

Vulnerabilidades en Servicios On Premise

TITULO

Vulnerabilidades en Servicios On Premise

Santiago Andres Arias Mancilla

Billy Efraín Moreno Martínez

William David Otalora Moreno

Directores:

Todos los docentes que les aportan en la construcción de este documento

UNIVERSIDAD SANTO TOMAS

FACULTAD DE INGENIERÍA DE TELECOMUNICACIONES

ESPECIALIZACIÓN EN GESTIÓN DE SERVICIOS DE TECNOLOGÍAS DE LA
INFORMACIÓN

BOGOTÁ, AÑO 2024

RESUMEN

El presente proyecto aborda las vulnerabilidades asociadas con la infraestructura tecnológica on-premise, particularmente en microempresas del sector TI. A través de un análisis detallado, se identifican las principales limitaciones de estos sistemas, tales como la obsolescencia tecnológica, la alta inversión en mantenimiento, las restricciones de escalabilidad y las crecientes amenazas de ciberseguridad.

Como solución, se propone la migración de los servicios on-premise a plataformas en la nube, destacando sus beneficios en términos de flexibilidad, escalabilidad, seguridad y reducción de costos. El documento detalla alternativas técnicas basadas en Infraestructura como Servicio (IaaS), Plataforma como Servicio (PaaS) y Software como Servicio (SaaS), respaldadas por tecnologías líderes como AWS, Azure y Google Cloud. Además, se considera la implementación de herramientas avanzadas para la gestión de la seguridad, almacenamiento y automatización.

Este enfoque no solo busca mitigar los riesgos actuales, sino también posicionar a las empresas para un crecimiento sostenible en un entorno tecnológico en constante evolución, garantizando la continuidad del negocio y mejorando su capacidad para competir en el mercado digital.

INTRODUCCION

En el contexto de un mundo empresarial cada vez más digitalizado, la infraestructura tecnológica desempeña un papel crucial en la continuidad y competitividad de las organizaciones. Sin embargo, muchas empresas, especialmente las microempresas del sector de Tecnologías de la Información (TI), enfrentan graves desafíos relacionados con el mantenimiento de servicios on-premise. Estos sistemas, caracterizados por la gestión local de servidores y aplicaciones, presentan vulnerabilidades significativas debido a la obsolescencia tecnológica, los altos costos de mantenimiento, la limitada escalabilidad y los riesgos de ciberseguridad.

A pesar de ofrecer mayor control sobre los datos, las infraestructuras on-premise requieren inversiones constantes en hardware y software, personal técnico especializado y la implementación de medidas robustas de seguridad. Estos requisitos dificultan su sostenibilidad a largo plazo, especialmente para empresas con recursos limitados. Los fallos de hardware, la falta de redundancia y las amenazas externas son riesgos constantes que pueden impactar la continuidad del negocio.

Ante este panorama, las soluciones en la nube han emergido como una alternativa eficiente, escalable y segura para las empresas que buscan optimizar sus operaciones. La migración a la nube permite aprovechar infraestructuras modernas, mantener altos niveles de disponibilidad, mejorar la seguridad de los datos y reducir significativamente los costos operativos mediante modelos de pago por uso. Este documento analiza las vulnerabilidades inherentes a los sistemas on-premise y propone alternativas técnicas basadas en tecnologías en la nube, ofreciendo un enfoque estratégico para la transición hacia una infraestructura digital más resiliente y adaptable.

Contenido

1.	OBJETIVOS.....	5
2.	PROBLEMA	6
3.	IDEACIÓN DE LA SOLUCIÓN	9
4.	ANÁLISIS DE LAS ALTERNATIVAS TÉCNICAS PARA SOLUCIONAR EL PROBLEMA	16
5.	MODELO DE NEGOCIO	28
6.	PROPUESTA DE LA SOLUCIÓN TECNOLÓGICA.....	30
7.	Análisis del Proceso de Transformación Digital.....	31
8.	Aspectos Legales y de Contratación	32
9.	REFERENCIAS.....	34

1. OBJETIVOS

Objetivo General

- Proponer una solución tecnológica basada en la migración a la nube que permita a las microempresas del sector TI superar las limitaciones y vulnerabilidades inherentes a los sistemas on-premise, mejorando la seguridad, escalabilidad y eficiencia operativa.

Objetivos Específicos

1. Analizar las vulnerabilidades actuales de los servicios on-premise, incluyendo riesgos de ciberseguridad, fallos de hardware y obsolescencia tecnológica.
2. Identificar y evaluar alternativas técnicas en la nube, considerando opciones como IaaS, PaaS y SaaS, y seleccionando las tecnologías más adecuadas para microempresas.
3. Diseñar una arquitectura tecnológica escalable y segura, basada en servicios en la nube, que contemple medidas avanzadas de seguridad, alta disponibilidad y recuperación ante desastres.
4. Establecer un plan de migración estructurado, que minimice riesgos operativos y asegure una transición eficiente desde entornos on-premise hacia plataformas en la nube.
5. Validar la viabilidad técnica y económica de la solución propuesta mediante un análisis comparativo, asegurando su alineación con las necesidades y capacidades de las microempresas del sector TI.

2. PROBLEMA

2.1. ARBOL DE PROBLEMAS

En la ilustración de árbol de problemas 1 se identifica el problema macro de la obsolescencia tecnológica en los servicios on-premise. Esta situación conlleva una serie de vulnerabilidades y desafíos que pueden afectar gravemente el rendimiento y la disponibilidad de los servicios. A continuación, se desglosan los principales problemas identificados: En la Ilustración de árbol de problemas 1 Ilustración 1 se identifica el problema macro, el cual es tener los servicios on-premise y esto puede presentar vulnerabilidades que afecten rendimiento y/o de negación de servicios.

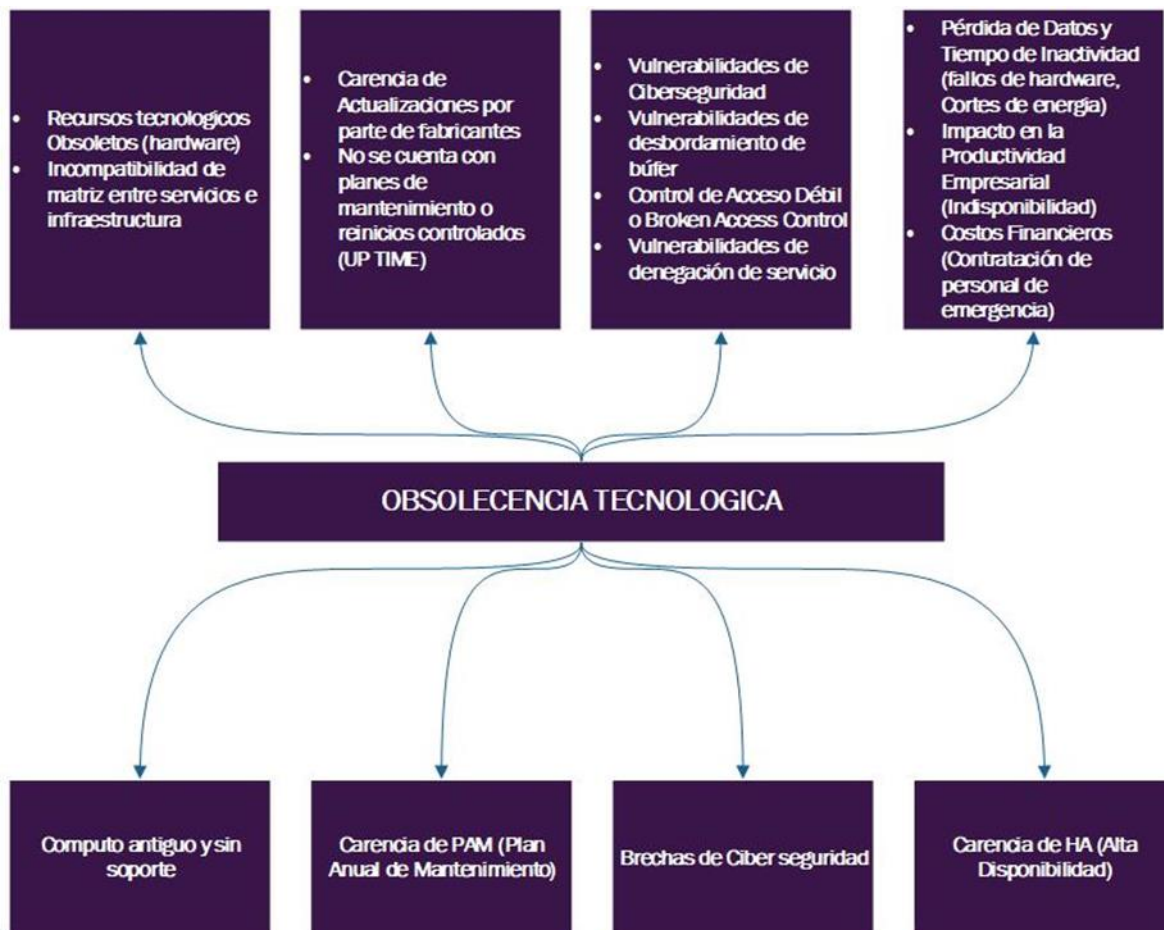


Ilustración de árbol de problemas

Fuente: autores

Este análisis detallado muestra cómo la obsolescencia tecnológica en los servicios on-premise no solo crea riesgos significativos de ciberseguridad, sino que también

impacta negativamente la operación y productividad de la empresa. Es esencial abordar estos problemas mediante la actualización de la infraestructura tecnológica, la implementación de planes de mantenimiento y la adopción de medidas de seguridad robustas.

