1 - No satisfactorio:** Representa una propuesta deficiente o inexistente.
- **2 - Bajo:** Indica que la propuesta es parcial o limitada.
- **3 - Medio:** Denota la propuesta es adecuada, pero con espacio para mejoras.
- **4 - Alto:** Refleja que la propuesta posee un buen nivel de cumplimiento.
- **5 - Excelente:** Representa una propuesta ejemplar y completa.

La propuesta que obtuviere puntaje entre 5 y 4 se la considera (Factible), 3 puntos (Necesita Mejora) y entre 1 y 2 puntos (No es factible):

Propuestas de Mecanismos	1 (No satisfactorio)	2 (Bajo)	3 (Medio)	4 (Alto)	5 (Excelente)	Puntaje asignado
Autenticación Multifactor (MFA)					X	5
Cifrado de Datos					X	5
Monitoreo de Amenazas					X	5
Plan de Capacitación				X		4

Observaciones generales

La propuesta presentada es altamente sólida y refleja una atención detallada a los aspectos clave de la ciberseguridad. Los mecanismos fundamentales como la Autenticación Multifactor (MFA), el Cifrado de Datos y el Monitoreo de Amenazas son evaluados con un puntaje de 5, lo que indica un nivel excelente en su implementación. Estas medidas son esenciales para proteger los datos sensibles y garantizar la integridad de la infraestructura de tecnología de la información (TI) en entornos de cloud computing de las PYMEs, frente a las amenazas cibernéticas. Además, la propuesta demuestra una integración coherente y estratégica de estas soluciones, lo que resulta en una defensa sólida y bien estructurada contra ataques potenciales. Sin lugar a duda, estos mecanismos cumplen con los estándares más altos y son apropiados para las PYMEs.

El Plan de Capacitación, con un puntaje de 4, es un componente clave que ha sido bien diseñado, aunque podría beneficiarse de algunas mejoras. Si bien es adecuado, una mayor profundidad en los módulos y una actualización constante para abordar las amenazas emergentes fortalecerían aún más la capacitación del personal. La sensibilización continua

y la formación práctica son fundamentales para garantizar que los empleados no solo comprendan los procedimientos de seguridad, sino que también estén preparados para actuar correctamente ante situaciones de riesgo. En general, la propuesta es factible y bien elaborada, pero, como en todo plan de seguridad, siempre es posible optimizar los detalles y adaptarlos a las necesidades específicas y cambiantes de las PYMEs.

Conclusiones

Las propuestas son factibles y están bien fundamentadas, ya que los mecanismos evaluados proporcionan una defensa sólida contra las vulnerabilidades y brechas de seguridad en el diseño de infraestructuras de TI para cloud computing. Además, con una mejora en el Plan de Capacitación, se lograría un nivel de seguridad aún mayor, asegurando que los empleados estén completamente preparados para enfrentar riesgos emergentes. Estos mecanismos son altamente recomendables para las PYMEs, ya que garantizan una protección efectiva de los sistemas y datos, adaptándose a las necesidades de seguridad en constante evolución.

Por lo tanto, una vez concluida la evaluación de las propuestas de mecanismos de seguridad avanzados para el diseño de la infraestructura de TI en entornos de cloud computing, y con el propósito de que este estudio sirva como apoyo académico en la resolución del problema planteado, procedemos a la validación de las propuestas presentadas en el presente trabajo de investigación de tesis de maestría en favor de la Ing. Ayde Marlene Rochina Rochina.

Datos del Validador
Mgs. Cristhian Gabriel Morales Hidalgo

Firma

Magíster en Seguridad Informática

Datos del Validador
Mgs. Edison Richard Condor Licero

Firma

Magíster en Ciberseguridad