2.2. QUE SE QUIERE SOLUCIONAR

Según la continua evolución digital y el continuo crecimiento de la industria TIC es indispensable contar con los recursos necesarios para garantizar el performance y disponibilidad de los servicios y aplicativos ofrecidos en la empresa, por lo cual se hace mandatorio tener los dispositivos o hardware que soporten el su correcto funcionamiento, ya que cada día las aplicaciones demandan más consumo de memoria RAM, CPU o unidad de almacenamiento y por ende se requieren soluciones escalables.

En el sector tecnológico, se ha observado una tendencia creciente hacia la migración de servidores on-premise a soluciones en la nube. Esta tendencia responde a la necesidad de enfrentar varios desafíos asociados con la obsolescencia tecnológica, como la falta de actualizaciones, las vulnerabilidades de ciberseguridad y la pérdida de datos debido a fallas de hardware. Las soluciones en la nube ofrecen infraestructura actualizada, escalabilidad y políticas de seguridad que se adaptan a las necesidades de los negocios modernos.

En nuestro caso particular, la empresa enfrenta problemas significativos con sus servidores on-premise, incluyendo tiempos de inactividad, falta de soporte técnico y vulnerabilidades de ciberseguridad. Estos problemas no solo afectan la eficiencia operativa, sino que también ponen en riesgo la seguridad de la información y la continuidad del negocio. Es crucial abordar estos desafíos mediante una estrategia que garantice la alta disponibilidad y la seguridad de los servicios.

- **Obsolescencia de los Servidores On-Premise:** Los servidores actuales están desactualizados y ya no reciben soporte ni actualizaciones de seguridad, lo que aumenta la vulnerabilidad a ataques y fallos.
- **Tiempos de Inactividad:** La infraestructura on-premise no cuenta con mecanismos robustos para garantizar la alta disponibilidad, resultando en tiempos de inactividad que afectan la productividad.
- **Vulnerabilidades de Ciberseguridad:** La falta de actualizaciones y medidas de seguridad adecuadas expone a la empresa a riesgos significativos de ciberataques.
- **Pérdida de Datos:** Fallos de hardware y falta de redundancia en el almacenamiento de datos pueden resultar en pérdida de información crítica.

Se propone realizar una migración de los servidores on-premise a un ambiente virtualizado y alojado en la nube. Esta solución debe incluir las siguientes características:

Vulnerabilidades en Servicios On Premise

- **Actualización y Mantenimiento Continuo:** El proveedor de servicios en la nube garantizará que las máquinas estén siempre parchadas y actualizadas, reduciendo significativamente las vulnerabilidades de seguridad.
- **Alta Disponibilidad:** Implementar políticas de alta disponibilidad para minimizar la inactividad, asegurando el acceso constante a los servicios y aplicaciones en la nube. Esto incluye carga continua, almacenamiento distribuido, replicación de datos y diversificación de proveedores para mitigar los riesgos asociados a los cambios climáticos y otros factores externos.
- **Ciberseguridad Mejorada:** Adoptar autenticaciones robustas, sistemas de detección de amenazas y auditorías de seguridad para proteger los datos privilegiados y prevenir filtraciones. Se debe asegurar que todas las políticas de seguridad estén alineadas con las necesidades del negocio y se actualicen regularmente.

3. IDEACIÓN DE LA SOLUCIÓN

La rápida evolución de las tecnologías de la información y la creciente adopción de soluciones en la nube están transformando significativamente el panorama empresarial. En la actualidad, muchas empresas del sector TI operan con infraestructura on-premise, gestionando sus propios servidores y centros de datos. Este enfoque presenta múltiples desafíos y riesgos, incluyendo altos costos de mantenimiento, limitaciones en la escalabilidad, y una vulnerabilidad constante frente a amenazas de seguridad, desastres naturales y fallos de hardware. Las actualizaciones y parches de seguridad a menudo requieren intervención manual, lo que incrementa el riesgo de exposición a vulnerabilidades y ciberataques. Además, la administración de esta infraestructura requiere personal especializado, lo cual puede resultar costoso y complicado de gestionar, especialmente para empresas de menor tamaño.

Frente a estos desafíos, la migración de servicios web a la nube se presenta como una solución viable y necesaria. Las tendencias actuales, como el incremento en la obsolescencia tecnológica, la necesidad de escalabilidad y flexibilidad, la alta disponibilidad y la recuperación ante desastres, y la reducción de costos operativos, están impulsando a las empresas a considerar esta transición. La tecnología actual ha alcanzado un nivel de madurez que proporciona confianza en la seguridad, escalabilidad y disponibilidad de las soluciones en la nube, ofreciendo una infraestructura más segura y eficiente. Esta migración promete resolver las limitaciones y vulnerabilidades inherentes a los sistemas on-premise, permitiendo a las empresas del sector TI optimizar recursos, mejorar la resiliencia de sus servicios y asegurar la continuidad del negocio en un entorno tecnológico en constante cambio.

3.1. POR QUÉ SE PLANTEA LA SOLUCIÓN

Para abordar la vulnerabilidad de los servicios web en un entorno on-premise [1], es fundamental analizar las tendencias tecnológicas actuales que impactan en esta problemática y entender por qué la migración a la nube se plantea como una solución viable en este momento.

En la actualidad, la rápida evolución de las tecnologías de la información y la creciente adopción de soluciones en la nube están transformando significativamente el panorama empresarial. Varias tendencias clave están influyendo en la necesidad de migrar servicios web desde entornos on-premise a la nube.

- **Incremento en la Obsolescencia Tecnológica:** Con el avance constante de la tecnología, los sistemas on-premise están quedando rápidamente obsoletos. Las empresas enfrentan desafíos para mantener sus infraestructuras actualizadas, lo que resulta en mayores riesgos de seguridad y problemas de compatibilidad. La falta de soporte y actualizaciones de los

fabricantes para equipos y software antiguos incrementa la vulnerabilidad ante ciberataques y fallos operativos [2].

- **Necesidad de Escalabilidad y Flexibilidad:** Las empresas modernas requieren infraestructura que pueda adaptarse rápidamente a cambios en la demanda. Los entornos on-premise, con su capacidad limitada para escalar, no satisfacen esta necesidad de manera eficiente. Las soluciones en la nube permiten una escalabilidad rápida y flexible, ajustando recursos según sea necesario y optimizando costos.
- **Alta Disponibilidad y Recuperación ante Desastres:** Garantizar la disponibilidad continua de los servicios es crucial para la continuidad del negocio. Los sistemas on-premise son susceptibles a fallos de hardware y desastres naturales que pueden causar tiempos de inactividad significativos. La nube ofrece opciones avanzadas de alta disponibilidad y planes de recuperación ante desastres, asegurando un funcionamiento ininterrumpido.
- **Reducción de Costos Operativos:** Migrar a la nube puede reducir significativamente los costos operativos. Los modelos de pago por uso y la eliminación de la necesidad de mantener y actualizar infraestructura física permiten a las empresas optimizar sus gastos. Además, los proveedores de la nube como Oracle, AWS, Azure y Google Cloud ofrecen una gama de servicios que pueden ser personalizados según las necesidades específicas de cada empresa.

Dadas estas tendencias, es evidente que migrar los servicios web a la nube es una solución necesaria y oportuna para abordar las vulnerabilidades y limitaciones actuales del entorno on-premise. La tecnología actual ha alcanzado un nivel de madurez que proporciona confianza en la seguridad, escalabilidad y disponibilidad de las soluciones en la nube, lo que no era posible en el pasado.

Para implementar esta migración, se propone realizar un levantamiento exhaustivo de información inicial, incluyendo detalles sobre los servicios existentes, el sistema operativo en uso y los requisitos mínimos a nivel físico de todos los servicios que tiene la empresa y cuáles son los que se van a subir a la nube [3]. Además, se llevará a cabo una evaluación de las opciones de migración a la nube ofrecidas por diferentes proveedores como Oracle [4], AWS [5], Azure [6] y Google Cloud [7], considerando el costo-beneficio y los servicios disponibles para realizar soluciones escalables, asegurando que las aplicaciones de la empresa no se vean afectadas por el cambio de plataforma en que se van a migrar. Este análisis permitirá establecer un plan de migración detallado, que incluirá cronogramas de tiempo y pasos específicos para minimizar cualquier interrupción en los servicios durante la transición. Además, se realizarán pruebas constantes de las vulnerabilidades que se pueden presentar mientras el servicio es on-premise con un protocolo de seguridad garantizado.

3.2 SECTOR OBJETIVO

3.2.1. DEFINIR EL SECTOR

El sector de Tecnologías de la Información (TI) que ofrece servicios web on-premise está dirigido a microempresas. Se definen como un tipo de organización de menor tamaño dentro de la clasificación por tamaño de empresas, por tanto, estas empresas generalmente cuentan con un equipo reducido de empleados y registran un volumen de facturación inferior al de las medianas y grandes empresas. Además, su gestión suele estar a cargo de sus propietarios, quienes pueden formar parte de un grupo familiar, y su objetivo principal es alcanzar un crecimiento constante y equilibrado. Por último, cabe destacar que su establecimiento no demanda una gran inversión de capital [12][10].

Las microempresas representan un sector crucial en la economía colombiana, especialmente dentro del ámbito de Tecnologías de la Información (TI). En Colombia, las microempresas constituyen el 87% de los negocios, demostrando su predominancia y relevancia en la estructura económica del país [13] [14].

La transformación digital ha sido un aspecto fundamental para estas empresas. Un estudio de Microsoft revela que el 96% de las pymes colombianas han acelerado su proceso de transformación digital, enfocándose en áreas clave como ventas, mercadeo y recursos humanos. Esta transformación es esencial para mejorar la competitividad y eficiencia de las microempresas [14]. Además, el 87% de estas empresas ha implementado programas de capacitación para sus empleados en habilidades digitales y de marketing, resaltando la importancia de la tecnología en sus operaciones diarias. En Colombia, las microempresas representan un sector TI importante de la economía, ya que conforman la mayoría de las empresas registradas y generan un alto porcentaje del empleo. Las microempresas que cuentan con servicios web on-premise son aquellas que alojan sus aplicaciones y datos en sus propios servidores [15][11], en lugar de recurrir a servicios basados en la nube. Esta modalidad de alojamiento puede ofrecer mayor control y seguridad sobre los datos, pero también requiere de una mayor inversión en infraestructura y mantenimiento, Esto incluye la compra de hardware costoso, como servidores y equipos de red, así como la adecuación de instalaciones físicas para albergar estos equipos. Además, se requiere un mantenimiento continuo, que implica actualizaciones regulares, soporte técnico especializado, y medidas de ciberseguridad avanzadas.

3.2.2. DESCRIPCIÓN DEL SECTOR

El sector TI se caracteriza por tener empresas con un número limitado de empleados, un volumen de ventas o ingresos reducido y una gestión generalmente llevada a cabo por sus propios dueños. Estas empresas operan en diversos sectores económicos, incluyendo comercio, servicios, manufactura y agroindustria. En el ámbito de las Tecnologías de la Información (TI), desempeñan un papel

significativo. Dentro de este sector, estas empresas se dedican a la provisión de servicios relacionados con la tecnología, como desarrollo de software, diseño web, soporte técnico, consultoría en sistemas, entre otros. Algunas de las actividades más comunes que realizan estas empresas en Colombia incluyen Las microempresas se caracterizan por tener un número limitado de empleados, un volumen de ventas o ingresos reducido y una gestión generalmente llevada a cabo por sus propios dueños. Las microempresas operan en diversos sectores económicos, incluyendo comercio, servicios, manufactura y agroindustria. En el ámbito de las Tecnologías de la Información (TI), las microempresas también desempeñan un papel significativo. Dentro de este sector, las microempresas TI se dedican a la provisión de servicios relacionados con la tecnología, como desarrollo de software, diseño web, soporte técnico, consultoría en sistemas, entre otros. Algunas de las actividades más comunes que realizan las microempresas en Colombia incluyen [15][11]:

- **Comercio al por menor:** Ventas al público en general, como tiendas de abarrotes, ropa, calzado, etc.
- **Servicios:** Prestación de servicios a individuos o empresas, como restaurantes, peluquerías, talleres mecánicos, etc.
- **Manufactura:** Transformación de materias primas en productos terminados, como panaderías, carpinterías, talleres de confección, etc.
- **Agroindustria:** Procesamiento y transformación de productos agrícolas, como lecherías, molinos de arroz, fábricas de conservas, etc.

3.2.3. APLICACIONES DEL SECTOR

En el sector objetivo las microempresas utilizan una variedad de aplicaciones informáticas para gestionar sus operaciones. Algunas de las aplicaciones más comunes incluyen [16][12]:

- **Software de contabilidad:** Para registrar ingresos, gastos y transacciones financieras.
- **Software de punto de venta (TPV):** Para registrar las ventas y gestionar el inventario.
- **Software de gestión de clientes (CRM):** Para almacenar información de clientes y realizar seguimiento de las interacciones con ellos.
- **Software de gestión de proyectos:** Para planificar, ejecutar y monitorear proyectos.
- **Software de nómina:** Para calcular y pagar los salarios de los empleados.

3.2.4. RELACIÓN DE LAS APLICACIONES CON LA PROPUESTA:

La propuesta de solución para la obsolescencia tecnológica en los servicios web vulnerabilidad de los servicios web en un entorno on-premise es relevante para sector TI las microempresas que utilizan aplicaciones informáticas para gestionar sus operaciones. La solución puede ayudar a las microempresas a proteger sus

datos y sistemas de información de ataques cibernéticos, lo cual puede tener un impacto significativo en su rentabilidad y competitividad.

El sector TI las microempresas que utilizan aplicaciones on-premise son particularmente vulnerables a ataques cibernéticos, ya que a menudo no cuentan con los recursos o la experiencia necesarios para implementar medidas de seguridad adecuadas. La propuesta de solución puede ayudar a las microempresas a abordar estas vulnerabilidades y mejorar su postura de seguridad cibernética.

3.3 TENDENCIAS DEL SECTOR

En la actualidad, el sector TI está experimentando una migración acelerada desde sistemas on-premise hacia los servicios en la nube. Esta tendencia se debe en gran medida a las vulnerabilidades inherentes a los servicios on-premise. Al estar alojados en servidores físicos dentro de las instalaciones de una organización, empresa o microempresa, estos sistemas están expuestos a riesgos significativos, como fallos de hardware, ataques físicos, amenazas ante desastres naturales y la necesidad de mantener una infraestructura costosa y compleja. La nube ofrece una alternativa que permite gestionar estos riesgos de manera más eficiente, proporcionando mayor flexibilidad, escalabilidad y opciones avanzadas de seguridad gestionadas por proveedores especializados, aunque también requiere una gestión adecuada para mitigar sus propios riesgos de seguridad y funcionamiento.

La migración a servicios en la nube ofrece una solución efectiva y económica para resolver las vulnerabilidades que se pueden presentar. Los proveedores de servicios cloud ofrecen una infraestructura altamente segura y escalable, reduciendo así la exposición a riesgos asociados con los sistemas on-premise. Además, la nube proporciona una mayor agilidad y flexibilidad, permitiendo a las microempresas adaptarse con rapidez al uso de estos servicios, y así brindando una mejor experiencia al trabajador, sus empleados o a los usuarios en los servicios.

Otra tendencia notable es la migración gradual hacia modelos de nube híbrida [18][14], donde se combina la infraestructura on-premise con servicios en la nube. Esta estrategia permite a las organizaciones o empresas mantener el control sobre sus datos y aplicaciones más sensibles, al tiempo que aprovechan la escalabilidad y flexibilidad de la nube para otros componentes de su infraestructura. Esto es particularmente relevante en sectores altamente regulados, donde existen requisitos estrictos de cumplimiento y privacidad de datos.

No obstante, la migración de los servicios en la nube de una microempresa mejora la calidad de sus aplicativos o servicios, además brinda una solución económica y escalable, ya que muchas microempresas no cuentan con la economía suficiente para tener y mantener una infraestructura sólida a la hora de brindar un servicio mediante internet por lo cual la mejor opción es tener todos los servicios en la nube.

Finalmente, otra tendencia clave es está, la creciente adopción de servicios de nube pública, como los ofrecidos por proveedores líderes como AWS, Azure y Google Cloud. Estos servicios ofrecen una amplia gama de herramientas y capacidades, desde almacenamiento y bases de datos hasta servicios de inteligencia artificial y aprendizaje automático. Las organizaciones y empresas están aprovechando estas ofertas para agilizar su transformación digital y mantenerse a la vanguardia en un entorno tecnológico en constante evolución.

3.4 ANALISIS DE MERCADO

3.5 ARBOL DE OBJETIVOS

El proceso de migración de on-premise a la nube representa un paso fundamental para las microempresas en busca de mayor eficiencia, flexibilidad y seguridad en sus servicios, por tal motivo se define el árbol de objetivos en la ilustración de árbol de objetivos para para guiar el proceso de una manera más estructurada.



Ilustración de árbol de objetivos

Fuente: autores

3.6 CUÁL ES LA SITUACIÓN DESEADA

En la situación deseada, el sector TI ha migrado sus servicios on-premise a la nube, logrando así una infraestructura más segura, eficiente y escalable. Esta migración ha permitido a al sector reducir significativamente los riesgos asociados con las vulnerabilidades inherentes a los sistemas locales, como el acceso no autorizado, fallos de hardware y desastres naturales. La adopción de soluciones en la nube ha proporcionado capacidades avanzadas de seguridad, respaldadas por proveedores que implementan protocolos de ciberseguridad robustos y actualizaciones automáticas. Esto ha resultado en una mayor resiliencia y disponibilidad de los servicios, asegurando la continuidad del negocio y una respuesta rápida ante incidentes.

Además, el sector ha experimentado una notable optimización en la gestión de recursos y costos operativos. Al utilizar servicios en la nube, se ha beneficiado de un modelo de pago por uso, que les permite escalar recursos según la demanda real, evitando así inversiones iniciales elevadas y costos asociados al mantenimiento de infraestructura física. La flexibilidad y agilidad que ofrece la nube han facilitado la innovación, permitiendo a las organizaciones del sector TI lanzar nuevos productos y servicios al mercado con mayor rapidez y adaptarse ágilmente a las cambiantes necesidades del mercado y las tecnologías emergentes.

3.7 INTRODUCCIÓN A LA SITUACIÓN DESEADA

Actualmente, muchas empresas del sector TI operan con infraestructura on-premise, gestionando sus propios servidores y centros de datos. [19] Este enfoque presenta múltiples desafíos y riesgos, incluyendo altos costos de mantenimiento, limitaciones en la escalabilidad, y una vulnerabilidad constante frente a amenazas de seguridad, desastres naturales y fallos de hardware [20]. Las actualizaciones y parches de seguridad a menudo requieren intervención manual, lo que incrementa el riesgo de exposición a vulnerabilidades y ciberataques. Además, la administración de esta infraestructura requiere personal especializado, lo cual puede resultar costoso y complicado de gestionar, especialmente para empresas de menor tamaño. [21]

La situación deseada implica una transición completa a servicios en la nube, donde las empresas del sector TI pueden aprovechar una infraestructura gestionada por proveedores de nube de confianza. Esta migración promete resolver los problemas actuales, proporcionando una infraestructura más segura y resiliente. Los proveedores de nube ofrecen capacidades avanzadas de seguridad, incluyendo detección de amenazas en tiempo real, cifrado de datos y cumplimiento con normativas de protección de datos. Además, la nube facilita la escalabilidad y flexibilidad, permitiendo a las empresas ajustar recursos según sus necesidades sin las limitaciones de la infraestructura física.[22]En esta situación deseada, las empresas pueden enfocarse a su propósito principal, innovar con mayor rapidez y responder más eficazmente a las demandas del mercado, gracias a una infraestructura tecnológica robusta, segura y adaptable.

4. ANÁLISIS DE LAS ALTERNATIVAS TÉCNICAS PARA SOLUCIONAR EL PROBLEMA

En esta sección, se analizarán las alternativas técnicas para abordar la problemática de la obsolescencia tecnológica en los servicios on-premise de microempresas del sector TI. Se propondrá una arquitectura basada en tecnologías Cloud y se definirán sus bloques funcionales, identificando las posibles tecnologías para cada bloque. Se evaluarán las ventajas, desventajas, requerimientos y restricciones de las tecnologías seleccionadas, y se realizará un análisis comparativo para evidenciar las mejores alternativas técnicas.

La propuesta implica la migración de los servicios on-premise a una infraestructura en la nube. La arquitectura propuesta se basará en servicios de nube pública ofrecidos por proveedores como AWS [23], Azure [24] y Google Cloud,[25] y constará de los siguientes bloques funcionales:

Infraestructura como Servicio (IaaS) [26]:

Tecnologías:

- **AWS EC2:** Proporciona capacidad de cómputo escalable en la nube. [27]
- **Azure Virtual Machines:** Ofrece máquinas virtuales escalables y gestionadas. [28]
- **Google Compute Engine:** Proporciona máquinas virtuales altamente configurables y escalables. [29]

Ventajas:

- Escalabilidad y flexibilidad para ajustar recursos según la demanda.
- Reducción de costos operativos mediante modelos de pago por uso.
- Alta disponibilidad y fiabilidad.

Desventajas:

- Dependencia del proveedor de servicios en la nube.
- Posibles problemas de latencia para aplicaciones críticas.
- Necesidad de gestionar la configuración y el mantenimiento continuo.

Requerimientos y Restricciones:

- Conexión a Internet de alta velocidad.
- Políticas claras de seguridad y acceso.
- Capacitación del personal para la gestión de la infraestructura en la nube.

Tecnología	Ventajas	Desventajas	Requerimientos y Restricciones
AWS EC2	- Escalabilidad y flexibilidad	- Dependencia del proveedor	- Conexión de alta velocidad

Vulnerabilidades en Servicios On Premise

	<ul style="list-style-type: none"> - Modelo de pago por uso - Alta disponibilidad y fiabilidad 	<ul style="list-style-type: none"> - Posibles problemas de latencia - Gestión continua necesaria 	<ul style="list-style-type: none"> - Políticas de seguridad - Capacitación técnica
Azure Virtual Machines	<ul style="list-style-type: none"> - Escalabilidad y gestión integrada - Ideal para entornos híbridos - Fuerte soporte empresarial 	<ul style="list-style-type: none"> - Dependencia del proveedor - Latencia en aplicaciones críticas 	<ul style="list-style-type: none"> - Igual que AWS EC2
Google Compute Engine	<ul style="list-style-type: none"> - Máquinas altamente configurables - Costos competitivos - Buen rendimiento de red 	<ul style="list-style-type: none"> - Igual que AWS EC2 	<ul style="list-style-type: none"> - Igual que AWS EC2

Plataforma como Servicio (PaaS) [30]:**Tecnologías:**

- **AWS Elastic Beanstalk:** Plataforma para desplegar y gestionar aplicaciones web. [31]
- **Azure App Service:** Servicio para construir y alojar aplicaciones web. [32]
- **Google App Engine:** Plataforma para desarrollar y desplegar aplicaciones en la nube. [33]

Ventajas:

- Reducción del tiempo de desarrollo y despliegue.
- Gestión simplificada de la infraestructura subyacente.
- Integración con otros servicios en la nube.

Desventajas:

- Menor control sobre el entorno subyacente.
- Dependencia del proveedor para actualizaciones y parches.
- Posibles limitaciones en la personalización.

Requerimientos y Restricciones:

- Aplicaciones compatibles con la plataforma seleccionada.
- Políticas de seguridad adecuadas para proteger los datos de la aplicación.
- Monitoreo y gestión continua del rendimiento de la aplicación.

Tecnología	Ventajas	Desventajas	Requerimientos y Restricciones
AWS Elastic Beanstalk	<ul style="list-style-type: none"> - Reducción de tiempo de desarrollo - Integración con servicios de AWS - Gestión simplificada 	<ul style="list-style-type: none"> - Menor control sobre el entorno - Dependencia del proveedor - Posibles limitaciones en la personalización. 	<ul style="list-style-type: none"> - Aplicaciones compatibles - Políticas de seguridad - Monitoreo y gestión continua del rendimiento de la aplicación.
Azure App Service	<ul style="list-style-type: none"> - Ideal para aplicaciones .NET - Buen soporte CI/CD 	<ul style="list-style-type: none"> - Igual que AWS Elastic Beanstalk 	<ul style="list-style-type: none"> - Igual que AWS Elastic Beanstalk
Google App Engine	<ul style="list-style-type: none"> - Escalabilidad óptima - Fuerte soporte para contenedores - Precios competitivos 	<ul style="list-style-type: none"> - Igual que AWS Elastic Beanstalk 	<ul style="list-style-type: none"> - Igual que AWS Elastic Beanstalk

Software como Servicio (SaaS) [34]:

Tecnologías:

- **Microsoft Office 365:** Suite de productividad basada en la nube. [35]
- **Google Workspace:** Herramientas de colaboración y productividad en la nube. [36]
- **Salesforce:** Plataforma de gestión de relaciones con clientes (CRM) basada en la nube. [37]

Ventajas:

- Acceso a aplicaciones avanzadas sin necesidad de gestión de infraestructura.
- Modelos de suscripción flexibles.
- Actualizaciones automáticas y soporte técnico del proveedor.

Desventajas:

- Menor control sobre los datos y las configuraciones de las aplicaciones.
- Dependencia del proveedor para la disponibilidad y el rendimiento del servicio.
- Posibles problemas de integración con otros sistemas internos.

Requerimientos y Restricciones:

Vulnerabilidades en Servicios On Premise

- Conectividad a Internet estable y segura.
- Políticas de administración de usuarios y acceso.
- Cumplimiento de normativas y regulaciones específicas del sector.

Tecnología	Ventajas	Desventajas	Requerimientos y Restricciones
Microsoft Office 365	<ul style="list-style-type: none"> - Amplia adopción empresarial - Excelente colaboración - Soporte técnico 	<ul style="list-style-type: none"> - Menor control de datos - Dependencia del proveedor - Posibles problemas de integración con otros sistemas internos. 	<ul style="list-style-type: none"> - Conectividad estable - Administración de usuarios - Cumplimiento de normativas y regulaciones específicas del sector.
Google Workspace	<ul style="list-style-type: none"> - Ideal para colaboración en tiempo real - Interfaz intuitiva 	<ul style="list-style-type: none"> - Igual que Microsoft Office 365 	<ul style="list-style-type: none"> - Igual que Microsoft Office 365
Salesforce	<ul style="list-style-type: none"> - Líder en CRM - Gestión avanzada de clientes 	<ul style="list-style-type: none"> - Igual que Microsoft Office 365 	<ul style="list-style-type: none"> - Igual que Microsoft Office 365

Seguridad y Cumplimiento

Tecnologías:

- **AWS Identity and Access Management (IAM):** Gestión de acceso y permisos. [38]
- **Azure Security Center:** Servicio de gestión de la seguridad. [39]
- **Google Cloud Identity:** Gestión de identidades y accesos. [40]

Ventajas:

- Mejora en la seguridad de los datos y el cumplimiento normativo.
- Herramientas avanzadas de detección y respuesta a amenazas.
- Gestión centralizada de políticas de seguridad.

Desventajas:

- Complejidad en la configuración y gestión inicial.
- Necesidad de capacitación especializada.

Vulnerabilidades en Servicios On Premise

- Posible sobrecarga de costos adicionales para servicios avanzados.

Requerimientos y Restricciones:

- Definición clara de roles y permisos.
- Implementación de políticas de seguridad consistentes.
- Monitoreo continuo y auditorías regulares.

Tecnología	Ventajas	Desventajas	Requerimientos y Restricciones
AWS IAM	<ul style="list-style-type: none"> - Gestión granular - Integración con servicios AWS 	<ul style="list-style-type: none"> - Complejidad inicial - Capacitación necesaria 	<ul style="list-style-type: none"> - Definición de roles - Políticas claras - Auditorías regulares
Azure Security Center	<ul style="list-style-type: none"> - Gestión avanzada de seguridad - Integración en entornos híbridos 	- Igual que AWS IAM	- Igual que AWS IAM
Google Cloud Identity	<ul style="list-style-type: none"> - Buenas capacidades de integración - Seguridad centralizada 	- Igual que AWS IAM	- Igual que AWS IAM

Almacenamiento y Recuperación de Datos

Tecnologías:

- **AWS S3:** Almacenamiento de objetos escalable. [41]
- **Azure Blob Storage:** Almacenamiento de datos no estructurados. [42]
- **Google Cloud Storage:** Almacenamiento unificado de objetos. [43]

Ventajas:

- Almacenamiento seguro y escalable.
- Opciones de recuperación ante desastres y copias de seguridad.
- Integración con otros servicios en la nube.

Desventajas:

- Costos asociados al almacenamiento y la recuperación de datos.
- Posible latencia en el acceso a datos grandes.
- Necesidad de gestionar políticas de retención y acceso.

Requerimientos y Restricciones:

- Políticas claras de respaldo y recuperación.

Vulnerabilidades en Servicios On Premise

- Monitoreo del uso del almacenamiento y costos asociados.
- Implementación de medidas de seguridad para proteger los datos almacenados.

Tecnología	Ventajas	Desventajas	Requerimientos y Restricciones
AWS S3	<ul style="list-style-type: none"> - Alta disponibilidad - Gestión eficiente - Integración con otros servicios 	<ul style="list-style-type: none"> - Costos elevados para grandes volúmenes - Posible latencia en el acceso a datos grandes. 	<ul style="list-style-type: none"> - Políticas de respaldo - Seguridad avanzada
Azure Blob Storage	<ul style="list-style-type: none"> - Excelente para datos no estructurados - Recuperación ante desastres 	- Igual que AWS S3	- Igual que AWS S3
Google Cloud Storage	<ul style="list-style-type: none"> - Precios competitivos - Buen rendimiento 	- Igual que AWS S3	- Igual que AWS S3

Gestión de la Configuración y Automatización

Tecnologías:

- **AWS CloudFormation:** Herramienta de administración de infraestructura como código. [44]
- **Azure Automation:** Automatización de procesos y tareas. [45]
- **Google Cloud Deployment Manager:** Gestión de despliegues y configuración. [46]

Ventajas:

- Reducción de errores humanos mediante automatización.
- Gestión eficiente de la infraestructura y aplicaciones.
- Consistencia en la configuración y despliegue.

Desventajas:

- Complejidad en la configuración inicial.
- Necesidad de habilidades técnicas avanzadas.
- Dependencia de herramientas específicas del proveedor.

Requerimientos y Restricciones:

- Capacitación del personal en herramientas de automatización.
- Definición clara de procesos y flujos de trabajo.

Vulnerabilidades en Servicios On Premise

- Monitoreo y ajuste continuo de las configuraciones automatizadas.

Tecnología	Ventajas	Desventajas	Requerimientos y Restricciones
AWS CloudFormation	- Gestión eficiente - Buena integración con AWS	- Configuración inicial compleja - Necesidad de habilidades técnicas avanzadas.	- Capacitación - Flujos definidos
Azure Automation	- Flexibilidad en scripting - Ideal para automatización de TI	- Igual que AWS CloudFormation	- Igual que AWS CloudFormation
Google Deployment Manager	- Fácil de usar - Buen soporte de infraestructura como código	- Igual que AWS CloudFormation	- Igual que AWS CloudFormation

Análisis Comparativo

A continuación, se presenta un análisis comparativo de las tecnologías seleccionadas para cada bloque funcional, destacando sus ventajas y desventajas en relación con las necesidades específicas de las microempresas del sector TI.

IaaS: AWS EC2 vs. Azure Virtual Machines vs. Google Compute Engine

- **AWS EC2:** Amplia variedad de tipos de instancias, excelente integración con otros servicios de AWS, alto nivel de seguridad.
- **Azure Virtual Machines:** Buenas opciones de integración con servicios de Microsoft, ideal para entornos híbridos, fuerte soporte empresarial.
- **Google Compute Engine:** Costos competitivos, excelente rendimiento de red, buena integración con servicios de Google.

Tecnología	Ventajas	Desventajas	Recomendación
AWS EC2	- Amplia variedad de tipos de instancias - Excelente integración con servicios AWS - Alto nivel de seguridad	- Dependencia del ecosistema AWS - Costos pueden escalar según el uso	Ideal para empresas con necesidades avanzadas y alto volumen de servicios en AWS
Azure Virtual Machines	- Buenas opciones para entornos híbridos	- Latencia en ciertas	Ideal para empresas con uso intensivo de

Vulnerabilidades en Servicios On Premise

	- Fuerte soporte empresarial - Integración con servicios Microsoft	aplicaciones críticas - Limitada fuera del ecosistema Microsoft	tecnologías Microsoft o entornos híbridos
Google Compute Engine	- Costos competitivos - Excelente rendimiento de red - Buena integración con servicios Google	- Ecosistema más limitado comparado con AWS y Azure	Recomendado para empresas con presupuesto limitado o que ya usen otros servicios de Google

PaaS: AWS Elastic Beanstalk vs. Azure App Service vs. Google App Engine

- **AWS Elastic Beanstalk:** Fácil de usar, soporte para múltiples lenguajes y entornos, buena integración con servicios de AWS.
- **Azure App Service:** Ideal para aplicaciones .NET y otras tecnologías Microsoft, buen soporte para CI/CD.
- **Google App Engine:** Buena para aplicaciones escalables, fuerte soporte para contenedores, precios competitivos.

Tecnología	Ventajas	Desventajas	Recomendación
AWS Elastic Beanstalk	- Soporte para múltiples lenguajes - Buena integración con servicios AWS - Fácil de usar	- Menor control sobre el entorno subyacente - Dependencia del proveedor	Adecuado para microempresas con proyectos en múltiples lenguajes que buscan escalabilidad rápida
Azure App Service	- Ideal para aplicaciones .NET - Buen soporte CI/CD - Fuerte integración con Microsoft	- Personalización limitada para entornos no Microsoft	Recomendado para desarrolladores que trabajen con tecnologías Microsoft
Google App Engine	- Escalabilidad óptima - Fuerte soporte para contenedores - Precios competitivos	- Ecosistema limitado comparado con AWS	Ideal para startups con aplicaciones modernas y necesidades de escalabilidad

SaaS: Microsoft Office 365 vs. Google Workspace vs. Salesforce

- **Microsoft Office 365:** Amplia adopción en empresas, excelente soporte y funcionalidades de colaboración, integración con servicios de Microsoft.
- **Google Workspace:** Excelente para colaboración en tiempo real, interfaz fácil de usar, integración con otros servicios de Google.
- **Salesforce:** Líder en CRM, fuerte enfoque en gestión de clientes y ventas, amplias capacidades de personalización.

Tecnología	Ventajas	Desventajas	Recomendación
Microsoft Office 365	<ul style="list-style-type: none"> - Amplia adopción empresarial - Soporte técnico avanzado - Funcionalidades de colaboración 	<ul style="list-style-type: none"> - Dependencia del proveedor para actualizaciones - Costos más altos comparados con Google 	Ideal para empresas que prioricen herramientas de oficina y colaboración robusta
Google Workspace	<ul style="list-style-type: none"> - Ideal para colaboración en tiempo real - Interfaz amigable - Precios competitivos 	Limitado en algunas funciones empresariales avanzadas	Recomendado para empresas jóvenes o equipos altamente colaborativos
Salesforce	<ul style="list-style-type: none"> - Líder en CRM - Altamente personalizable - Foco en gestión de clientes 	<ul style="list-style-type: none"> - Requiere capacitación especializada - Costos altos 	Ideal para microempresas con necesidades avanzadas de gestión de clientes y ventas

Seguridad: AWS IAM vs. Azure Security Center vs. Google Cloud Identity

- **AWS IAM:** Gestión granular de permisos, buena integración con servicios de AWS, soporte robusto.
- **Azure Security Center:** Amplias capacidades de gestión de seguridad, excelente para entornos híbridos, buena integración con herramientas de Microsoft.
- **Google Cloud Identity:** Buena para gestión de identidades y accesos, fuerte enfoque en seguridad, fácil integración con otros servicios de Google.

Tecnología	Ventajas	Desventajas	Recomendación
AWS IAM	<ul style="list-style-type: none"> - Gestión granular de permisos 	<ul style="list-style-type: none"> - Complejidad inicial 	Ideal para empresas que trabajan

Vulnerabilidades en Servicios On Premise

	- Integración avanzada con AWS - Soporte robusto	- Depende del ecosistema AWS	exclusivamente en AWS
Azure Security Center	- Gestión avanzada de seguridad - Ideal para entornos híbridos - Buen soporte técnico	- Requiere configuración inicial compleja	Adecuado para empresas con tecnologías Microsoft
Google Cloud Identity	- Buen manejo de accesos - Integración sencilla con Google - Enfoque en seguridad centralizada	- Menor flexibilidad fuera del ecosistema Google	Recomendado para empresas que ya utilicen servicios en Google Cloud

Almacenamiento: AWS S3 vs. Azure Blob Storage vs. Google Cloud Storage

- **AWS S3:** Alta durabilidad y disponibilidad, amplias opciones de gestión de datos, buen rendimiento.
- **Azure Blob Storage:** Excelente para datos no estructurados, buenas opciones de recuperación ante desastres, integración con herramientas de Microsoft.
- **Google Cloud Storage:** Precios competitivos, excelente rendimiento de red, buena integración con otros servicios de Google.

Tecnología	Ventajas	Desventajas	Recomendación
AWS S3	- Alta durabilidad y disponibilidad - Gestión eficiente - Amplias opciones de integración	- Costos elevados para grandes volúmenes - Necesidad de gestionar políticas de retención	Ideal para empresas con necesidades críticas de almacenamiento
Azure Blob Storage	- Excelente para datos no estructurados - Integración con Microsoft - Opciones de recuperación	- Costos asociados a grandes cantidades de datos	Recomendado para empresas con ecosistema Microsoft

Google Cloud Storage	<ul style="list-style-type: none"> - Precios competitivos - Buen rendimiento - Fácil integración con Google 	<ul style="list-style-type: none"> - Latencia en datos muy grandes 	Ideal para startups con necesidades de almacenamiento asequibles
----------------------	--	---	--

Automatización: AWS CloudFormation vs. Azure Automation vs. Google Cloud Deployment Manager

- **AWS CloudFormation:** Gestión eficiente de la infraestructura, fuerte soporte y comunidad, buena integración con servicios de AWS.
- **Azure Automation:** Buena para automatización de procesos de TI, fuerte integración con servicios de Microsoft, opciones flexibles de scripting.
- **Google Cloud Deployment Manager:** Buena para gestión de despliegues, fácil de usar, fuerte soporte para infraestructura como código.

Tecnología	Ventajas	Desventajas	Recomendación
AWS CloudFormation	<ul style="list-style-type: none"> - Gestión eficiente - Amplio soporte y comunidad - Buena integración 	<ul style="list-style-type: none"> - Configuración inicial compleja - Necesidad de habilidades avanzadas 	Ideal para empresas que ya usen AWS
Azure Automation	<ul style="list-style-type: none"> - Flexibilidad en scripting - Fuerte integración con Microsoft - Ideal para procesos de TI 	<ul style="list-style-type: none"> - Configuración inicial compleja - Dependencia del ecosistema 	Recomendado para empresas con entornos de TI basados en Microsoft
Google Deployment Manager	<ul style="list-style-type: none"> - Fácil de usar - Fuerte soporte para infraestructura como código - Buena integración 	<ul style="list-style-type: none"> - Menor personalización comparado con AWS 	Ideal para empresas que buscan una implementación rápida y sencilla

La migración a una infraestructura en la nube proporciona múltiples ventajas para las microempresas del sector TI, incluyendo escalabilidad, reducción de costos y mayor agilidad. La elección de tecnologías específicas debe basarse en las necesidades particulares de cada empresa, considerando factores como la integración con sistemas existentes, el nivel de control deseado y los costos asociados. La arquitectura propuesta, basada en una combinación de IaaS, PaaS, SaaS, y soluciones de seguridad, almacenamiento y automatización, ofrece una

Vulnerabilidades en Servicios On Premise

solución robusta y flexible para abordar la problemática de la obsolescencia tecnológica en servicios on-premise.

5. MODELO DE NEGOCIO

5.1 PROPUESTA DE MODELO DE NEGOCIO

La propuesta de modelo de negocio se basa en un enfoque centrado en el cliente, donde la prestación de servicios TI se realiza de manera eficiente, flexible y orientada a resultados. El objetivo principal es proporcionar soluciones tecnológicas que no solo respondan a las necesidades operativas, sino que también aporten valor agregado mediante la optimización de procesos y la innovación continua.

Este modelo se apoya en los siguientes pilares:

- **Servicios Modulares:** El negocio ofrece una cartera de servicios TI escalables y modulares, lo que permite a los clientes seleccionar los componentes que mejor se ajusten a sus necesidades específicas, desde infraestructura hasta aplicaciones, con la posibilidad de personalización.
- **Innovación y Automatización:** Se apuesta por la automatización de procesos y la adopción de tecnologías emergentes como la inteligencia artificial, el big data y el internet de las cosas (IoT), para garantizar una mejora constante en la entrega de los servicios y la eficiencia operativa.
- **Modelo Basado en Resultados:** Se plantea un enfoque de pago por uso o por resultados, donde los clientes solo pagan por los servicios que efectivamente generan valor para sus negocios. Esto fomenta la transparencia y la confianza en la relación proveedor-cliente.
- **Atención al Cliente y Soporte Integral:** El modelo se centra en ofrecer una atención al cliente proactiva y personalizada, disponible 24/7, lo que garantiza que las operaciones críticas no se vean interrumpidas y que se mantenga la continuidad del negocio.
- **Alianzas Estratégicas:** El éxito del modelo también dependerá de la creación de alianzas con otros actores del ecosistema tecnológico (proveedores de hardware, software y servicios en la nube), permitiendo ofrecer soluciones integrales y robustas a los clientes.

5.2 VALIDACIÓN DEL MODELO DE NEGOCIO

Para asegurar que el modelo de negocio propuesto sea viable y efectivo, es esencial validarlo a través de una serie de pruebas y análisis. Esta validación permite comprobar si el modelo responde adecuadamente a las necesidades del mercado y si es sostenible a largo plazo. A continuación, se detallan los métodos utilizados para validar el modelo:

- **Análisis de Mercado**
Se realizó un análisis de mercado para entender las necesidades actuales de las empresas en cuanto a servicios TI. Los resultados mostraron una creciente demanda de soluciones flexibles, personalizables y escalables, lo

cual confirma que el enfoque modular del modelo propuesto es atractivo para los clientes. Las empresas buscan servicios que se adapten a sus necesidades específicas y puedan crecer a medida que sus operaciones lo requieran.

- **Pruebas Piloto**

Se implementaron pruebas piloto del modelo de negocio con un grupo seleccionado de clientes. Estas pruebas sirvieron para evaluar cómo funciona el modelo en un entorno real. Durante estas pruebas, se ofrecieron servicios TI bajo el enfoque modular y de pago por resultados.

Los resultados mostraron que las empresas que participaron lograron una mejora significativa en su eficiencia operativa y una reducción en los costos, lo que sugiere que el modelo es efectivo en la práctica.

- **Feedback de los Clientes**

Tras las pruebas piloto, se recopilaron opiniones de los clientes para entender mejor su experiencia con el modelo propuesto. Las respuestas fueron positivas en su mayoría. Los clientes valoraron la flexibilidad del modelo, que les permitió seleccionar solo los servicios que realmente necesitaban. Además, la modalidad de pago por resultados les brindó una mayor tranquilidad, ya que solo pagaron por los servicios que demostraron generar valor en sus operaciones.

- **Evaluación Financiera**

Se realizó un análisis financiero para determinar si el modelo de negocio es rentable. Si bien la implementación inicial del modelo, con su enfoque en la automatización y la innovación tecnológica, requiere una inversión significativa, el análisis mostró que los costos operativos disminuyen con el tiempo, y la escalabilidad del modelo asegura una recuperación rápida de la inversión. Además, la flexibilidad del modelo permite captar una mayor cantidad de clientes, lo que incrementa el potencial de ingresos.

- **Sostenibilidad a Largo Plazo**

Finalmente, se consideró la sostenibilidad del modelo a largo plazo. El análisis indicó que, gracias a su capacidad para adaptarse a las necesidades cambiantes del mercado y la incorporación continua de nuevas tecnologías, el modelo tiene un alto potencial de mantenerse competitivo en el tiempo. Además, el enfoque en la satisfacción del cliente y la creación de alianzas estratégicas refuerza su viabilidad a largo plazo.

6. PROPUESTA DE LA SOLUCIÓN TECNOLÓGICA

La solución tecnológica propuesta para migrar de servidores on-premise a un entorno en la nube busca simplificar la infraestructura tecnológica de la empresa, mejorando la escalabilidad, seguridad y disponibilidad de los servicios sin agregar demasiada complejidad al proceso. En primer lugar, se plantea que el almacenamiento de datos se realice en plataformas en la nube como Google Cloud Storage o Amazon S3, que ofrecen la capacidad de almacenar grandes volúmenes de datos de forma segura y escalable. Estas soluciones permiten mantener múltiples copias de los datos en diferentes ubicaciones geográficas, lo que garantiza la disponibilidad de la información en caso de fallos del hardware o interrupciones en un datacenter. Además, al ser servicios gestionados, no requieren que el equipo interno de la empresa se ocupe del mantenimiento o las actualizaciones de los servidores.

Para el procesamiento de datos, se recomienda utilizar soluciones simples y eficientes como Google Cloud Run [47] o AWS Lambda [48], que permiten ejecutar aplicaciones o funciones en la nube sin necesidad de gestionar servidores directamente. Estas herramientas se activan únicamente cuando hay datos que procesar, lo que optimiza el uso de recursos y reduce costos, ya que la empresa solo paga por el uso real en lugar de mantener infraestructura constantemente activa. Esta opción es ideal para empresas que buscan reducir la complejidad operativa, ya que no es necesario contar con un equipo técnico especializado para la gestión diaria de los servidores.

En términos de ciberseguridad, se puede implementar una solución básica pero efectiva que incluya autenticación multifactor (MFA) para proteger el acceso a los datos críticos, así como cifrado automático de los datos almacenados y en tránsito. Estas medidas no requieren un esfuerzo técnico complejo, ya que los principales proveedores de servicios en la nube, como Google Cloud y AWS, ofrecen estas funcionalidades como parte de sus soluciones predeterminadas, lo que asegura que la información esté protegida contra accesos no autorizados y ataques cibernéticos sin necesidad de desarrollar soluciones de seguridad personalizadas.

Para asegurar la alta disponibilidad de los servicios, se propone implementar la replicación automática de los datos y utilizar balanceadores de carga sencillos que distribuyan las solicitudes de los usuarios entre múltiples servidores o instancias en la nube. De esta forma, si un servidor o centro de datos experimenta un fallo, las solicitudes pueden ser redirigidas automáticamente a otro servidor activo, garantizando que los servicios permanezcan disponibles en todo momento. Además, los principales proveedores de servicios en la nube ofrecen herramientas de recuperación ante desastres, lo que permite restaurar los datos y servicios de manera rápida en caso de un incidente mayor, como desastres naturales o fallos masivos de hardware.

En cuanto al mantenimiento y las actualizaciones, las soluciones en la nube como Google Cloud y AWS gestionan automáticamente los parches y actualizaciones de software, eliminando la necesidad de que el equipo de la empresa se encargue de estas tareas. Esto asegura que los sistemas estén siempre actualizados y protegidos contra vulnerabilidades conocidas, reduciendo el riesgo de ciberataques y fallos de seguridad. Esta automatización del mantenimiento permite que el personal de TI se enfoque en otras tareas más estratégicas y menos operativas.

En resumen, esta propuesta de migración a la nube ofrece una solución simple pero efectiva para los problemas de obsolescencia, ciberseguridad y disponibilidad que enfrenta la empresa. La adopción de tecnologías de almacenamiento, procesamiento y seguridad gestionadas en la nube reduce la complejidad operativa y asegura que los servicios sean escalables, seguros y siempre disponibles, sin requerir una inversión significativa en hardware o mantenimiento constante. Esto permitirá a la empresa mejorar la eficiencia operativa y garantizar la continuidad del negocio en un entorno cada vez más digitalizado y exigente.

7. ANÁLISIS DEL PROCESO DE TRANSFORMACIÓN DIGITAL

7.1 CONTEXTO Y DESAFÍOS ACTUALES

El proceso de transformación digital para muchas microempresas, especialmente en el sector de Tecnologías de la Información (TI), enfrenta un obstáculo principal: la **obsolescencia tecnológica de los servicios on-premise**. Este modelo presenta diversos problemas, como tiempos de inactividad, vulnerabilidades de ciberseguridad, y la pérdida de datos debido a la falta de actualizaciones y mantenimiento continuo. La infraestructura física on-premise también limita la escalabilidad, adaptabilidad y disponibilidad de los servicios, aspectos críticos para el rendimiento de una empresa que depende de aplicaciones y plataformas digitales.

7.2 PROCESO DE MIGRACIÓN A LA NUBE

La migración de servidores on-premise a **soluciones en la nube** se perfila como la respuesta a estos desafíos. Este proceso implica trasladar aplicaciones, datos y servicios a plataformas de **nube pública** (como AWS, Azure, Google Cloud) o híbrida, lo que permite:

- **Escalabilidad:** Proveer recursos de infraestructura bajo demanda.
- **Alta disponibilidad y recuperación ante desastres:** Minimizar tiempos de inactividad.
- **Ciberseguridad mejorada:** Con un enfoque de seguridad integral, incluyendo autenticación robusta y monitoreo de amenazas.

La adopción de estas tecnologías permite a las microempresas optimizar costos operativos, ya que la nube opera bajo un modelo "**pago por uso**", reduciendo la necesidad de mantener una infraestructura física costosa. Asimismo, la flexibilidad de la nube permite ajustarse rápidamente a las necesidades cambiantes del mercado y el entorno tecnológico.

7.3 SOLUCIÓN PROPUESTA Y BENEFICIOS

El **levantamiento de información**, evaluación de proveedores, y la implementación de un **plan de migración estructurado** garantizarán una transición eficiente, minimizando interrupciones operativas. Esta solución:

- Mejora la **resiliencia** de los servicios.
- Proporciona **actualizaciones automáticas** y soporte continuo, mitigando el riesgo de ciberataques.
- Permite una **gestión eficiente** de los recursos tecnológicos, apoyando el crecimiento sostenible de las microempresas en el contexto digital.

8. ASPECTOS LEGALES Y DE CONTRATACIÓN

8.1 ASPECTOS LEGALES EN LA MIGRACIÓN A LA NUBE

La migración de datos y servicios a la nube involucra una serie de consideraciones legales que las microempresas deben tener en cuenta, como los **derechos sobre los datos**, **protección de la privacidad**, y **cumplimiento normativo**. Los principales aspectos legales incluyen:

- **Protección de Datos:** La empresa debe asegurarse de que el proveedor de servicios en la nube cumpla con las normativas locales e internacionales de protección de datos, como la **Ley de Protección de Datos Personales** (en Colombia, la Ley 1581 de 2012) y regulaciones del **RGPD** (Reglamento General de Protección de Datos) en la Unión Europea.
- **Confidencialidad y Seguridad:** El contrato debe especificar las medidas de seguridad y protocolos de ciberseguridad que el proveedor implementará para proteger los datos almacenados en la nube, incluyendo cifrado, autenticación, y monitoreo de accesos.
- **Jurisdicción y Ley Aplicable:** La elección de la jurisdicción es fundamental, especialmente si los servicios en la nube son proporcionados por empresas internacionales. Es necesario definir cuál será la ley que regirá los contratos, cómo se manejarán los conflictos, y los mecanismos de resolución de disputas.
- **Propiedad Intelectual y Derechos de Uso:** Es fundamental que se clarifique en el contrato la titularidad de los datos y las aplicaciones en la nube,

asegurándose de que la empresa mantenga el control sobre la propiedad intelectual relacionada con sus servicios.

8.2 CONTRATACIÓN CON PROVEEDORES DE NUBE

En el proceso de migración, la relación contractual con el **proveedor de servicios en la nube** debe ser cuidadosamente gestionada. Algunos puntos clave en la contratación incluyen:

- **Acuerdo de Nivel de Servicio (SLA):** El contrato debe especificar claramente los **niveles de servicio** acordados, tales como la **disponibilidad del servicio**, tiempos de respuesta ante incidentes, y el soporte técnico ofrecido. Un SLA bien definido establece las expectativas sobre la calidad del servicio y las compensaciones en caso de incumplimiento.
- **Condiciones de Rescisión y Transferencia de Datos:** El contrato debe abordar las condiciones bajo las cuales cualquiera de las partes puede rescindir el acuerdo, así como los procedimientos para la transferencia de datos a otro proveedor en caso de que la empresa decida cambiar de plataforma en el futuro.
- **Responsabilidades de Ciberseguridad y Auditorías:** Definir las responsabilidades de las partes en cuanto a **ciberseguridad**, incluyendo auditorías regulares, pruebas de vulnerabilidades y monitoreo de accesos, es esencial para garantizar la protección de los datos en la nube.
- **Condiciones de Pago y Facturación:** Establecer claramente cómo se gestionarán los costos asociados a la **migración**, el modelo **pago por uso**, y cualquier gasto adicional relacionado con la escalabilidad o el almacenamiento de datos. Este aspecto debe alinearse con los objetivos de eficiencia y optimización de costos de las microempresas.

9. REFERENCIAS

- [1] Know How, “On-premises: el modelo de software basado en el servidor,” <https://www.ionos.es/digitalguide/servidores/know-how/que-es-on-premises/>.
- [2] “Gartner Inc. 2021 Annual Report”.
- [3] Zimmergren, ShannonLeavitt, and jmart1428, “Migration assessment checklist,” <https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/migrate/assess/>.
- [4] “Oracle Cloud Infrastructure (OCI),” <https://www.oracle.com/co/cloud/>.
- [5] Luis Cosio, “¿Qué es AWS?,” <https://www.inbest.cloud/comunidad/qu%C3%A9-es-aws>.
- [6] Conzultek, “Microsoft Azure: qué es, cómo funciona y cómo ayuda en su empresa,” <https://blog.conzultek.com/microsoft-azure-que-es-como-funciona-como-ayuda-a-las-empresas>.
- [7] Ignacio Ordorica, “¿Qué es Google Cloud y para qué sirve?,” <https://www.incentro.com/es-ES/blog/que-es-google-cloud-platform>.
- [8] redhat.com, “Servicios de nube gerenciados,” <https://www.redhat.com/es/topics/cloud-computing/what-are-cloud-services>.
- [9] ausum.cloud, “Pasos a seguir en la migración de infraestructura al cloud para empresas,” <https://ausum.cloud/pasos-a-seguir-en-la-migracion-cloud-para-empresas/>.
- [10] ikusi.com, “Ventajas y desventajas de sistemas de ciberseguridad on-premise,” <https://www.ikusi.com/mx/blog/on-premise/>.
- [11] itdigitalsecurity.es, “El 46% de todas las bases de datos on-prem son vulnerables,” <https://www.itdigitalsecurity.es/actualidad/2021/09/el-46-de-todas-las-bases-de-datos-onprem-son-vulnerables>.
- [12] QuickBooks en español, “¿Qué es una microempresa? Características y ejemplos en Latinoamérica,” <https://quickbooks.intuit.com/global/resources/es/controla-tu-negocio/que-es-microempresa/>.
- [13] America Inhouse, “El papel fundamental de las pymes en la economía colombiana,” <https://www.infobae.com/america/inhouse/2023/06/23/el-papel-fundamental-de-las-pymes-en-la-economia-colombiana/>.
- [14] News Center Microsoft Latinoamérica, “Estudio de Microsoft revela que 6 de cada 10 pymes han desarrollado tecnología en los últimos meses como parte de su proceso de transformación digital,” <https://news.microsoft.com/es-xl/estudio-de-microsoft-revela-que-6-de-cada-10-pymes-han-desarrollado-tecnologia-en-los-ultimos-meses-como-parte-de-su-proceso-de-transformacion-digital/>.
- [15] Juanita Moreno, “Pymes en Colombia: qué son, cuántas hay y ejemplos,” <https://blog.hubspot.es/marketing/la-importancia-de-las-pymes-en-colombia>.

Vulnerabilidades en Servicios On Premise

- [16] Stefano Gasbarrino, “Los 29 mejores software de contabilidad para 2024,” <https://blog.hubspot.es/sales/software-de-contabilidad>.
- [17] amchamcolombia.co, “Migración a la nube, la nueva apuesta en transformación digital de las empresas,” <https://amchamcolombia.co/noticias-colombia/migracion-a-la-nube-la-nueva-apuesta-en-transformacion-digital-de-las-empresas/>.
- [18] ibm, “¿Cómo funciona la nube híbrida?,” <https://www.ibm.com/es-es/topics/hybrid-cloud>.
- [19] Gtalent, & Gtalent. (2024, 5 septiembre). Por qué las empresas están migrando de la nube al On-Premise. GTALENT - Tu Partner Tecnológico - Desde el primer día, nos esforzamos por ser más que un proveedor de servicios. <https://gtalent.cl/blog/por-que-las-empresas-estan-migrando-de-la-nube-al-on-premise/>
- [20] Ibm. (2024, 18 julio). ¿Qué es la gestión de parches? | IBM. <https://www.ibm.com/es-es/topics/patch-management>
- [21] Vega, P. (2024, 5 septiembre). La importancia de las actualizaciones en la Ciberseguridad Industrial - Centro de Ciberseguridad Industrial. Centro de Ciberseguridad Industrial. <https://www.cci-es.org/la-importancia-de-las-actualizaciones-en-la-ciberseguridad-industrial/>
- [22] Ventajas de la computación en la nube | Google Cloud. (s. f.). Google Cloud. <https://cloud.google.com/learn/advantages-of-cloud-computing?hl=es-419>
- [23] Descripción general de Amazon Web Services. (2024). https://docs.aws.amazon.com/es_es/whitepapers/latest/aws-overview/aws-overview.pdf
- [24] La guía de Azure para desarrolladores. (2019). https://download.microsoft.com/download/3/F/2/3F2FFA90-1B49-478A-9199-94106D5FB89A/Azure_Developer_Guide_eBook_es-ES.pdf
- [25] Documentación de Google Cloud. (s. f.). Google Cloud. <https://cloud.google.com/docs?hl=es-419>
- [26] ¿Qué es IaaS (infraestructura como servicio)? | Google Cloud. (s. f.). Google Cloud. <https://cloud.google.com/learn/what-is-iaas?hl=es>
- [27] ¿Qué es Amazon EC2? - Amazon Elastic Compute Cloud. (s. f.). https://docs.aws.amazon.com/es_es/AWSEC2/latest/UserGuide/concepts.html
- [28] Admin-Factoria. (2024, 10 mayo). Azure Virtual Machine: qué es, para qué sirve, cómo funciona y ventajas. Ausum Cloud: Servicios y Soluciones Cloud. <https://ausum.cloud/azure-virtual-machine-que-es-para-que-sirve-como-funciona-y-ventajas/>
- [29] Valero, J. (2024, 21 marzo). ¿Qué es Google Compute Engine? beservices. <https://blog.beservices.es/blog/google-cloud-platform-que-es-google-compute-engine>
- [30] ¿Qué es una PaaS? Google Cloud. (s. f.). Google Cloud. <https://cloud.google.com/learn/what-is-paas?hl=es>

Vulnerabilidades en Servicios On Premise

- [31] ¿Qué es AWS Elastic Beanstalk? - AWS Elastic Beanstalk. (s. f.). https://docs.aws.amazon.com/es_es/elasticbeanstalk/latest/dg/Welcome.html
- [32] Msangapu-Msft. (2024, 23 agosto). Información general de Azure App Service - Azure App Service. Microsoft Learn. <https://learn.microsoft.com/es-es/azure/app-service/overview>
- [33] Presta, M. (2021, 31 marzo). ¿Qué es Google App Engine? Back4App Blog. <https://blog.back4app.com/es/que-es-google-app-engine/>
- [34] ¿Qué es el SaaS? - Explicación del software como servicio - AWS. (s. f.). Amazon Web Services, Inc. <https://aws.amazon.com/es/what-is/saas/>
- [35] ¿Qué es Microsoft 365? - Soporte técnico de Microsoft. (s. f.). <https://support.microsoft.com/es-es/office/-qu%C3%A9-es-microsoft-365-847caf12-2589-452c-8aca-1c009797678b>
- [36] ¿Qué es Google Workspace y para qué sirve? (2022, 27 febrero). ¿Qué Es Google Workspace y Para Qué Sirve? <https://www.incentro.com/es-ES/blog/que-es-google-workspace>
- [37] Caurell, D. L. (2024, 22 agosto). ¿Qué es Salesforce? La plataforma que integra soluciones. ExpandLatam. <https://www.expandlatam.com/blog/crm/que-es-salesforce-crm/>
- [38] ¿Qué es IAM? - AWS Identity and Access Management. (s. f.). https://docs.aws.amazon.com/es_es/IAM/latest/UserGuide/introduction.html
- [39] Chkadmin. (2022, 11 mayo). What is Azure Security? Check Point Software. <https://www.checkpoint.com/es/cyber-hub/cloud-security/what-is-microsoft-azure-security/>
- [40] ¿Qué es Cloud Identity? - Ayuda de Cloud Identity. (s. f.). <https://support.google.com/cloudidentity/answer/7319251?hl=es-419>
- [41] ¿Qué es Amazon S3? - Amazon Simple Storage Service. (s. f.). https://docs.aws.amazon.com/es_es/AmazonS3/latest/userguide/Welcome.html
- [42] Akashdubey-Ms. (2023, 29 marzo). Acerca del almacenamiento de blobs (objeto) - Azure Storage. Microsoft Learn. <https://learn.microsoft.com/es-es/azure/storage/blobs/storage-blobs-overview>
- [43] ¿Qué es Cloud Storage y cómo funciona? | Google Cloud | Google Cloud. (s. f.). Google Cloud. <https://cloud.google.com/learn/what-is-cloud-storage?hl=es>
- [44] ¿Qué es AWS CloudFormation? - AWS CloudFormation. (s. f.). https://docs.aws.amazon.com/es_es/AWSCloudFormation/latest/UserGuide/Welcome.html
- [45] SnehaSudhirG. (2024, 6 noviembre). Información general sobre Azure Automation. Microsoft Learn. <https://learn.microsoft.com/es-es/azure/automation/overview>
- [46] Descripción general de Cloud Deploy. (s. f.). Google Cloud. <https://cloud.google.com/deploy/docs/overview?hl=es-419>
- [47] Cloud Run. (s. f.). Google Cloud. <https://cloud.google.com/run?hl=es>

Vulnerabilidades en Servicios On Premise

[48] ¿Qué es AWS Lambda? - AWS Lambda. (s. f.).

https://docs.aws.amazon.com/es_es/lambda/latest/dg/welcome.html